Guia do usuário

Amazon Simple Storage Service



Versão da API 2006-03-01

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon Simple Storage Service: Guia do usuário

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

As marcas comerciais e imagens comerciais da Amazon não podem ser usadas no contexto de nenhum produto ou serviço que não seja da Amazon, nem de qualquer maneira que possa gerar confusão entre os clientes ou que deprecie ou desprestigie a Amazon. Todas as outras marcas comerciais que não pertencem à Amazon pertencem a seus respectivos proprietários, que podem ou não ser afiliados, patrocinados pela Amazon ou ter conexão com ela.

Table of Contents

O que é o Amazon S3? 1
Recursos do Amazon S3 1
Classes de armazenamento 1
Gerenciamento de armazenamento 2
Gerenciamento de acesso e segurança 3
Processamento de dados 4
Registro e monitoramento do armazenamento 4
Análise e insights 5
Consistência forte 6
Como funciona o Amazon S3 6
Buckets 7
Objetos 9
Chaves 10
Versionamento do S3 10
ID da versão 10
Política de bucket 11
Pontos de Acesso S3 11
Listas de controle de acesso (ACLs) 12
Regiões 12
Modelo de consistência de dados do Amazon S3 13
Aplicações simultâneas 14
Serviços relacionados 16
Acesso ao Amazon S3 17
AWS Management Console 17
AWS Command Line Interface 17
SDKs da AWS 17
API REST do Amazon S3 18
Pagar pelo Amazon S3 18
Conformidade do PCI DSS 19
Conceitos básicos 20
Configuração 20
Inscrever-se para uma Conta da AWS 21
Criar um usuário com acesso administrativo 21
Etapa 1: Criar um bucket 23

Etapa 2: Fazer upload de um objeto ... 30
Etapa 3: fazer download de um objeto ... 31
Uso do console do S3 ... 31
Etapa 4: copiar um objeto ... 32
Etapa 5: excluir os objetos e o bucket ... 33
Excluir um objeto ... 34
Esvaziar o bucket ... 34
Excluir bucket ... 35
Próximas etapas ... 35
Entender casos de uso comuns ... 36
Controlar o acesso a buckets e objetos ... 37
Proteger e monitorar o armazenamento ... 38
Desenvolvimento com o Amazon S3 ... 38
Aprenda com os tutoriais ... 40
Explore o treinamento e o suporte ... 41
Como usar o Amazon S3 com a AWS CLI ... 41
Configuração ... 42
Etapa 1: criar seu primeiro bucket do Amazon S3 ... 43
Etapa 2: fazer upload de um objeto para o seu bucket ... 49
Etapa 3: fazer download de um objeto ... 50
Etapa 4: copiar seu objeto para uma pasta ... 51
Etapa 5: excluir seus objetos e bucket ... 52
Próximas etapas ... 55
Trabalhar com buckets de uso geral ... 57
Visão geral dos buckets de uso geral ... 58
Visão geral dos buckets de uso geral ... 59
Padrões comuns de bucket de uso geral ... 60
Permissões ... 60
Gerenciar o acesso público a buckets de uso geral ... 61
configuração de bucket de uso geral ... 62
operações de bucket de uso geral ... 65
monitoramento de desempenho de buckets de uso geral ... 65
Padrões comuns de buckets ... 67
Padrão de bucket de uso geral multilocatário ... 67
Padrão de bucket por uso ... 68
Regras de nomenclatura ... 69

Regras de nomenclatura de buckets de uso geral 70
Exemplos de nomes de buckets de uso geral 71
Práticas recomendadas 72
Criar um bucket que usa um GUID no nome 74
Cotas, restrições e limitações 75
Cotas de bucket 75
Limitações de objetos e buckets 76
Regras de nomeação de bucket 76
Acessar um bucket 76
..... 76
Hospedagem virtual de buckets de uso geral 80
Criar um bucket de uso geral 89
Configurações de bucket de uso geral 89
Visualizar propriedades de buckets 104
Listar buckets 107
Esvaziar um bucket de uso geral 113
Esvaziar um bucket de uso geral com o AWS CloudTrail configurado 116
Excluir um bucket de uso geral 117
Mountpoint para Amazon S3 123
Instalar o Mountpoint 124
Configurar e usar o Mountpoint 129
Solução de problemas do Mountpoint 135
Navegador de Armazenamento para Amazon S3 136
Usar o Navegador de Armazenamento para S3 137
Instalar o Navegador de Armazenamento para S3 138
Configurar o Navegador de Armazenamento para S3 138
Configurar o Navegador de Armazenamento para S3 153
Solução de problemas do Navegador de Armazenamento para S3 154
Configurar o Transfer Acceleration 155
Por que usar o Transfer Acceleration? 155
Requisitos para usar o Transfer Acceleration 155
Conceitos básicos 157
Habilitar o Transfer Acceleration 159
Ferramenta de comparação de velocidade 167
Uso de Pagamento pelo solicitante 167
Como funcionam as cobranças de Pagamento pelo solicitante 169

Configurar Pagamento pelo solicitante ... 170
Recuperação da configuração de requestPayment ... 172
Fazer download de objetos de buckets de Pagamento pelo solicitante ... 172
Trabalhar com objetos ... 175
Visão geral de objetos ... 176
Sub-recursos ... 178
Nomear objetos ... 178
Escolher nomes de chave de objeto ... 179
Diretrizes de nomeação de chave de objeto ... 180
Trabalhar com metadados ... 183
Metadados do objeto definidos pelo sistema ... 185
Metadados do objeto definidos pelo usuário ... 188
Editar os metadados do objeto ... 190
Acelerar a descoberta de dados ... 194
Fazer upload de objetos ... 237
Fazer upload de um objeto ... 238
Impedir o upload de objetos com nomes de chave idênticos ... 251
Usar multipart upload ... 252
Fazer solicitações condicionais ... 330
Como recuperar ou copiar objetos com base em metadados ... 331
Como evitar substituições de objeto ... 333
Copiar, mover e renomear objetos ... 343
Para copiar um objeto ... 347
Como mover um objeto ... 357
Para renomear um objeto ... 359
Baixar objetos ... 360
Fazer download de um objeto ... 361
Baixar vários objetos ... 363
Baixar parte de um objeto ... 365
Baixar um objeto de outra Conta da AWS ... 366
Baixar objetos arquivados ... 367
Baixar objetos com base em metadados ... 367
Solução de problemas de download de objetos ... 367
Verificar a integridade do objeto no Amazon S3 ... 368
Usar algoritmos de soma de verificação compatíveis ... 368
Tipos de soma de verificação de objeto inteiro e composta ... 370

Usar somas de verificação de objetos inteiros para upload fracionado ... 372
Usar somas de verificação ao nível da parte para upload fracionado ... 373
Operações de soma de verificação ... 374
Usar Content-MD5 ao carregar objetos ... 383
Usar Content-MD5 e a ETag para verificar objetos carregados ... 383
Usar somas de verificação à direita ... 384
Excluir objetos ... 390
Práticas recomendadas a serem consideradas antes de excluir um objeto ... 390
Excluir objetos de um bucket com versionamento habilitado ... 391
Excluir objetos de um bucket com versionamento suspenso ... 392
Excluir objetos de um bucket sem versionamento ... 392
Excluir objetos de um bucket com MFA habilitada ... 392
Excluir um único objeto ... 393
Excluir vários objetos ... 405
Organizar e listar objetos ... 408
Usar prefixos ... 409
Listar objetos ... 411
Usar pastas ... 414
Visualizar propriedades de objeto ... 419
Categorizar objetos com tags ... 421
Usar URLs pré-assinados para baixar e fazer upload de objetos ... 435
Quem pode criar um URL pré-assinado ... 436
Tempo de validade para URLs pré-assinados ... 437
Limitar recursos de pre-signed URLs ... 437
Compartilhar objetos com URLs pré-assinados ... 439
Carregar objetos com URLs pré-assinados ... 444
Transformar objetos ... 448
Criar pontos de acesso do Object Lambda ... 450
Usar pontos de acesso do Amazon S3 Object Lambda ... 465
Considerações sobre segurança ... 469
Escrever funções do Lambda ... 476
Usar funções criadas pela AWS ... 508
Práticas recomendadas e diretrizes para o S3 Object Lambda ... 510
Tutoriais do S3 Object Lambda ... 512
Solucionar problemas do S3 Object Lambda ... 551
Executar operações de objetos em massa ... 552

Conceitos básicos do Batch Operations ... 553
Tutorial Operações em lote do S3 ... 555
Conceder permissões ... 555
Criar um trabalho ... 566
Operações compatíveis ... 590
Gerenciar trabalhos ... 635
Monitoramento de relatórios de status e conclusão ... 640
Usar tags ... 656
Gerenciar o Bloqueio de Objetos com o Operações em Lote ... 672
Tutorial: vídeos de transcodificação em lote ... 697
Solução de problemas do Operações em Lote ... 739
Consultar dados no local ... 742
Requisitos e limites ... 743
Criar uma solicitação ... 744
Erros ... 745
Exemplos do S3 Select ... 745
Referência SQL ... 750
Trabalhar com buckets de diretório ... 792
Nomes de bucket de diretório ... 793
Diretórios ... 793
Nomes de chave ... 793
Gerenciamento de acesso ... 794
Buckets de diretório ... 794
Criar e usar buckets de diretório ... 795
Usar casos para buckets de diretório ... 796
Workloads de alto desempenho ... 796
Workloads de residência de dados ... 855
Diferenças de buckets de diretório ... 872
Diferenças de buckets de diretório ... 873
Operações de API compatíveis com buckets de diretório ... 875
Recursos do Amazon S3 não compatíveis com buckets de diretório ... 875
Rede para buckets de diretório ... 876
Endpoints ... 876
Configurar endpoints de gateway da VPC ... 877
Regras de nomenclatura de buckets de diretório ... 877
Visualizar propriedades ... 879

Gerenciar políticas de bucket 879
Adicionar uma política de bucket 880
Visualizar uma política de bucket 883
Excluir uma política de bucket 883
Esvaziar um bucket de diretório 884
Excluir um bucket de diretório 886
Listar buckets de diretório 888
Determinar se você pode acessar um bucket 891
Trabalhar com objetos em um bucket de diretório 892
Importar objetos em um bucket de diretório 893
Trabalhar com o S3 Lifecycle 895
Usar a funcionalidade Operações em Lote com a classe S3 Express One Zone 908
Anexar dados a objetos 911
Renomear um objeto 913
Fazer upload de um objeto 920
Copiar um objeto 953
Excluir um objeto 959
Fazer download de um objeto 964
Gerar URLs pré-assinados para compartilhar objetos 966
Recuperar metadados do objeto 966
Listar objetos 967
Segurança para buckets de diretório 968
Proteção e criptografia de dados 968
Autenticar e autorizar solicitações 993
Práticas recomendadas de segurança 1003
Trabalhar com pontos de acesso para buckets de diretório 1008
Regras de nomenclatura, restrições e limitações 1009
Referência a pontos de acesso para buckets de diretório 1010
Operações de objeto dos pontos de acesso 1011
Configurar políticas do IAM 1012
Monitorar e registrar em log 1018
Como criar pontos de acesso para buckets de diretório 1019
Gerenciar pontos de acesso 1023
Registro em log com o AWS CloudTrail para buckets de diretório 1036
Eventos de gerenciamento do CloudTrail para buckets de diretório 1036
Eventos de dados do CloudTrail para buckets de diretório 1037

... 1038
Otimizar o desempenho do bucket de diretório ... 1045
Usar a autenticação baseada em sessão ... 1046
Práticas recomendadas adicionais de soma de verificação do S3 ... 1046
Usar a versão mais recente dos AWS SDKs e das bibliotecas de tempo de execução comuns ... 1046
Desenvolvimento com buckets de diretório ... 1047
Endpoints regionais e zonais para buckets de diretório ... 1047
Trabalhar com buckets de diretório usando o console do S3, a AWS CLI e AWS SDKs ... 1048
Operações de API de bucket de diretório ... 1050
Atribuir tags a buckets de diretório ... 1051
Como as tags funcionam ... 1052
Maneiras comuns de usar tags ... 1053
Como trabalhar com tags ... 1059
Criar buckets de diretórios com tags ... 1059
Adicionar uma tag a um bucket de diretório ... 1064
Visualizar tags de buckets de diretório ... 1067
Excluir uma tag de um bucket de diretório ... 1070
Trabalhar com a funcionalidade Tabelas do Amazon S3 e com buckets de tabela ... 1073
Recursos da funcionalidade Tabelas do S3 ... 1074
Serviços relacionados ... 1075
Tutorial: conceitos básicos da funcionalidade Tabelas do S3 ... 1076
Etapa 1: criar um bucket de tabela e integrá-lo aos serviços de analytics da AWS ... 1077
Etapa 2: criar um namespace de tabela e uma tabela ... 1078
(Opcional) Etapa 3: conceder permissões do Lake Formation na tabela ... 1081
Etapa 4: consultar dados com SQL no Athena ... 1082
Buckets de tabela ... 1083
Regras de nomenclatura de buckets de tabela ... 1085
Criar um bucket de tabela ... 1086
Excluir um bucket de tabela ... 1089
Visualizar detalhes do bucket de tabela ... 1089
Gerenciamento de políticas ... 1090
Manutenção da funcionalidade Tabelas do S3 ... 1091
Status de trabalhos de manutenção da funcionalidade Tabelas do S3 ... 1092
Manutenção de buckets de tabela ... 1093
Manutenção de tabelas ... 1095

Considerações e limitações ... 1101
Namespaces ... 1103
Crie um namespace ... 1104
Excluir um namespace ... 1106
Tabelas ... 1106
Criar uma tabela ... 1108
Excluir uma tabela ... 1113
Gerenciamento de políticas ... 1114
Acessar tabelas ... 1116
Acessar tabelas por meio da integração com o Amazon SageMaker Lakehouse ... 1117
Acessar tabelas diretamente ... 1118
Usar tabelas do S3 com serviços de analytics da AWS ... 1119
Acessar tabelas usando o endpoint Iceberg REST do AWS Glue ... 1132
Acessar tabelas usando o endpoint Iceberg REST do serviço Tabelas do Amazon S3 ... 1137
Acessar tabelas com o catálogo de cliente ... 1143
Amazon Athena ... 1146
Amazon Redshift ... 1148
Amazon EMR ... 1148
QuickSight ... 1153
Amazon Data Firehose ... 1155
AWS Glue ETL ... 1161
Regiões da AWS, endpoints e cotas ... 1172
Regiões da AWS e endpoints da funcionalidade Tabelas do S3 ... 1172
Cotas da funcionalidade Tabelas do S3 ... 1177
Segurança para a funcionalidade Tabelas do S3 ... 1178
Criptografia ... 1180
Gerenciamento de acesso ... 1194
Conectividade da VPC ... 1226
Restrições e limitações ... 1230
Registro em log com o AWS CloudTrail para a funcionalidade Tabelas do S3 ... 1230
Eventos de gerenciamento do CloudTrail para a funcionalidade Tabelas do S3 ... 1231
Eventos de dados do CloudTrail para a funcionalidade Tabelas do S3 ... 1232
Exemplo de log do CloudTrail ... 1233
Controle de acesso ... 1237
Recursos do S3 ... 1238
Identidades ... 1244

Proprietários de bucket ou recurso ... 1246
Ferramentas de gerenciamento de acesso ... 1246
Ações ... 1253
Casos de uso do gerenciamento de acesso ... 1254
Solução de problemas de gerenciamento de acesso ... 1261
Identity and Access Management (IAM) ... 1263
Público ... 1264
Autenticação com identidades ... 1264
Gerenciar o acesso usando políticas ... 1268
Como o Amazon S3 funciona com o IAM ... 1271
Solicitar autorização ... 1299
Permissões obrigatórias para operações de API do S3 ... 1309
Políticas e permissões ... 1352
Políticas de buckets ... 1356
Políticas baseadas em identidade ... 1405
Demonstrações usando políticas ... 1441
Usar funções vinculadas a serviços para o Amazon S3 Storage Lens ... 1483
Solução de problemas de identidade e acesso do Amazon S3 ... 1487
Políticas gerenciadas AWS ... 1513
Trabalhar com pontos de acesso ... 1516
Regras de nomenclatura, restrições e limitações ... 1517
Fazer referência a pontos de acesso ... 1520
Compatibilidade dos pontos de acesso ... 1524
Configurar políticas do IAM ... 1527
Monitorar e registrar ... 1535
Criar um ponto de acesso ... 1537
Gerenciar pontos de acesso ... 1545
Usar pontos de acesso ... 1550
Gerenciar o acesso com a funcionalidade Concessões de Acesso do S3 ... 1563
Conceitos da funcionalidade Concessões de Acesso do S3 ... 1565
Concessões de Acesso do S3 e identidades de diretórios corporativos ... 1570
Conceitos básicos da funcionalidade Concessões de Acesso do S3 ... 1579
Trabalhar com instâncias do recurso Concessão de Acesso do S3 ... 1581
Trabalhar com locais do recurso Concessão de Acesso do S3 ... 1595
Trabalhar com concessões no recurso Concessão de Acesso do S3 ... 1619
Obter dados do S3 usando concessões de acesso ... 1633

Acesso entre contas da funcionalidade Concessões de Acesso do S3 1650
Usar etiquetas da AWS com a funcionalidade Concessões de Acesso do S3 1663
Limitações da funcionalidade Concessões de Acesso do S3 1666
Integrações da funcionalidade Concessões de Acesso do S3 1669
Gerenciar o acesso com ACLs 1670
Visão geral da ACL 1671
Configurar ACLs 1693
Exemplos de políticas 1711
Bloquear o acesso público 1715
Configurações do bloqueio de acesso público 1717
Executar operações de bloqueio de acesso público em um ponto de acesso 1721
O significado de "público" 1722
Usar o IAM Access Analyzer para S3 para revisar buckets públicos 1725
Permissões 1726
Configurar o bloqueio de acesso público 1727
Definir as configurações da conta 1728
Definir configurações de bucket e ponto de acesso 1730
Revisar o acesso ao bucket 1733
Quais informações o IAM Access Analyzer para S3 fornece? 1735
Habilitar o IAM Access Analyzer para S3 1736
Bloquear todo o acesso público 1737
Revisar e alterar o acesso ao bucket 1738
Arquivar descobertas de bucket 1739
Ativar uma descoberta de bucket arquivada 1740
Visualizar detalhes de descobertas 1740
Baixar um relatório do IAM Access Analyzer para S3 1741
Verificar a propriedade do bucket 1741
Quando usar a condição do proprietário do bucket 1742
Verificar um proprietário do bucket 1743
Exemplos 1744
Restrições e limitações 1746
Controlar a propriedade do objeto 1747
Configurações do Object Ownership 1749
Alterações introduzidas ao desabilitar ACLs 1750
Pré-requisitos para desabilitar ACLs 1753
Permissões do Object Ownership 1753

Desabilitar ACLs para todos os novos buckets ... 1753
Replicação e Object Ownership ... 1753
Configurar propriedade de objeto ... 1754
Pré-requisitos para desabilitar ACLs ... 1755
Como criar um bucket ... 1771
Configurar propriedade de objeto ... 1780
Visualizar configurações do Object Ownership ... 1784
Desabilitar ACLs para todos os novos buckets ... 1786
Solução de problemas ... 1789
Segurança ... 1792
Práticas recomendadas de segurança ... 1794
Práticas recomendadas de segurança para o Amazon S3 ... 1794
Práticas recomendadas de auditoria e monitoramento do Amazon S3 ... 1800
Monitorar a segurança dos dados ... 1804
Proteção de dados ... 1808
Criptografia de dados ... 1809
Criptografia do lado do servidor ... 1812
Uso de criptografia do lado do cliente ... 1915
Privacidade do tráfego entre redes ... 1916
Tráfego entre clientes de serviço e on-premises e os aplicativos ... 1916
Tráfego entre recursos da AWS na mesma região ... 1917
AWS PrivateLink para Amazon S3 ... 1917
Validação de compatibilidade ... 1935
Resiliência ... 1937
Criptografia de backup ... 1939
Segurança da infraestrutura ... 1940
Análise de configuração e vulnerabilidade ... 1941
Gerenciamento de acesso ... 1941
Proteção de dados ... 1945
Replicar objetos dentro de uma região e entre regiões ... 1947
Por que usar a replicação? ... 1948
Quando usar a replicação entre regiões ... 1950
Quando usar Replicação na mesma região ... 1950
Quando usar a replicação bidirecional ... 1951
Quando usar S3 Batch Replication ... 1951
Requisitos de workload e replicação em tempo real ... 1952

O que é replicado? ... 1953
Requisitos e considerações de replicação ... 1956
Configurar a replicação em tempo real ... 1960
Gerenciar ou pausar a replicação em tempo real ... 2057
Replicar objetos existentes ... 2059
Solução de problemas de replicação ... 2074
Monitoramento do progresso e obtenção de status ... 2083
Gerenciar o tráfego multirregional ... 2108
Criação de pontos de acesso multirregionais ... 2110
Configurar pontos de acesso multirregionais ... 2120
Usando pontos de acesso multirregionais ... 2124
Reter várias versões de objetos ... 2177
Buckets não versionados, habilitados para versão e suspensos de versão ... 2178
Usando o versionamento do S3 com o ciclo de vida do S3 ... 2179
Versionamento do S3 ... 2180
Habilitar o versionamento em buckets ... 2184
Configurando a exclusão de MFA ... 2192
Trabalhando com objetos habilitados para versão ... 2194
Trabalhando com objetos suspensos de versão ... 2226
Solucionar problemas de versionamento ... 2230
Bloquear objetos ... 2235
Como o bloqueio de objetos do S3 funciona ... 2236
Considerações sobre a funcionalidade Bloqueio de Objetos ... 2240
Configurar o Object Lock ... 2247
Fazer backup de seus dados ... 2258
Otimização de custo ... 2260
Relatórios de uso e faturamento ... 2261
Usar tags de alocação de custos ... 2262
Relatórios de faturamento ... 2264
Relatórios de uso ... 2267
Entender os relatórios de uso e faturamento ... 2270
Cobrança pelas respostas de erro do Amazon S3 ... 2300
Compreender e gerenciar classes de armazenamento ... 2324
Objetos acessados frequentemente ... 2325
Otimização automática de dados com padrões de acesso alterados ou desconhecidos ... 2326
Objetos acessados com pouca frequência ... 2328

Objetos acessados raramente ... 2329
Amazon S3 on Outposts ... 2330
Comparação de classes de armazenamento ... 2331
Configurar a classe de armazenamento de um objeto ... 2333
Análise de classe de armazenamento ... 2337
Gerenciar custos de armazenamento com o Amazon S3 Intelligent-Tiering ... 2345
Classes de armazenamento do Amazon S3 Glacier ... 2358
Trabalhando com objetos arquivados ... 2365
Gerenciando o ciclo de vida ... 2379
Gerenciar o ciclo de vida completo dos objetos ... 2381
Fazer a transição de objetos ... 2382
Expirando objetos ... 2391
Definir a configuração do ciclo de vida ... 2394
Usando outras configurações de bucket ... 2414
Configurar notificações de evento do Ciclo de Vida do S3 ... 2416
Elementos de configuração do ciclo de vida ... 2418
Conflitos na configuração do ciclo de vida ... 2437
Exemplos de configurações do Ciclo de Vida do S3 ... 2442
Solucionar problemas de ciclo de vida ... 2458
Registro em log e monitoramento ... 2466
Ferramentas de monitoramento ... 2470
Ferramentas automatizadas ... 2470
Ferramentas manuais ... 2470
Opções de registro em log ... 2471
Registrar em log com o CloudTrail ... 2475
Usar logs do CloudTrail com logs de acesso ao servidor do Amazon S3 e CloudWatch Logs ... 2476
Rastreamento do CloudTrail com chamadas de API SOAP do Amazon S3 ... 2477
Eventos do CloudTrail ... 2478
Exemplos de arquivos de log ... 2491
Habilitar o CloudTrail ... 2495
Identificar solicitações do S3 ... 2499
Registrando acesso ao servidor ... 2507
Como faço para habilitar a entrega de logs? ... 2507
Formato da chave de objeto de log ... 2510
Como os logs são entregues? ... 2511

Entrega de logs do servidor de melhor esforço ... 2512
As alterações do status do registro de bucket em logs entram em vigor ao longo do tempo 2512
Habilitar o log de acesso ao servidor do ... 2513
Formato do log ... 2537
Excluir arquivos de log ... 2552
Identificar solicitações do S3 ... 2552
Solução de problemas do registro em log de acessos ao servidor ... 2560
Monitoramento de métricas com o CloudWatch ... 2563
Métricas e dimensões ... 2566
Acessar métricas do CloudWatch ... 2585
Configurações de métricas do CloudWatch ... 2587
Notificações de eventos do Amazon S3 ... 2597
Visão geral ... 2597
Tipos e destinos de notificações ... 2599
Usar o SQS, o SNS e o Lambda ... 2607
Usar o EventBridge ... 2637
Visualizar a atividade e o uso de armazenamento ... 2648
Métricas e recursos da Lente de Armazenamento do S3 ... 2649
Noções básicas sobre o S3 Storage Lens ... 2651
Glossário de métricas ... 2663
Configuração de permissões ... 2694
Trabalhar com o S3 Storage Lens ... 2699
Exibição de métricas de armazenamento ... 2740
Trabalhar com organizações ... 2801
Trabalhar com grupos da Lente de Armazenamento ... 2812
Catalogar e analisar seus dados ... 2858
Buckets do Amazon S3 Inventory ... 2859
Listas de inventário ... 2860
Configurar o inventário do Amazon S3 ... 2865
Localização de inventário ... 2876
Configuração de notificações para conclusão de inventário ... 2880
Consultar o inventário com o Athena ... 2881
Converter strings de ID de versão vazias em cadeias de caracteres null ... 2887
Trabalhar com o campo ACL de objetos ... 2890
Otimizar o desempenho ... 2893
Diretrizes de desempenho para o Amazon S3 ... 2894

Avalie a performance ... 2895
Escalar horizontalmente ... 2896
Usar consultas na escala de bytes ... 2896
Solicitações de repetição ... 2896
Associar o Amazon S3 e o Amazon EC2 na mesma região ... 2897
Usar a Aceleração de Transferências para minimizar a latência ... 2897
Usar os SDKs da AWS mais recentes ... 2897
Padrões de design de desempenho do Amazon S3 ... 2898
Armazenamento em cache de conteúdo acessado com frequência ... 2898
Tempo limite e repetição para aplicações sensíveis à latência ... 2899
Escalabilidade horizontal e paralelização de solicitações ... 2900
Acelerar transferências de dados geograficamente dispersas ... 2902
Hospedar sites estáticos ... 2903
Endpoints de site ... 2904
Exemplos de endpoint de site ... 2905
Adicionar um registro DNS CNAME ... 2906
Usar um domínio personalizado com o Route 53 ... 2906
Principais diferenças entre um endpoint de site e um endpoint de API REST ... 2907
Habilitar a hospedagem de sites ... 2908
Configurar um documento de índice ... 2913
Pastas e documentos de índice ... 2914
Configurar um documento de índice ... 2915
Configurar um documento de erro personalizado ... 2916
Códigos de resposta HTTP do Amazon S3 ... 2917
Configurar um documento de erro personalizado ... 2920
Configuração de permissões para acesso ao site ... 2921
Etapa 1: Editar configurações de bloqueio de acesso público do S3 ... 2922
Etapa 2: Adicionar uma política de bucket ... 2924
Listas de controle de acesso de objetos ... 2926
Registro de tráfego da Web ... 2927
Configuração de um redirecionamento ... 2928
Redirecionar solicitações para outro host ... 2928
Configurar regras de redirecionamento ... 2929
Redirecionar solicitações para um objeto ... 2937
Usar o CORS ... 2940
Compartilhamento de recursos de origem cruzada: cenários de caso de uso ... 2940

Como o Amazon S3 avalia a configuração de CORS em um bucket? 2941
Como o ponto de acesso do Object Lambda é compatível com o CORS 2941
Elementos de uma configuração de CORS 2942
Configurar CORS 2947
Testar o CORS 2956
Solução de problemas do CORS 2959
Tutoriais de site estático 2964
Hospedagem de streaming de vídeo 2965
Configurar um site estático 2986
Configurar um site estático usando um domínio personalizado 2996
Implantar um site estático para o Amplify pelo Amazon S3 3022
Cotas 3026
Aumentos de cota 3026
Referência 3027
Histórico do documento 3029
Atualizações anteriores 3083

O que é o Amazon S3?

O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos que oferece escalabilidade líder do setor, disponibilidade de dados, segurança e performance. Clientes de todos os tamanhos e setores podem usar o Amazon S3 para armazenar e proteger qualquer volume de dados para uma variedade de casos de uso, como data lakes, sites, aplicações móveis, backup e restauração, arquivamento, aplicações corporativas, dispositivos IoT e análises de big data. O Amazon S3 fornece recursos de gerenciamento para que você possa otimizar, organizar e configurar o acesso aos seus dados para atender aos seus requisitos específicos de negócios, organizacionais e de compatibilidade.

> **Note**
>
> Para obter mais informações sobre o uso da classe de armazenamento Amazon S3 Express One Zone com buckets de diretório, consulte S3 Express One Zone e Trabalhar com buckets de diretório.

Tópicos

- Recursos do Amazon S3
- Como funciona o Amazon S3
- Modelo de consistência de dados do Amazon S3
- Serviços relacionados
- Acesso ao Amazon S3
- Pagar pelo Amazon S3
- Conformidade do PCI DSS

Recursos do Amazon S3

Classes de armazenamento

O Amazon S3 oferece uma ampla variedade de classes de armazenamento para diferentes casos de uso. Por exemplo, você pode armazenar dados de produção essenciais à missão nas classes S3 Standard ou S3 Express One Zone para acesso frequente, economizar custos armazenando dados acessados com pouca frequência nas classes S3 Standard-IA ou S3 One Zone-IA e arquivar dados

com os menores custos nas classes S3 Glacier Instant Retrieval, S3 Glacier Flexible Retrieval e S3 Glacier Deep Archive.

A classe Amazon S3 Express One Zone é uma classe de armazenamento de zona única e alto desempenho do Amazon S3 desenvolvida com o propósito específico de fornecer acesso consistente aos dados e com latência inferior a dez milissegundos para as aplicações mais sensíveis à latência. A classe S3 Express One Zone é a classe de armazenamento de objetos em nuvem de menor latência disponível atualmente, com velocidades de acesso aos dados até dez vezes mais rápidas e custos de solicitação 50% mais baixos do que a classe S3 Standard. S3 Express One Zone é a primeira classe de armazenamento do S3 em que é possível selecionar uma única zona de disponibilidade com a opção de manter o armazenamento de objetos e os recursos de computação na mesma localização, o que fornece a maior velocidade de acesso possível. Além disso, para aumentar ainda mais a velocidade de acesso e oferecer suporte a centenas de milhares de solicitações por segundo, os dados são armazenados em um novo tipo de bucket: um bucket de diretório do Amazon S3. Para obter mais informações, consulte S3 Express One Zone e Trabalhar com buckets de diretório.

Você pode armazenar dados com padrões de acesso alterados ou desconhecidos no S3 Intelligent-Tiering, o que otimiza os custos de armazenamento movendo automaticamente seus dados entre quatro camadas de acesso quando seus padrões de acesso mudam. Esses quatro níveis de acesso incluem dois níveis de acesso de baixa latência otimizados para acesso frequente e infrequente e dois níveis de acesso de arquivamento de inclusão projetados para acesso assíncrono para dados acessados raramente.

Para obter mais informações, consulte Compreender e gerenciar classes de armazenamento do Amazon S3.

Gerenciamento de armazenamento

O Amazon S3 tem recursos de gerenciamento de armazenamento que você pode usar para gerenciar custos, atender aos requisitos normativos, reduzir a latência e salvar várias cópias distintas de seus dados para requisitos de compatibilidade.

- Ciclo de vida do S3: configure uma política de ciclo de vida para gerenciar os objetos e armazená-los de maneira econômica durante todo o ciclo de vida. Você pode fazer a transição de objetos para outras classes de armazenamento do S3 ou expirar objetos que atingem o fim de suas vidas.
- Bloqueio de objetos do S3: evita que os objetos do Amazon S3 sejam excluídos ou substituídos por um período de tempo fixo ou indefinidamente. Você pode usar o bloqueio de objetos para

ajudar a atender aos requisitos regulamentares que exigem armazenamento write-once-read-many (WORM) ou simplesmente adicionar outra camada de proteção contra alterações e exclusão de objetos.

- Replicação do S3: replica objetos e seus respectivos metadados e etiquetas de objeto para um ou mais buckets de destino nas mesmas Regiões da AWS, ou diferentes, para reduzir a latência, compatibilidade, segurança e outros casos de uso.
- Operações em lote do S3: gerencia bilhões de objetos em escala com uma única solicitação de API do S3 ou com alguns cliques no console do Amazon S3. Você pode usar operações em lote para executar operações como Copy (Copiar), Invoke AWS Lambda function (Chamar função Lambda da) e Restore (Restaurar) em milhões ou bilhões de objetos.

Gerenciamento de acesso e segurança

O Amazon S3 fornece recursos para auditoria e gerenciamento de acesso a seus buckets e objetos. Por padrão, os buckets do S3 e os objetos deles são privados. Você tem acesso somente aos recursos do S3 criados. Para conceder permissões de recursos detalhadas que suportam seu caso de uso específico ou para auditar as permissões de seus recursos do Amazon S3, você pode usar os seguintes recursos.

- Bloqueio de acesso público do S3: bloqueie o acesso público a buckets e objetos do S3. Por padrão, as configurações do Bloqueio de Acesso Público são ativadas no nível do bucket. Recomendamos que você mantenha todas as configurações do Bloqueio de Acesso Público habilitadas, a menos que precise desativar uma ou mais delas para seu caso de uso específico. Para obter mais informações, consulte Configurar o bloqueio de acesso público para seus buckets do S3.
- AWS Identity and Access Management (IAM): o IAM é um serviço da Web que ajuda você a controlar de maneira segura o acesso aos recursos da AWS, incluindo recursos do Amazon S3. Com o IAM, é possível gerenciar, de maneira centralizada, permissões que controlam quais recursos da AWS os usuários poderão acessar. Você usa o IAM para controlar quem é autenticado (fez login) e autorizado (tem permissões) a usar os recursos.
- Políticas de buckets: use a linguagem de política baseada em IAM para configurar permissões baseadas em recursos para os buckets do S3 e os objetos neles contidos.
- Pontos de acesso do Amazon S3: configure endpoints nomeados com políticas de acesso dedicadas para gerenciar o acesso a dados em escala para conjuntos de dados compartilhados no Amazon S3.

- Listas de controle de acesso (ACLs): conceda permissões de leitura e gravação para buckets e objetos individuais a usuários autorizados. Como regra geral, recomendamos o uso de políticas baseadas em recursos do S3 (políticas de bucket e políticas de ponto de acesso) ou políticas de usuários do IAM para controle de acesso, em vez de ACLs. As políticas são uma opção de controle de acesso simplificada e mais flexível. Com políticas de bucket e políticas de ponto de acesso, é possível definir regras que se aplicam amplamente a todas as solicitações para seus recursos do Amazon S3. Para obter mais informações sobre os casos específicos em que você usaria ACLs, em vez de políticas baseadas em recursos ou políticas de usuário do IAM, consulte Gerenciar o acesso com ACLs.
- Propriedade de objeto do S3: assuma a propriedade de cada objeto do bucket simplificando o gerenciamento de acesso para dados armazenados no Amazon S3. A Propriedade de objeto do S3 é uma configuração no nível do bucket do Amazon S3 que você pode usar para desabilitar ou habilitar as ACLs. Por padrão, as ACLs estão desabilitadas. Com as ACLs desabilitadas, o proprietário do bucket possui todos os objetos do bucket e gerencia o acesso aos dados exclusivamente usando políticas de gerenciamento de acesso.
- IAM Access Analyzer para S3: avalie e monitore as políticas de acesso ao bucket do S3, garantindo que elas forneçam apenas o acesso pretendido aos recursos do S3.

Processamento de dados

Para transformar dados e acionar fluxos de trabalho para automatizar uma variedade de outras atividades de processamento em escala, você pode usar os seguintes recursos.

- S3 Object Lambda: adiciona seu próprio código às solicitações GET, HEAD e LIST do S3 para modificar e processar dados, conforme eles são retornados para uma aplicação. Filtra linhas, redimensiona imagens dinamicamente, edita dados confidenciais e muito mais.
- Notificações de eventos: aciona fluxos de trabalho que usam o Amazon Simple Notification Service (Amazon SNS), o Amazon Simple Queue Service (Amazon SQS) e o AWS Lambda quando uma alteração for feita em seus recursos do S3.

Registro e monitoramento do armazenamento

O Amazon S3 fornece ferramentas de registro e monitoramento que você pode usar para monitorar e controlar como seus recursos do Amazon S3 estão sendo usados. Para obter mais informações, consulte Ferramentas de monitoramento.

Ferramentas de monitoramento automatizadas

- Métricas do Amazon CloudWatch para o Amazon S3: acompanha a integridade operacional de seus recursos do S3 e configura alertas de faturamento quando as cobranças estimadas atingirem um limite definido pelo usuário.
- AWS CloudTrail: registra ações executadas por um usuário, uma função ou um AWS service (Serviço da AWS) no Amazon S3. Os logs do CloudTrail fornecem rastreamento detalhado de API para operações no nível de bucket e objeto do S3.

Ferramentas de monitoramento manual

- Log de acesso ao servidor: fornece detalhes sobre as solicitações que são feitas a um bucket. Você pode usar logs de acesso ao servidor para muitos casos de uso, como conduzir auditorias de segurança e acesso, saber mais sobre sua base de clientes e entender sua fatura do Amazon S3.
- AWSTrusted Advisor: avalia sua conta usando verificações de práticas recomendadas da AWS para identificar maneiras de otimizar sua infraestrutura da AWS, melhorar a segurança e a performance, reduzir custos e monitorar cotas de serviço. Em seguida, você pode seguir as recomendações para otimizar seus serviços e recursos.

Análise e insights

O Amazon S3 oferece recursos para ajudá-lo a obter visibilidade do uso do armazenamento, o que permite que você entenda melhor, analise e otimize seu armazenamento em escala.

- Amazon S3 Storage Lens: entende, analisa e otimiza seu armazenamento. O S3 Storage Lens fornece mais de 60 métricas de uso e atividade e painéis interativos para agregar dados de toda a sua organização, contas específicas, Regiões da AWS, buckets ou prefixos.
- Análise de classe de armazenamento: analisa padrões de acesso ao armazenamento para decidir quando é hora de mover seus dados para uma classe de armazenamento mais econômica.
- Inventário do S3: audita e relata sobre objetos e seus metadados correspondentes e configura outros recursos do Amazon S3 para executar ações nos relatórios de inventário. Por exemplo, você pode gerar relatórios sobre o status da replicação e da criptografia de seus objetos. Para obter uma lista de todos os metadados disponíveis para cada objeto nos relatórios de inventário, consulte Lista de inventário do Amazon S3.

Consistência forte

O Amazon S3 oferece uma forte consistência de leitura após gravação para solicitações de PUT e DELETE de objetos no bucket do Amazon S3 em todas as Regiões da AWS. Isso se aplica a ambas as gravações em novos objetos, bem como solicitações PUT que sobrescrevem objetos existentes e solicitações DELETE. Além disso, as operações de leitura no Amazon S3 Select, listas de controle de acesso (ACLs) do Amazon S3, etiquetas de objeto do Amazon S3 e metadados de objeto (por exemplo, objeto HEAD) são fortemente consistentes. Para obter mais informações, consulte Modelo de consistência de dados do Amazon S3.

Como funciona o Amazon S3

O Amazon S3 é um serviço de armazenamento de objetos que armazena dados, dados hierárquicos ou dados tabulares em buckets. Um objeto é um arquivo e quaisquer metadados que descrevam o arquivo. Um bucket é um contêiner de objetos.

Para armazenar seus dados no Amazon S3, crie um bucket e especifique um nome de bucket e a Região da AWS. Em seguida, carregue seus dados para esse bucket como objetos no Amazon S3. Cada objeto tem uma chave (ou nome de chave), que é um identificador exclusivo do objeto no bucket.

O S3 fornece recursos que você pode configurar para oferecer suporte ao seu caso de uso específico. Você pode usar o versionamento do S3 para manter várias versões de um objeto no mesmo bucket que permite que você restaure objetos excluídos ou substituídos acidentalmente.

Os buckets e os objetos neles são privados e poderão ser acessados somente se você conceder explicitamente permissões de acesso. Você pode usar políticas de bucket, políticas do AWS Identity and Access Management (IAM), listas de controle de acesso (ACLs) e pontos de acesso do S3 para gerenciar o acesso.

Tópicos

- Buckets
- Objetos
- Chaves
- Versionamento do S3
- ID da versão

- Política de bucket
- Pontos de Acesso S3
- Listas de controle de acesso (ACLs)
- Regiões

Buckets

O Amazon S3 comporta três tipos de bucket: de uso geral, de diretório e de tabela. Cada tipo de bucket oferece um conjunto exclusivo de recursos para diferentes casos de uso.

Buckets de uso geral: eles são recomendados para a maioria dos casos de uso e padrões de acesso e são o tipo original de bucket do S3. Um bucket de uso geral é um contêiner para objetos armazenados no Amazon S3, e você pode armazenar qualquer número de objetos em um bucket e em todas as classes de armazenamento (exceto na classe S3 Express One Zone). Desse modo, é possível armazenar objetos de forma redundante em várias zonas de disponibilidade. Para ter mais informações, consulte Criar, configurar e trabalhar com buckets de uso geral do Amazon S3.

> **Note**
>
> Por padrão, todos os buckets de uso geral são privados. Mas você pode conceder acesso público a buckets de uso geral. É possível controlar o acesso a buckets de uso geral em nível de bucket, prefixo (pasta) ou tag de objeto. Para ter mais informações, consulte Controle de acesso no Amazon S3.

Buckets de diretório: recomendados para casos de uso de baixa latência e de residência de dados. Por padrão, é possível criar até cem buckets de diretório em suas Conta da AWS, sem limite no número de objetos que podem ser armazenados em um bucket de diretório. Os buckets de diretório organizam os dados em diretórios hierárquicos (prefixos), e não na estrutura de armazenamento plana dos buckets de uso geral. Esse tipo de bucket não tem limites de prefixo, e diretórios individuais podem escalar horizontalmente. Para ter mais informações, consulte Trabalhar com buckets de diretório.

- Para casos de uso de baixa latência, você pode criar um bucket de diretório em uma única zona de disponibilidade da AWS para armazenar dados. Buckets de diretório em zonas de disponibilidade permitem a classe de armazenamento S3 Express One Zone. Com a classe S3 Express One Zone, os dados são armazenados de forma redundante em vários dispositivos dentro

de uma única zona de disponibilidade. A classe de armazenamento S3 Express One Zone é recomendada se a aplicação é sensível ao desempenho e se beneficia de latências inferiores a dez milissegundos para PUT e GET. Para saber mais sobre como criar buckets de diretório em zonas de disponibilidade, consulte Workloads de alto desempenho.

- Para casos de uso de residência de dados, você pode criar um bucket de diretório em uma única zona local dedicada (DLZ) da AWS para armazenar dados. Nas zonas locais dedicadas, é possível criar buckets de diretório do S3 para armazenar dados em um perímetro de dados específico, o que ajuda a apoiar casos de uso de isolamento e residência de dados. Os buckets de diretório em zonas locais são compatíveis com a classe de armazenamento S3 One Zone-Infrequent Access (S3 One Zone-IA; Z-IA). Para saber mais sobre como criar buckets de diretório em zonas locais, consulte Workloads de residência de dados.

> **Note**
>
> Nos buckets de diretório, todo acesso público é desabilitado por padrão. Esse comportamento não pode ser alterado. Você não pode conceder acesso a objetos armazenados em buckets de diretório. Você pode conceder acesso somente aos seus buckets de diretório. Para ter mais informações, consulte Autenticar e autorizar solicitações.

Buckets de tabela: recomendados para armazenar dados tabulares, como transações de compras diárias, dados de sensores de streaming ou impressões de anúncios. Os dados tabulares representam dados em colunas e linhas, como em uma tabela de banco de dados. Os buckets de tabela oferecem armazenamento do S3 otimizado para workloads de analytics e machine learning, com recursos projetados para melhorar continuamente a performance das consultas e reduzir os custos de armazenamento de tabelas. As tabelas do S3 são criadas especificamente para armazenar dados tabulares no formato Apache Iceberg. Você pode consultar dados tabulares nas tabelas do S3 com mecanismos de consulta conhecidos, como Amazon Athena, Amazon Redshift e Apache Spark. Por padrão, é possível criar até 10 buckets de tabela por Conta da AWS por Região da AWS e até 10 mil tabelas por bucket de tabela. Para ter mais informações, consulte Trabalhar com a funcionalidade Tabelas do Amazon S3 e com buckets de tabela.

> **Note**
>
> Todas as tabelas e buckets de tabela são privados e não podem ser tornados públicos. Esses recursos só podem ser acessados por usuários que tenham recebido acesso explícito. Para conceder acesso, você pode usar políticas baseadas em recurso do IAM para tabelas e

buckets de tabela, e políticas baseadas em identidade do IAM para usuários e perfis. Para ter mais informações, consulte Segurança para a funcionalidade Tabelas do S3.

Informações adicionais sobre todos os tipos de bucket

Ao criar um bucket, você insere um nome de bucket e escolhe a Região da AWS onde o bucket residirá. Assim que você cria um bucket, não pode mais alterar o nome do bucket ou sua região. Os nomes de bucket devem seguir as regras de nomenclatura de bucket.

- Regras de nomenclatura de buckets de uso geral
- Regras de nomenclatura de buckets de diretório
- Regras de nomenclatura de buckets de tabela

Os buckets também:

- Organizam o namespace do Amazon S3 no nível mais elevado. Para buckets de uso geral, esse namespace é `S3`. Para buckets de diretório, esse namespace é `s3express`. Para buckets de tabela, esse namespace é `s3tables`.
- Identificam a conta responsável por cobranças de transferência de dados e armazenamento.
- Serve como a unidade de agregação para relatório de uso.

Objetos

Os objetos são as entidades fundamentais armazenadas no Amazon S3. Os objetos consistem em metadados e dados de objeto. Os metadados são um conjunto de pares de nome e valor que descrevem o objeto. Esses pares incluem alguns metadados padrão, como a data da última modificação, e metadados HTTP padrão, como o `Content-Type`. Você também pode especificar metadados personalizados no momento em que o objeto é armazenado.

Cada objeto está contido em um bucket. Por exemplo, se o objeto chamado `photos/puppy.jpg` estiver armazenado no bucket de uso geral `amzn-s3-demo-bucket` da região Oeste dos EUA (Oregon), ele poderá ser endereçado usando o URL `https://amzn-s3-demo-bucket.s3.us-west-2.amazonaws.com/photos/puppy.jpg`. Para obter mais informações, consulte Accessing a Bucket (Como acessar um bucket).

Um objeto é identificado exclusivamente em um bucket por uma chave (nome) e um ID da versão (se o Versionamento do S3 estiver habilitado no bucket). Para obter mais informações sobre objetos, consulte Visão geral de objetos Amazon S3.

Chaves

Uma chave de objeto (ou nome da chave) é um identificador exclusivo de um objeto em um bucket. Cada objeto em um bucket tem exatamente uma chave. A combinação de um bucket, chave de objeto e, opcionalmente, o ID de versão (se o Versionamento do S3 estiver habilitado para o bucket) identifica exclusivamente cada objeto. Portanto, é possível pensar no Amazon S3 como um mapa de dados básico entre "bucket + chave + versão" e o objeto em si.

Cada objeto no Amazon S3 pode ser endereçado exclusivamente por meio da combinação do endpoint de serviço da web, do nome de bucket, da chave e, opcionalmente, de uma versão. Por exemplo, no URL `https://amzn-s3-demo-bucket.s3.us-west-2.amazonaws.com/photos/puppy.jpg`, *`amzn-s3-demo-bucket`* é o nome do bucket e `photos/puppy.jpg` é a chave.

Para obter mais informações sobre chaves de objeto, consulte Nomear objetos do Amazon S3.

Versionamento do S3

Use o versionamento do S3 para manter diversas variantes de um objeto no mesmo bucket. Com o versionamento do S3, você pode preservar, recuperar e restaurar todas as versões de cada objeto armazenado em seus buckets. Você pode se recuperar facilmente de ações não intencionais do usuário e de falhas da aplicação.

Para obter mais informações, consulte Reter várias versões de objetos com o Versionamento do S3.

ID da versão

Se você habilitar o versionamento do S3 em um bucket, o Amazon S3 gerará um ID de versão exclusivo para cada objeto adicionado ao bucket. Os objetos que já existiam no bucket no momento em que você habilita o controle de versão têm um ID de versão `null`. Se você modificar esses (ou quaisquer outros) objetos com outras operações, como CopyObject e PutObject, os novos objetos obtêm um ID de versão exclusivo.

Para obter mais informações, consulte Reter várias versões de objetos com o Versionamento do S3.

Política de bucket

Uma política de bucket é baseada em recursos do AWS Identity and Access Management (IAM) que você pode usar para conceder permissões de acesso ao bucket e aos objetos nele contidos. Só o proprietário do bucket pode associar uma política a um bucket. As permissões anexadas ao bucket se aplicam a todos os objetos do bucket que pertencem ao proprietário do bucket. As políticas de bucket são limitadas a 20 KB.

As políticas de bucket usam uma linguagem de políticas de acesso baseada em JSON que é padrão na AWS. Você pode usar políticas de bucket para adicionar ou negar permissões para os objetos em um bucket. As políticas de bucket permitem ou negam solicitações com base nos elementos da política, incluindo o solicitante, ações do S3, recursos e aspectos ou condições da solicitação (por exemplo, o endereço IP usado para fazer a solicitação). Por exemplo, você pode criar uma política de bucket que conceda permissões entre contas para carregar objetos em um bucket do S3 enquanto garante que o proprietário do bucket tenha controle total dos objetos carregados. Para obter mais informações, consulte Exemplos de políticas de bucket do Amazon S3.

Na política de bucket, você pode usar caracteres curinga nos nomes de recursos da Amazon (ARNs) e outros valores para conceder permissões a um subconjunto de objetos. Por exemplo, você pode controlar o acesso a grupos de objetos que começam com um prefixo ou termine com uma determinada extensão, como `.html`.

Pontos de Acesso S3

Os Pontos de Acesso Amazon S3 são endpoints de rede nomeados com políticas de acesso dedicadas que descrevem como os dados podem ser acessados usando esse endpoint. Os pontos de acesso são anexados a uma fonte de dados subjacente, como um bucket de uso geral, bucket de diretório ou um volume do FSx para OpenZFS, que você pode usar para executar operações de objeto do S3, como `GetObject` e `PutObject`. Os pontos de acesso simplificam o gerenciamento do acesso a dados em escala para conjuntos de dados compartilhados no Amazon S3.

Cada ponto de acesso tem sua própria política. Você também pode configurar as definições do Bloqueio de Acesso Público para cada ponto de acesso anexado a um bucket. Você pode configurar qualquer ponto de acesso para aceitar solicitações somente de uma nuvem virtual privada (VPC) para restringir o acesso a dados do Amazon S3 a uma rede privada.

Para ter mais informações sobre pontos de acesso para buckets de uso geral, consulte Gerenciar o acesso a conjuntos de dados compartilhados com pontos de acesso. Para ter mais informações

sobre pontos de acesso para buckets de diretório, consulte Gerenciar o acesso a conjuntos de dados compartilhados em buckets de diretório por meio de pontos de acesso.

Listas de controle de acesso (ACLs)

Você pode usar ACLs para conceder permissões de leitura e gravação a usuários autorizados referentes a buckets de uso geral e objetos individuais. Cada bucket de uso geral e objeto tem uma ACL anexada como um sub-recurso. Uma ACL define a quais grupos ou Contas da AWS é concedido acesso, bem como o tipo de acesso. As ACLs são mecanismos de controle de acesso que antecedem o IAM. Para obter mais informações sobre ACLs, consulte Visão geral da lista de controle de acesso (ACL).

A Propriedade de objetos do S3 é uma configuração no nível do bucket do Amazon S3 que você pode usar para controlar a propriedade de objetos carregados no bucket e para desabilitar ou habilitar as ACLs. Por padrão, a Propriedade de Objetos está definida com a configuração Imposto pelo proprietário do bucket e todas as ACLs estão desabilitadas. Quando as ACLs são desabilitadas, o proprietário do bucket possui todos os objetos do bucket e gerencia o acesso a eles exclusivamente usando políticas de gerenciamento de acesso.

A maioria dos casos de uso modernos no Amazon S3 não exige mais o uso de ACLs. Recomendamos manter as ACLs desabilitadas, exceto em circunstâncias incomuns em que seja necessário controlar o acesso para cada objeto individualmente. Com as ACLs desabilitadas, é possível usar políticas para controlar o acesso a todos os objetos no bucket, independentemente de quem carregou os objetos para o bucket. Para obter mais informações, consulte Controlar a propriedade de objetos e desabilitar ACLs para seu bucket.

Regiões

Você pode escolher a região da Região da AWS geográfica onde o Amazon S3 armazena os buckets criados. É possível escolher uma r[Região para otimizar a latência, minimizar os custos ou atender a requisitos regulatórios. Os objetos armazenados em uma Região da AWS nunca saem dela, a não ser que você os transfira ou os replique explicitamente para outra região. Por exemplo, os objetos armazenados na região da UE (Irlanda) nunca saem dela.

> **Note**
>
> Só é possível acessar o Amazon S3 e seus recursos em Regiões da AWS que estão habilitadas para sua conta. Para obter mais informações sobre como habilitar uma região

para criar e gerenciar recursos da AWS, consulte Como gerenciar Regiões da AWS na Referência geral da AWS.

Para obter uma lista de regiões e endpoints do Amazon S3, consulte Regiões e endpoints na Referência geral da AWS.

Modelo de consistência de dados do Amazon S3

O Amazon S3 oferece uma forte consistência de leitura após gravação para solicitações de PUT e DELETE de objetos no bucket do Amazon S3 em todas as Regiões da AWS. Isso se aplica a ambas as gravações em novos objetos, bem como solicitações PUT que sobrescrevem objetos existentes e solicitações DELETE. Além disso, as operações de leitura no Amazon S3 Select, listas de controle de acesso (ACLs) do Amazon S3, etiquetas de objeto do Amazon S3 e metadados de objeto (por exemplo, objeto HEAD) são muito consistentes.

As atualizações em uma única chave são atômicas. Por exemplo, se você executar uma solicitação PUT em uma chave existente de um thread e executar uma solicitação GET na mesma chave de um segundo thread simultaneamente, você obterá os dados antigos ou os novos dados, mas nunca dados parciais ou corrompidos.

O Amazon S3 atinge alta disponibilidade replicando dados entre vários servidores nos datacenters da AWS. Se uma solicitação PUT for bem-sucedida, os dados serão armazenados com segurança. Qualquer leitura (solicitação de GET ou LIST) iniciada após o recebimento de uma resposta PUT bem-sucedida retornará os dados escritos pelo PUT. Veja alguns exemplos desse comportamento:

- Um processo grava um novo objeto no Amazon S3 e imediatamente lista as chaves em seu bucket. O novo objeto aparecerá na lista.
- Um processo substitui um objeto existente e imediatamente tenta lê-lo. O Amazon S3 retorna os novos dados.
- Um processo exclui um objeto existente e imediatamente tenta lê-lo. O Amazon S3 não retorna dados porque o objeto foi excluído.
- Um processo exclui um objeto existente e imediatamente lista as chaves em seu bucket. O objeto não aparecerá na listagem.

> **Note**
>
> - O Amazon S3 não oferece suporte ao bloqueio de objetos para escritores simultâneos. Se duas solicitações PUT forem realizadas simultaneamente na mesma chave, a solicitação com o time stamp mais recente será a escolhida. Se isso for um problema, você precisará criar um mecanismo de bloqueio de objetos em sua aplicação.
> - As atualizações são baseadas em chave. Não há possibilidade de realizar atualizações atômicas entre chaves. Por exemplo, você não pode tornar a atualização de uma chave dependente da atualização de outra chave a menos que você desenvolva essa funcionalidade em seu aplicativo.

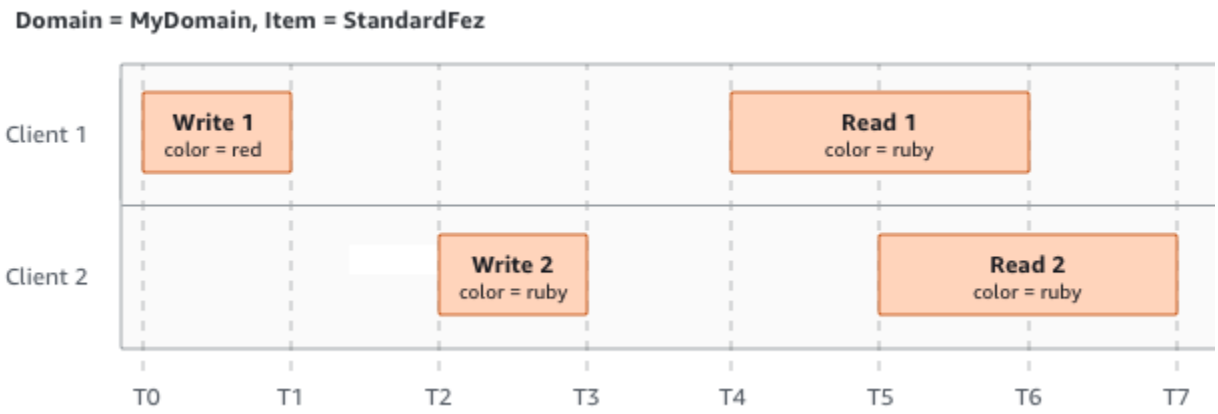
As configurações de bucket têm um modelo de consistência eventual. Especificamente, isso significa que:

- Por exemplo, se você excluir um bucket e listar imediatamente todos os buckets, o bucket excluído ainda poderá ser exibido na lista.
- Se você ativar o versionamento em um bucket pela primeira vez, pode levar um curto período de tempo para que a alteração seja totalmente propagada. Recomendamos que você aguarde 15 minutos após ativar o versionamento antes de emitir operações de gravação (solicitações PUT ou DELETE) em objetos no bucket.

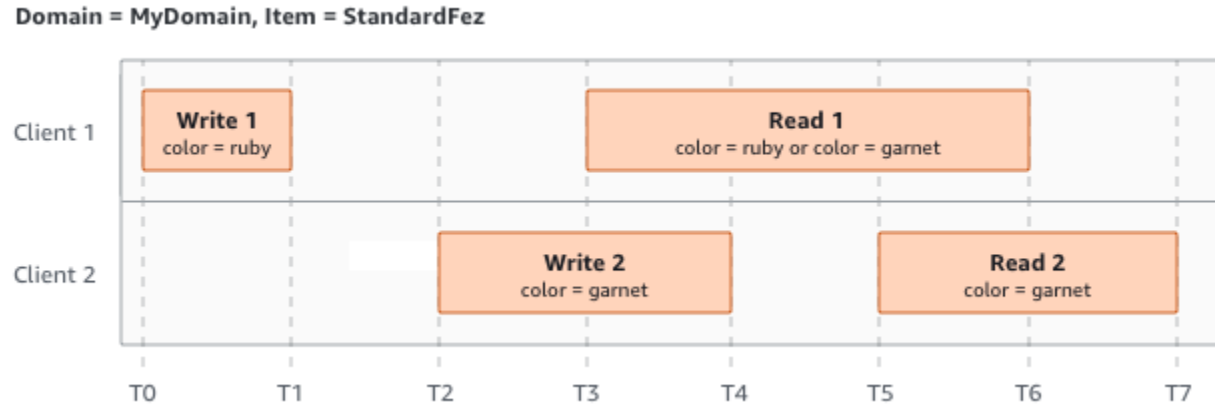
Aplicações simultâneas

Esta seção fornece exemplos de comportamento a serem esperados do Amazon S3 quando vários clientes estão gravando nos mesmos itens.

Neste exemplo, W1 (gravação 1) e W2 (gravação 2) são concluídas antes do início de R1 (leitura 1) e R2 (leitura 2). Como o S3 é fortemente consistente, R1 e R2 retornam `color = ruby`.



No próximo exemplo, a W2 não é encerrada antes do início da R1. Portanto, R1 pode retornar `color = ruby` ou `color = garnet`. No entanto, como W1 e W2 terminam antes do início do R2, o R2 retorna `color = garnet`.



No último exemplo, o W2 começa antes que o W1 tenha recebido uma confirmação. Portanto, essas gravações são consideradas simultâneas. O Amazon S3 usa internamente a semântica do último escritor para determinar qual gravação tem precedência. No entanto, a ordem em que o Amazon S3 recebe as solicitações e a ordem em que as aplicações recebem confirmações não podem ser previstas devido a fatores como a latência de rede. Por exemplo, o W2 pode ser iniciado por uma instância do Amazon EC2 na mesma região, enquanto o W1 pode ser iniciado por um host que está mais longe. A melhor maneira de determinar o valor final é realizar uma leitura após ambas as gravações terem sido confirmadas.



Serviços relacionados

Depois de carregar os dados no Amazon S3, você poderá usá-los com outros serviços da AWS. Os serviços a seguir podem ser usados com mais frequência:

- Amazon Elastic Compute Cloud (Amazon EC2): oferece capacidade de computação escalável na Nuvem AWS. O uso do Amazon EC2 elimina a necessidade de investir em hardware inicialmente, portanto, você pode desenvolver e implantar aplicações com mais rapidez. É possível usar o Amazon EC2 para executar quantos servidores virtuais forem necessários, configurar a segurança e as redes e gerenciar o armazenamento.
- Amazon EMR: ajuda empresas, pesquisadores, analistas de dados e desenvolvedores a processar de maneira fácil e econômica grandes quantidades de dados. O Amazon EMR usa um framework do Hadoop hospedado que é executado na infraestrutura de escala da Web do Amazon EC2 e do Amazon S3.
- Família do AWS Snow: ajuda os clientes que precisam executar operações em ambientes austeros e não datacenter e em locais onde há falta de conectividade de rede consistente. Você pode usar dispositivos da família do AWS Snow para acesso ao armazenamento localmente e de potência computacional da Nuvem AWS em lugares onde talvez não haja conexão à Internet.
- AWS Transfer Family: fornece suporte totalmente gerenciado para transferências de arquivos diretamente para dentro e fora do Amazon S3 ou Amazon Elastic File System (Amazon EFS) usando Secure Shell (SSH), File Transfer Protocol (SFTP), File Transfer Protocol over SSL (FTPS) e File Transfer Protocol (FTP).

Acesso ao Amazon S3

Você pode trabalhar com o Amazon S3 de qualquer uma das seguintes formas:

AWS Management Console

O console é uma interface de usuário baseada na Web para gerenciar o Amazon S3 e o recursos da AWS. Se você se inscreveu em uma Conta da AWS, pode acessar o console do Amazon S3 fazendo login no AWS Management Console e escolhendo S3 na página inicial do AWS Management Console.

AWS Command Line Interface

Você pode usar as ferramentas de linha de comando da AWS para emitir comandos ou criar scripts na linha de comando de seu sistema e executar tarefas da AWS (incluindo o S3).

A AWS Command Line Interface (AWS CLI) fornece comandos para um amplo conjunto de Serviços da AWS. A AWS CLI é compatível com Windows, macOS e Linux. Para começar a usar, consulte o Guia do usuário do AWS Command Line Interface. Para obter mais informações sobre os comandos do Amazon S3, consulte s3api e s3control na Referência de comandos da AWS CLI.

SDKs da AWS

A AWS fornece SDKs (kits de desenvolvimento de software) que consistem em bibliotecas e códigos de exemplo para várias linguagens de programação e plataformas (Java, Python, Ruby, .NET, iOS, Android etc.). Os AWS SDKs constituem uma forma conveniente de criar acesso programático para o S3 e a AWS. O Amazon S3 é um serviço REST. É possível enviar solicitações para o Amazon S3 usando a API REST ou as bibliotecas SDK da AWS, que envolvem a API REST do Amazon S3 e simplificam as tarefas de programação. Por exemplo, os SDKs processam tarefas como calcular assinaturas, assinar solicitações de forma criptográfica, gerenciar erros e novas tentativas automáticas de solicitações. Para obter informações sobre os AWS SDKs, incluindo como baixar e instalá-los, consulte Ferramentas da AWS.

Cada interação com o Amazon S3 é autenticada ou anônima. Se você estiver usando os AWS SDKs, as bibliotecas calcularão a assinatura das chaves fornecidas. Consulte mais informações sobre como fazer solicitações ao Amazon S3 em Making requests.

API REST do Amazon S3

A arquitetura do Amazon S3 foi desenvolvida para ser neutra em termos de linguagem de programação, usando nossas interfaces compatíveis com a AWS para armazenar e recuperar objetos. Você pode acessar o S3 e a AWS de forma programada usando a API REST do Amazon S3. A API REST é uma interface HTTP para o Amazon S3. Usando a API REST, você usa solicitações HTTP padrão para criar, buscar e excluir buckets e objetos.

Você pode usar qualquer toolkit compatível com HTTP para usar a API REST. Você pode até usar um navegador para buscar objetos, desde que eles possam ser lidos anonimamente.

A API REST usa os cabeçalhos padrão e os códigos de status HTTP para que os navegadores e os toolkits padrão funcionem como esperado. Em algumas áreas, adicionamos funcionalidade ao HTTP (por exemplo, adicionamos cabeçalhos para oferecer suporte ao controle de acesso). Nesses casos, fizemos o melhor para adicionar nova funcionalidade de uma forma que correspondesse ao estilo de uso padrão do HTTP.

Se fizer chamadas diretas da API REST na aplicação, você deverá escrever o código para calcular a assinatura e adicioná-la à solicitação. Consulte mais informações sobre como fazer solicitações ao Amazon S3 em Making requests na Referência de API do Amazon S3.

> **Note**
>
> O suporte da API de SOAP via HTTP está defasado, mas continua disponível via HTTPS. Os novos recursos do Amazon S3 não são compatíveis com o SOAP. Recomendamos usar a API REST ou os AWS SDKs.

Pagar pelo Amazon S3

A definição de preço para o Amazon S3 foi desenvolvida para que você não precise planejar para os requisitos de armazenamento da aplicação. A maioria dos provedores de armazenamento exige que você adquira uma quantidade predeterminada de armazenamento e capacidade de transferência de rede. Nesse cenário, se você exceder essa capacidade, o serviço é desativado ou você é cobrado por altas taxas excedentes. Se você não exceder essa capacidade, você paga como se tivesse usado tudo.

O Amazon S3 cobra apenas pelo que você realmente usa, sem taxas ocultas e nenhuma taxa excedente. Este modelo fornece a você um serviço com custo variável que pode aumentar com seus

negócios enquanto proporciona a você as vantagens de custos de infraestrutura da AWS. Para obter mais informações, consulte Preços do Amazon S3.

Ao cadastrar-se na AWS, sua Conta da AWS é automaticamente cadastrada em todos os serviços da AWS incluindo o Amazon S3. Entretanto, você será cobrado apenas pelos serviços que usar. Se você for um novo cliente do Amazon S3, você pode começar a usar o Amazon S3 gratuitamente. Para obter mais informações, consulte nível gratuito da AWS.

Para ver sua fatura, acesse o Painel de Billing and Cost Management no console da Gerenciamento de Faturamento e Custos da AWS. Para saber mais sobre o faturamento da Conta da AWS, consulte o Guia do usuário doAWS Billing. Se tiver dúvidas sobre o faturamento da AWS e as Contas da AWS, entre em contato com o AWS Support.

Conformidade do PCI DSS

O Amazon S3 é compatível com o processamento, o armazenamento e a transmissão de dados de cartão de crédito por um comerciante ou um provedor de serviços e foi validada como em conformidade com o Data Security Standard (DSS, Padrão de segurança de dados) da Payment Card Industry (PCI, Padrão de cartão de crédito). Para obter mais informações sobre o PCI DSS, incluindo como solicitar uma cópia do pacote de conformidade com o PCI da AWS, consulte Nível 1 do PCI DSS.

Conceitos básicos do Amazon S3

Você pode começar a usar o Amazon S3 trabalhando com buckets e objetos. Um bucket é um contêiner de objetos. Um objeto é um arquivo e qualquer metadado que descreva esse arquivo.

Para armazenar um objeto no Amazon S3, crie um bucket e faça upload do objeto para o bucket. Quando o objeto estiver no bucket, você poderá abri-lo, fazer download dele e movê-lo. Quando você não precisar mais de um objeto ou um bucket, poderá limpar seus recursos.

Com o Amazon S3, você paga somente pelo que for usado. Para obter mais informações sobre os recursos e a definição de preço do Amazon S3, consulte Amazon S3. Se você for um novo cliente do Amazon S3, você pode começar a usar o Amazon S3 gratuitamente. Para obter mais informações, consulte Nível gratuito da AWS.

> **Note**
>
> Para obter mais informações sobre o uso da classe de armazenamento Amazon S3 Express One Zone com buckets de diretório, consulte S3 Express One Zone e Trabalhar com buckets de diretório.

Vídeo: Conceitos básicos do Amazon S3

Pré-requisitos

Antes de começar, confirme que concluiu as etapas em Configuração do Amazon S3.

Configuração do Amazon S3

Ao cadastrar-se na AWS, sua Conta da AWS é automaticamente cadastrada em todos os serviços da AWS incluindo o Amazon S3. Você será cobrado apenas pelos serviços que usar.

Com o Amazon S3, você paga somente pelo que for usado. Para obter mais informações sobre os recursos e a definição de preço do Amazon S3, consulte Amazon S3. Se você for um novo cliente do Amazon S3, você pode começar a usar o Amazon S3 gratuitamente. Para obter mais informações, consulte Nível gratuito da AWS.

Para configurar o Amazon S3, use as etapas nas seções a seguir.

Quando você se inscreve na AWS e configura o Amazon S3, você pode, se quiser, alterar o idioma de exibição no AWS Management Console. Para obter mais informações, consulte Alterar o idioma do AWS Management Console no Guia de conceitos básicos do AWS Management Console.

Tópicos

- Inscrever-se para uma Conta da AWS
- Criar um usuário com acesso administrativo

Inscrever-se para uma Conta da AWS

Se você ainda não tem uma Conta da AWS, siga as etapas abaixo para criar uma.

Como cadastrar uma Conta da AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga as instruções online.

   Parte do procedimento de inscrição envolve receber uma chamada telefônica ou uma mensagem de texto e inserir um código de verificação pelo teclado do telefone.

   Quando você se inscreve para uma Conta da AWS, um Usuário raiz da conta da AWS é criado. O usuário-raiz tem acesso a todos os Serviços da AWS e recursos na conta. Como prática recomendada de segurança, atribua o acesso administrativo a um usuário e use somente o usuário-raiz para executar tarefas que exigem acesso de usuário-raiz.

A AWS envia um e-mail de confirmação depois que o processo de inscrição é concluído. A qualquer momento, é possível exibir as atividades da conta atual e gerenciar sua conta acessando https://aws.amazon.com/ e selecionando Minha conta.

Criar um usuário com acesso administrativo

Depois de se cadastrar em uma Conta da AWS, proteja seu Usuário raiz da conta da AWS, habilite o AWS IAM Identity Center e crie um usuário administrativo para não usar o usuário-raiz em tarefas cotidianas.

Proteger o Usuário raiz da conta da AWS

1. Faça login no AWS Management Console como o proprietário da conta ao escolher a opção Usuário-raiz e inserir o endereço de e-mail da Conta da AWS. Na próxima página, insira a senha.

   Para obter ajuda ao fazer login usando o usuário-raiz, consulte Fazer login como usuário-raiz no Guia do usuário do Início de Sessão da AWS.
2. Habilite a autenticação multifator (MFA) para o usuário-raiz.

   Para obter instruções, consulte Habilitar um dispositivo MFA virtual para sua Conta da AWS de usuário-raiz (console) no Guia do usuário do IAM.

Criar um usuário com acesso administrativo

1. Habilita o Centro de Identidade do IAM.

   Para obter instruções, consulte Habilitar o AWS IAM Identity Center no Guia do usuário do AWS IAM Identity Center.
2. No Centro de Identidade do IAM, conceda o acesso administrativo a um usuário.

   Para obter um tutorial sobre como usar o Diretório do Centro de Identidade do IAM como a fonte de identidade, consulte Configurar o acesso dos usuários com o Diretório do Centro de Identidade do IAM padrão no Guia do usuário do AWS IAM Identity Center.

Iniciar sessão como o usuário com acesso administrativo

- Para fazer login com o seu usuário do Centro de Identidade do IAM, use o URL de login enviado ao seu endereço de e-mail quando o usuário do Centro de Identidade do IAM foi criado.

  Para obter ajuda para fazer login usando um usuário do Centro de Identidade do IAM, consulte Fazer login no portal de acesso da AWS, no Guia do usuário do Início de Sessão da AWS.

Atribuir acesso a usuários adicionais

1. No Centro de Identidade do IAM, crie um conjunto de permissões que siga as práticas recomendadas de aplicação de permissões com privilégio mínimo.

Para obter instruções, consulte Criar um conjunto de permissões no Guia do usuário do AWS IAM Identity Center.

2. Atribua usuários a um grupo e, em seguida, atribua o acesso de autenticação única ao grupo.

   Para obter instruções, consulte Adicionar grupos no Guia do usuário do AWS IAM Identity Center.

Etapa 1: criar seu primeiro bucket do S3

Depois de se inscrever na AWS, você estará pronto para criar um bucket no Amazon S3 usando o AWS Management Console. Cada objeto no Amazon S3 é armazenado em um bucket. Antes de poder armazenar dados no Amazon S3, você deve criar um bucket.

> **Note**
>
> Para obter mais informações sobre o uso da classe de armazenamento Amazon S3 Express One Zone com buckets de diretório, consulte S3 Express One Zone e Trabalhar com buckets de diretório.

> **Note**
>
> Você não é cobrado pela criação de um bucket. Você é cobrado somente pelo armazenamento de objetos no bucket e pela transferência de objetos para dentro e para fora do bucket. Você estará sujeito a uma cobrança mínima (menos de 1 USD) ao seguir os exemplos contidos neste guia. Para obter mais informações sobre os custos de armazenamento, consulte Definição de preço do Amazon S3.

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Na barra de navegação na parte superior da página, escolha o nome da Região da AWS exibida no momento. Em seguida, escolha a região na qual você deseja criar um bucket.

> **Note**
>
> - Depois de criado um bucket, você não pode mudar sua região.
> - Para reduzir a latência e os custos e atender aos requisitos regulatórios, selecione uma região perto de você. Os objetos armazenados em uma região nunca saem dessa região, a menos que você os transfira para outra região. Para obter uma lista de Regiões da AWS do Amazon S3, consulte Endpoints de AWS service (Serviço da AWS) no Referência geral da Amazon Web Services.

3. No painel de navegação à esquerda, escolha Buckets de uso geral.
4. Selecione Create bucket (Criar bucket). A página Create bucket (Criar bucket) é aberta.
5. Para Nome do bucket, insira um nome para o bucket.

   O nome do bucket deve:

   - Ser exclusivo em uma partição. Uma partição é um agrupamento de regiões. No momento, a AWS tem três partições: `aws` (regiões comerciais), `aws-cn` (regiões da China) e `aws-us-gov` (AWS GovCloud (US) Regions).
   - Ter entre 3 e 63 caracteres.
   - Consistir em apenas letras minúsculas, números, pontos (`.`) e hifens (`-`). Para alcançar a melhor compatibilidade, recomendamos evitar o uso de pontos (`.`) em nomes de bucket, exceto em buckets usados apenas para hospedagem de sites estáticos.
   - Inicie e termine com uma letra ou um número.
   - Para obter uma lista completa de regras de nomenclatura de buckets, consulte Regras de nomenclatura de buckets de uso geral.

   > **Important**
   >
   > - Depois de criado o bucket, você não pode mudar seu nome.
   > - Não inclua informações confidenciais no nome do bucket. O nome do bucket é visível nos URLs que apontam para os objetos no bucket.

6. (Opcional) Em Configuração geral, você pode optar por copiar as configurações de um bucket existente para seu novo bucket. Prossiga·para·a·próxima·etapa·se você não quiser copiar as configurações de um bucket existente.

   > **Note**
   >
   > Essa opção:
   >
   > - Não está disponível na AWS CLI, mas apenas no console do Amazon S3.
   > - Não copia a política de bucket existente para o novo bucket.

   Para copiar as configurações de um bucket existente, em Copiar configurações do bucket existente, selecione Escolher bucket. A janela Escolher bucket é aberta. Encontre o bucket com as configurações que você quer copiar e selecione Escolher bucket. A janela Escolher bucket é fechada e a janela Criar bucket é reaberta.

   Agora, em Copiar configurações do bucket existente, você vê o nome do bucket selecionado. As configurações do novo bucket agora correspondem às configurações do bucket que você selecionou. Se você quiser remover as configurações copiadas, escolha Restaurar padrões. Revise as configurações restantes do bucket na página Criar bucket. Se não quiser fazer nenhuma alteração, você poderá pular para a etapa final.

7. Em Object Ownership, para desabilitar ou habilitar ACLs e controlar a propriedade de objetos carregados em seu bucket, escolha uma das seguintes configurações:

   ACLs desabilitadas

   - Imposto pelo proprietário do bucket (padrão): as ACLs são desabilitadas e o proprietário do bucket automaticamente tem propriedade e controle total sobre todos os objetos do bucket de uso geral. As ACLs não afetam mais as permissões de acesso aos dados no bucket de uso geral do S3. O bucket usa políticas exclusivamente para definir o controle de acesso.

     Por padrão, as ACLs estão desabilitadas. A maioria dos casos de uso modernos no Amazon S3 não exige mais o uso de ACLs. Recomendamos manter as ACLs desabilitadas, exceto em circunstâncias incomuns em que seja necessário controlar o acesso para cada objeto individualmente. Para obter mais informações, consulte Controlar a propriedade de objetos e desabilitar ACLs para seu bucket.

ACLs habilitadas

- Bucket owner preferred (Preferencial do proprietário do bucket): o proprietário do bucket tem a propriedade e o controle total sobre novos objetos que outras contas gravam no bucket com a ACL `bucket-owner-full-control` pré-configurada.

  Se você aplicar a configuração Proprietário do bucket preferido para exigir que todos os uploads do Amazon S3 incluam a ACL `bucket-owner-full-control` pré-configurada, será possível adicionar uma política de bucket que só permita uploads de objetos que usem essa ACL.
- Object writer (Gravador de objetos): a Conta da AWS que carrega um objeto é a proprietária do objeto, tem controle total sobre ele e pode conceder acesso a outros usuários por meio de ACLs.

> **Note**
>
> A configuração padrão é Imposto pelo proprietário do Bucket. Para aplicar a configuração padrão e manter as ACLs desabilitadas, somente a permissão `s3:CreateBucket` é necessária. Para habilitar ACLs, é necessário ter a permissão `s3:PutBucketOwnershipControls`.

8. Em Configurações de bloqueio de acesso público para este bucket, selecione as configurações de bloqueio de acesso público que deseja aplicar ao bucket.

   Por padrão, todas as quatro configurações do Bloqueio de Acesso Público são habilitadas. Recomendamos que você mantenha todas as configurações habilitadas, a menos que precise desativar uma ou mais delas para seu caso de uso específico. Para obter mais informações sobre como bloquear o acesso público, consulte Bloquear o acesso público ao armazenamento do Amazon S3.

   > **Note**
   >
   > Para habilitar todas as configurações do Bloqueio de Acesso Público, somente a permissão `s3:CreateBucket` é necessária. Para desabilitar qualquer

configuração do Bloqueio de Acesso Público, é necessário ter a permissão `s3:PutBucketPublicAccessBlock`.

9. (Opcional) Por padrão, Versionamento de bucket está desabilitado. Versionamento é um meio de manter diversas variantes de um objeto no mesmo bucket. O versionamento pode ser usado para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do . Com o versionamento, você pode se recuperar mais facilmente de ações não intencionais do usuário e de falhas da aplicação. Para obter mais informações sobre versionamento, consulte Reter várias versões de objetos com o Versionamento do S3.

   Para habilitar o versionamento no bucket, escolha Habilitar.

10. (Opcional) Em Tags (Etiquetas), você pode optar por adicionar etiquetas ao seu bucket. Com a alocação de custos da AWS, você pode usar tags de bucket para anotar o faturamento referente ao uso de um bucket. Uma tag é um par chave-valor que representa uma etiqueta que você atribui a um bucket. Para obter mais informações, consulte the section called “Usar tags de alocação de custos”.

    Para adicionar uma etiqueta, escolha Add Tag (Adicionar etiqueta) e insira uma chave e um valor para cada etiqueta.

11. Para configurar Criptografia padrão, em Tipo de criptografia, selecione uma das seguintes opções:

    - Criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3)
    - Criptografia no lado do servidor com chaves do AWS Key Management Service (SSE-KMS)
    - Criptografia de camada dupla do lado do servidor com chaves do AWS Key Management Service (AWS KMS) (DSSE-KMS)

    > **Important**
    >
    > Se você usar a opção SSE-KMS ou a DSSE-KMS em sua configuração de criptografia padrão, poderão ser cobradas cotas de solicitações por segundo (RPS) do AWS KMS. Para obter mais informações sobre as cotas do AWS KMS e como solicitar um aumento de cota, consulte Cotas no Guia do desenvolvedor do AWS Key Management Service.

Buckets e novos objetos são criptografados por meio da criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3) como nível básico da configuração de criptografia. Para obter mais informações sobre criptografia padrão, consulte Definir o comportamento padrão da criptografia para os buckets do Amazon S3. Para ter mais informações sobre SSE-S3, consulte Usar a criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3).

Para obter mais informações sobre como usar a criptografia no lado do servidor para criptografar seus dados, consulte the section called “Criptografia de dados”.

12. Se você escolheu Criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3) ou Criptografia de camada dupla do lado do servidor com chaves do AWS Key Management Service (AWS KMS) (DSSE-KMS), faça o seguinte:

    a. Em Chave do AWS KMS, especifique sua chave do KMS de uma das seguintes maneiras:

    - Para escolher entre uma lista de chaves do KMS disponíveis, selecione Escolher entre suas AWS KMS keys e escolha sua chave do KMS na lista de chaves disponíveis.

      As chaves Chave gerenciada pela AWS (`aws/s3`) e as chaves gerenciadas pelo cliente são exibidas nessa lista. Para ter mais informações sobre chaves gerenciadas pelo cliente, consulte Chaves de clientes e chaves da AWS no Guia do desenvolvedor do AWS Key Management Service.
    - Para inserir o ARN da chave do KMS, escolha Inserir ARN da AWS KMS key e insira o ARN da chave do KMS no campo exibido.
    - Para criar uma chave gerenciada pelo cliente no console do AWS KMS, selecione Criar uma chave do KMS.

      Para ter mais informações sobre como criar uma AWS KMS key, consulte Criação de chaves no Guia do desenvolvedor do AWS Key Management Service.

> **Important**
>
> Você só pode usar chaves do KMS disponíveis na mesma Região da AWS que o bucket. O console do Amazon S3 lista somente as primeiras 100 chaves do KMS na mesma região que o bucket. Para usar uma chave do KMS que não esteja listada, você deve inserir o respectivo ARN. Se quiser usar uma chave do KMS

pertencente a outra conta, primeiro você deverá ter permissão para usar a chave e, depois, inserir o respectivo ARN. Para obter mais informações sobre permissões entre contas referentes a chaves do KMS, consulte Creating KMS keys that other accounts can use no Guia do desenvolvedor do AWS Key Management Service. Para obter mais informações sobre SSE-KMS, consulte Especificando criptografia no lado do servidor com o AWS KMS (SSE-KMS). Para ter mais informações sobre DSSE-KMS, consulte the section called “Criptografia de camada dupla do lado do servidor (DSSE-KMS)”.

Ao usar uma AWS KMS key para criptografia no lado do servidor no Amazon S3, você deve escolher uma chave de criptografia do KMS simétrica. O Amazon S3 só é compatível com chaves do KMS de criptografia simétrica, e não com chaves assimétricas do KMS. Para ter mais informações, consulte Identificar chaves do KMS simétricas e assimétricas no Guia do desenvolvedor do AWS Key Management Service.

b. Ao configurar o bucket para usar a criptografia padrão com SSE-KMS, você também pode usar as chaves de bucket do S3. As chaves de bucket do S3 diminuem o custo de criptografia reduzindo o tráfego de solicitações do Amazon S3 para o AWS KMS. Para obter mais informações, consulte Redução do custo do SSE-KMS com chaves de bucket do Amazon S3. As chaves de bucket do S3 não comportam DSSE-KMS.

   Por padrão, as chaves de bucket do S3 estão habilitadas no console do Amazon S3. Recomendamos deixá-las habilitadas para reduzir os custos. Para desabilitar as chaves de bucket do S3 do seu bucket, em Chave de bucket, escolha Desabilitar.

13. (Opcional) O Bloqueio de Objetos do S3 ajuda a proteger novos objetos contra exclusão ou substituição. Para obter mais informações, consulte Bloquear objetos com o Bloqueio de Objetos. Se você quiser habilitar o Bloqueio de Objetos do S3, faça o seguinte:

    a. Selecione Advanced settings (Configurações avançadas).

> **Important**
>
> A habilitação do Bloqueio de Objetos habilita automaticamente o versionamento do bucket. Depois de habilitar e criar o bucket com sucesso, você também deverá definir as configurações de retenção padrão e de retenção jurídica do Bloqueio de Objetos na guia Propriedades do bucket.

b. Se quiser habilitar o bloqueio de objetos, escolha Enable (Habilitar), leia o aviso que aparece e confirme-o.

> **Note**
>
> Para criar um bucket com o Bloqueio de Objetos habilitado, você deve ter as seguintes permissões: `s3:CreateBucket`, `s3:PutBucketVersioning` e `s3:PutBucketObjectLockConfiguration`.

14. Selecione Create bucket (Criar bucket).

Você criou um bucket no Amazon S3.

Próxima etapa

Para adicionar um objeto ao bucket, consulte Etapa 2: fazer upload de um objeto para o seu bucket.

Etapa 2: fazer upload de um objeto para o seu bucket

Depois de criar um bucket no Amazon S3, você estará pronto para fazer upload de um objeto no bucket. Um objeto pode ser qualquer tipo de arquivo: um arquivo de texto, uma foto, um vídeo etc.

> **Note**
>
> Para obter mais informações sobre o uso da classe de armazenamento Amazon S3 Express One Zone com buckets de diretório, consulte S3 Express One Zone e Trabalhar com buckets de diretório.

Para fazer upload de um objeto em um bucket

1. Abra o console do Amazon S3, em https://console.aws.amazon.com/s3/.
2. Na lista Buckets, escolha o nome do bucket no qual você deseja fazer upload do objeto.
3. Na guia Objects (Objetos) do bucket, escolha Upload (Fazer upload).
4. Em Files and folders (Arquivos e pastas), escolha Add files (Adicionar arquivos).
5. Escolha um arquivo para carregar e, em seguida, escolha Open (Abrir).

6. Escolha Carregar.

O upload de um objeto no bucket foi realizado corretamente.

Próxima etapa

Para visualizar o objeto, consulte Etapa 3: fazer download de um objeto.

Etapa 3: fazer download de um objeto

Depois de fazer upload de um objeto para um bucket, você já pode visualizar informações e fazer download do objeto em seu computador local.

> **Note**
>
> Para obter mais informações sobre o uso da classe de armazenamento Amazon S3 Express One Zone com buckets de diretório, consulte S3 Express One Zone e Trabalhar com buckets de diretório.

Uso do console do S3

Esta seção explica como usar o console do Amazon S3 para fazer baixar um objeto de um bucket do S3.

> **Note**
>
> - Só é possível baixar um objeto por vez.
> - Se você usar o console do Amazon S3 para baixar um objeto cujo nome da chave termine com um ponto (`.`), o ponto será removido do nome da chave do objeto baixado. Para reter o ponto no final do nome do objeto baixado, você deve usar a AWS Command Line Interface (AWS CLI), AWS SDKs ou a API REST do Amazon S3.

Fazer download de um objeto de um bucket do S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.

2. No painel de navegação à esquerda, escolha Buckets de uso geral ou Buckets de diretórios.
3. Na lista de buckets, escolha o nome do bucket do qual você deseja fazer download de um objeto.
4. Você pode baixar um objeto de um bucket do S3 de uma das seguintes formas:
   - Marque a caixa de seleção ao lado do objeto e escolha Fazer download. Se você quiser baixar o objeto em uma pasta específica, no menu Ações, escolha Fazer download como.
   - Se você quiser baixar uma versão específica do objeto, ative Mostrar versões (ao lado da caixa de pesquisa). Marque a caixa de seleção ao lado da versão do objeto que você deseja e escolha Fazer Download. Se você quiser baixar o objeto em uma pasta específica, no menu Ações, escolha Fazer download como.

Você baixou seu objeto com êxito.

Próxima etapa

Para copiar e colar seu objeto no Amazon S3, consulte Etapa 4: copiar seu objeto para uma pasta.

Etapa 4: copiar seu objeto para uma pasta

Você já adicionou um objeto a um bucket e fez download do objeto. Agora, você cria uma pasta e copia o objeto e o cola na pasta.

> **Note**
>
> Para obter mais informações sobre o uso da classe de armazenamento Amazon S3 Express One Zone com buckets de diretório, consulte S3 Express One Zone e Trabalhar com buckets de diretório.

Como copiar um objeto em uma pasta

1. Na lista Buckets, escolha o nome do bucket.
2. Selecione Create folder (Criar pasta) e configure uma nova pasta:
   a. Insira um nome para a pasta (por exemplo, `favorite-pics`).

b. Para a configuração de criptografia de pasta, escolha Disable (Desabilitar).

c. Escolha Salvar.

3. Navegue até o bucket ou pasta do Amazon S3 que contém os objetos que você deseja copiar.
4. Marque a caixa de seleção à esquerda dos nomes dos objetos que você deseja copiar.
5. Escolha Actions (Ações) e escolha Copy (Copiar) na lista de opções exibida.

   Como alternativa, escolha Copy (Copiar) nas opções no canto superior direito.
6. Escolha a pasta de destino:

   a. Selecione Browse S3 (Navegar no S3).

   b. Escolha o botão de opção à esquerda do nome da pasta.

      Para navegar em uma pasta e escolher uma subpasta como seu destino, escolha o nome da pasta.

   c. Escolha Choose destination (Escolher destino).

   O caminho para a pasta de destino aparece na caixa Destination (Destino) . Em Destination (Destino), você pode, também, inserir o caminho de destino, por exemplo, s3://*bucket-name*/*folder-name*/.
7. No canto inferior direito, escolha Copy (Copiar).

   O Amazon S3 copia seus objetos na pasta de destino.

Próxima etapa

Para excluir um objeto e um bucket no Amazon S3, consulte Etapa 5: excluir seus objetos e bucket.

Etapa 5: excluir seus objetos e bucket

Quando você não precisar mais de um objeto ou bucket, recomendamos excluí-los para evitar cobranças adicionais. Se você concluiu esta demonstração de conceitos básicos como um exercício de aprendizagem e não planeja usar o bucket ou os objetos, recomendamos que exclua os dois para não acumular cobranças.

Antes de excluir seu bucket, esvazie-o ou exclua os objetos contidos nele. Depois de excluir seus objetos e o bucket, eles não estarão mais disponíveis.

Se você quiser continuar usando o mesmo nome de bucket, recomendamos excluir os objetos ou esvaziar o bucket, mas não excluir o bucket. Depois de excluir um bucket, o nome dele fica disponível para ser reutilizado. No entanto, outra Conta da AWS pode criar um bucket com o mesmo nome antes de você ter a chance de reutilizá-lo.

> **Note**
>
> Para obter mais informações sobre o uso da classe de armazenamento Amazon S3 Express One Zone com buckets de diretório, consulte S3 Express One Zone e Trabalhar com buckets de diretório.

Tópicos

- Excluir um objeto
- Esvaziar o bucket
- Excluir bucket

Excluir um objeto

Se quiser escolher quais objetos excluir sem esvaziar todos os objetos do bucket, você pode excluir um objeto.

1. Na lista Buckets, escolha o nome do bucket do qual deseja excluir um objeto.
2. Selecione o objeto que deseja excluir.
3. Escolha Excluir nas opções no canto superior direito.
4. Na página Excluir objetos, digite **`delete`** para confirmar a exclusão de seus objetos.
5. Escolha Delete objects (Excluir objetos).

Esvaziar o bucket

Se pretender excluir seu bucket, primeiro você deve esvaziar seu bucket, o que exclui todos os objetos contidos nele.

Para esvaziar um bucket

1. Na lista Buckets, selecione o bucket que deseja esvaziar e escolha Empty (Vazio).

2. Para confirmar que deseja esvaziar o bucket e excluir todos os objetos contidos nele, em Empty bucket (Esvaziar bucket), digite **`permanently delete`**.

   > **Important**
   >
   > Não é possível desfazer a ação de esvaziar bucket. Os objetos adicionados ao bucket enquanto a ação de esvaziamento do bucket estiver em andamento serão excluídos.

3. Para esvaziar o bucket e excluir todos os objetos contidos nele, escolha Empty (Esvaziar).

   Uma página Empty bucket :Status (Esvaziar bucket: status) é aberta, para que você possa revisar um resumo de exclusões de objetos com falha e bem-sucedidas.

4. Para retornar à sua lista de buckets, escolha Exit (Sair).

Excluir bucket

Depois de esvaziar o bucket ou excluir todos os objetos dele, você poderá excluir o bucket.

1. Para excluir um bucket, selecione o bucket na lista Buckets.
2. Escolha Excluir.
3. Para confirmar a exclusão, digite o nome do bucket em Delete bucket (Excluir bucket).

   > **Important**
   >
   > Não é possível desfazer a ação de excluir um bucket. Nomes de bucket são exclusivos. Se você excluir seu bucket, outro usuário da AWS poderá usar o nome. Se quiser continuar usando o mesmo nome de bucket, não exclua o bucket. Em vez disso, esvazie e conserve o bucket.

4. Para excluir seu bucket, escolha Delete bucket (Excluir bucket).

Próximas etapas

Nos exemplos anteriores, você aprendeu a executar alguma tarefas básicas no Amazon S3.

Os seguintes tópicos explicam os caminhos de aprendizado que você pode usar para conhecer o Amazon S3 detalhamente para que você possa implementá-lo em suas aplicações.

> **Note**
>
> Para obter mais informações sobre o uso da classe de armazenamento Amazon S3 Express One Zone com buckets de diretório, consulte S3 Express One Zone e Trabalhar com buckets de diretório.

Tópicos

- Entender casos de uso comuns
- Controlar o acesso a buckets e objetos
- Proteger e monitorar o armazenamento
- Desenvolvimento com o Amazon S3
- Aprenda com os tutoriais
- Explore o treinamento e o suporte

Entender casos de uso comuns

Você pode usar o Amazon S3 para oferecer suporte ao seu caso de uso específico. A Biblioteca de soluções da AWS e o Blog da AWS fornecem informações e tutoriais específicos para casos de uso. Veja a seguir alguns casos de uso comuns do Amazon S3:

- Backup e armazenamento: use os recursos de gerenciamento de armazenamento do Amazon S3 para gerenciar custos, atender aos requisitos normativos, reduzir a latência e salvar várias cópias distintas de seus dados para requisitos de conformidade.
- Hospedagem de aplicações: implante, instale e gerencie aplicações Web confiáveis, altamente escaláveis e de baixo custo. Por exemplo, você pode configurar seu bucket do Amazon S3 para hospedar um site estático. Para obter mais informações, consulte Hospedagem de um site estático usando o Amazon S3.
- Hospedagem de mídia: crie uma infraestrutura altamente disponível que hospede carregamentos e downloads de vídeos, fotos ou músicas.
- Entrega de software: hospede suas aplicações de software para que sejam baixadas pelos clientes.

Controlar o acesso a buckets e objetos

O Amazon S3 fornece uma variedade de recursos e ferramentas de segurança. Para obter uma visão geral, consulte Controle de acesso no Amazon S3.

Por padrão, os buckets do S3 e os objetos deles são privados. Você tem acesso somente aos recursos do S3 criados. Você pode usar os seguintes recursos para conceder permissões de recursos detalhadas que ofereçam suporte a seu caso de uso específico ou para auditar as permissões de seus recursos do Amazon S3.

- Bloqueio de acesso público do S3: bloqueie o acesso público a buckets e objetos do S3. Por padrão, as configurações do Bloqueio de Acesso Público são ativadas no nível do bucket.
- Identidades do AWS Identity and Access Management (IAM): use o IAM ou o AWS IAM Identity Center para criar identidades do IAM em sua Conta da AWS a fim de gerenciar o acesso aos recursos do Amazon S3. Por exemplo, é possível usar o IAM com o Amazon S3 para controlar o tipo de acesso que um usuário ou grupo de usuários tem a um bucket do Amazon S3 pertencente à sua Conta da AWS. Para obter mais informações sobre as identidades do IAM e as práticas recomendadas, consulte Identidades do IAM (usuários, grupos de usuários e perfis) no Guia do usuário do IAM.
- Políticas de buckets: use a linguagem de política baseada em IAM para configurar permissões baseadas em recursos para os buckets do S3 e os objetos neles contidos.
- Listas de controle de acesso (ACLs): conceda permissões de leitura e gravação para buckets e objetos individuais a usuários autorizados. Como regra geral, recomendamos o uso de políticas baseadas em recursos do S3 (políticas de bucket e políticas de ponto de acesso) ou políticas de usuários do IAM para controle de acesso, em vez de ACLs. As políticas são uma opção de controle de acesso simplificada e mais flexível. Com políticas de bucket e políticas de ponto de acesso, é possível definir regras que se aplicam amplamente a todas as solicitações para seus recursos do Amazon S3. Para obter mais informações sobre os casos específicos em que você usaria ACLs, em vez de políticas baseadas em recursos ou políticas de usuário do IAM, consulte Gerenciamento de identidade e acesso para o Amazon S3.
- Propriedade de objeto do S3: assuma a propriedade de cada objeto do bucket simplificando o gerenciamento de acesso para dados armazenados no Amazon S3. A Propriedade de objeto do S3 é uma configuração no nível do bucket do Amazon S3 que você pode usar para desabilitar ou habilitar as ACLs. Por padrão, as ACLs estão desabilitadas. Com as ACLs desabilitadas, o proprietário do bucket possui todos os objetos do bucket e gerencia o acesso aos dados exclusivamente usando políticas de gerenciamento de acesso.

- IAM Access Analyzer para S3: avalie e monitore as políticas de acesso ao bucket do S3, garantindo que elas forneçam apenas o acesso pretendido aos recursos do S3.

Proteger e monitorar o armazenamento

- Proteger o armazenamento: depois de criar buckets e fazer upload de objetos no Amazon S3, você pode gerenciar o armazenamento de objetos. Por exemplo, é possível usar os controles de failover do Versionamento do S3, da Replicação do S3 e do Ponto de Acesso Multirregional para recuperação de desastres, o AWS Backup para fazer backup de dados e o Bloqueio de Objetos do S3 para definir períodos de retenção, evitar exclusões e substituições e atender aos requisitos de conformidade.
- Monitoramento de seu armazenamento: o monitoramento é uma parte importante para manter a confiabilidade, a disponibilidade e a performance do Amazon S3 e das soluções da AWS. Você pode monitorar a atividade e os custos de armazenamento. Além disso, recomendamos que você colete dados de monitoramento de todas as partes de sua solução da AWS para que possa depurar mais facilmente uma falha multiponto, caso ocorra.

  Você também pode usar analytics e insights no Amazon S3 para entender, analisar e otimizar o uso do armazenamento. Por exemplo, use o Amazon S3 Storage Lens para entender, analisar e otimizar seu armazenamento. O S3 Storage Lens fornece mais de 29 métricas de uso e atividade e painéis interativos para agregar dados de toda a sua organização, contas específicas, regiões, buckets ou prefixos. Use a Análise de classe de armazenamento para analisar padrões de acesso ao armazenamento para decidir quando é hora de mover seus dados para uma classe de armazenamento mais econômica. Para gerenciar seus custos, você pode usar o Ciclo de Vida do S3.

Desenvolvimento com o Amazon S3

O Amazon S3 é um serviço REST. Você pode enviar solicitações para o Amazon S3 usando a API REST ou as bibliotecas do SDK da AWS que envolvem a API REST subjacente do Amazon S3, simplificando as tarefas de programação. Você também pode usar o AWS Command Line Interface (AWS CLI) para fazer chamadas de API do Amazon S3. Consulte mais informações em Making requests na Referência da API do Amazon S3.

A API REST do Amazon S3 é uma interface HTTP para o Amazon S3. Usando a API REST, você usa solicitações HTTP padrão para criar, buscar e excluir buckets e objetos. Você pode usar qualquer toolkit compatível com HTTP para usar a API REST. Você pode até usar um navegador

para buscar objetos, desde que eles possam ser lidos anonimamente. Consulte mais informações em Developing with Amazon S3 na Referência de API do Amazon S3.

Para ajudá-lo a criar aplicações usando a linguagem de sua escolha, fornecemos os seguintes recursos.

AWS CLI

Você pode acessar os recursos do Amazon S3 usando a AWS CLI. Para baixar e configurar oAWS CLI, consulte Desenvolvendo com o Amazon S3 usando a AWS CLI na Referência de API do Amazon S3.

A AWS CLI oferece dois níveis de comandos para acessar o Amazon S3: comandos de alto nível (s3) e comandos no nível de API (s3api e `s3control`). Os comandos de alto nível do S3 simplificam a execução de tarefas comuns, como criar, manipular e excluir objetos e buckets. Os comandos s3api e s3control expõem acesso direto a todas as operações de API do Amazon S3, que podem ser usadas para executar operações avançadas que podem não ser possíveis com os comandos de alto nível.

Para obter uma lista dos comandos da AWS CLI do Amazon S3, consulte s3, s3api e s3control.

SDKs e Explorers da AWS

Você pode usar os AWS SDKs ao desenvolver aplicações com o Amazon S3. Os AWS SDKs simplificam as tarefas de programação integrando a API REST subjacente. Os SDKs móveis da AWS e a biblioteca JavaScript do Amplify também estão disponíveis para a compilação de aplicações Web e aplicações para dispositivos móveis conectados usando a AWS.

Além dos AWS SDKs, os Explorers da AWS estão disponíveis para Visual Studio e Eclipse para Java IDE. Nesse caso, os SDKs e os explorers estão empacotados como toolkits da AWS.

Consulte mais informações em Developing with Amazon S3 using the AWS SDKs na Referência de API do Amazon S3.

Bibliotecas e código de exemplo

O Centro do Desenvolvedor da AWS e o Catálogo de exemplos de código da AWS contêm código de exemplo e bibliotecas escritos especialmente para o Amazon S3. Você pode usar esses exemplos de códigos para entender como implementar a API do Amazon S3. Você também pode visualizar a Referência da API de Serviço do Amazon Simple Storage para entender as operações da API do Amazon S3 em detalhes.

Aprenda com os tutoriais

Você pode começar usando tutoriais passo a passo para saber mais sobre a Amazon S3. Esses tutoriais foram projetados para um ambiente de tipo de laboratório e usam nomes de empresas, nomes de usuários fictícios e assim por diante. O objetivo é fornecer orientação geral. Eles não se destinam ao uso direto em um ambiente de produção sem uma revisão e adaptação cuidadosas para atender às necessidades exclusivas do ambiente da organização.

Conceitos básicos

- Tutorial: Armazenar e recuperar um arquivo com o Amazon S3
- Tutorial: Começar a usar o S3 Intelligent-Tiering
- Tutorial: Começar a usar as classes de armazenamento do Amazon S3 Glacier

Otimizar custos do armazenamento

- Tutorial: Começar a usar o S3 Intelligent-Tiering
- Tutorial: Começar a usar as classes de armazenamento do Amazon S3 Glacier
- Tutorial: Otimizar custos e obter visibilidade do uso com a Lente de Armazenamento do S3

Gerenciar o armazenamento

- Tutorial: Introdução aos pontos de acesso multirregionais do Amazon S3
- Tutorial: replicar objetos existentes nos buckets do Amazon S3 com o S3 Batch Replication

Hospedar vídeos e sites

- Tutorial: Hospedagem de transmissão sob demanda com o Amazon S3, Amazon CloudFront e Amazon Route 53
- Tutorial: configurar um site estático no Amazon S3
- Tutorial: Configurar um site estático usando um domínio personalizado registrado no Route 53

Processar dados

- Tutorial: Como transformar dados para sua aplicação com o S3 Object Lambda

- Tutorial: Detectar e editar dados PII com o S3 Object Lambda e o Amazon Comprehend
- Tutorial: Using S3 Object Lambda to dynamically watermark images as they are retrieved (Tutorial: Como usar o S3 Object Lambda para colocar marca d'água em imagens de maneira dinâmica à medida que são recuperadas)
- Tutorial: vídeos de transcodificação em lote com o Operações em Lote do S3

Proteger dados

- Tutorial: Verificar a integridade dos dados no Amazon S3 com somas de verificação adicionais
- Tutorial: Replicar dados em uma região ou entre Regiões da AWS usando a Replicação do S3
- Tutorial: Proteger dados no Amazon S3 contra exclusão acidental ou bugs de aplicações usando o Versionamento do S3, o Bloqueio de Objeto do S3 e a Replicação do S3
- Tutorial: replicar objetos existentes nos buckets do Amazon S3 com o S3 Batch Replication

Explore o treinamento e o suporte

Você pode aprender com especialistas da AWS para aprimorar suas habilidades e obter assistência especializada para alcançar seus objetivos.

- Treinamento: os recursos de treinamento oferecem uma abordagem prática para o aprendizado do Amazon S3. Para obter mais informações, consulte Treinamentos e certificações da AWS e as AWS Online Tech Talks.
- Fóruns de discussão: no fórum, você pode analisar as publicações para entender o que pode e o que não pode ser feito com o Amazon S3. Você também pode publicar suas dúvidas. Para obter mais informações, consulte os Fóruns de discussão.
- Suporte técnico: se você tiver mais dúvidas, entre em contato com o Suporte técnico.

Comece a usar o Amazon S3 por meio da AWS CLI

Você pode começar a usar o Amazon S3 utilizando a AWS Command Line Interface (AWS CLI) para trabalhar com buckets de uso geral e objetos. Um bucket é um contêiner de objetos. Um objeto é um arquivo e qualquer metadado que descreva esse arquivo.

Para armazenar um objeto no Amazon S3, crie um bucket e faça upload do objeto para o bucket. Quando o objeto estiver no bucket, você poderá abri-lo, fazer download dele e movê-lo. Quando você não precisar mais de um objeto ou um bucket, poderá limpar seus recursos.

Com o Amazon S3, você paga somente pelo que for usado. Para obter mais informações sobre os recursos e a definição de preço do Amazon S3, consulte Amazon S3. Se você for um novo cliente do Amazon S3, você pode começar a usar o Amazon S3 gratuitamente. Para obter mais informações, consulte Nível gratuito da AWS.

> **Note**
>
> Para obter mais informações sobre o uso da classe de armazenamento Amazon S3 Express One Zone com buckets de diretório, consulte Tutorial: Conceitos básicos da classe S3 Express One Zone e Trabalhar com buckets de diretório.

Configuração

Antes de começar a usar a AWS CLI com o Amazon S3, você deve:

- Cadastrar-se em uma conta da AWS. Para instruções, consulte Configuração do Amazon S3.
- Criar um usuário com permissões `s3:*`. Para instruções, consulte Configuração do Amazon S3.
- Instalar e configurar a AWS CLI. Para instruções, consulte Instalar ou atualizar a versão mais recente da AWS CLI no Guia do usuário do AWS Command Line Interface.

Para verificar se o perfil da AWS CLI está configurado adequadamente, execute o seguinte comando:

```
aws sts get-caller-identity
```

Para obter informações, consulte get-caller-identity na Referência de comandos da AWS CLI.

Esse comando exibe uma lista dos comandos disponíveis do Amazon S3 se a AWS CLI estiver instalada e configurada corretamente.

Etapa 1: criar seu primeiro bucket do Amazon S3

Depois de configurar a AWS CLI, você já pode criar um bucket no Amazon S3. Cada objeto no Amazon S3 é armazenado em um bucket. Antes de poder armazenar dados no Amazon S3, você deve criar um bucket.

> **Note**
>
> Você não é cobrado pela criação de um bucket. Você é cobrado somente pelo armazenamento de objetos no bucket e pela transferência de objetos para dentro e para fora do bucket. Você estará sujeito a uma cobrança mínima (menos de 1 USD) ao seguir os exemplos contidos neste guia. Para obter mais informações sobre os custos de armazenamento, consulte Definição de preço do Amazon S3.

Para criar um bucket

1. Crie um bucket usando o comando `s3api create-bucket`. Substitua *amzn-s3-demo-bucket* por um nome de bucket exclusivo e `us-east-1` pela região desejada:

```
aws s3api create-bucket --bucket amzn-s3-demo-bucket --region us-east-1
```

   Para regiões diferentes de us-east-1, você precisa especificar a restrição de localização:

```
aws s3api create-bucket --bucket amzn-s3-demo-bucket --region us-west-2 --create-
bucket-configuration LocationConstraint=us-west-2
```

   > **Note**
   >
   > - Depois de criar um bucket, você não pode mudar sua região.
   > - Para reduzir a latência e os custos e atender aos requisitos regulatórios, selecione uma região perto de você. Os objetos armazenados em uma região nunca saem dessa região, a menos que você os transfira para outra região. Para obter uma lista de regiões da AWS do Amazon S3, consulte Endpoints de serviço da AWS na Referência geral da Amazon Web Services.
   > - O nome do bucket deve:

- Ser exclusivo em uma partição. Uma partição é um agrupamento de regiões. No momento, a AWS tem três partições: `aws` (regiões comerciais), `aws-cn` (regiões da China) e `aws-us-gov` (regiões AWS GovCloud (US)).
- Ter entre 3 e 63 caracteres.
- Consistir em apenas letras minúsculas, números, pontos (.) e hifens (-). Para obter a melhor compatibilidade, recomendamos evitar o uso de pontos () em nomes de bucket, exceto em buckets usados apenas para hospedagem de sites estáticos.
- Inicie e termine com uma letra ou um número.

- Depois de criado o bucket, você não pode mudar seu nome.
- Não inclua informações confidenciais no nome do bucket. O nome do bucket é visível nos URLs que apontam para os objetos no bucket.

2. Liste todos os buckets para verificar se o seu bucket foi criado:

```
aws s3 ls
```

3. Em Propriedade de objeto, você pode desabilitar ou habilitar ACLs e controlar a propriedade de objetos enviado ao seu bucket.

   ACLs desabilitadas

   Para definir Imposto pelo proprietário do bucket (padrão): as ACLs são desabilitadas e o proprietário do bucket automaticamente tem propriedade e controle total sobre todos os objetos do bucket de uso geral:

```
aws s3api put-bucket-ownership-controls --bucket amzn-s3-demo-bucket --ownership-controls="Rules=[{ObjectOwnership=BucketOwnerEnforced}]"
```

> **Note**
>
> Por padrão, as ACLs estão desabilitadas. A maioria dos casos de uso modernos no Amazon S3 não exige mais o uso de ACLs. Recomendamos manter as ACLs desabilitadas, exceto em circunstâncias incomuns em que seja necessário controlar o acesso para cada objeto individualmente. Para obter mais informações, consulte Controlar a propriedade de objetos e desabilitar ACLs para seu bucket.

ACLs habilitadas

- Para definir Proprietário do bucket preferido: o bucket tem a propriedade e o controle total sobre novos objetos que outras contas gravam no bucket com a ACL pré-configurada `bucket-owner-full-control`.

```
aws s3api put-bucket-ownership-controls --bucket amzn-s3-demo-bucket --ownership-controls="Rules=[{ObjectOwnership=BucketOwnerPreferred}]"
```

  Se você aplicar a configuração Proprietário do bucket preferido e desejar exigir que todos os uploads do Amazon S3 incluam a ACL pré-configurada `bucket-owner-full-control`, será possível Exigir a ACL pré-configurada bucket-owner-full-control para operações PUT do Amazon S3 (preferencial do proprietário do bucket), que permite somente uploads de objetos que usem essa ACL.

- Para definir Autor do objeto: a conta da AWS que faz upload de um objeto é a proprietária do objeto, tem controle total sobre ele e pode conceder acesso a outros usuários por meio de ACLs.

```
aws s3api put-bucket-ownership-controls --bucket amzn-s3-demo-bucket --ownership-controls="Rules=[{ObjectOwnership=ObjectWriter}]"
```

> **Note**
>
> A configuração padrão é Imposto pelo proprietário do Bucket. Para aplicar a configuração padrão e manter as ACLs desabilitadas, somente a permissão `s3:CreateBucket` é necessária. Para habilitar ACLs, é necessário ter a permissão `s3:PutBucketOwnershipControls`.

Para verificar a configuração atual de propriedade de objeto do seu bucket:

```
aws s3api get-bucket-ownership-controls --bucket amzn-s3-demo-bucket
```

4. Para verificar se o Bloqueio de Acesso Público está habilitado (ele está habilitado por padrão para novos buckets):

```
aws s3api get-public-access-block --bucket amzn-s3-demo-bucket
```

Por padrão, as quatro configurações de Bloqueio de Acesso Público estão habilitadas para novos buckets. Recomendamos que você mantenha todas as configurações habilitadas, a menos que precise desativar uma ou mais delas para seu caso de uso específico. Para obter mais informações sobre como bloquear o acesso público, consulte Bloquear o acesso público ao armazenamento do Amazon S3.

Se você precisar habilitar o Bloqueio de Acesso Público, use o seguinte comando:

```
aws s3api put-public-access-block --bucket amzn-s3-demo-bucket --public-access-
block-configuration
 "BlockPublicAcls=true,IgnorePublicAcls=true,BlockPublicPolicy=true,RestrictPublicBuckets=t
```

> **Note**
>
> Para habilitar todas as configurações do Bloqueio de Acesso Público, somente a permissão `s3:CreateBucket` é necessária. Para desabilitar qualquer configuração do Bloqueio de Acesso Público, é necessário ter a permissão `s3:PutBucketPublicAccessBlock`.

5. Para habilitar o versionamento para um bucket

```
aws s3api put-bucket-versioning --bucket amzn-s3-demo-bucket --versioning-
configuration Status=Enabled
```

Por padrão, o versionamento de bucket está desabilitado. Versionamento é um meio de manter diversas variantes de um objeto no mesmo bucket. O versionamento pode ser usado para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do . Com o versionamento, você pode se recuperar mais facilmente de ações não intencionais do usuário e de falhas da aplicação. Para obter mais informações sobre versionamento, consulte Reter várias versões de objetos com o Versionamento do S3.

6. O Bloqueio de Objetos do S3 ajuda a proteger novos objetos contra exclusão ou substituição. Para obter mais informações, consulte Bloquear objetos com o Bloqueio de Objetos. Para habilitar o recurso para Bloquear objetos com o Bloqueio de Objetos (requer versionamento do bucket):

Para um novo bucket:

```
aws s3api create-bucket --bucket amzn-s3-demo-bucket --region us-east-1 --object-lock-enabled-for-bucket
```

Para um bucket existente:

```
aws s3api put-object-lock-configuration --bucket amzn-s3-demo-bucket --object-lock-configuration '{"ObjectLockEnabled": "Enabled"}'
```

Se você quiser definir um padrão para Bloquear objetos com o Bloqueio de Objetos com a habilitação do Bloqueio de Objetos, você poderá usar:

```
aws s3api put-object-lock-configuration --bucket amzn-s3-demo-bucket --object-lock-configuration '{"ObjectLockEnabled":"Enabled","Rule":{"DefaultRetention":{"Mode":"COMPLIANCE","Days":30}}}'
```

Você pode substituir `"COMPLIANCE"` por `"GOVERNANCE"` para ter um modo menos restritivo e ajustar o número de dias conforme necessário.

> **Note**
>
> Para criar um bucket com o Bloqueio de Objetos habilitado, você deve ter as seguintes permissões: `s3:CreateBucket`, `s3:PutBucketVersioning` e `s3:PutBucketObjectLockConfiguration`.

7. É possível adicionar ao seu bucket. Com a alocação de custos da AWS, você pode usar tags de bucket para anotar o faturamento referente ao uso de um bucket. Uma tag é um par chave-valor que representa uma etiqueta que você atribui a um bucket. Para obter mais informações, consulte Usar tags de alocação de custos para buckets do S3.

   Para adicionar tags ao seu bucket:

   ```
   aws s3api put-bucket-tagging --bucket amzn-s3-demo-bucket --tagging
    'TagSet=[{Key=Purpose,Value=Testing},{Key=Environment,Value=Development}]'
   ```

8. Buckets e novos objetos são criptografados por meio da criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3) como o nível básico da configuração de criptografia. Para verificar a criptografia padrão do seu bucket, use o seguinte comando:

```
aws s3api get-bucket-encryption --bucket amzn-s3-demo-bucket
```

Você também pode configurar a criptografia do lado do servidor com chaves do AWS KMS (SSE-KMS) e a criptografia do lado do servidor de camada dupla com chaves do AWS KMS (DSSE-KMS) para o seu bucket. Tanto a chave gerenciada pela AWS (aws/s3) quanto as chaves gerenciadas pelo cliente podem ser usadas como sua chave do AWS KMS para a configuração de criptografia SSE-KMS e DSSE-KMS. Para ter mais informações sobre chaves gerenciadas pelo cliente, consulte Chaves de clientes e chaves da AWS no Guia do desenvolvedor do AWS Key Management Service. Para ter mais informações sobre como criar uma chave do AWS KMS, consulte Creating keys no Guia do desenvolvedor do AWS Key Management Service.

> **Important**
>
> A chave do AWS KMS deve estar na mesma região da AWS que o bucket do Amazon S3. Não é possível usar chaves do KMS entre regiões para criptografia de bucket do Amazon S3.

Ao configurar o bucket para usar a criptografia padrão com SSE-KMS, você também pode usar as chaves de bucket do Amazon S3. As chaves de bucket do Amazon S3 diminuem o custo de criptografia reduzindo o tráfego de solicitações do Amazon S3 para o AWS KMS. Para obter mais informações, consulte Redução do custo do SSE-KMS com chaves de bucket do Amazon S3. As chaves de bucket do Amazon S3 não comportam DSSE-KMS. Na AWS CLI, as chaves de bucket do Amazon S3 NÃO são habilitadas por padrão ao criar um bucket. Isso é diferente do comportamento do console, onde elas estão habilitadas por padrão.

Para configurar o SSE-KMS e habilitar as chaves de bucket do Amazon S3:

```
aws s3api put-bucket-encryption --bucket amzn-s3-demo-bucket --server-side-
encryption-configuration "{\"Rules\":[{\"ApplyServerSideEncryptionByDefault
\":{\"SSEAlgorithm\":\"aws:kms\",\"KMSMasterKeyID\":\"YOUR-KMS-KEY-ARN\"},
\"BucketKeyEnabled\":true}]}"
```

Para verificar se as chaves de Bucket do Amazon S3 estão habilitadas para um bucket:

```
aws s3api get-bucket-encryption --bucket amzn-s3-demo-bucket
```

A saída incluirá um campo `BucketKeyEnabled` definido como `true` ou `false`.

Para configurar o `DSSE-KMS`, execute o seguinte comando:

```
aws s3api put-bucket-encryption --bucket amzn-s3-demo-bucket --server-side-
encryption-configuration '{"Rules":[{"ApplyServerSideEncryptionByDefault":
{"SSEAlgorithm":"aws:kms:dsse","KMSMasterKeyID":"YOUR-KMS-KEY-ARN"}}]}'
```

Para obter mais informações sobre criptografia padrão, consulte Definir o comportamento padrão da criptografia para os buckets do Amazon S3. Para ter mais informações sobre SSE-S3, consulte Usar a criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3).

> **Important**
>
> Se você usar a opção SSE-KMS ou a DSSE-KMS em sua configuração de criptografia padrão, poderão ser cobradas cotas de solicitações por segundo (RPS) do AWS KMS. Você pode reduzir as chamadas de API do KMS habilitando as chaves de bucket do Amazon S3, o que diminui o número de solicitações enviadas ao AWS KMS. Para obter mais informações sobre as cotas do AWS KMS e como solicitar um aumento de cota, consulte Cotas no Guia do desenvolvedor do AWS Key Management Service.

Você criou um bucket no Amazon S3. A próxima etapa é fazer upload de um objeto em seu bucket.

Etapa 2: fazer upload de um objeto para o seu bucket

Depois de criar um bucket no Amazon S3, você estará pronto para fazer upload de um objeto no bucket. Um objeto pode ser qualquer tipo de arquivo: um arquivo de texto, uma foto, um vídeo etc.

Para fazer upload de um objeto em um bucket

1. Crie um arquivo de texto simples para fazer upload. Você pode usar qualquer editor de texto ou executar o seguinte comando:

```
echo 'Hello, Amazon S3!' > example.txt
```

2. Faça upload do arquivo no bucket usando o comando s3 cp.

```
aws s3 cp example.txt s3://amzn-s3-demo-bucket/
```

Se o upload for bem-sucedido, você verá uma saída semelhante a:

```
upload: ./example.txt to s3://amzn-s3-demo-bucket/example.txt
```

3. Liste o conteúdo do seu bucket para verificar se o objeto foi carregado:

```
aws s3 ls s3://amzn-s3-demo-bucket/
```

O upload de um objeto no bucket foi realizado corretamente. A próxima etapa é baixar um objeto.

Etapa 3: fazer download de um objeto

Depois de fazer upload de um objeto para um bucket, você já pode visualizar informações e fazer download do objeto em seu computador local.

Como baixar um objeto de um bucket do Amazon S3

1. Para obter informações sobre seu objeto:

```
aws s3api head-object --bucket amzn-s3-demo-bucket --key example.txt
```

Esse comando retorna metadados sobre o objeto, como tipo de conteúdo, tamanho do conteúdo e data da última modificação.

2. Baixe o objeto em seu computador local:

```
aws s3 cp s3://amzn-s3-demo-bucket/example.txt downloaded-example.txt
```

Se o download for bem-sucedido, você verá uma saída semelhante a:

```
download: s3://amzn-s3-demo-bucket/example.txt to ./downloaded-example.txt
```

3. Verifique o conteúdo do arquivo baixado:

```
cat downloaded-example.txt
```

> **Note**
>
> - Ao contrário do console, a AWS CLI pode baixar vários objetos ao mesmo tempo usando curingas ou o sinalizador `--recursive`.
> - Ao baixar objetos com a AWS CLI, o ponto (.) no final do nome das chaves de objeto é preservado, diferentemente do console, onde é removido. Isso é importante se suas chaves de objeto terminarem com pontos.

Exemplo de download de vários objetos:

Para baixar vários objetos de um bucket do Amazon S3 com extensões de arquivo específicas, use o comando de cópia recursiva com os filtros `exclude` e `include`, conforme mostrado no exemplo.

```
aws s3 cp s3://amzn-s3-demo-bucket/ . --recursive --exclude "*" --include "*.txt"
```

Você baixou seu objeto com êxito. A próxima etapa é copiar seu objeto para uma pasta.

Etapa 4: copiar seu objeto para uma pasta

Você já adicionou um objeto a um bucket e fez download do objeto. Agora, crie uma pasta e copie e cole o objeto na pasta.

Como copiar um objeto em uma pasta

1. No Amazon S3, as pastas são representadas como prefixos em chaves de objeto. Crie uma "pasta" copiando um objeto com um prefixo:

```
aws s3 cp s3://amzn-s3-demo-source-bucket/example.txt s3://amzn-s3-demo-
destination-bucket/favorite-files/example.txt
```

   Se a cópia for bem-sucedida, você verá uma saída semelhante a:

```
copy: s3://amzn-s3-demo-source-bucket/example.txt to s3://amzn-s3-demo-destination-bucket/favorite-files/example.txt
```

2. Liste o conteúdo da pasta para verificar se o objeto foi copiado:

```
aws s3 ls s3://amzn-s3-demo-destination-bucket/favorite-files/
```

Você conseguiu copiar seu objeto para uma pasta. A próxima etapa é excluir seus objetos e o bucket.

Etapa 5: excluir seus objetos e bucket

Quando você não precisar mais de um objeto ou bucket, recomendamos excluí-los para evitar cobranças adicionais. Se você concluiu esta demonstração de conceitos básicos como um exercício de aprendizagem e não planeja usar o bucket ou os objetos, recomendamos que exclua os dois para não acumular cobranças.

Antes de excluir seu bucket, esvazie-o ou exclua os objetos contidos nele. Depois de excluir seus objetos e o bucket, eles não estarão mais disponíveis.

Se você quiser continuar usando o mesmo nome de bucket, recomendamos excluir os objetos ou esvaziar o bucket, mas não excluir o bucket. Depois de excluir um bucket, o nome dele fica disponível para ser reutilizado. No entanto, outra conta da AWS pode criar um bucket com o mesmo nome antes de você ter a chance de reutilizá-lo.

Excluir um objeto

Se quiser escolher quais objetos excluir sem esvaziar todos os objetos do bucket, você pode excluir um objeto.

Exclua um objeto específico:

```
aws s3 rm s3://amzn-s3-demo-bucket/example.txt
```

Se a exclusão for bem-sucedida, você verá uma saída semelhante a:

```
delete: s3://amzn-s3-demo-bucket/example.txt
```

Esvaziar o bucket

Se você pretende excluir seu bucket, primeiro deve esvaziá-lo, o que exclui todos os objetos, versões e os marcadores de exclusão que estão nele.

Para esvaziar um bucket

> **Important**
>
> Não é possível desfazer a ação de esvaziar bucket. Os objetos adicionados ao bucket enquanto a ação de esvaziamento do bucket estiver em andamento serão excluídos.

1. Opção 1: para buckets menores, usar o comando `rm` com o sinalizador `--recursive` para excluir todos os objetos no bucket:

   ```
   aws s3 rm s3://amzn-s3-demo-bucket --recursive
   ```

   Esse comando exclui todos os objetos no bucket, incluindo objetos em pastas.

   > **Note**
   >
   > Se seu bucket contiver muitos objetos ou objetos grandes, esse comando poderá atingir o tempo limite. Para buckets com grandes quantidades de dados, use a regra de ciclo de vida do Amazon S3 para expirar objetos nos buckets.

   Opção 2: usar as regras de ciclo de vida do Amazon S3 (recomendadas para buckets grandes)

   Para buckets com muitos objetos ou objetos grandes, use uma regra de ciclo de vida do Amazon S3 para expirar e excluir automaticamente todos os objetos. Aguarde o processamento da regra de ciclo de vida (isso pode levar até 24 horas). Para ter mais informações sobre como usar regras de ciclo de vida para esvaziar buckets, consulte Como usar uma regra de configuração de ciclo de vida para esvaziar um bucket do Amazon S3?.

2. Verifique se o bucket está vazio:

   ```
   aws s3 ls s3://amzn-s3-demo-bucket
   ```

3. Se o versionamento do bucket estiver habilitado, use os comandos a seguir para excluir objetos versionados e marcadores de exclusão.

   Remova objetos versionados:

   ```
   aws s3api delete-objects --bucket amzn-s3-demo-bucket --delete "$(aws s3api list-
   object-versions --bucket amzn-s3-demo-bucket --output json --query='{Objects:
    Versions[].{Key:Key,VersionId:VersionId}}')"
   ```

   Remova marcadores de exclusão:

   ```
   aws s3api delete-objects --bucket amzn-s3-demo-bucket --delete "$(aws s3api list-
   object-versions --bucket amzn-s3-demo-bucket --output json --query='{Objects:
    DeleteMarkers[].{Key:Key,VersionId:VersionId}}')"
   ```

4. Verifique se o bucket não contém mais nenhuma versão de objeto e nenhum marcador de exclusão:

   ```
   aws s3api list-object-versions --bucket amzn-s3-demo-bucket
   ```

   Não deve haver nenhuma versão nem nenhum marcador de exclusão restante na saída.

Excluir bucket

Depois de esvaziar o bucket ou excluir todos os objetos dele, você poderá excluir o bucket.

> **Important**
>
> Não é possível desfazer a ação de excluir um bucket. Nomes de bucket são exclusivos. Se você excluir seu bucket, outro usuário da AWS poderá usar o nome. Se quiser continuar usando o mesmo nome de bucket, não exclua o bucket. Em vez disso, esvazie e conserve o bucket.

Para excluir seu bucket do

1. Exclua seu bucket:

   ```
   aws s3api delete-bucket --bucket amzn-s3-demo-bucket
   ```

2. Liste todos os seus buckets para verificar se o bucket foi excluído:

```
aws s3 ls
```

Próximas etapas

Nos exemplos anteriores, você aprendeu a executar alguma tarefas básicas no Amazon S3 usando a AWS CLI.

Os seguintes tópicos explicam os caminhos de aprendizado que você pode usar para conhecer o Amazon S3 detalhamente para que você possa implementá-lo em suas aplicações.

- Entender casos de uso comuns
- Controlar o acesso a buckets e objetos
- Proteger e monitorar o armazenamento
- Desenvolvimento com o Amazon S3
- Entender casos de uso comuns
- Explore o treinamento e o suporte

A lista a seguir mostra comandos comuns da AWS CLI para o Amazon S3:

- cp: copia arquivos ou objetos entre seu sistema de arquivos local e o Amazon S3 ou entre locais do Amazon S3.
- ls: lista objetos e prefixos comuns do Amazon S3 em um bucket e prefixo especificados.
- mb: cria um bucket do Amazon S3.
- mv: move arquivos ou objetos entre seu sistema de arquivos local e o Amazon S3 ou entre locais do Amazon S3.
- presign: gera um URL pré-assinado para um objeto do Amazon S3 que permite acesso temporário sem credenciais da AWS.
- rb: remove um bucket vazio do Amazon S3. Você pode usar o sinalizador `--force` para esvaziar e excluir automaticamente um bucket com conteúdo por meio de um único comando. Essa ação não pode ser desfeita.
- rm: exclui objetos do Amazon S3.

- sync: sincroniza diretórios e prefixos do Amazon S3 copiando recursivamente arquivos novos e atualizados do diretório de origem para o destino.
- website: configura um bucket como um site estático.

Para ter mais informações sobre os comandos da AWS CLI para o Amazon S3, consulte os seguintes recursos:

- s3: comandos gerais do Amazon S3 que simplificam operações comuns.
- s3api: acesso direto a todas as operações de API do Amazon S3.
- control: acesso direto a todas as operações de API de controle do Amazon S3.

Criar, configurar e trabalhar com buckets de uso geral do Amazon S3

Para armazenar seus dados no Amazon S3, você trabalha com recursos conhecidos como buckets e objetos. Um bucket é um contêiner de objetos. Um objeto é um arquivo e qualquer metadado que descreva esse arquivo.

Para armazenar um objeto no Amazon S3, crie um bucket e faça upload do objeto em um bucket. Quando o objeto estiver no bucket, você poderá abri-lo, fazer download dele e movê-lo. Quando você não precisar mais de um objeto ou um bucket, poderá limpar seus recursos.

Os tópicos desta seção apresentam uma visão geral do trabalho com buckets de uso geral no Amazon S3. Eles incluem informações sobre nomeação, criação, acesso e exclusão de buckets de uso geral. Para obter mais informações sobre como visualizar ou listar objetos em um bucket, consulte Organizar, listar e trabalhar com seus objetos.

Há vários tipos de bucket do Amazon S3. Antes de criar um bucket, escolha o tipo de bucket que melhor se adapte aos requisitos de performance e da aplicação. Para obter mais informações sobre os vários tipos de bucket e os casos de uso apropriados para cada um, consulte Buckets.

> **Note**
>
> Para obter mais informações sobre o uso da classe de armazenamento Amazon S3 Express One Zone com buckets de diretório, consulte S3 Express One Zone e Trabalhar com buckets de diretório.

> **Note**
>
> Com o Amazon S3, você paga somente pelo que for usado. Para obter mais informações sobre os recursos e a definição de preço do Amazon S3, consulte Amazon S3. Se você for um novo cliente do Amazon S3, você pode começar a usar o Amazon S3 gratuitamente. Para obter mais informações, consulte Nível gratuito da AWS.

Tópicos

- Visão geral dos buckets de uso geral
- Padrões comuns de bucket de uso geral para criar aplicações no Amazon S3
- Regras de nomenclatura de buckets de uso geral
- Cotas, limitações e restrições de buckets de uso geral
- Acessar um bucket de uso geral do Amazon S3
- Criar um bucket de uso geral
- Visualizar das propriedades de um bucket de uso geral do S3
- Listar buckets de uso geral do Amazon S3
- Esvaziar um bucket de uso geral
- Excluir um bucket de uso geral
- Montar um bucket do Amazon S3 como um sistema de arquivos local
- Como trabalhar com o Navegador de Armazenamento para Amazon S3
- Configurar transferências de arquivos rápidas e seguras usando o Amazon S3 Transfer Acceleration
- Utilizar buckets de uso geral com pagamento pelo solicitante para transferência e uso de armazenamento

Visão geral dos buckets de uso geral

Para fazer upload de seus dados (fotos, vídeos, documentos etc.) para o Amazon S3, primeiro é necessário criar um bucket do S3 em uma das Regiões da AWS.

Há vários tipos de bucket do Amazon S3. Antes de criar um bucket, escolha o tipo de bucket que melhor se adapte aos requisitos de performance e da aplicação. Para obter mais informações sobre os vários tipos de bucket e os casos de uso apropriados para cada um, consulte Buckets.

As seções a seguir fornecem mais informações sobre buckets de uso geral, incluindo regras de nomenclatura de buckets, cotas e detalhes de configuração de buckets. Consulte uma lista de restrições e limitações relacionadas aos buckets do Amazon S3 em Cotas, limitações e restrições de buckets de uso geral.

Tópicos

- Visão geral dos buckets de uso geral
- Padrões comuns de bucket de uso geral

- Permissões
- Gerenciar o acesso público a buckets de uso geral
- opções de configuração de bucket de uso geral
- operações de bucket de uso geral
- monitoramento de desempenho de buckets de uso geral

Visão geral dos buckets de uso geral

Cada objeto está contido em um bucket. Por exemplo, se o objeto chamado `photos/puppy.jpg` estiver armazenado no bucket de uso geral `amzn-s3-demo-bucket` da região Oeste dos EUA (Oregon), ele poderá ser endereçado usando o URL `https://amzn-s3-demo-bucket.s3.us-west-2.amazonaws.com/photos/puppy.jpg`. Para obter mais informações, consulte Accessing a Bucket (Como acessar um bucket).

- As cotas de buckets de uso geral para regiões comerciais só podem ser visualizadas e gerenciadas na região Leste dos EUA (N. da Virgínia).
- As cotas de buckets de uso geral para AWS GovCloud (US) só podem ser visualizadas e gerenciadas em AWS GovCloud (Oeste dos EUA).

Em termos de implementação, os buckets e objetos são recursos da AWS, e o Amazon S3 fornece APIs para você gerenciá-los. Por exemplo, é possível criar um bucket e fazer upload de objetos usando a API do Amazon S3. Também é possível usar o console do Amazon S3 para executar essas operações. O console usa as APIs do Amazon S3 para enviar solicitações ao Amazon S3.

Esta seção descreve como trabalhar com buckets de uso geral. Para obter mais informações sobre como trabalhar com objetos, consulte Visão geral de objetos Amazon S3.

O Amazon S3 permite o uso de buckets de uso geral globais, o que significa que cada nome de bucket deve ser exclusivo em todas as Contas da AWS de todas as Regiões da AWS dentro de uma partição. Uma partição é um agrupamento de regiões. Atualmente, a AWS tem três partições: `aws` (regiões padrão), `aws-cn` (regiões da China) e `aws-us-gov` (AWS GovCloud (US)).

Após a criação de um bucket de uso geral, o nome dele não poderá ser usado por outra Conta da AWS na mesma partição enquanto ele não for excluído. Você não pode depender de convenções de nomenclatura de buckets específicos para fins de disponibilidade ou verificação de segurança. Para ver as diretrizes de nomeação de bucket, consulte Regras de nomenclatura de buckets de uso geral.

O Amazon S3 cria buckets na região que você especificar. Para reduzir a latência, minimizar os custos ou atender a requisitos regulatórios, escolha qualquer Região da AWS geograficamente próxima a você. Por exemplo, se você residir na Europa, poderá considerar vantajoso criar buckets nas regiões UE (Irlanda) ou UE (Frankfurt). Para obter uma lista de regiões do Amazon S3, consulte Regiões e endpoints na Referência geral da AWS.

> **Note**
>
> Os objetos pertencentes a um bucket criado em uma Região da AWS específica jamais saem dela, a menos que você os transfira explicitamente para outra região. Por exemplo, os objetos que são armazenados na região UE (Irlanda) nunca saem dela.

Padrões comuns de bucket de uso geral

Ao criar aplicações no Amazon S3, você pode usar buckets de uso geral exclusivos para separar diferentes conjuntos de dados ou workloads. Dependendo do seu caso de uso, existem diferentes padrões de design e práticas recomendadas para a utilização de buckets de uso geral. Para obter mais informações, consulte Padrões comuns de bucket de uso geral para criar aplicações no Amazon S3.

Permissões

É possível usar suas credenciais de Usuário raiz da conta da AWS para criar um bucket de uso geral e executar qualquer outra operação do Amazon S3. No entanto, recomendamos não usar as credenciais de usuário root da sua Conta da AWS para fazer solicitações, como criar um bucket. Em vez disso, crie um usuário do AWS Identity and Access Management (IAM) e conceda a esse usuário acesso total (por padrão, os usuários não têm nenhuma permissão).

Esses usuários são referidos como administradores. As credenciais do usuário administrador podem ser usadas em vez das credenciais do usuário root da conta para interagir com a AWS e executar tarefas, tais como criar um bucket, criar usuários e conceder permissões a eles.

Para obter mais informações, consulte Credenciais de Usuário raiz da conta da AWS e credenciais de usuário do IAM na Referência geral da AWS e Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.

A Conta da AWS que cria um recurso é proprietária daquele recurso. Por exemplo, se você criar um usuário do IAM na sua Conta da AWS e conceder permissões para esse usuário criar um

bucket, o usuário poderá criar um bucket. Mas o usuário não é proprietário do bucket; a Conta da AWS à qual o usuário pertence é que é a proprietária do bucket. O usuário precisará de permissão adicional do proprietário do recurso para executar qualquer outra operação de bucket. Para obter mais informações sobre o gerenciamento de permissões para recursos do Amazon S3, consulte Gerenciamento de identidade e acesso para o Amazon S3.

Gerenciar o acesso público a buckets de uso geral

O acesso público a buckets de uso geral e objetos é concedido por meio de políticas de bucket, listas de controle de acesso (ACLs) ou ambas. Para ajudar você a gerenciar o acesso público aos recursos do Amazon S3, o Amazon S3 fornece configurações de bloqueio de acesso público. As configurações de bloqueio de acesso público do Amazon S3 podem substituir ACLs e políticas de bucket para que você possa impor limites uniformes ao acesso público a esses recursos. Você pode aplicar as configurações de bloqueio de acesso público a buckets individualmente ou grupos de buckets na sua conta.

Para garantir que todos os buckets de uso geral e objetos do Amazon S3 tenham o acesso público bloqueado, todas as quatro configurações do Bloqueio de Acesso Público devem estar habilitadas por padrão ao criar um bucket. Recomendamos ativar todas as quatro configurações do Bloqueio de Acesso Público na sua conta também. Estas configurações bloqueiam o acesso público a todos os buckets atuais e futuros.

Antes de aplicar estas configurações, verifique se seus aplicativos funcionarão corretamente sem acesso público. Se você precisa de um nível determinado de acesso público aos buckets ou objetos, por exemplo, para hospedar um site estático como descrito em Hospedagem de um site estático usando o Amazon S3, é possível personalizar as configurações individualmente para atender aos seus casos de uso de armazenamento. Para obter mais informações, consulte Bloquear o acesso público ao armazenamento do Amazon S3.

No entanto, é altamente recomendável manter o Bloqueio de Acesso Público habilitado. Se quiser manter todas as quatro configurações do Bloqueio de Acesso Público habilitadas e hospedar um site estático, use o controle de acesso à origem (OAC) do Amazon CloudFront. O Amazon CloudFront fornece os recursos necessários para configurar um site estático seguro. Os sites estáticos do Amazon S3 só são compatíveis com endpoints HTTP. O Amazon CloudFront usa o armazenamento durável do Amazon S3 ao mesmo tempo que fornece cabeçalhos de segurança adicionais, como HTTPS. O HTTPS adiciona segurança criptografando uma solicitação HTTP normal e protegendo-a contra ataques cibernéticos comuns.

Para obter mais informações, consulte Conceitos básicos de um site estático seguro no Guia do desenvolvedor do Amazon CloudFront.

> **Note**
>
> Se você vir um `Error` ao listar seus buckets de uso geral e as respectivas configurações de acesso público, talvez você não tenha as permissões necessárias. Verifique se você tem as seguintes permissões adicionadas à política de usuário ou perfil:
>
> ```
> s3:GetAccountPublicAccessBlock
> s3:GetBucketPublicAccessBlock
> s3:GetBucketPolicyStatus
> s3:GetBucketLocation
> s3:GetBucketAcl
> s3:ListAccessPoints
> s3:ListAllMyBuckets
> ```
>
> Em alguns casos raros, as solicitações também podem falhar devido a uma interrupção da Região da AWS.

opções de configuração de bucket de uso geral

O Amazon S3 permite várias opções de configuração de bucket. Por exemplo, você pode configurar seu bucket para hospedagem de site, adicionar configuração para gerenciar o ciclo de vida de objetos no bucket e configurar o bucket para registrar todos os acessos a ele. O Amazon S3 é compatível com sub-recursos para que você armazene e gerencie informações de configuração do bucket. É possível usar a API do Amazon S3 para criar e gerenciar esses sub-recursos. No entanto, você também pode usar o console ou os SDKs da AWS.

> **Note**
>
> Há também configurações no nível do objeto. Por exemplo, você pode configurar permissões no nível do objeto configurando uma lista de controle de acesso (ACL) específica para aquele objeto.

São chamados de sub-recursos porque existem no contexto de um bucket ou objeto específico. A tabela a seguir lista os sub-recursos que permitem gerenciar configurações específicas de bucket.

Sub-recurso	Descrição
cors (compartilhamento de recurso de origem cruzada)	Você pode configurar seu bucket para autorizar solicitações de origem cruzada. Para obter mais informações, consulte Usar o compartilhamento de recursos de origem cruzada (CORS).
notificação de evento	Você pode permitir que seu bucket envie notificações de eventos do bucket especificado. Para obter mais informações, consulte Notificações de eventos do Amazon S3.
ciclo de vida	Você pode definir regras de ciclo de vida para objetos em seu bucket que têm um ciclo de vida bem definido. Por exemplo, você pode definir uma regra para arquivar objetos um ano após a criação ou excluir um objeto 10 anos após a criação. Para obter mais informações, consulte Gerenciar o ciclo de vida dos objetos.
location	Ao criar um bucket, você especifica a Região da AWS onde deseja que o Amazon S3 crie o bucket. O Amazon S3 armazena essas informações no sub-recurso local e fornece uma API para que você recupere essas informações.
registro em log	O registro em log permite que você rastreie solicitações de acesso ao seu bucket. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso, como solicitante, nome do bucket, horário da solicitação, ação da solicitação, status de resposta e código de erro, se houver. As informações de log de acesso podem ser úteis em auditorias de segurança e acesso. Isso também pode ajudá-lo a conhecer sua base de clientes e entender a conta do Amazon S3. Para obter mais informações, consulte Registrar em log as solicitações com registro em log de acesso ao servidor.

Sub-recurso	Descrição
bloqueio de objetos	Para usar o bloqueio de objetos do S3, é necessário habilitá-lo para um bucket. Também é possível configurar um modo e um período de retenção padrão que se aplicam a novos objetos colocados no bucket. Para obter mais informações, consulte Bloquear objetos com o Bloqueio de Objetos.
política e ACL (lista de controle de acesso)	Todos os seus recursos (como buckets e objetos) são privados por padrão. O Amazon S3 é compatível com opções de política de bucket e de lista de controle de acesso (ACL) para que você conceda e gerencie permissões no nível do bucket. O Amazon S3 armazena as informações de permissão nos sub-recursos política e acl. Para obter mais informações, consulte Gerenciamento de identidade e acesso para o Amazon S3.
replicação	A replicação é a cópia assíncrona automática de objetos em buckets na mesma Regiões da AWS ou em regiões diferentes. Para obter mais informações, consulte Replicar objetos dentro de uma região e entre regiões.
requestPayment	Por padrão, a Conta da AWS que cria o bucket (o proprietário do bucket) paga pelos downloads do bucket. Usando esse sub-recurso, o proprietário do bucket pode especificar que a pessoa que solicita o download será cobrada pelo download. O Amazon S3 fornece uma API para gerenciamento desse sub-recurso. Para obter mais informações, consulte Utilizar buckets de uso geral com pagamento pelo solicitante para transferência e uso de armazenamento.
marcação	Você pode adicionar tags de alocação de custo ao seu bucket para classific ar e acompanhar seus custos com a AWS. O Amazon S3 fornece o sub-recurso marcação para armazenar e gerenciar tags em um bucket. Com o uso de tags em seu bucket, a AWS gera um relatório de alocação de custos com o uso e custos agregados por suas tags. Para obter mais informações, consulte Relatórios de uso e faturamento do Amazon S3.

Sub-recurso	Descrição
aceleração de transferência	O Transfer Acceleration possibilita transferências de arquivos rápidas, fáceis e seguras entre seu cliente e um bucket do S3 em longas distâncias. O Transfer Acceleration tira proveito dos pontos de presença distribuídos globalmente no Amazon CloudFront. Para obter mais informações, consulte Configurar transferências de arquivos rápidas e seguras usando o Amazon S3 Transfer Acceleration.
versionamento	O versionamento ajuda a recuperar substituições e exclusões acidentais. Recomendamos o versionamento como melhor prática para impedir a exclusão ou substituição de objetos por engano. Para obter mais informações, consulte Reter várias versões de objetos com o Versionamento do S3.
site	Você pode configurar seu bucket para hospedagem de site estático. O Amazon S3 armazena essa configuração criando um sub-recurso site. Para obter mais informações, consulte Hospedagem de um site estático usando o Amazon S3.

operações de bucket de uso geral

A engenharia de alta disponibilidade do Amazon S3 é focada nas operações get, put, list e delete. Como as operações de bucket de uso geral funcionam utilizando um espaço centralizado e global de recursos, recomendamos criar, excluir ou configurar buckets no caminho de código de alta disponibilidade da aplicação. É melhor criar, excluir ou configurar buckets em uma rotina de inicialização ou configuração separada que você execute com menor frequência.

monitoramento de desempenho de buckets de uso geral

Quando você tem aplicações e processos empresariais críticos que dependem de recursos da AWS, é importante monitorar e receber alertas referentes ao sistema. Monitorar seus dados pode ajudar a manter a confiabilidade, a disponibilidade e o desempenho do Amazon S3 e das soluções da

AWS. Há vários serviços da AWS que você pode usar para coletar e agregar métricas e logs para os buckets do S3.

Dependendo do caso de uso, você pode escolher qual serviço da AWS melhor atende às necessidades da sua organização para depurar problemas, monitorar dados, otimizar os custos de armazenamento ou solucionar problemas em vários pontos. Por exemplo:

- Como melhorar o desempenho das aplicações que usam o S3: configure os alarmes do CloudWatch para monitorar dados de armazenamento, métricas de replicação ou métricas de solicitação.
- Como planejar o uso do armazenamento, otimizar custos de armazenamento ou descobrir quanto você tem de armazenamento em toda a organização: use a funcionalidade Lente de Armazenamento do Amazon S3. Se preferir, você poderá usar esse recurso para aprimorar o desempenho dos dados habilitando métricas avançadas e usando as métricas detalhadas de código de status para obter contagens de solicitações bem-sucedidas ou malsucedidas.
- Como ter uma visualização unificada de sua integridade operacional: publique as métricas de uso e atividade da Lente de Armazenamento do S3 em um painel do Amazon CloudWatch.

> **Note**
>
> A opção de publicação do Amazon CloudWatch está disponível para painéis da Lente de Armazenamento do S3 atualizados para Métricas e recomendações avançadas. É possível habilitar a opção de publicação do CloudWatch para uma configuração de painel nova ou existente no S3 Storage Lens.

- Como obter um registro das ações realizadas por um usuário, perfil ou serviço do AWS: configure logs do AWS CloudTrail. Você também pode usar logs do AWS CloudTrail para analisar chamadas de API para o Amazon S3 como eventos.
- Como receber notificações sobre quando determinado evento ocorre no bucket do S3: configure notificações de eventos do Amazon S3.
- Como obter registros detalhados das solicitações feitas a um bucket do S3: configure os logs de acesso do S3.

Consulte uma lista de todos os diferentes serviços da AWS que você pode usar para monitorar dados em Registrar em log e monitorar no Amazon S3.

Padrões comuns de bucket de uso geral para criar aplicações no Amazon S3

Ao criar aplicações no Amazon S3, você pode usar buckets de uso geral exclusivos para separar diferentes conjuntos de dados ou workloads. Ao criar aplicações que atendem usuários finais ou diferentes grupos de usuários, use nossos padrões de design de práticas recomendadas para criar aplicações que possam aproveitar melhor os recursos e a escalabilidade do Amazon S3.

> **Important**
>
> Recomendamos que você crie nomes de bucket de uso geral que não sejam previsíveis. Não escreva código presumindo que o nome do bucket escolhido esteja disponível, a menos que você já tenha criado o bucket. Um método para criar nomes de buckets que não sejam previsíveis é acrescentar um identificador único universal (GUID) ao nome do bucket, por exemplo, `amzn-s3-demo-bucket-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`. Consulte mais informações sobre regras de nomenclatura de buckets de uso geral em Regras de nomenclatura de buckets de uso geral.

Tópicos

- Padrão de bucket de uso geral multilocatário
- Padrão de bucket por uso

Padrão de bucket de uso geral multilocatário

Com buckets multilocatário, você cria um único bucket para uma equipe ou workload. Você usa prefixos exclusivos do S3 para organizar os objetos que armazena no bucket. Um prefixo é uma string no início do nome da chave do objeto. Um prefixo pode ter qualquer comprimento, sujeito ao comprimento máximo do nome da chave do objeto (1.024 bytes). Você pode pensar nos prefixos como uma forma de organizar seus dados de forma semelhante aos diretórios. No entanto, os prefixos não são diretórios.

Por exemplo, para armazenar informações sobre cidades, você pode organizá-las por continente, país, província ou estado. Como esses nomes geralmente não usam pontuação, você pode usar a barra (/) como delimitador. Os exemplos a seguir mostram prefixos sendo usados para organizar

nomes de cidades por continente, país e, depois, província ou estado, usando um delimitador de barra (/).

- Europa/França/Nova-Aquitânia/Bordeaux
- América do Norte/Canadá/Quebec/Montreal
- América do Norte /EUA/Washington/Bellevue
- América do Norte /EUA/Washington/Seattle

Esse padrão é bem escalado quando você tem centenas de conjuntos de dados exclusivos em um bucket de uso geral. Com prefixos, você pode facilmente organizar e agrupar esses conjuntos de dados.

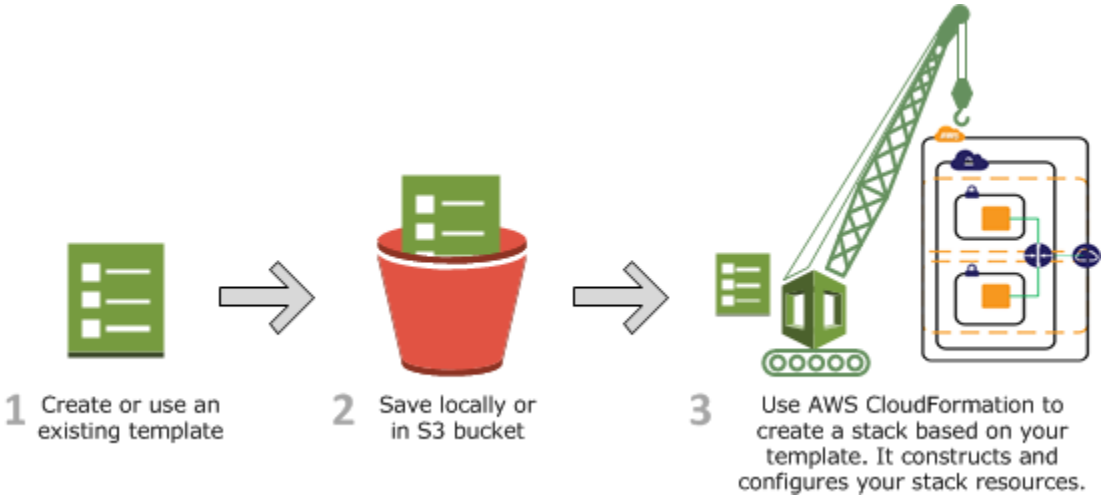
Entretanto, uma possível desvantagem do padrão de bucket de uso geral multilocatário é que muitos recursos no nível do bucket do S3, como criptografia de bucket padrão, versionamento do S3 e pagamento pelo solicitante do S3, são definidos em nível de bucket e não de prefixo. Se os diferentes conjuntos de dados dentro do bucket multilocatário tiverem requisitos exclusivos, o fato de você não poder configurar muitos recursos no nível do bucket do S3 no nível do prefixo pode dificultar a especificação das configurações corretas para cada conjunto de dados. Além disso, em um bucket multilocatário, a alocação de custos pode se tornar complexa à medida que você trabalha para entender o armazenamento, as solicitações e a transferência de dados associados a prefixos específicos.

Padrão de bucket por uso

Com o padrão de bucket por uso, você cria um bucket de uso geral para cada conjunto de dados, usuário final ou equipe distintos. Como é possível configurar recursos no nível do bucket do S3 para cada um desses buckets, você pode usar esse padrão para definir configurações exclusivas no nível do bucket. Por exemplo, é possível configurar recursos como criptografia de bucket padrão, Versionamento do S3 e Pagamentos a cargo do solicitante do S3 de uma forma personalizada para o conjunto de dados em cada bucket. Usar um bucket para cada conjunto de dados, usuário final ou equipe distintos também pode ajudar a simplificar suas estratégias de gerenciamento de acesso e alocação de custos.

Uma possível desvantagem dessa estratégia é que você possivelmente precisará gerenciar milhares de buckets. Todas as Contas da AWS têm uma cota padrão de 10 mil buckets de uso geral. É possível aumentar a cota de bucket para uma conta enviando uma solicitação de aumento de cota. Para solicitar um aumento de buckets de uso geral, acesse o console do Service Quotas.

Para gerenciar seu padrão de bucket por uso e simplificar o gerenciamento da infraestrutura, você pode usar o AWS CloudFormation. Você pode criar um modelo do AWS CloudFormation personalizado para seu padrão que já defina todas as configurações desejadas para buckets de uso geral do S3. Dessa foram, será seja possível implantar e rastrear facilmente quaisquer alterações na infraestrutura. Consulte mais informações em AWS::S3::Bucket no Guia do usuário do AWS CloudFormation.



Regras de nomenclatura de buckets de uso geral

Ao criar um bucket de uso geral, considere o tamanho, os caracteres válidos, a formatação e a exclusividade dos nomes do bucket. As seções a seguir fornecem informações sobre a nomenclatura de buckets de uso geral, incluindo regras de nomenclatura, práticas recomendadas e um exemplo para criar um bucket de uso geral com um nome que inclui um identificador único universal (GUID).

Para obter informações sobre nomes de chave de objeto, consulte Escolher nomes de chave de objeto.

Para criar um bucket de uso geral, consulte the section called “Criar um bucket de uso geral”.

Tópicos

- Regras de nomenclatura de buckets de uso geral
- Exemplos de nomes de buckets de uso geral
- Práticas recomendadas
- Criar um bucket que usa um GUID no nome

Regras de nomenclatura de buckets de uso geral

As seguintes regras de nomenclatura se aplicam à buckets de uso geral:

- Os nomes dos buckets devem ter entre 3 (mínimo)e 63 (máximo) caracteres.
- Os nomes dos buckets podem consistir apenas em letras minúsculas, números, pontos (`.`) e hifens (`-`).
- Os nomes dos buckets devem começar e terminar com uma letra ou um número.
- O nome do bucket não deve conter pontos adjacentes.
- Os nomes de bucket não devem ser formatados como um endereço IP (por exemplo, `192.168.5.4`).
- O nome do bucket não deve iniciar com o prefixo `xn--`.
- O nome do bucket não deve iniciar com o prefixo `sthree-`.
- O nome do bucket não deve iniciar com o prefixo `amzn-s3-demo-`.
- Os nomes de bucket não podem terminar com o sufixo `-s3alias`. Esse sufixo se reserva a nomes de alias de ponto de acesso. Para obter mais informações, consulte Alias de ponto de acesso.
- Os nomes de bucket não podem terminar com o sufixo `--ol-s3`. Esse sufixo é reservado a nomes de alias de ponto de acesso de objeto do Lambda. Para obter mais informações, consulte Como usar um alias no estilo do bucket para o ponto de acesso do Object Lambda do bucket do S3.
- Os nomes de bucket não podem terminar com o sufixo `.mrap`. Esse sufixo é reservado para nomes de ponto de acesso de várias regiões. Para obter mais informações, consulte Regras para nomear pontos de acesso multirregionais do Amazon S3.
- Os nomes de bucket não podem terminar com o sufixo `--x-s3`. Esse sufixo é reservado para buckets de diretório. Para obter mais informações, consulte Regras de nomenclatura de buckets de diretório.
- Os nomes de bucket não podem terminar com o sufixo `--table-s3`. Esse sufixo é reservado para buckets do serviço Tabelas do S3. Para obter mais informações, consulte Regras de nomenclatura de buckets de tabela, tabelas e namespaces do Amazon S3.
- Os buckets usados com a funcionalidade Aceleração de Transferências do Amazon S3 não podem ter pontos (`.`) nos nomes. Para obter mais informações sobre o Transfer Acceleration, consulte Configurar transferências de arquivos rápidas e seguras usando o Amazon S3 Transfer Acceleration.

Important

- Os nomes de bucket devem ser exclusivos em todas as Contas da AWS e em todas as Regiões da AWS dentro de uma partição. Uma partição é um agrupamento de regiões. No momento, a AWS tem três partições: `aws` (regiões comerciais), `aws-cn` (regiões da China) e `aws-us-gov` (regiões AWS GovCloud (US)).
- Um nome de bucket não pode ser usado por outra Conta da AWS na mesma partição enquanto o bucket não for excluído. Depois que você excluir um bucket, esteja ciente de que outra Conta da AWS na mesma partição poderá usar o mesmo nome de bucket para um novo bucket e, portanto, potencialmente receber solicitações destinadas ao bucket excluído. Para evitar que isso aconteça, ou se quiser continuar a usar o mesmo nome do bucket, não exclua o bucket. Recomendamos que você esvazie o bucket e o mantenha, bloqueando quaisquer solicitações de bucket conforme necessário. Com relação a buckets não usados ativamente, recomendamos esvaziar todos o bucket de todos os objetos para minimizar os custos e, ao mesmo tempo, reter o bucket em si.
- Ao criar um bucket de uso geral, você escolhe seu nome e a Região da AWS onde criá-lo. Depois de criar um bucket de uso geral, não é necessário alterar o nome nem a região.
- Não inclua informações confidenciais no nome do bucket. O nome do bucket é visível nos URLs que apontam para os objetos no bucket.

Note

Antes de 1º de março de 2018, os buckets criados na região Leste dos EUA (Norte da Virgínia) podiam ter nomes com até 255 caracteres e incluíam letras maiúsculas e sublinhados. A partir de 1º de março de 2018, os novos buckets na região Leste dos EUA (Norte da Virgínia) devem estar em conformidade com as mesmas regras aplicadas em todas as outras regiões.

Exemplos de nomes de buckets de uso geral

Os nomes de bucket a seguir mostram exemplos de quais caracteres são permitidos em nomes de bucket de uso geral: a–z, 0–9 e hifens (-). O prefixo reservado `amzn-s3-demo-` é usado aqui somente para fins ilustrativos. Como é um prefixo reservado, não é possível criar nomes de bucket que comecem com `amzn-s3-demo-`.

- `amzn-s3-demo-bucket1-a1b2c3d4-5678-90ab-cdef-example11111`
- `amzn-s3-demo-bucket`

Os exemplos de nomes de bucket a seguir são válidos, mas não recomendados para usos que não sejam hospedagem de sites estáticos porque contêm pontos (`.`):

- `example.com`
- `www.example.com`
- `my.example.s3.bucket`

Os nomes de buckets de exemplo a seguir não são válidos:

- `amzn_s3_demo_bucket` (contém sublinhados)
- `AmznS3DemoBucket` (contém letras maiúsculas)
- `amzn-s3-demo-bucket-` (começa com o prefixo `amzn-s3-demo-` e termina com um hífen)
- `example..com` (contém dois pontos consecutivos)
- `192.168.5.4` (corresponde ao formato de um endereço IP)

Práticas recomendadas

Ao nomear buckets de uso geral, considere as práticas recomendadas de nomenclatura de buckets a seguir.

Escolha um esquema de nomenclatura de bucket que não seja suscetível a causar conflitos de nomenclatura

Se a sua aplicação cria buckets automaticamente, escolha um esquema de nomenclatura de bucket que não seja suscetível a causar conflitos de nomenclatura. Certifique-se de que a lógica do seu aplicativo escolha um nome de bucket diferente, caso um nome de bucket já esteja em uso.

Anexe identificadores únicos universais (GUIDs) aos nomes de bucket

Recomendamos que você crie nomes de bucket que não sejam previsíveis. Não escreva código presumindo que o nome do bucket escolhido esteja disponível, a menos que você já tenha criado o bucket. Um método para criar nomes de bucket que não sejam previsíveis é acrescentar um identificador único universal (GUID) ao nome do bucket, por exemplo, `amzn-s3-demo-bucket-`

`a1b2c3d4-5678-90ab-cdef-example11111`. Para obter mais informações, consulte the section called “Criar um bucket que usa um GUID no nome”.

Evite usar pontos (`.`) em nomes de bucket

Para obter a melhor compatibilidade, recomendamos evitar o uso de pontos (`.`) em nomes de bucket, exceto em buckets usados apenas para hospedagem de sites estáticos. Se você incluir pontos no nome de um bucket, não poderá usar o endereçamento no estilo de host virtual por HTTPS, a menos que execute a própria validação de certificado. Os certificados de segurança usados para hospedagem virtual de buckets não funcionam para buckets com pontos nos nomes.

Essa limitação não afeta os buckets usados para hospedagem de sites estáticos, pois essa hospedagem só está disponível via HTTP. Para obter mais informações sobre o endereçamento no estilo de hospedagem virtual, consulte Hospedagem virtual de buckets de uso geral. Para obter mais informações sobre hospedagem de sites estáticos, consulte Hospedagem de um site estático usando o Amazon S3.

Escolha um nome relevante

Ao nomear um bucket, recomendamos que você escolha um nome que seja relevante para você ou para sua empresa. Evite usar nomes associados a outros. Por exemplo, evite usar `AWS` ou `Amazon` no nome do bucket.

Não exclua buckets com o intuito de reutilizar os nomes de bucket

Se um bucket estiver vazio, você poderá excluí-lo. Depois de excluído, o nome do bucket fica disponível para reutilização. No entanto, não há garantia de que você poderá reutilizar o nome imediatamente ou de forma alguma. Após a exclusão de um bucket, pode levar algum tempo até que você possa reutilizar o nome. Além disso, outra Conta da AWS pode criar um bucket com o mesmo nome antes que você consiga reutilizar o nome.

Depois que você excluir um bucket de uso geral, esteja ciente de que outra Conta da AWS na mesma partição poderá usar o mesmo nome de bucket para um novo bucket e, portanto, possivelmente receber solicitações destinadas ao bucket excluído. Para evitar que isso aconteça, ou se quiser continuar a usar o mesmo nome do bucket de uso geral, não exclua o bucket de uso geral. Recomendamos que você esvazie o bucket e o mantenha, bloqueando quaisquer solicitações de bucket conforme necessário.

Criar um bucket que usa um GUID no nome

Os exemplos a seguir mostram como criar um bucket de uso geral que usa um GUID no final do nome.

Como usar o AWS CLI

O exemplo a seguir da AWS CLI cria um bucket de uso geral na região Oeste dos EUA (N. da Califórnia) (`us-west-1`) com um exemplo de nome de bucket que usa um identificador único universal (GUID). Para usar esse exemplo de comando, substitua os *`user input placeholders`* por suas próprias informações.

```
aws s3api create-bucket \
    --bucket amzn-s3-demo-bucket1$(uuidgen | tr -d - | tr '[:upper:]' '[:lower:]' ) \
    --region us-west-1 \
    --create-bucket-configuration LocationConstraint=us-west-1
```

Usar o AWS SDK para Java

O exemplo a seguir mostra como criar um bucket de uso geral com um GUID no final do nome na região Leste dos EUA (Norte da Virgínia) (`us-east-1`) usando o AWS SDK para Java. Para usar esse exemplo, substitua os *`user input placeholders`* por suas próprias informações. Consulte mais informações sobre outros AWS SDKs em Ferramentas para criar com a AWS.

```
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.Bucket;
import com.amazonaws.services.s3.model.CreateBucketRequest;

import java.util.List;
import java.util.UUID;

public class CreateBucketWithUUID {
    public static void main(String[] args) {
        final AmazonS3 s3 =
 AmazonS3ClientBuilder.standard().withRegion(Regions.US_EAST_1).build();
        String bucketName = "amzn-s3-demo-bucket" +
 UUID.randomUUID().toString().replace("-", "");
        CreateBucketRequest createRequest = new CreateBucketRequest(bucketName);
```

```
        System.out.println(bucketName);
        s3.createBucket(createRequest);
    }
}
```

Cotas, limitações e restrições de buckets de uso geral

Um bucket de uso geral do Amazon S3 pertence à Conta da AWS que o criou. A propriedade do bucket não é transferível para outra conta.

Cotas de bucket

Por padrão, é possível criar até dez mil buckets de uso geral por Conta da AWS. Para solicitar um aumento de cota para buckets de uso geral, acesse o console do Service Quotas.

Important

É altamente recomendável usar somente solicitações `ListBuckets` paginadas. Solicitações `ListBuckets` não paginadas só são aceitas para Contas da AWS definidas com a cota de bucket de uso geral padrão de dez mil. Se você tiver uma cota de bucket de uso geral aprovada acima de dez mil, deverá enviar solicitações `ListBuckets` paginadas para listar os buckets da conta. Todas as solicitações `ListBuckets` não paginadas serão rejeitadas para Contas da AWS com uma cota de bucket de uso geral maior que dez mil.

Note

Você deve usar as Regiões da AWS a seguir para visualizar a cota e a utilização do bucket ou solicitar um aumento dos buckets de uso geral em sua Conta da AWS.

- As cotas de buckets de uso geral para regiões comerciais só podem ser visualizadas e gerenciadas na região Leste dos EUA (N. da Virgínia).
- As cotas de buckets de uso geral para AWS GovCloud (US) só podem ser visualizadas e gerenciadas em AWS GovCloud (Oeste dos EUA).

Consulte informações sobre cotas de serviço em AWS Service Quotas na Referência geral da Amazon Web Services.

Limitações de objetos e buckets

Não há tamanho máximo para o bucket ou limite para o número de objetos que você pode armazenar em um bucket. Você pode armazenar todos os objetos em um único bucket, ou pode organizá-los em vários buckets. No entanto, você não pode criar um bucket de dentro de outro bucket.

Regras de nomeação de bucket

Ao criar um bucket, você escolhe seu nome e a Região da AWS onde criá-lo. Depois de criar um bucket, não é necessário alterar o nome nem a região. Para obter mais informações sobre nomeação de bucket, consulte Regras de nomenclatura de buckets de uso geral.

Acessar um bucket de uso geral do Amazon S3

É possível acessar buckets de uso geral do Amazon S3 usando o console do Amazon S3, a AWS Command Line Interface, os SDKs AWS ou a API REST do Amazon S3. Cada método de acesso a um bucket de uso geral do S3 atende a casos de uso específicos. Para obter mais informações, consulte as seções a seguir.

Tópicos

- Casos de uso
- Console do Amazon S3
- AWS CLI
- SDKs da AWS
- API REST do Amazon S3

Casos de uso

Dependendo do caso de uso do bucket de uso geral do Amazon S3, existem diferentes métodos recomendados para acessar os dados subjacentes nos buckets. A lista a seguir inclui casos de uso comuns para acessar seus dados.

- Sites estáticos — você pode usar o Amazon S3 para hospedar um site estático. Neste caso de uso, você pode configurar o bucket de uso geral do S3 para funcionar como um site. Para obter orientação nas etapas de hospedagem de um site no Amazon S3, consulte Tutorial: configurar um site estático no Amazon S3.

Para hospedar um site estático com configurações de segurança como Bloquear acesso público habilitado, recomendamos usar o Amazon CloudFront com Origin Access Control (OAC) e implementar cabeçalhos de segurança adicionais, como HTTPS. Para obter mais informações, consulte Conceitos básicos de site estático seguro.

> **Note**
>
> O Amazon S3 oferece suporte tanto ao URL de estilo hospedado virtual quanto de estilo de caminho para acesso estático a sites. Como os buckets podem ser acessados usando URLs no estilo de hospedagem virtual e estilo de caminho, recomendamos criar buckets com nomes compatíveis com DNS. Para obter mais informações, consulte Cotas, limitações e restrições de buckets de uso geral.

- Conjuntos de dados compartilhados: à medida que você escala no Amazon S3, é comum adotar um modelo multilocatário, no qual você atribui diferentes clientes finais ou unidades de negócios a prefixos exclusivos em um bucket de uso geral compartilhado. Ao usar os pontos de acesso Amazon S3, você pode dividir uma política de grande bucket em políticas de ponto de acesso separadas e discretas para cada aplicativo que precisa acessar o conjunto de dados compartilhado. Essa abordagem simplifica o foco na criação da política de acesso correta para um aplicativo, sem interromper o que qualquer outro aplicativo está fazendo no conjunto de dados compartilhado. Para obter mais informações, consulte Gerenciar o acesso a conjuntos de dados compartilhados com pontos de acesso.
- Workloads de alto throughput: o Mountpoint para Amazon S3 é um cliente de arquivo de código aberto de alto throughput para montar um bucket de uso geral do Amazon S3 como um sistema de arquivos local. Com o Mountpoint, os aplicativos podem acessar arquivos armazenados no Amazon S3 por meio de operações do sistema de arquivos, como abrir e ler. O Mountpoint traduz automaticamente essas operações em chamadas de API de objetos do S3, dando aos aplicativos acesso ao armazenamento elástico e ao throughput do Amazon S3 por meio de uma interface de arquivo. Para obter mais informações, consulte Montar um bucket do Amazon S3 como um sistema de arquivos local.
- Aplicações multirregionais: os pontos de acesso multirregionais do Amazon S3 fornecem um endpoint global que as aplicações podem usar para atender a solicitações de buckets de uso geral do S3 localizados em várias Regiões da AWS. Você pode usar pontos de acesso multirregionais para criar aplicações de várias regiões com a mesma arquitetura usada em uma única região, depois executar essas aplicações em qualquer lugar do mundo. Em vez de enviar solicitações pela Internet pública, os pontos de acesso multirregionais fornecem resiliência de rede integrada com

aceleração de solicitações baseadas na Internet para o Amazon S3. Para obter mais informações, consulte Gerenciar o tráfego multirregional com Pontos de Acesso Multirregionais.

- Secure Shell (SSH) File Transfer Protocol (SFTP): se estiver tentando transferir dados sensíveis com segurança pela internet, é possível usar um servidor habilitado para SFTP com o bucket de uso geral do Amazon S3. AWS SFTP é um protocolo de rede compatível com toda a funcionalidade de segurança e autenticação do SSH. Com esse protocolo, você tem controle aprimorado sobre a identidade, as permissões e as chaves do usuário ou pode usar políticas do IAM para gerenciar o acesso. Para associar um servidor habilitado para SFTP ao bucket do Amazon S3, crie o servidor habilitado para SFTP. Em seguida, configure contas de usuário e associe o servidor a um bucket de uso geral do Amazon S3. Para obter instruções sobre esse processo, consulte AWS Transfer for SFTP — Serviço SFTP totalmente gerenciado para Amazon S3 em AWS Blogs.

Console do Amazon S3

O console é uma interface de usuário baseada na Web para gerenciar o Amazon S3 e o recursos da AWS. Com o console do Amazon S3, você pode acessar um bucket e modificar as propriedades dele. Você também pode executar a maioria das operações de bucket usando a IU do console, sem precisar escrever nenhum código.

Se você se inscreveu em uma Conta da AWS, poderá acessar o console do Amazon S3 fazendo login no console do Amazon S3 e escolhendo S3 na página inicial do console do Amazon S3. Você também pode usar este link de acesso direto https://console.aws.amazon.com/s3/.

AWS CLI

Você pode usar a AWS CLI a fim de emitir comandos ou criar scripts na linha de comando do sistema para executar tarefas da AWS (incluindo o S3). Por exemplo, caso precise acessar vários buckets, você pode economizar tempo usando a AWS CLI para automatizar tarefas comuns e repetitivas. A capacidade de script e a consistência para ações comuns são considerações frequentes à medida que as organizações crescem.

A AWS CLI fornece comandos para um amplo conjunto de Serviços da AWS. A AWS CLI é compatível com Windows, macOS e Linux. Para começar a usar, consulte o Guia do usuário do AWS Command Line Interface. Para obter mais informações sobre os comandos do Amazon S3, consulte s3api e s3control na Referência de comandos da AWS CLI.

SDKs da AWS

A AWS fornece SDKs (kits de desenvolvimento de software) que consistem em bibliotecas e códigos de exemplo para várias linguagens de programação e plataformas (Java, Python, Ruby, .NET, iOS, Android etc.). Os AWS SDKs constituem uma forma conveniente de criar acesso programático para o S3 e a AWS. O Amazon S3 é um serviço REST. É possível enviar solicitações para o Amazon S3 usando a API REST ou as bibliotecas SDK da AWS, que envolvem a API REST do Amazon S3 e simplificam as tarefas de programação. Por exemplo, os SDKs processam tarefas como calcular assinaturas, assinar solicitações de forma criptográfica, gerenciar erros e novas tentativas automáticas de solicitações. Para obter informações sobre os AWS SDKs, incluindo como baixar e instalá-los, consulte Ferramentas da AWS.

Cada interação com o Amazon S3 é autenticada ou anônima. Se você estiver usando os AWS SDKs, as bibliotecas calcularão a assinatura das chaves fornecidas. Consulte mais informações sobre como fazer solicitações ao Amazon S3 em Making requests.

API REST do Amazon S3

A arquitetura do Amazon S3 foi desenvolvida para ser neutra em termos de linguagem de programação, usando nossas interfaces compatíveis com a AWS para armazenar e recuperar objetos. Você pode acessar o S3 e a AWS de forma programada usando a API REST do Amazon S3. A API REST é uma interface HTTP para o Amazon S3. Usando a API REST, você usa solicitações HTTP padrão para criar, buscar e excluir buckets e objetos.

Você pode usar qualquer toolkit compatível com HTTP para usar a API REST. Você pode até usar um navegador para buscar objetos, desde que eles possam ser lidos anonimamente.

A API REST usa os cabeçalhos padrão e os códigos de status HTTP para que os navegadores e os toolkits padrão funcionem como esperado. Em algumas áreas, adicionamos funcionalidade ao HTTP (por exemplo, adicionamos cabeçalhos para oferecer suporte ao controle de acesso). Nesses casos, fizemos o melhor para adicionar nova funcionalidade de uma forma que correspondesse ao estilo de uso padrão do HTTP.

Se fizer chamadas diretas da API REST na aplicação, você deverá escrever o código para calcular a assinatura e adicioná-la à solicitação. Consulte mais informações sobre como fazer solicitações ao Amazon S3 em Making requests na Referência de API do Amazon S3.

Hospedagem virtual de buckets de uso geral

Hospedagem virtual é a prática de atender vários sites a partir de um único servidor web. Uma maneira de diferenciar sites em suas solicitações de API REST do Amazon S3 é usar o nome de host aparente do URI da solicitação em vez de apenas a parte do nome do caminho do URI. Uma solicitação REST comum do Amazon S3 especifica um bucket usando o primeiro componente delimitado por barra do caminho do URI da solicitação. Em vez disso, você pode usar a hospedagem virtual do Amazon S3 para endereçar um bucket de uso geral em uma chamada de API REST usando o cabeçalho `Host` HTTP. Na prática, o Amazon S3 interpreta `Host` como um aviso de que a maioria dos buckets são acessíveis automaticamente (para tipos limitados de solicitações) em `https://`*`bucket-name`*`.s3.`*`region-code`*`.amazonaws.com`. Para obter uma lista completa de regiões e endpoints do Amazon S3, consulte Endpoints e cotas do Amazon S3 na Referência geral da Amazon Web Services.

Além disso, a hospedagem virtual tem outros benefícios. Ao nomear o bucket com o nome do domínio registrado e ao tornar esse nome um alias do DNS para o Amazon S3, você pode personalizar totalmente o URL dos recursos do Amazon S3, por exemplo, `http://my.`*`bucket-name`*`.com/`. Você também pode publicar no “diretório raiz” do servidor virtual do bucket. Esta habilidade pode ser importante pois muitos aplicativos buscam arquivos nesse local padrão. Por exemplo, `favicon.ico`, `robots.txt` e `crossdomain.xml` serão todos encontrados na raiz.

> **Important**
>
> Ao utilizar buckets de uso geral no estilo de hospedagem virtual com SSL, o certificado SSL curinga corresponde apenas a buckets que não contêm pontos (`.`). Para contornar essa limitação, use HTTP ou escreva sua própria lógica de verificação de certificado. Para obter mais informações, consulte Amazon S3 Path Deprecation Plan (Plano de depreciação de caminhos do Amazon S3) no AWS News Blog.

Tópicos

- Solicitações no estilo de caminho
- Solicitações no estilo de hospedagem virtual
- Especificação de bucket do cabeçalho Host HTTP
- Exemplos
- Personalizar URLs do Amazon S3 com registros CNAME

- Como associar um nome de host a um bucket do Amazon S3
- Limitações
- Compatibilidade retroativa

Solicitações no estilo de caminho

Atualmente, o Amazon S3 é compatível com o acesso a URLs no estilo de hospedagem virtual e no estilo de caminho em todas as Regiões da AWS. No entanto, os URLs no estilo de caminho serão descontinuados no futuro. Para obter mais informações, consulte a observação Importante a seguir.

No Amazon S3, os URLs no estilo de caminho usam o seguinte formato:

```
https://s3.region-code.amazonaws.com/bucket-name/key-name
```

Por exemplo, se você criar um bucket chamado `amzn-s3-demo-bucket1` na região Oeste dos EUA (Oregon) e quiser acessar o objeto `puppy.jpg` nele, use o seguinte URL no estilo de caminho:

```
https://s3.us-west-2.amazonaws.com/amzn-s3-demo-bucket1/puppy.jpg
```

Important

Atualização (23 de setembro de 2020): para garantir que os clientes tenham o tempo necessário para fazer a transição para URLs no estilo de hospedagem virtual, decidimos postergar a desativação de URLs no estilo de caminho. Para obter mais informações, consulte Amazon S3 Path Deprecation Plan – The Rest of the Story no Blog de notícias da AWS.

Warning

Ao hospedar o conteúdo de um site que será acessado de um navegador da web, evite usar URLs no estilo de caminho, que podem interferir no modelo de segurança da mesma origem do navegador. Para hospedar o conteúdo do site, recomendamos que você use os endpoints do site do S3 ou uma distribuição do CloudFront. Para obter mais informações, consulte Endpoints de site e Implantar uma aplicação de página única baseado em reação no Amazon S3 e no CloudFront nos Padrões de orientação de perspectiva da AWS.

Solicitações no estilo de hospedagem virtual

Em um URL de estilo hospedado virtual, o nome do bucket faz parte do nome do domínio no URL.

Os URLs no estilo de hospedagem virtual do Amazon S3 usam o seguinte formato:

```
https://bucket-name.s3.region-code.amazonaws.com/key-name
```

Neste exemplo, `amzn-s3-demo-bucket1` é o nome do bucket, Oeste dos EUA (Oregon) é a região, e `puppy.png` é o nome da chave.

```
https://amzn-s3-demo-bucket1.s3.us-west-2.amazonaws.com/puppy.png
```

Especificação de bucket do cabeçalho **`Host`** HTTP

Desde que a solicitação `GET` não use o endpoint SSL, você pode especificar o bucket para a solicitação usando o cabeçalho `Host` HTTP. O cabeçalho `Host` em uma solicitação REST é interpretado da seguinte forma:

- Se o cabeçalho `Host` estiver omitido ou se o seu valor for `s3.region-code.amazonaws.com`, o bucket para a solicitação será o primeiro componente delimitado por barra no URI da solicitação e a chave da solicitação será o restante do URI. Este é o método comum, conforme ilustrado pelos dois primeiros exemplos desta seção. Omitir o cabeçalho `Host` é válido apenas para solicitações HTTP 1.0.
- Caso contrário, se o valor do cabeçalho `Host` terminar com `.s3.region-code.amazonaws.com`, o nome do bucket será o componente inicial do valor do cabeçalho `Host` até `.s3.region-code.amazonaws.com`. A chave da solicitação será o seu URI. Essa interpretação expõe buckets como subdomínios do `.s3.region-code.amazonaws.com`, conforme ilustrado pelo terceiro e pelo quarto exemplos nesta seção.
- Caso contrário, o bucket da solicitação é o valor em letras minúsculas do cabeçalho `Host`, e a chave da solicitação é o seu URI. Essa interpretação é útil se você tiver registrado o mesmo nome DNS que o nome do bucket e se tiver configurado o nome para ser um alias (CNAME) de nome canônico para o Amazon S3. O procedimento para registrar nomes de domínio e configurar o CNAME DNS está além do escopo deste guia, mas o resultado é ilustrado pelo último exemplo desta seção.

Exemplos

Esta seção fornece exemplos de URLs e solicitações.

Example – URLs no estilo de caminho e solicitações

Este exemplo usa o seguinte:

- Nome do bucke - `example.com`
- Região: Leste dos EUA (Norte da Virgínia)
- Nome da chave: `homepage.html`

O URL é o seguinte:

```
http://s3.us-east-1.amazonaws.com/example.com/homepage.html
```

A solicitação é a seguinte:

```
GET /example.com/homepage.html HTTP/1.1
Host: s3.us-east-1.amazonaws.com
```

A solicitação com HTTP 1.0 e a omissão do cabeçalho `Host` é a seguinte:

```
GET /example.com/homepage.html HTTP/1.0
```

Para obter informações sobre nomes compatíveis do DNS, consulte Limitações. Para obter mais informações sobre chaves, consulte Chaves.

Example – Solicitações e URLs no estilo de hospedagem virtual

Este exemplo usa o seguinte:

- Nome do bucket: `amzn-s3-demo-bucket1`
- Região: Europa (Irlanda)
- Nome da chave: `homepage.html`

O URL é o seguinte:

```
http://amzn-s3-demo-bucket1.s3.eu-west-1.amazonaws.com/homepage.html
```

A solicitação é a seguinte:

```
GET /homepage.html HTTP/1.1
Host: amzn-s3-demo-bucket1.s3.eu-west-1.amazonaws.com
```

Example – método de alias CNAME

Para usar este método, é necessário configurar o nome de DNS como um alias CNAME para *bucket-name*.s3.us-east-1.amazonaws.com. Para obter mais informações, consulte Personalizar URLs do Amazon S3 com registros CNAME.

Este exemplo usa o seguinte:

- Nome do bucke - example.com
- Nome da chave: homepage.html

O URL é o seguinte:

```
http://www.example.com/homepage.html
```

O exemplo é o seguinte:

```
GET /homepage.html HTTP/1.1
Host: www.example.com
```

Personalizar URLs do Amazon S3 com registros CNAME

Dependendo da necessidade, é possível que você não queira que s3.*region-code*.amazonaws.com apareça no site ou serviço. Por exemplo, se você estiver hospedando as imagens do site no Amazon S3, talvez prefira http://images.example.com/ em vez de http://images.example.com.s3.us-east-1.amazonaws.com/. Qualquer bucket com um nome compatível com o DNS pode ser mencionado da seguinte forma: http://*BucketName*.s3.*Region*.amazonaws.com/[*Filename*], por exemplo, http://images.example.com.s3.us-east-1.amazonaws.com/mydog.jpg. Ao usar o CNAME, mapeie images.example.com para um nome de host do Amazon S3, para que o URL anterior se torne http://images.example.com/mydog.jpg.

O nome do bucket deve ser o mesmo que o CNAME. Por exemplo, se você criar um CNAME para mapear `images.example.com` para `images.example.com.s3.us-east-1.amazonaws.com`, `http://images.example.com/filename` e `http://images.example.com.s3.us-east-1.amazonaws.com/filename` serão o mesmo.

O registro DNS do CNAME deve apelidar o nome do domínio para o nome de host apropriado do estilo de hospedagem virtual. Por exemplo, se o nome do bucket e o nome do domínio forem `images.example.com` e o bucket estiver na região Leste dos EUA (Norte da Virgínia), o alias do registro do CNAME deverá ser `images.example.com.s3.us-east-1.amazonaws.com`.

```
images.example.com CNAME    images.example.com.s3.us-east-1.amazonaws.com.
```

O Amazon S3 usa o nome de host para determinar o nome do bucket. O nome do CNAME e o nome do bucket devem ser os mesmos. Por exemplo, suponha que você tenha configurado `www.example.com` como um CNAME para `www.example.com.s3.us-east-1.amazonaws.com`. Quando você acessa `http://www.example.com`, o Amazon S3 recebe uma solicitação semelhante à seguinte:

Example

```
GET / HTTP/1.1
Host: www.example.com
Date: date
Authorization: signatureValue
```

O Amazon S3 vê apenas o nome do host original `www.example.com` e não tem conhecimento do mapeamento CNAME usado para resolver a solicitação.

Você pode usar qualquer endpoint do Amazon S3 em um alias CNAME. Por exemplo, `s3.ap-southeast-1.amazonaws.com` pode ser usado em aliases CNAME. Consulte mais informações sobre endpoints em Request endpoints na Referência de API do Amazon S3. Para criar um site estático usando um domínio personalizado, consulte Tutorial: Configurar um site estático usando um domínio personalizado registrado no Route 53.

> **Important**
>
> Ao usar URLs personalizados com CNAMEs, você precisará garantir que exista um bucket correspondente para qualquer registro CNAME ou alias configurado. Por exemplo,

se você criar entradas DNS para `www.example.com` e `login.example.com` com o objetivo de publicar conteúdo da Web usando o S3, será necessário criar os dois buckets, `www.example.com` e `login.example.com`.
Quando um registro CNAME ou alias é configurado apontando para um endpoint do S3 sem um bucket correspondente, qualquer usuário da AWS pode criar esse intervalo e publicar conteúdo com o alias configurado, mesmo que a propriedade não seja a mesma.
Pelo mesmo motivo, recomendamos que você altere ou remova o CNAME ou o alias correspondente ao excluir um bucket.

Como associar um nome de host a um bucket do Amazon S3

Como associar um nome de host a um bucket do Amazon S3 usando um alias CNAME

1. Selecione um nome de host que pertença a um domínio controlado por você.

   Este exemplo usa o subdomínio `images` do domínio `example.com`.

2. Crie um bucket que corresponda ao nome de host.

   Neste exemplo, os nomes de host e do bucket são `images.example.com`. O nome do bucket deve ser exatamente igual ao nome de host.

3. Crie um registro de DNS CNAME que defina o nome de host como um alias para o bucket do Amazon S3.

   Por exemplo:

   ```
   images.example.com CNAME images.example.com.s3.us-west-2.amazonaws.com
   ```

   > **Important**
   >
   > Por motivos de encaminhamento de solicitações, o registro de DNS CNAME deve estar definido exatamente como mostrado no exemplo anterior. Do contrário, a operação pode parecer correta, mas acabará causando um comportamento imprevisível.

   O procedimento para configurar registros de DNS CNAME depende do servidor DNS ou do provedor DNS. Para obter informações específicas, consulte a documentação do servidor ou entre em contato com o provedor.

Limitações

As APIs SOAP não estão disponíveis para novos clientes e chegam ao fim da vida útil (EOL) em 31 de agosto de 2025. Recomendamos usar a API REST ou os AWS SDKs.

Compatibilidade retroativa

As seções a seguir abordam vários aspectos da compatibilidade com versões anteriores do Amazon S3 relacionados a solicitações de URL no estilo de caminho e no estilo de hospedagem virtual.

Endpoints herdados

Algumas regiões oferecem suporte a endpoints legados. Você poderá ver esses endpoints nos logs de acesso ao servidor ou nos logs do AWS CloudTrail. Para obter mais informações, leia as informações a seguir. Para obter uma lista completa de regiões e endpoints do Amazon S3, consulte Endpoints e cotas do Amazon S3 na Referência geral da Amazon Web Services.

> **Important**
>
> Embora você possa ver endpoints legados nos seus logs, recomendamos que você sempre use a sintaxe do endpoint padrão para acessar os buckets.
> Os URLs no estilo de hospedagem virtual do Amazon S3 usam o seguinte formato:
>
> ```
> https://bucket-name.s3.region-code.amazonaws.com/key-name
> ```
>
> No Amazon S3, os URLs no estilo de caminho usam o seguinte formato:
>
> ```
> https://s3.region-code.amazonaws.com/bucket-name/key-name
> ```

s3-Region

Algumas regiões mais antigas do Amazon S3 são compatíveis com endpoints que contêm um traço (`-`) entre o `s3` e a região (por exemplo, `s3-us-west-2`), em vez de um ponto (por exemplo, `s3.us-west-2`). Se o bucket estiver em uma dessas regiões, você poderá ver o seguinte formato de endpoint nos logs de acesso ao servidor ou nos logs do CloudTrail:

```
https://bucket-name.s3-region-code.amazonaws.com
```

Neste exemplo, o nome do bucket é amzn-s3-demo-bucket1 e a região é Oeste dos EUA (Oregon):

```
https://amzn-s3-demo-bucket1.s3-us-west-2.amazonaws.com
```

Endpoint global herdado

Para algumas regiões, é possível usar o endpoint global herdado para criar solicitações que não explicitam um endpoint específico da região. A seguir, o endpoint global herdado:

```
bucket-name.s3.amazonaws.com
```

Nos logs de acesso ao servidor ou nos logs do CloudTrail, você poderá ver solicitações que usam o endpoint global herdado. Neste exemplo, o nome do bucket é `amzn-s3-demo-bucket1` e o endpoint global herdado é:

```
https://amzn-s3-demo-bucket1.s3.amazonaws.com
```

Solicitações no estilo de hospedagem virtual para Leste dos EUA (N. da Virgínia)

Por padrão, as solicitações feitas com o endpoint global herdado vão para a região Leste dos EUA (N. da Virgínia). Portanto, o endpoint global herdado às vezes é usado no lugar do endpoint regional para o Leste dos EUA (Norte da Virgínia). Se você criar um bucket no Leste dos EUA (Norte da Virgínia) e usar o endpoint global, o Amazon S3 roteará sua solicitação para essa região por padrão.

Solicitações no estilo de hospedagem virtual para outras regiões

O endpoint global herdado também é usado para solicitações no estilo de hospedagem virtual em outras regiões compatíveis. Se você criar um bucket em uma região lançada antes de 20 de março de 2019 e usar o endpoint global herdado, o Amazon S3 atualizará o registro DNS para encaminhar novamente a solicitação ao local correto, o que pode levar algum tempo. Enquanto isso, a regra padrão se aplica e sua solicitação no estilo de hospedagem virtual vai para a região Leste dos EUA (N. da Virgínia). Depois, o Amazon S3 a redireciona com um redirecionamento temporário HTTP 307 à região correta.

Para buckets do S3 em regiões lançadas após 20 de março de 2019, o servidor DNS não encaminha a solicitação diretamente à Região da AWS na qual o bucket reside. Em vez disso, ele retorna um erro de solicitação incorreta HTTP 400. Consulte mais informações em Making requests na Referência da API do Amazon S3.

Solicitações no estilo de caminho

Para a região Leste dos EUA (N. da Virgínia), você pode usar o endpoint global herdado para solicitações no estilo de caminho.

Para todas as outras regiões, a sintaxe de caminho exige usar o endpoint específico da região ao tentar acessar um bucket. Se tentar acessar um bucket com o endpoint global legado ou outro endpoint diferente daquele para a região onde o bucket reside, você receberá um erro de redirecionamento permanente com o código 301 de resposta HTTP e uma mensagem indicando o URI correto para o recurso. Por exemplo, se usar `https://s3.amazonaws.com/`*`bucket-name`* para um bucket criado na região Oeste dos EUA (Oregon), você receberá um erro de redirecionamento permanente HTTP 301.

Criar um bucket de uso geral

Para fazer upload de seus dados no Amazon S3, você deve primeiro criar um bucket de uso geral do Amazon S3 em uma das Regiões da AWS. A Conta da AWS que cria o bucket é a proprietária do bucket. Ao criar um bucket, você deve escolher um nome de bucket e Região. Durante o processo de criação, você pode, opcionalmente, escolher outras opções de gerenciamento de armazenamento para o bucket.

> **Important**
>
> Depois que o bucket é criado, não é possível mais alterar o respectivo nome ou proprietário nem a região. Para obter mais informações sobre nomeação de bucket, consulte the section called “Regras de nomenclatura”.

Por padrão, é possível criar até dez mil buckets de uso geral por Conta da AWS. Para solicitar um aumento de cota para buckets de uso geral, acesse o console do Service Quotas.

Você pode armazenar qualquer número de objetos no bucket. Consulte uma lista de restrições e limitações relacionadas aos buckets de uso geral do Amazon S3 em Cotas, limitações e restrições de buckets de uso geral.

Configurações de bucket de uso geral

Ao criar um bucket de uso geral, é possível usar as seguintes configurações para controlar vários aspectos do comportamento do bucket:

- Propriedade de objetos do S3: é uma configuração em nível de bucket do Amazon S3 que você pode usar para controlar a propriedade de objetos carregados no bucket e para desabilitar ou habilitar listas de controle de acesso (ACLs). Por padrão, a Propriedade de Objetos está definida com a configuração Imposto pelo proprietário do bucket e todas as ACLs estão desabilitadas. Com as ACLs desabilitadas, o proprietário do bucket possui cada objeto no bucket e gerencia o acesso aos dados exclusivamente usando políticas. Para obter mais informações, consulte Controlar a propriedade de objetos e desabilitar ACLs para seu bucket.
- Bloqueio de Objetos do S3: pode ajudar a evitar que os objetos do Amazon S3 sejam excluídos ou substituídos por um período fixo ou indefinidamente. A funcionalidade Bloqueio de Objetos usa um modelo de gravação única e várias leituras (WORM). Você pode usar a funcionalidade Bloqueio de Objetos para ajudar a atender aos requisitos regulamentares que exigem armazenamento WORM ou para adicionar outra camada de proteção contra alterações ou exclusão de objetos. Para obter mais informações, consulte the section called “Bloquear objetos”.

Depois de criar um bucket de uso geral ou ao criar um bucket de uso geral usando o console do Amazon S3, você também pode usar as seguintes configurações para controlar outros aspectos do comportamento do bucket:

- Bloqueio de Acesso Público do S3: esse recurso oferece configurações para pontos de acesso, buckets e contas a fim de ajudar você a gerenciar o acesso público aos recursos do Amazon S3. Por padrão, novos buckets, pontos de acesso e objetos não permitem acesso público. No entanto, os usuários podem modificar políticas de bucket, políticas de ponto de acesso ou permissões de objeto para permitir acesso público. As configurações do Bloqueio de acesso público do S3 substituem essas políticas e permissões, de maneira que seja possível limitar o acesso público a esses recursos. Para obter mais informações, consulte the section called “Bloquear o acesso público”.
- Versionamento do S3: é um meio de manter diversas variantes de um objeto no mesmo bucket. O versionamento pode ser usado para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do . Com o versionamento, você pode se recuperar, facilmente, de ações não intencionais do usuário e de falhas de aplicativo. Por padrão, o versionamento é desabilitado para buckets. Para obter mais informações, consulte the section called “Reter várias versões de objetos”.
- Criptografia padrão: é possível definir o tipo de criptografia padrão para todos os objetos no bucket. A criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3) é o nível básico de configuração de criptografia para cada bucket no Amazon S3. Todos os novos objetos carregados em um bucket do S3 são automaticamente criptografados com SSE-S3 como

nível básico de criptografia. Se quiser usar um tipo diferente de criptografia padrão, você pode especificar a criptografia do lado do servidor com chaves do AWS Key Management Service (AWS KMS) (SSE-KMS), criptografia de camada dupla do lado do servidor com chaves do AWS KMS (DSSE-KMS) ou criptografia do lado do servidor com chaves fornecidas pelo cliente (SSE-C) para criptografar seus dados. Para obter mais informações, consulte Definir o comportamento padrão da criptografia para os buckets do Amazon S3.

É possível usar o console do Amazon S3, a API REST do Amazon S3, a AWS Command Line Interface (AWS CLI) ou os SDKs da AWS para criar um bucket de uso geral. Para ter mais informações sobre as permissões necessárias para criar um bucket de uso geral, consulte CreateBucket na Referência de API do Amazon Simple Storage Service.

Se você estiver tendo problemas para criar um bucket do Amazon S3, consulte Como soluciono problemas quando tento criar um bucket do Amazon S3? no AWS re:Post.

Usar o console do S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Na barra de navegação na parte superior da página, escolha o nome da Região da AWS exibida no momento. Em seguida, escolha a região na qual você deseja criar um bucket.

   > **Note**
   >
   > - Depois de criar um bucket, você não pode mudar sua região.
   > - Para reduzir a latência e os custos e atender aos requisitos regulatórios, selecione uma região perto de você. Os objetos armazenados em uma região nunca saem dessa região, a menos que você os transfira para outra região. Para obter uma lista de Regiões da AWS do Amazon S3, consulte Endpoints de AWS service (Serviço da AWS) no Referência geral da Amazon Web Services.

3. No painel de navegação à esquerda, escolha Buckets de uso geral.
4. Selecione Create bucket (Criar bucket). A página Create bucket (Criar bucket) é aberta.
5. Para Nome do bucket, insira um nome para o bucket.

   O nome do bucket deve:

- Ser exclusivo em uma partição. Uma partição é um agrupamento de regiões. No momento, a AWS tem três partições: `aws` (regiões comerciais), `aws-cn` (regiões da China) e `aws-us-gov` (AWS GovCloud (US) Regions).
- Ter entre 3 e 63 caracteres.
- Consistir em apenas letras minúsculas, números, pontos (`.`) e hifens (`-`). Para obter a melhor compatibilidade, recomendamos evitar o uso de pontos (`.`) em nomes de bucket, exceto em buckets usados apenas para hospedagem de sites estáticos.
- Inicie e termine com uma letra ou um número.
- Para obter uma lista completa de regras de nomenclatura de buckets, consulte Regras de nomenclatura de buckets de uso geral.

> **Important**
>
> - Depois de criado o bucket, você não pode mudar seu nome.
> - Não inclua informações confidenciais no nome do bucket. O nome do bucket é visível nos URLs que apontam para os objetos no bucket.

6. (Opcional) Em Configuração geral, você pode optar por copiar as configurações de um bucket existente para seu novo bucket. Prossiga·para·a·próxima·etapa·se você não quiser copiar as configurações de um bucket existente.

> **Note**
>
> Essa opção:
>
> - Não está disponível na AWS CLI, mas apenas no console do Amazon S3.
> - Não copia a política de bucket existente para o novo bucket.

Para copiar as configurações de um bucket existente, em Copiar configurações do bucket existente, selecione Escolher bucket. A janela Escolher bucket é aberta. Encontre o bucket com as configurações que você quer copiar e selecione Escolher bucket. A janela Escolher bucket é fechada e a janela Criar bucket é reaberta.

Agora, em Copiar configurações do bucket existente, você vê o nome do bucket selecionado. As configurações do novo bucket agora correspondem às configurações do bucket que você selecionou. Se você quiser remover as configurações copiadas, escolha Restaurar padrões. Revise as configurações restantes do bucket na página Criar bucket. Se não quiser fazer nenhuma alteração, você poderá pular para a etapa final.

7. Em Object Ownership, para desabilitar ou habilitar ACLs e controlar a propriedade de objetos carregados em seu bucket, escolha uma das seguintes configurações:

   ACLs desabilitadas

   - Imposto pelo proprietário do bucket (padrão): as ACLs são desabilitadas e o proprietário do bucket automaticamente tem propriedade e controle total sobre todos os objetos do bucket de uso geral. As ACLs não afetam mais as permissões de acesso aos dados no bucket de uso geral do S3. O bucket usa políticas exclusivamente para definir o controle de acesso.

     Por padrão, as ACLs estão desabilitadas. A maioria dos casos de uso modernos no Amazon S3 não exige mais o uso de ACLs. Recomendamos manter as ACLs desabilitadas, exceto em circunstâncias incomuns em que seja necessário controlar o acesso para cada objeto individualmente. Para obter mais informações, consulte Controlar a propriedade de objetos e desabilitar ACLs para seu bucket.

   ACLs habilitadas

   - Bucket owner preferred (Preferencial do proprietário do bucket): o proprietário do bucket tem a propriedade e o controle total sobre novos objetos que outras contas gravam no bucket com a ACL `bucket-owner-full-control` pré-configurada.

     Se você aplicar a configuração Proprietário do bucket preferido para exigir que todos os uploads do Amazon S3 incluam a ACL `bucket-owner-full-control` pré-configurada, será possível adicionar uma política de bucket que só permita uploads de objetos que usem essa ACL.

   - Object writer (Gravador de objetos): a Conta da AWS que carrega um objeto é a proprietária do objeto, tem controle total sobre ele e pode conceder acesso a outros usuários por meio de ACLs.

> **Note**
>
> A configuração padrão é Imposto pelo proprietário do Bucket. Para aplicar a configuração padrão e manter as ACLs desabilitadas, somente a permissão `s3:CreateBucket` é necessária. Para habilitar ACLs, é necessário ter a permissão `s3:PutBucketOwnershipControls`.

8. Em Configurações de bloqueio de acesso público para este bucket, selecione as configurações de bloqueio de acesso público que deseja aplicar ao bucket.

   Por padrão, todas as quatro configurações do Bloqueio de Acesso Público são habilitadas. Recomendamos que você mantenha todas as configurações habilitadas, a menos que precise desativar uma ou mais delas para seu caso de uso específico. Para obter mais informações sobre como bloquear o acesso público, consulte Bloquear o acesso público ao armazenamento do Amazon S3.

   > **Note**
   >
   > Para habilitar todas as configurações do Bloqueio de Acesso Público, somente a permissão `s3:CreateBucket` é necessária. Para desabilitar qualquer configuração do Bloqueio de Acesso Público, é necessário ter a permissão `s3:PutBucketPublicAccessBlock`.

9. (Opcional) Por padrão, Versionamento de bucket está desabilitado. Versionamento é um meio de manter diversas variantes de um objeto no mesmo bucket. O versionamento pode ser usado para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do . Com o versionamento, você pode se recuperar mais facilmente de ações não intencionais do usuário e de falhas da aplicação. Para obter mais informações sobre versionamento, consulte Reter várias versões de objetos com o Versionamento do S3.

   Para habilitar o versionamento no bucket, escolha Habilitar.

10. (Opcional) Em Tags (Etiquetas), você pode optar por adicionar etiquetas ao seu bucket. Com a alocação de custos da AWS, você pode usar tags de bucket para anotar o faturamento referente ao uso de um bucket. Uma tag é um par chave-valor que representa uma etiqueta que você atribui a um bucket. Para obter mais informações, consulte the section called “Usar tags de alocação de custos”.

Para adicionar uma etiqueta, escolha Add Tag (Adicionar etiqueta) e insira uma chave e um valor para cada etiqueta.

11. Para configurar Criptografia padrão, em Tipo de criptografia, selecione uma das seguintes opções:

    - Criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3)
    - Criptografia no lado do servidor com chaves do AWS Key Management Service (SSE-KMS)
    - Criptografia de camada dupla do lado do servidor com chaves do AWS Key Management Service (AWS KMS) (DSSE-KMS)

    > **Important**
    >
    > Se você usar a opção SSE-KMS ou a DSSE-KMS em sua configuração de criptografia padrão, poderão ser cobradas cotas de solicitações por segundo (RPS) do AWS KMS. Para obter mais informações sobre as cotas do AWS KMS e como solicitar um aumento de cota, consulte Cotas no Guia do desenvolvedor do AWS Key Management Service.

    Buckets e novos objetos são criptografados por meio da criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3) como o nível básico da configuração de criptografia. Para obter mais informações sobre criptografia padrão, consulte Definir o comportamento padrão da criptografia para os buckets do Amazon S3. Para ter mais informações sobre SSE-S3, consulte Usar a criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3).

    Para obter mais informações sobre como usar a criptografia no lado do servidor para criptografar seus dados, consulte the section called “Criptografia de dados”.

12. Se você escolheu Criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3) ou Criptografia de camada dupla do lado do servidor com chaves do AWS Key Management Service (AWS KMS) (DSSE-KMS), faça o seguinte:

    a. Em Chave do AWS KMS, especifique sua chave do KMS de uma das seguintes maneiras:

        - Para escolher entre uma lista de chaves do KMS disponíveis, selecione Escolher entre suas AWS KMS keys e escolha sua chave do KMS na lista de chaves disponíveis.

As chaves Chave gerenciada pela AWS (`aws/s3`) e as chaves gerenciadas pelo cliente são exibidas nessa lista. Para ter mais informações sobre chaves gerenciadas pelo cliente, consulte Chaves de clientes e chaves da AWS no Guia do desenvolvedor do AWS Key Management Service.

- Para inserir o ARN da chave do KMS, escolha Inserir ARN da AWS KMS key e insira o ARN da chave do KMS no campo exibido.
- Para criar uma chave gerenciada pelo cliente no console do AWS KMS, selecione Criar uma chave do KMS.

  Para ter mais informações sobre como criar uma AWS KMS key, consulte Criação de chaves no Guia do desenvolvedor do AWS Key Management Service.

> **Important**
>
> Você só pode usar chaves do KMS disponíveis na mesma Região da AWS que o bucket. O console do Amazon S3 lista somente as primeiras 100 chaves do KMS na mesma região que o bucket. Para usar uma chave do KMS que não esteja listada, você deve inserir o respectivo ARN. Se quiser usar uma chave do KMS pertencente a outra conta, primeiro você deverá ter permissão para usar a chave e, depois, inserir o respectivo ARN. Para obter mais informações sobre permissões entre contas referentes a chaves do KMS, consulte Creating KMS keys that other accounts can use no Guia do desenvolvedor do AWS Key Management Service. Para obter mais informações sobre SSE-KMS, consulte Especificando criptografia no lado do servidor com o AWS KMS (SSE-KMS). Para ter mais informações sobre DSSE-KMS, consulte the section called “Criptografia de camada dupla do lado do servidor (DSSE-KMS)”.
>
> Ao usar uma AWS KMS key para criptografia no lado do servidor no Amazon S3, você deve escolher uma chave de criptografia do KMS simétrica. O Amazon S3 só é compatível com chaves do KMS de criptografia simétrica, e não com chaves assimétricas do KMS. Para ter mais informações, consulte Identificar chaves do KMS simétricas e assimétricas no Guia do desenvolvedor do AWS Key Management Service.

b. Ao configurar o bucket para usar a criptografia padrão com SSE-KMS, você também pode usar as chaves de bucket do S3. As chaves de bucket do S3 diminuem o custo de criptografia reduzindo o tráfego de solicitações do Amazon S3 para o AWS KMS. Para

obter mais informações, consulte Redução do custo do SSE-KMS com chaves de bucket do Amazon S3. As chaves de bucket do S3 não comportam DSSE-KMS.

Por padrão, as chaves de bucket do S3 estão habilitadas no console do Amazon S3. Recomendamos deixá-las habilitadas para reduzir os custos. Para desabilitar as chaves de bucket do S3 do seu bucket, em Chave de bucket, escolha Desabilitar.

13. (Opcional) O Bloqueio de Objetos do S3 ajuda a proteger novos objetos contra exclusão ou substituição. Para obter mais informações, consulte Bloquear objetos com o Bloqueio de Objetos. Se você quiser habilitar o Bloqueio de Objetos do S3, faça o seguinte:

    a. Selecione Advanced settings (Configurações avançadas).

    > **Important**
    >
    > A habilitação do Bloqueio de Objetos habilita automaticamente o versionamento do bucket. Depois de habilitar e criar o bucket com sucesso, você também deverá definir as configurações de retenção padrão e de retenção jurídica do Bloqueio de Objetos na guia Propriedades do bucket.

    b. Se quiser habilitar o bloqueio de objetos, escolha Enable (Habilitar), leia o aviso que aparece e confirme-o.

    > **Note**
    >
    > Para criar um bucket com o Bloqueio de Objetos habilitado, você deve ter as seguintes permissões: `s3:CreateBucket`, `s3:PutBucketVersioning` e `s3:PutBucketObjectLockConfiguration`.

14. Escolha Criar bucket.

Uso dos SDKs da AWS

Ao usar os SDKs da AWS para criar um bucket de uso geral, você deve criar um cliente e então usá-lo para enviar uma solicitação para criar um bucket. Como prática recomendada, crie o cliente e o bucket na mesma Região da AWS. Se você não especificar uma região ao criar um cliente ou um bucket, o Amazon S3 usará a região padrão Leste dos EUA (Norte da Virgínia).

Se você quiser restringir a criação do bucket a determinada Região da AWS, use a chave de condição LocationConstraint.

Para criar um cliente a fim de acessar um endpoint de pilha dupla, é necessário especificar uma Região da AWS. Consulte mais informações em Using Amazon S3 dual-stack endpoints na Referência de API do Amazon S3. Para obter uma lista de Regiões da AWS disponíveis, consulte Amazon Simple Storage Service endpoints and quotas na Referência geral da AWS.

Ao criar um cliente, a região mapeia para o endpoint específico da região. O cliente usa esse endpoint para se comunicar com o Amazon S3: `s3.region.amazonaws.com`. Se a sua região foi lançada após 20 de março de 2019,, seu cliente e bucket devem estar na mesma região. No entanto, é possível usar um cliente na região Leste dos EUA (Norte da Virgínia) para criar um bucket em qualquer região iniciada antes de 20 de março de 2019. Para obter mais informações, consulte Endpoints herdados.

Os exemplos de código do AWS SDK executam as seguintes tarefas:

- Crie um cliente especificando explicitamente uma região da Região da AWS: no exemplo, o cliente usa o endpoint `s3.us-west-2.amazonaws.com` para se comunicar com o Amazon S3. É possível especificar qualquer Região da AWS. Para obter uma lista de Regiões da AWS, consulte Regiões e endpoints na Referência geral da AWS.
- Envie uma solicitação de bucket de criação especificando apenas um nome de bucket: o cliente envia uma solicitação ao Amazon S3 para criar o bucket na região onde você criou um cliente.
- Recupere as informações sobre a localização do bucket: o Amazon S3 armazena as informações de localização do bucket no sub-recurso location que está associado ao bucket.

Para obter exemplos adicionais de SDK da AWS e exemplos em outras linguagens, consulte Use CreateBucket with an AWS SDK or CLI na Referência de API do Amazon Simple Storage Service.

Java

Example Criar um bucket que use um identificador único universal (GUID) no nome

O exemplo a seguir mostra como criar um bucket de uso geral com um GUID no final do nome na região Leste dos EUA (Norte da Virgínia) (`us-east-1`) usando o AWS SDK para Java. Para usar esse exemplo, substitua os *`user input placeholders`* por suas próprias informações. Consulte mais informações sobre outros AWS SDKs em Ferramentas para criar com a AWS.

```
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.Bucket;
import com.amazonaws.services.s3.model.CreateBucketRequest;

import java.util.List;
import java.util.UUID;

public class CreateBucketWithUUID {
    public static void main(String[] args) {
        final AmazonS3 s3 =
 AmazonS3ClientBuilder.standard().withRegion(Regions.US_EAST_1).build();
        String bucketName = "amzn-s3-demo-bucket" +
 UUID.randomUUID().toString().replace("-", "");
        CreateBucketRequest createRequest = new CreateBucketRequest(bucketName);
        System.out.println(bucketName);
        s3.createBucket(createRequest);
    }
}
```

Example Criar um bucket de uso geral

Este exemplo mostra como criar um bucket do Amazon S3 usando o AWS SDK para Java. Consulte instruções sobre como criar e testar uma amostra funcional no Guia do desenvolvedor do AWS SDK for Java 2.x.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.CreateBucketRequest;
import com.amazonaws.services.s3.model.GetBucketLocationRequest;

import java.io.IOException;

public class CreateBucket2 {

    public static void main(String[] args) throws IOException {
        Regions clientRegion = Regions.DEFAULT_REGION;
```

```
        String bucketName = "*** Bucket name ***";

        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(clientRegion)
                    .build();

            if (!s3Client.doesBucketExistV2(bucketName)) {
                // Because the CreateBucketRequest object doesn't specify a region,
 the
                // bucket is created in the region specified in the client.
                s3Client.createBucket(new CreateBucketRequest(bucketName));

                // Verify that the bucket was created by retrieving it and checking
 its
                // location.
                String bucketLocation = s3Client.getBucketLocation(new
 GetBucketLocationRequest(bucketName));
                System.out.println("Bucket location: " + bucketLocation);
            }
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

.NET

Consulte informações sobre como criar e testar uma amostra funcional em AWS SDK for .NET Version 3 API Reference.

Example

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
```

```
using Amazon.S3.Util;
using System;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class CreateBucketTest
    {
        private const string bucketName = "*** bucket name ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 s3Client;
        public static void Main()
        {
            s3Client = new AmazonS3Client(bucketRegion);
            CreateBucketAsync().Wait();
        }

        static async Task CreateBucketAsync()
        {
            try
            {
                if (!(await AmazonS3Util.DoesS3BucketExistAsync(s3Client,
 bucketName)))
                {
                    var putBucketRequest = new PutBucketRequest
                    {
                        BucketName = bucketName,
                        UseClientRegion = true
                    };

                    PutBucketResponse putBucketResponse = await
 s3Client.PutBucketAsync(putBucketRequest);
                }
                // Retrieve the bucket location.
                string bucketLocation = await FindBucketLocationAsync(s3Client);
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered on server. Message:'{0}' when
 writing an object", e.Message);
            }
            catch (Exception e)
```

```
            {
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
 writing an object", e.Message);
            }
        }
        static async Task<string> FindBucketLocationAsync(IAmazonS3 client)
        {
            string bucketLocation;
            var request = new GetBucketLocationRequest()
            {
                BucketName = bucketName
            };
            GetBucketLocationResponse response = await
 client.GetBucketLocationAsync(request);
            bucketLocation = response.Location.ToString();
            return bucketLocation;
        }
    }
}
```

Ruby

Consulte informações sobre como criar e testar uma amostra funcional em AWS SDK for Ruby - Version 3.

Example

```
require 'aws-sdk-s3'

# Wraps Amazon S3 bucket actions.
class BucketCreateWrapper
  attr_reader :bucket

  # @param bucket [Aws::S3::Bucket] An Amazon S3 bucket initialized with a name.
 This is a client-side object until
  #                                 create is called.
  def initialize(bucket)
    @bucket = bucket
  end

  # Creates an Amazon S3 bucket in the specified AWS Region.
  #
  # @param region [String] The Region where the bucket is created.
```

```
  # @return [Boolean] True when the bucket is created; otherwise, false.
  def create?(region)
    @bucket.create(create_bucket_configuration: { location_constraint: region })
    true
  rescue Aws::Errors::ServiceError => e
    puts "Couldn't create bucket. Here's why: #{e.message}"
    false
  end

  # Gets the Region where the bucket is located.
  #
  # @return [String] The location of the bucket.
  def location
    if @bucket.nil?
      'None. You must create a bucket before you can get its location!'
    else
      @bucket.client.get_bucket_location(bucket: @bucket.name).location_constraint
    end
  rescue Aws::Errors::ServiceError => e
    "Couldn't get the location of #{@bucket.name}. Here's why: #{e.message}"
  end
end

# Example usage:
def run_demo
  region = "us-west-2"
  wrapper = BucketCreateWrapper.new(Aws::S3::Bucket.new("amzn-s3-demo-bucket-
#{Random.uuid}"))
  return unless wrapper.create?(region)

  puts "Created bucket #{wrapper.bucket.name}."
  puts "Your bucket's region is: #{wrapper.location}"
end

run_demo if $PROGRAM_NAME == __FILE__
```

Como usar o AWS CLI

O exemplo a seguir da AWS CLI cria um bucket de uso geral na região Oeste dos EUA (N. da Califórnia) (`us-west-1`) com um exemplo de nome de bucket que usa um identificador único universal (GUID). Para usar esse exemplo de comando, substitua os *`user input placeholders`* por suas próprias informações.

```
aws s3api create-bucket \
    --bucket amzn-s3-demo-bucket1$(uuidgen | tr -d - | tr '[:upper:]' '[:lower:]' ) \
    --region us-west-1 \
    --create-bucket-configuration LocationConstraint=us-west-1
```

Para obter mais informações e exemplos adicionais, consulte create-bucket na Referência de comandos da AWS CLI.

Visualizar das propriedades de um bucket de uso geral do S3

É possível visualizar propriedades de qualquer bucket do Amazon S3 que você possua. Essas configurações incluem o seguinte:

- Versionamento de bucket: mantenha várias versões de um objeto em um bucket de uso geral usando o versionamento. Por padrão, o versionamento é desabilitado para um novo bucket. Para obter informações sobre como ativar o versionamento, consulte Habilitar o versionamento em buckets.
- Tags: com a alocação de custos da AWS, você pode usar tags de bucket para anotar o faturamento de uso de um bucket de uso geral. Uma tag é um par chave-valor que representa uma etiqueta que você atribui a um bucket. Para obter mais informações, consulte Usar tags de alocação de custos para buckets do S3.
- Default encryption (Criptografia padrão) — a ativação da criptografia padrão fornece criptografia automática no lado do servidor. O Amazon S3 criptografa um objeto antes de salvá-lo em um disco e descriptografa o objeto ao baixá-lo. Para obter mais informações, consulte Definir o comportamento padrão da criptografia para os buckets do Amazon S3.
- Registro em log de acesso ao servidor: obtenha registros detalhados das solicitações feitas ao bucket de uso geral com registro em log de acesso ao servidor. Por padrão, o Amazon S3 não coleta logs de acesso ao servidor. Para obter informações sobre como habilitar o registro em log de acesso ao servidor, consulte Habilitar o log de acesso ao servidor do Amazon S3.
- Eventos de dados do AWS CloudTrail: use o CloudTrail para registrar eventos de dados. Por padrão, as trilhas não registram eventos de dados. Há cobranças adicionais para eventos de dados. Para obter mais informações, consulte Registro eventos de dados em logs para trilhas no Manual do usuário do AWS CloudTrail.
- Notificações de evento: habilite determinados eventos de bucket de uso geral do Amazon S3 para enviar mensagens de notificação a um destino sempre que ocorrer eventos. Para obter mais

informações, consulte Habilitar e configurar notificações de eventos usando o console do Amazon S3.

- Transfer Acceleration — possibilita transferências de arquivos rápidas, fáceis e seguras entre seu cliente e um bucket do S3 em longas distâncias. Para obter informações sobre como habilitar o Transfer Acceleration, consulte Habilitar e usar o S3 Transfer Acceleration.
- Object Lock (Bloqueio de objetos) — use o bloqueio de objetos do S3 para evitar que um objeto seja excluído ou substituído por um período fixo ou indefinidamente. Para obter mais informações, consulte Bloquear objetos com o Bloqueio de Objetos.
- Pagamento pelo solicitante: habilite essa opção para que o solicitante (em vez do proprietário do bucket de uso geral) pague por solicitações e transferências de dados. Para obter mais informações, consulte Utilizar buckets de uso geral com pagamento pelo solicitante para transferência e uso de armazenamento.
- Static website hosting – você pode hospedar um site estático no Amazon S3. Para obter mais informações, consulte Hospedagem de um site estático usando o Amazon S3.

É possível visualizar as propriedades do bucket usando o AWS Management Console, a AWS CLI ou AWS SDKs

Usar o console do S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets de uso geral ou Buckets de diretórios.
3. Na lista de buckets, escolha o nome do bucket cujas propriedades deseja visualizar.
4. Escolha a guia Properties (Propriedades).
5. Na página Propriedades, você pode configurar as propriedades acima para o bucket.

Como usar o AWS CLI

Visualizar as propriedades do bucket com a AWS CLI

Os comandos a seguir mostram como você pode usar a AWS CLI para listar diferentes propriedades de bucket de uso geral.

A resposta a seguir exibe o conjunto de tags associadas ao bucket *amzn-s3-demo-bucket1*. Para obter mais informações sobre as etiquetas de buckets, consulte Usar tags de alocação de custos para buckets do S3.

```
aws s3api get-bucket-tagging --bucket amzn-s3-demo-bucket1
```

Para obter mais informações e exemplos, consulte get-bucket-tagging na Referência de comandos da AWS CLI.

A resposta a seguir exibe o estado de versionamento do bucket *amzn-s3-demo-bucket1*. Para obter informações sobre o versionamento de buckets, consulte Reter várias versões de objetos com o Versionamento do S3.

```
aws s3api get-bucket-versioning --bucket amzn-s3-demo-bucket1
```

Para obter mais informações e exemplos, consulte get-bucket-versioning na Referência de comandos da AWS CLI.

A resposta a seguir exibe a configuração de criptografia padrão para o bucket *amzn-s3-demo-bucket1*. Por padrão, todos os buckets têm uma configuração de criptografia padrão que usa criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3). Para obter informações sobre a criptografia padrão de buckets, consulte Definir o comportamento padrão da criptografia para os buckets do Amazon S3.

```
aws s3api get-bucket-encryption --bucket amzn-s3-demo-bucket1
```

Para obter mais informações e exemplos, consulte get-bucket-encryption na Referência de comandos da AWS CLI.

A resposta a seguir exibe a configuração de notificação do bucket *amzn-s3-demo-bucket1*. Para obter informações sobre notificações de eventos de buckets, consulte Notificações de eventos do Amazon S3.

```
aws s3api get-bucket-notification-configuration --bucket amzn-s3-demo-bucket1
```

Para obter mais informações e exemplos, consulte get-bucket-notification-configuration na Referência de comandos da AWS CLI.

A resposta a seguir exibe o status de registro em log do bucket *amzn-s3-demo-bucket1*. Para obter informações sobre o registro em log do bucket, consulte Registrar em log as solicitações com registro em log de acesso ao servidor.

```
aws s3api get-bucket-logging --bucket amzn-s3-demo-bucket1
```

Para obter mais informações e exemplos, consulte get-bucket-logging na Referência de comandos da AWS CLI.

Uso dos SDKs da AWS

Consulte exemplos de como retornar propriedades de bucket de uso geral com os SDKs da AWS, como versionamento, tags e muito mais, em Code examples na Referência de API do Amazon S3.

Consulte informações gerais sobre como usar diferentes SDKs da AWS em Developing with Amazon S3 using the AWS SDKs na Referência de API do Amazon S3.

Listar buckets de uso geral do Amazon S3

Para retornar uma lista de buckets de uso geral que você possui, é possível usar ListBuckets. Você pode listar buckets usando o console do Amazon S3, a AWS Command Line Interface ou os AWS SDKs. Para solicitações `ListBuckets` que usam a AWS CLI, os AWS SDKs e a API REST do Amazon S3, as Contas da AWS que usam a cota de serviço padrão para buckets (dez mil buckets) permitem solicitações paginadas e não paginadas. Independentemente de quantos buckets existam na conta, você pode criar tamanhos de página entre um e dez mil buckets para listar todos os seus buckets. Para solicitações paginadas, as solicitações `ListBuckets` retornam os nomes dos buckets e as Regiões da AWS correspondentes de cada bucket. Os exemplos da AWS Command Line Interface e do AWS SDK a seguir mostram como usar a paginação em sua solicitação `ListBuckets`. Observe que alguns AWS SDKs ajudam na paginação.

Permissões

Para listar todos os buckets de uso geral, você precisa ter a permissão `s3:ListAllMyBuckets`. Caso encontre um erro `HTTP Access Denied (403 Forbidden)`, consulte Solucionar erros de acesso negado (403 Forbidden) no Amazon S3.

> **Important**
>
> É altamente recomendável usar somente de solicitações `ListBuckets` paginadas. Solicitações `ListBuckets` não paginadas só são aceitas para Contas da AWS definidas

com a cota de bucket de uso geral padrão de dez mil. Se você tiver uma cota de bucket de uso geral aprovada acima de dez mil, deverá enviar solicitações `ListBuckets` paginadas para listar os buckets da conta. Todas as solicitações `ListBuckets` não paginadas serão rejeitadas para Contas da AWS com uma cota de bucket de uso geral maior que dez mil.

Usar o console do S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets de uso geral.
3. Na guia Buckets de uso geral, você pode ver uma lista dos buckets de uso geral.
4. Para encontrar buckets por nome, insira um nome de bucket no campo Localizar buckets por nome.

Como usar o AWS CLI

Para usar a AWS CLI a fim de gerar uma lista de buckets de uso geral, você pode usar os comandos `ls` ou `list-buckets`. Os exemplos a seguir mostram como criar uma solicitação `list-buckets` paginada e uma solicitação `ls` não paginada. Para usar esses exemplos, substitua os *espaços reservados de entrada do usuário*.

Example – Listar todos os buckets em sua conta usando **`ls`** (não paginado)

O comando de exemplo a seguir mostra todos os buckets de uso geral em sua conta em uma única chamada não paginada. Essa chamada retorna uma lista de todos os buckets em sua conta (até dez mil resultados):

```
$ aws s3 ls
```

Para obter mais informações e exemplos, consulte Listar buckets e objetos.

Example – Listar todos os buckets em sua conta usando **`ls`** (paginado)

O comando de exemplo a seguir faz uma ou mais chamadas paginadas para listar todos os buckets de uso geral em sua conta, retornando cem buckets por página:

```
$ aws s3 ls --page-size 100
```

Para obter mais informações e exemplos, consulte Listar buckets e objetos.

Example – Listar todos os buckets em sua conta (paginado)

O exemplo a seguir fornece um comando `list-buckets` paginado para listar todos os buckets de uso geral em sua conta. As opções `--max-items` e `--page-size` limitam o número de buckets listados a cem por página.

```
$ aws s3api list-buckets /
    --max-items 100 /
    --page-size 100
```

Se o número de saída de itens (`--max-items`) for menor do que o número total de itens retornados pelas chamadas de API subjacentes, a saída incluirá um token de continuação, especificado pelo argumento `starting-token` que pode ser passado para um comando subsequente a fim de recuperar o próximo conjunto de itens. O exemplo a seguir mostra como usar o valor `starting-token` retornado pelo exemplo anterior. Você pode especificar o `starting-code` para recuperar os próximos cem buckets.

```
$ aws s3api list-buckets /
    --max-items 100 /
    --page-size 100 /
    --starting-token eyJNYXJrZXIiOiBudWxsLCAiYm90b190cnVuY2F0ZV9hbW91bnQiOiAxfQ==
```

Example – Listar todos os buckets em uma Região da AWS (paginado)

O exemplo de comando a seguir usa o parâmetro `--bucket-region` para listar até cem buckets em uma conta que está na região `us-east-2`. Solicitações feitas para um endpoint regional diferente do valor especificado no parâmetro `--bucket-region` não são permitidas. Por exemplo, se quiser limitar a resposta aos buckets em `us-east-2`, você deverá fazer a solicitação a um endpoint em `us-east-2`.

```
$ aws s3api list-buckets /
    --region us-east-2 /
    --max-items 100 /
    --page-size 100 /
```

```
    --bucket-region us-east-2
```

Example – Listar todos os buckets que começam com um prefixo de nome de bucket específico (paginado)

O exemplo de comando a seguir lista até cem buckets que têm um nome que começa com o prefixo *amzn-s3-demo-bucket*.

```
$ aws s3api list-buckets /
    --max-items 100 /
    --page-size 100 /
    --prefix amzn-s3-demo-bucket
```

Uso dos SDKs da AWS

Os exemplos a seguir mostram como listar buckets de uso geral usando os AWS SDKs

SDK for Python

Example – Solicitação ListBuckets (paginado)

```
import boto3

s3 = boto3.client('s3')
response = s3.list_buckets(MaxBuckets=100)
```

Example – Resposta a ListBuckets (paginado)

```
import boto3

s3 = boto3.client('s3')
response =
 s3.list_buckets(MaxBuckets=1,ContinuationToken="eyJNYXJrZXIiOiBudWxsLCAiYm90b190cnVuY2F0ZVV
```

SDK for Java

```
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.Bucket;
```

```
import com.amazonaws.services.s3.model.ListBucketsPaginatedRequest;
import com.amazonaws.services.s3.model.ListBucketsPaginatedResult;

import java.util.List;

public class ListBuckets {
    public static void main(String[] args) {
        final AmazonS3 s3 =
 AmazonS3ClientBuilder.standard().withRegion(Regions.DEFAULT_REGION).build();
        ListBucketsPaginatedRequest listBucketsPaginatedRequest = new
 ListBucketsPaginatedRequest().withMaxBuckets(1);
        ListBucketsPaginatedResult listBucketsPaginatedResult =
 s3.listBuckets(listBucketsPaginatedRequest);
        List<Bucket> buckets = listBucketsPaginatedResult.getBuckets();
        System.out.println("Your Amazon S3 buckets are:");
        for (Bucket b : buckets) {
            System.out.println("* " + b.getName() + " region: " + b.getRegion());
        }
        System.out.println("continuation token: " +
 listBucketsPaginatedResult.getContinuationToken());
    }
}
```

SDK for Java 2.x

```
import software.amazon.awssdk.auth.credentials.DefaultCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3.S3Client;
import software.amazon.awssdk.services.s3.model.Bucket;
import software.amazon.awssdk.services.s3.model.ListBucketsRequest;
import software.amazon.awssdk.services.s3.model.ListBucketsResponse;

import java.util.List;

public class ListBuckets {
    public static void main(String[] args) {
        // Create an S3 client
        S3Client s3 = S3Client.builder()
                .region(Region.US_EAST_1) // Replace with your preferred region
                .credentialsProvider(DefaultCredentialsProvider.create())
                .build();

        try {
```

```
            // List buckets
            ListBucketsRequest listBucketsRequest = ListBucketsRequest.builder()
                    .maxBuckets(10)
                    .build();
            ListBucketsResponse listBucketsResponse =
 s3.listBuckets(listBucketsRequest);
            List<Bucket> buckets = listBucketsResponse.buckets();

            // Print bucket names
            System.out.println("Your Amazon S3 buckets are:");
            for (Bucket bucket : buckets) {
                System.out.println(bucket.name());
                System.out.println(bucket.getBucketRegion());
            }

        } catch (Exception e) {
            System.err.println("Error listing buckets: " + e.getMessage());
            e.printStackTrace();
        } finally {
            // Close the S3 client to release resources
            s3.close();
        }
    }
}
```

SDK for Go

```
package main
import (
 "context"
 "fmt"
 "log"
 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/config"
 "github.com/aws/aws-sdk-go-v2/service/s3"
)
func main() {
 cfg, err := config.LoadDefaultConfig(context.TODO(), config.WithRegion("us-
east-2"))
 if err != nil {
  log.Fatal(err)
 }
 client := s3.NewFromConfig(cfg)
```

```
 maxBuckets := 1000
 resp, err := client.ListBuckets(context.TODO(), management
 portals3.ListBucketsInput{MaxBuckets: aws.Int32(int32(maxBuckets))})
 if err != nil {
  log.Fatal(err)
 }
 fmt.Println("S3 Buckets:")
 for _, bucket := range resp.Buckets {
     fmt.Println("- Name:", *bucket.Name)
     fmt.Println("-BucketRegion", *bucket.BucketRegion)
 }
 fmt.Println(resp.ContinuationToken == nil)
 fmt.Println(resp.Prefix == nil)
}
```

Esvaziar um bucket de uso geral

Você pode esvaziar o conteúdo de um bucket de uso geral usando o console do Amazon S3, SDKs da AWS ou a AWS Command Line Interface (AWS CLI). Ao esvaziar um bucket de uso geral, você exclui todos os objetos, mas mantém o bucket. Não é possível desfazer a ação de esvaziar um bucket. Os objetos adicionados ao bucket enquanto a ação de esvaziar estiver em andamento também poderão ser excluídos. Todos os objetos (incluindo todas as versões do objeto e marcadores de exclusão) no bucket devem ser excluídos antes que o próprio bucket possa ser excluído.

Ao esvaziar um bucket de uso geral com o versionamento do S3 habilitado ou suspenso, todas as versões de todos os objetos no bucket são excluídas. Para obter mais informações, consulte Trabalhar com objetos em um bucket com versionamento habilitado.

Ao esvaziar um bucket, recomendamos que você também remova todos os uploads fracionados incompletos. Você pode usar multipart uploads para fazer upload de objetos muito grandes (até 5 TB) como um conjunto de partes para obter uma throughput aprimorada e uma recuperação mais rápida diante de problemas de rede. Quando o processo de multipart upload não termina, as partes incompletas permanecem no bucket (em um estado inutilizável). Essas partes incompletas incorrem em custos de armazenamento até que o processo de upload seja concluído, ou até que as partes incompletas sejam removidas. Para obter mais informações, consulte Carregar e copiar objetos usando upload fracionado no Amazon S3.

Uma prática recomendada é configurar regras de ciclo de vida para encerrar objetos e uploads fracionados incompletos que ultrapassem determinada quantidade de dias. Ao criar uma regra de ciclo de vida para expirar multipart uploads incompletos, recomendamos 7 dias como um bom ponto de partida. Para obter mais informações, consulte Definir uma configuração do Ciclo de Vida do S3 em um bucket.

Como a expiração do ciclo de vida é um processo assíncrono, pode levar alguns dias para que a regra seja executada e o bucket fique vazio. Depois da primeira vez que o Amazon S3 executa a regra, todos os objetos que estão qualificados para expiração são marcados para exclusão. Você não recebe mais cobranças pelos objetos marcados para exclusão. Para obter mais informações, consulte Como esvaziar um bucket do Amazon S3 usando uma regra de configuração do ciclo de vida?.

Usar o console do S3

Você pode usar o console do Amazon S3 para esvaziar um bucket de uso geral, o que exclui todos os objetos no bucket sem excluir o bucket.

Para esvaziar um bucket do S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets de uso geral.
3. Na lista de buckets, selecione a opção ao lado do nome do bucket que deseja esvaziar, depois escolha Vazio.
4. Na página Empty bucket (Esvaziar bucket), confirme se deseja esvaziar o bucket inserindo o nome do bucket no campo de texto e escolha Empty (Esvaziar).
5. Monitore o andamento do processo de esvaziamento do bucket na página Esvaziar bucket: status.

Como usar o AWS CLI

Você só pode esvaziar um bucket de uso geral usando a AWS CLI se o bucket não tiver o versionamento habilitado. Se o versionamento não estiver habilitado, você poderá usar o comando `rm` (remove) da AWS CLI com o parâmetro `--recursive` para esvaziar um bucket (ou remover um subconjunto de objetos com um prefixo de nome de chave específico).

O comando `rm` a seguir remove os objetos com o prefixo de nome de chave `doc`, por exemplo, `doc/doc1` e `doc/doc2`.

```
$ aws s3 rm s3://bucket-name/doc --recursive
```

Use o comando a seguir para remover todos os objetos sem especificar um prefixo.

```
$ aws s3 rm s3://bucket-name --recursive
```

Para obter informações, consulte Uso de comandos de alto nível do S3 com a AWS CLI no Manual do usuário da AWS Command Line Interface.

> **Note**
>
> Não é possível remover objetos de um bucket que tenha o versionamento ativado. O Amazon S3 adiciona um marcador de exclusão quando você exclui um objeto, que é o que este comando faz. Para obter mais informações sobre o S3 Bucket Versioning, consulte Reter várias versões de objetos com o Versionamento do S3.

Uso da SDKs AWS

Você pode usar os SDKs da AWS para esvaziar um bucket de uso geral ou para remover um subconjunto de objetos com um prefixo de nome de chave específico.

Para obter um exemplo de como esvaziar um bucket usando o AWS SDK para Java, consulte Excluir um bucket de uso geral. O código exclui todos os objetos, independentemente de o bucket ter versionamento habilitado e, em seguida, exclui o bucket. Para só esvaziar o bucket, certifique-se de remover o comando que exclui o bucket.

Para obter mais informações sobre como usar outros AWS SDKs, consulte Ferramentas para a Amazon Web Services.

Usando uma configuração de ciclo de vida

Para esvaziar um bucket de uso geral grande, recomendamos usar uma regra de configuração do ciclo de vida do S3. A expiração do ciclo de vida é um processo assíncrono, portanto, a regra pode levar alguns dias para ser executada antes que o bucket fique vazio. Depois da primeira vez

que o Amazon S3 executa a regra, todos os objetos que estão qualificados para expiração são marcados para exclusão. Você não recebe mais cobranças pelos objetos marcados para exclusão. Para obter mais informações, consulte Como esvaziar um bucket do Amazon S3 usando uma regra de configuração do ciclo de vida?.

Se você usar uma configuração de ciclo de vida para esvaziar seu bucket, a configuração deverá incluir versões atuais, versões não atuais, marcadores de exclusão e uploads fracionados incompletos.

Você pode adicionar regras de configuração de ciclo de vida para tornar todos os objetos ou um subconjunto de objetos expirados com um prefixo de nome de chave específico. Por exemplo, para remover todos os objetos em um bucket, você pode definir uma regra de ciclo de vida para tornar os objetos expirados um dia após a criação.

O Amazon S3 é compatível com uma regra de ciclo de vida de bucket que você pode usar para interrompe uploads fracionados que não são concluídos dentro de um número especificado de dias após a inicialização. Recomendamos que você configure essa regra de ciclo de vida para minimizar os custos de armazenamento. Para obter mais informações, consulte Configurar uma política de ciclo de vida de bucket para anular uploads incompletos de várias partes.

Para obter mais informações sobre como usar uma configuração de ciclo de vida para esvaziar um bucket, consulte Definir uma configuração do Ciclo de Vida do S3 em um bucket e Expirando objetos.

Esvaziar um bucket de uso geral com o AWS CloudTrail configurado

O AWS CloudTrail rastreia eventos de dados em nível de objeto em um bucket de uso geral do Amazon S3, como a exclusão de objetos. Se você usa um bucket de uso geral como destino para registrar em log os eventos do CloudTrail e está excluindo objetos desse mesmo bucket, é provável que esteja criando objetos enquanto esvazia o bucket. Para evitar isso, pare as trilhas do AWS CloudTrail. Para obter mais informações sobre como impedir que as trilhas do CloudTrail registrem eventos, consulte Desativar o registro de uma trilha no Guia do usuário do AWS CloudTrail.

Outra alternativa para impedir que as trilhas do CloudTrail sejam adicionadas ao bucket é adicionar uma instrução de negação `s3:PutObject` à política de bucket. Se você quiser armazenar novos objetos no bucket posteriormente, precisará remover essa declaração `s3:PutObject` de negação. Para obter mais informações, consulte Operações com objetos e Elementos da política de JSON do IAM: efeito no Guia do usuário do IAM.

Excluir um bucket de uso geral

Você pode excluir um bucket de uso geral vazio do Amazon S3. Para ter mais informações sobre como esvaziar um bucket de uso geral, consulte the section called “Esvaziar um bucket de uso geral”.

Você pode excluir um bucket usando o console do Amazon S3, a AWS Command Line Interface (AWS CLI), os AWS SDKs ou a API REST do Amazon S3.

Important

Antes de excluir um bucket de uso geral, considere o seguinte:

- Os nomes de bucket de uso geral são exclusivos em um namespace global. Se você excluir um bucket, esteja ciente de que outra Conta da AWS poderá usar o mesmo nome de bucket de uso geral para um novo bucket e, portanto, possivelmente receber solicitações destinadas ao bucket excluído. Para evitar que isso aconteça, ou se quiser continuar a usar o mesmo nome do bucket, não exclua o bucket. Recomendamos que você esvazie o bucket e o mantenha, bloqueando quaisquer solicitações de bucket conforme necessário. Com relação a buckets não usados ativamente, recomendamos esvaziar todos o bucket de todos os objetos para minimizar os custos e, ao mesmo tempo, reter o bucket em si.
- Quando você exclui um bucket de uso geral, ele pode não ser removido imediatamente. Em vez disso, o Amazon S3 o coloca em fila para exclusão. Como o Amazon S3 é distribuído entre Regiões da AWS, o processo de exclusão leva tempo para se propagar totalmente e obter consistência em todo o sistema.
- Se o bucket hospedar um site estático e você tiver criado e configurado uma zona hospedada do Amazon Route 53 conforme descrito em Tutorial: Configurar um site estático usando um domínio personalizado registrado no Route 53, você deverá limpar as configurações da zona hospedada do Route 53 relacionadas ao bucket. Para obter mais informações, consulte Etapa 2: exclua a zona hospedada do Route 53.
- Se o bucket receber dados de log do Elastic Load Balancing (ELB), recomendamos a interrupção da entrega de logs do ELB para o bucket antes da exclusão. Após excluir o bucket, se outro usuário criar um bucket usando o mesmo nome, os dados de log poderão ser entregues a esse bucket. Para ter informações sobre os logs de acesso do ELB, consulte Access logs for your Classic Load Balancer no Guia do usuário para Classic

Load Balancers e Access logs for your Application Load Balancer no Guia do usuário para Application Load Balancers.

Solução de problemas

Se você não conseguir excluir um bucket de uso geral do Amazon S3, considere o seguinte:

- Verifique se o bucket está vazio: só é possível excluir buckets que não contêm nenhum objeto. Verifique se o bucket está vazio. Para ter mais informações sobre como esvaziar um bucket, consulte the section called “Esvaziar um bucket de uso geral”.
- Verifique se não há nenhum ponto de acesso anexado: só é possível excluir buckets que não contêm nenhum ponto de acesso do S3 ou ponto de acesso multirregional anexado na mesma conta. Antes de excluir o bucket, exclua todos os pontos de acesso da mesma conta que estão anexados ao bucket.
- Verifique se você tem a permissão **`s3:DeleteBucket`**: se não conseguir excluir um bucket, consulte o administrador do IAM para confirmar se você tem a permissão `s3:DeleteBucket`. Para obter informações sobre como visualizar ou atualizar permissões do IAM, consulte Alteração de permissões de um usuário do IAM no Guia do usuário do IAM. Para obter informações sobre a solução de problemas, consulte the section called “Solucionar erros (403 Forbidden) de acesso negado”.
- Verifique se há instruções **`s3:DeleteBucket Deny`** nas políticas de controle de serviços (SCPs) e nas políticas de controle de recursos (RCPs) do AWS Organizations: SCPs e RCPs podem negar a permissão de exclusão em um bucket. Consulte mais informações em Políticas de controle de serviços (SCPs) e em Resource control policies no Guia do usuário do AWS Organizations.
- Verifique se há instruções **`s3:DeleteBucket Deny`** em sua política de bucket: se você tiver permissões `s3:DeleteBucket` em sua política de usuário ou perfil do IAM e não conseguir excluir um bucket, talvez a política de bucket inclua uma instrução `Deny` para `s3:DeleteBucket`. Os buckets criados pelo AWS Elastic Beanstalk têm uma política que contém essa instrução por padrão. Antes de excluir o bucket, você deve excluir essa instrução ou a política de bucket.

Pré-requisitos

Para excluir um bucket de uso geral, é necessário excluir o respectivo conteúdo. Para ter mais informações sobre como esvaziar um bucket, consulte the section called “Esvaziar um bucket de uso geral”.

Usar o console do S3

Para excluir um bucket do S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets de uso geral.
3. Na lista de buckets, selecione a botão de opção ao lado do nome do bucket que deseja excluir e selecione Excluir na parte superior da página.
4. Na página Delete bucket (Excluir bucket), confirme se deseja excluir o bucket inserindo o nome do bucket no campo de texto e escolha Delete bucket (Excluir bucket).

   > **Note**
   >
   > Se o bucket contiver objetos, esvazie o bucket antes de excluí-lo selecionando o botão Esvaziar bucket no alerta de erro Este bucket não está vazio e seguindo as instruções na página Esvaziar bucket. Depois, volte para a página Delete bucket (Excluir bucket) e exclua o bucket.

5. Para verificar se você excluiu o bucket, abra a lista Buckets de uso geral e insira o nome do bucket que você excluiu. Se não for possível encontrar o bucket, sua exclusão foi bem-sucedida.

Usar o AWS SDK para Java

O exemplo a seguir mostra como esvaziar e excluir um bucket de uso geral usando o AWS SDK para Java. Primeiro, o código exclui todos os objetos no bucket, depois exclui o bucket.

Para obter exemplos em outras linguagens, consulte Use DeleteBucket com um AWS SDK ou CLI na Referência de API do Amazon Simple Storage Service. Para ter mais informações sobre como usar outros AWS SDKs, consulte Ferramentas para a Amazon Web Services.

Java

O exemplo de Java a seguir exclui um bucket que contém objetos. O exemplo exclui todos os objetos e, em seguida, exclui o bucket. O exemplo também funciona para buckets com ou sem versionamento habilitado.

> **Note**
>
> Para buckets sem versionamento habilitado, você pode excluir todos os objetos diretamente e, em seguida, excluir o bucket. Para buckets com versionamento habilitado, você deve excluir todas as versões do objeto antes de excluir o bucket.

Consulte instruções sobre como criar e testar uma amostra funcional no Guia do desenvolvedor do AWS SDK for Java 2.x.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.*;

import java.util.Iterator;

public class DeleteBucket2 {

    public static void main(String[] args) {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "*** Bucket name ***";

        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(clientRegion)
                    .build();

            // Delete all objects from the bucket. This is sufficient
            // for unversioned buckets. For versioned buckets, when you attempt to
 delete
            // objects, Amazon S3 inserts
            // delete markers for all objects, but doesn't delete the object
 versions.
            // To delete objects from versioned buckets, delete all of the object
 versions
            // before deleting
```

```
            // the bucket (see below for an example).
            ObjectListing objectListing = s3Client.listObjects(bucketName);
            while (true) {
                Iterator<S3ObjectSummary> objIter =
objectListing.getObjectSummaries().iterator();
                while (objIter.hasNext()) {
                    s3Client.deleteObject(bucketName, objIter.next().getKey());
                }

                // If the bucket contains many objects, the listObjects() call
                // might not return all of the objects in the first listing. Check
to
                // see whether the listing was truncated. If so, retrieve the next
page of
                // objects
                // and delete them.
                if (objectListing.isTruncated()) {
                    objectListing = s3Client.listNextBatchOfObjects(objectListing);
                } else {
                    break;
                }
            }

            // Delete all object versions (required for versioned buckets).
            VersionListing versionList = s3Client.listVersions(new
ListVersionsRequest().withBucketName(bucketName));
            while (true) {
                Iterator<S3VersionSummary> versionIter =
versionList.getVersionSummaries().iterator();
                while (versionIter.hasNext()) {
                    S3VersionSummary vs = versionIter.next();
                    s3Client.deleteVersion(bucketName, vs.getKey(),
vs.getVersionId());
                }

                if (versionList.isTruncated()) {
                    versionList = s3Client.listNextBatchOfVersions(versionList);
                } else {
                    break;
                }
            }

            // After all objects and object versions are deleted, delete the bucket.
            s3Client.deleteBucket(bucketName);
```

```
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
 couldn't
            // parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Como usar o AWS CLI

Você poderá usar a AWS CLI para excluir um bucket de uso geral que contém objetos se ele não tiver o versionamento habilitado. Ao excluir um bucket que contém objetos, todos os objetos no bucket são excluídos permanentemente, incluindo objetos que passaram para a classe de armazenamento S3 Glacier Flexible Retrieval.

Se o bucket não tiver o versionamento habilitado, você poderá usar o comando `rb` (remover bucket) da AWS CLI com o parâmetro `--force` para excluir o bucket e todos os objetos nele. Esse comando primeiro exclui todos os objetos e, em seguida, o bucket.

Se o versionamento estiver habilitado, usar o comando `rb` com o parâmetro `--force` não excluirá objetos com versionamento, portanto, a exclusão do bucket falhará porque o bucket não estará vazio. Para obter mais informações sobre como excluir objetos com versionamento, consulte Excluir versões de objetos.

Para usar o seguinte comando, substitua *`amzn-s3-demo-bucket`* pelo nome do bucket que deseja excluir:

```
$ aws s3 rb s3://amzn-s3-demo-bucket --force
```

Para ter informações, consulte Como usar comandos de alto nível (s3) na AWS Command Line Interface no Guia do usuário da AWS Command Line Interface.

Montar um bucket do Amazon S3 como um sistema de arquivos local

O Mountpoint para Amazon S3 é um cliente de arquivos de código aberto com alta taxa de throughput para montar um bucket do Amazon S3 como um sistema de arquivos local. Com o Mountpoint, as aplicações podem acessar objetos armazenados no Amazon S3 por meio de operações do sistema de arquivo, como abertura e leitura. O Mountpoint traduz automaticamente essas operações em chamadas de API de objetos do S3, dando aos aplicativos acesso ao armazenamento elástico e ao throughput do Amazon S3 por meio de uma interface de arquivo.

O Mountpoint para Amazon S3 está disponível para uso na produção, em aplicações em grande escala com uso intenso de leitura: data lakes, treinamento de machine learning, renderização de imagens, simulação de veículos autônomos, extração, transformação e carregamento (ETL) e muito mais.

O Mountpoint permite operações básicas de sistema de arquivos e pode ler arquivos de até 5 TB. Ele pode listar e ler arquivos existentes e criar outros. Ele não pode modificar arquivos existentes nem excluir diretórios e não é compatível com links simbólicos ou bloqueio de arquivos. O Mountpoint é ideal para aplicações que não precisam de todos os recursos de um sistema de arquivos compartilhado e de permissões no estilo POSIX, mas exigem o throughput elástico do Amazon S3 para ler e gravar grandes conjuntos de dados do S3. Para obter detalhes, consulte Comportamento do sistema de arquivos do Mountpoint no GitHub. Quanto a workloads que exigem compatibilidade total com o POSIX, recomendamos o Amazon FSx para Lustre, que permite vincular buckets do Amazon S3.

O Mountpoint para Amazon S3 está disponível somente para sistemas operacionais Linux. Você pode usar o Mountpoint para acessar objetos do S3 em todas as classes de armazenamento, exceto S3 Glacier Flexible Retrieval, S3 Glacier Deep Archive, S3 Intelligent-Tiering Archive Access Tier e S3 Intelligent-Tiering Deep Archive Access Tier.

Tópicos

- Instalar o Mountpoint
- Configurar e usar o Mountpoint
- Solução de problemas do Mountpoint

Instalar o Mountpoint

Você pode baixar e instalar pacotes pré-compilados do Mountpoint para Amazon S3 usando a linha de comando. As instruções para baixar e instalar o Mountpoint variam, dependendo de qual sistema operacional Linux você está usando.

Tópicos

- Distribuições baseadas em RPM (Amazon Linux, Fedora, CentOS, RHEL)
- Distribuições baseadas em DEB (Debian, Ubuntu)
- Outras distribuições do Linux
- Conferir a assinatura do pacote do Mountpoint para Amazon S3

Distribuições baseadas em RPM (Amazon Linux, Fedora, CentOS, RHEL)

1. Copie o URL de download a seguir referente à sua arquitetura.

   x86_64:

   ```
   https://s3.amazonaws.com/mountpoint-s3-release/latest/x86_64/mount-s3.rpm
   ```

   ARM64 (Graviton):

   ```
   https://s3.amazonaws.com/mountpoint-s3-release/latest/arm64/mount-s3.rpm
   ```

2. Baixe o pacote do Mountpoint para Amazon S3. Substitua *download-link* pelo URL de download apropriado da etapa anterior.

   ```
   wget download-link
   ```

3. (Opcional) Verifique a integridade e a autenticidade do arquivo baixado. Primeiro, copie o URL de assinatura apropriado para a sua arquitetura.

   x86_64:

   ```
   https://s3.amazonaws.com/mountpoint-s3-release/latest/x86_64/mount-s3.rpm.asc
   ```

   ARM64 (Graviton):

```
https://s3.amazonaws.com/mountpoint-s3-release/latest/arm64/mount-s3.rpm.asc
```

Depois, consulte Verificar a assinatura do pacote do Mountpoint para Amazon S3.

4. Instale o pacote usando o seguinte comando:

```
sudo yum install ./mount-s3.rpm
```

5. Confira se o Mountpoint foi instalado com êxito digitando o seguinte comando:

```
mount-s3 --version
```

Você deve ver uma saída semelhante a:

```
mount-s3 1.3.1
```

Distribuições baseadas em DEB (Debian, Ubuntu)

1. Copie o URL de download para a arquitetura.

   x86_64:

```
https://s3.amazonaws.com/mountpoint-s3-release/latest/x86_64/mount-s3.deb
```

   ARM64 (Graviton):

```
https://s3.amazonaws.com/mountpoint-s3-release/latest/arm64/mount-s3.deb
```

2. Baixe o pacote do Mountpoint para Amazon S3. Substitua *download-link* pelo URL de download apropriado da etapa anterior.

```
wget download-link
```

3. (Opcional) Verifique a integridade e a autenticidade do arquivo baixado. Primeiro, copie o URL de assinatura para a arquitetura.

   x86_64:

```
https://s3.amazonaws.com/mountpoint-s3-release/latest/x86_64/mount-s3.deb.asc
```

ARM64 (Graviton):

```
https://s3.amazonaws.com/mountpoint-s3-release/latest/arm64/mount-s3.deb.asc
```

Depois, consulte Verificar a assinatura do pacote do Mountpoint para Amazon S3.

4. Instale o pacote usando o seguinte comando:

```
sudo apt-get install ./mount-s3.deb
```

5. Confira se o Mountpoint para Amazon S3 foi instalado com êxito digitando o seguinte comando:

```
mount-s3 --version
```

Você deve ver uma saída semelhante a:

```
mount-s3 1.3.1
```

Outras distribuições do Linux

1. Consulte a documentação do sistema operacional para instalar os pacotes `FUSE` e `libfuse2`, que são obrigatórios.
2. Copie o URL de download para a arquitetura.

   x86_64:

```
https://s3.amazonaws.com/mountpoint-s3-release/latest/x86_64/mount-s3.tar.gz
```

   ARM64 (Graviton):

```
https://s3.amazonaws.com/mountpoint-s3-release/latest/arm64/mount-s3.tar.gz
```

3. Baixe o pacote do Mountpoint para Amazon S3. Substitua *`download-link`* pelo URL de download apropriado da etapa anterior.

```
wget download-link
```

4. (Opcional) Verifique a integridade e a autenticidade do arquivo baixado. Primeiro, copie o URL de assinatura para a arquitetura.

   x86_64:

   ```
   https://s3.amazonaws.com/mountpoint-s3-release/latest/x86_64/mount-s3.tar.gz.asc
   ```

   ARM64 (Graviton):

   ```
   https://s3.amazonaws.com/mountpoint-s3-release/latest/arm64/mount-s3.tar.gz.asc
   ```

   Depois, consulte Verificar a assinatura do pacote do Mountpoint para Amazon S3.

5. Instale o pacote usando o seguinte comando:

   ```
   sudo mkdir -p /opt/aws/mountpoint-s3 && sudo tar -C /opt/aws/mountpoint-s3 -xzf ./
   mount-s3.tar.gz
   ```

6. Adicione o `mount-s3` binário à variável de ambiente `PATH`. No arquivo `$HOME/.profile`, anexe a seguinte linha:

   ```
   export PATH=$PATH:/opt/aws/mountpoint-s3/bin
   ```

   Salve o arquivo `.profile` e execute o seguinte comando:

   ```
   source $HOME/.profile
   ```

7. Confira se o Mountpoint para Amazon S3 foi instalado com êxito digitando o seguinte comando:

   ```
   mount-s3 --version
   ```

   Você deve ver uma saída semelhante a:

   ```
   mount-s3 1.3.1
   ```

Conferir a assinatura do pacote do Mountpoint para Amazon S3

1. Instale GnuPG (o comando gpg). É necessário verificar a autenticidade e a integridade de um pacote do Mountpoint para Amazon S3 baixado. GnuPG é instalado por padrão em imagens de máquina da Amazon (AMIs) do Linux Amazon. Depois de instalar GnuPG, vá para a etapa 2.
2. Baixe a chave pública do Mountpoint executando o seguinte comando:

   ```
   wget https://s3.amazonaws.com/mountpoint-s3-release/public_keys/KEYS
   ```

3. Importe a chave pública do Mountpoint para o token de autenticação executando o seguinte comando:

   ```
   gpg --import KEYS
   ```

4. Verifique a impressão digital da chave pública do Mountpoint executando o seguinte comando:

   ```
   gpg --fingerprint mountpoint-s3@amazon.com
   ```

   Confirme se a string de impressões digitais exibida corresponde ao seguinte:

   ```
   673F E406 1506 BB46 9A0E  F857 BE39 7A52 B086 DA5A
   ```

   Se a string de impressões digitais não coincidir, não conclua a instalação do Mountpoint. Nesse caso, entre em contato com o AWS Support.

5. Faça download do arquivo SIGNATURE do pacote. Substitua *signature-link* pelo link de assinatura apropriado das seções anteriores.

   ```
   wget signature-link
   ```

6. Verifique a assinatura do pacote baixado executando o comando a seguir. Substitua *signature-filename* pelo nome do arquivo da etapa anterior.

   ```
   gpg --verify signature-filename
   ```

   Por exemplo, em distribuições com base em RPM, incluindo o Amazon Linux, execute o seguinte comando:

```
gpg --verify mount-s3.rpm.asc
```

7. A saída deve incluir a frase `Good signature`. Se a saída incluir a frase `BAD signature`, baixe novamente o arquivo do pacote do Mountpoint e repita essas etapas. Se o problema persistir, não conclua a instalação do Mountpoint. Nesse caso, entre em contato com o AWS Support.

   A saída pode incluir um aviso sobre uma assinatura confiável. Isso não indica um problema. Significa apenas que você não verificou de forma independente a chave pública do Mountpoint.

Configurar e usar o Mountpoint

Para usar o Mountpoint para Amazon S3, o host precisa de credenciais válidas da AWS, com acesso ao bucket do Amazon S3 ou aos buckets que você gostaria de montar. Para diferentes formas de autenticação, consulte Credenciais da AWS para o Mountpoint no GitHub.

Por exemplo, você pode criar um usuário e um perfil do AWS Identity and Access Management (IAM) para essa finalidade. Esse perfil deve ter acesso ao bucket ou aos buckets que você gostaria de montar. É possível transmitir o perfil do IAM à instância do Amazon EC2 com um perfil de instância.

Tópicos

- Usar o Mountpoint para Amazon S3
- Configurar o armazenamento em cache no Mountpoint

Usar o Mountpoint para Amazon S3

Use o Mountpoint para Amazon S3 para fazer o seguinte:

1. Monte seus buckets do Amazon S3.

   a. Você pode montar os buckets do Amazon S3 manualmente usando o comando `mount-s3`.

      No exemplo a seguir, substitua *amzn-s3-demo-bucket* pelo nome do bucket do S3 e substitua *~/mnt* pelo diretório no host em que você deseja montar o bucket do S3.

      ```
      mkdir ~/mnt
      mount-s3 amzn-s3-demo-bucket ~/mnt
      ```

Como o cliente do Mountpoint é executado em segundo plano por padrão, o diretório *~/mnt* agora oferece acesso aos objetos no bucket do Amazon S3.

b. Como alternativa, você pode configurar a montagem automática de buckets do Amazon S3 quando uma instância é inicializada ou reinicializada.

Para instâncias do Amazon EC2 existentes ou em execução, encontre o arquivo `fstab` no diretório `/etc/fstab` do seu sistema Linux. Em seguida, adicione uma linha ao seu arquivo `fstab`. Por exemplo, para montar *amzn-s3-demo-bucket* usando o prefixo `example-prefix/` do caminho do sistema `/mnt/mountpoint`, consulte o seguinte. Para usar o exemplo a seguir, substitua os *espaços reservados para entrada do usuário* por suas próprias informações.

```
s3://amzn-s3-demo-bucket/example-prefix/ /mnt/mountpoint mount-s3
 _netdev,nosuid,nodev,nofail,rw 0 0
```

Consulte a tabela a seguir para obter uma explicação sobre as opções usadas no exemplo.

Opção	Descrição
`_netdev`	Especifica que o sistema de arquivos requer rede para ser montado.
`nosuid`	Especifica que o sistema de arquivos não pode conter arquivos com ID de usuário definido.
`nodev`	Especifica que o sistema de arquivos não pode conter dispositivos especiais.
`nofail`	Especifica que a falha na montagem do sistema de arquivos ainda deve permitir que o sistema inicialize.
`rw`	Especifica que o ponto de montagem seja criado com permissões de leitura e gravação. Como alternativa, use `ro` somente para leitura.

Para novas instâncias do Amazon EC2, você pode modificar os dados do usuário em um modelo do Amazon EC2 e configurar o arquivo `fstab` da forma a seguir. Para usar o exemplo a seguir, substitua os *espaços reservados para entrada do usuário* por suas próprias informações.

```
#!/bin/bash -e
MP_RPM=$(mktemp --suffix=.rpm)
curl https://s3.amazonaws.com/mountpoint-s3-release/latest/x86_64/mount-s3.rpm
 > $MP_RPM
yum install -y $MP_RPM
rm $MP_RPM

MNT_PATH=/mnt/mountpoint
echo "s3://amzn-s3-demo-bucket/ ${MNT_PATH} mount-s3
 _netdev,nosuid,nodev,rw,allow-other,nofail" >> /etc/fstab
mkdir $MNT_PATH

systemctl daemon-reload
mount -a
```

2. Acesse os objetos no bucket do Amazon S3 por meio do Mountpoint.

   Depois de montar o bucket localmente, você pode usar os comandos Linux comuns, como `cat` ou `ls`, para trabalhar com os objetos do S3. O Mountpoint para Amazon S3 interpreta as chaves no bucket do Amazon S3 como caminhos do sistema de arquivos dividindo-as com o caractere de barra (`/`). Por exemplo, se você tiver a chave do objeto `Data/2023-01-01.csv` no bucket, terá um diretório chamado `Data` no sistema de arquivos do Mountpoint, o qual contém um arquivo chamado `2023-01-01.csv`.

   O Mountpoint para Amazon S3 não implementa intencionalmente a especificação padrão completa POSIX para sistemas de arquivos. O Mountpoint é otimizado para workloads que, embora precisem de alta taxa de throughput para acesso de leitura e gravação aos dados armazenados no Amazon S3 por meio de uma interface de sistema de arquivos, de outra forma não dependem dos atributos do sistema de arquivos. Para receber mais informações, consulte Comportamento do sistema de arquivos do Mountpoint para Amazon S3 no GitHub. Os clientes que precisam de uma semântica mais completa do sistema de arquivos devem considerar outros serviços de arquivos AWS, como Amazon Elastic File System (Amazon EFS) ou Amazon FSx.

3. Desmonte o bucket do Amazon S3 usando o comando `umount`. Esse comando desmonta o bucket do S3 e sai do Mountpoint.

   Para usar o comando de exemplo a seguir, substitua *~/mnt* pelo diretório no host em que o bucket do S3 está montado.

   ```
   umount ~/mnt
   ```

   > **Note**
   >
   > Para receber uma lista de opções para esse comando, execute `umount --help`.

Para obter detalhes adicionais sobre a configuração do Mountpoint, consulte S3 bucket configuration e File system configuration no GitHub.

Configurar o armazenamento em cache no Mountpoint

O Mountpoint para Amazon S3 é compatível com diferentes tipos de armazenamento em cache de dados. Para acelerar as solicitações de leitura repetidas, você pode optar pelo seguinte:

- Cache local: você pode usar um cache local em seu armazenamento de instância do Amazon EC2 ou em um volume do Amazon Elastic Block Store. Se você ler repetidamente os mesmos dados da mesma instância de computação e tiver espaço não utilizado no armazenamento da instância local para o conjunto de dados lido repetidamente, opte por um cache local.
- Cache compartilhado: você pode usar um cache compartilhado na classe S3 Express One Zone. Se você lê repetidamente objetos pequenos de várias instâncias de computação ou se não sabe o tamanho do conjunto de dados lido repetidamente e quer se beneficiar da elasticidade do tamanho do cache, opte pelo cache compartilhado. Depois de definir essa opção, o Mountpoint retém objetos com tamanhos de até um megabyte em um bucket de diretório que usa a classe S3 Express One Zone.
- Cache local e compartilhado combinados: se você tem espaço não utilizado no cache local, mas também quer um cache compartilhado em várias instâncias, pode optar por um cache local e um cache compartilhado.

O armazenamento em cache no Mountpoint é ideal para casos de uso em que você lê repetidamente os mesmos dados que não mudam durante as várias leituras. Por exemplo, você pode usar o

armazenamento em cache com trabalhos de treinamento de machine learning que precisam ler um conjunto de dados de treinamento várias vezes para melhorar a precisão do modelo.

Consulte mais informações sobre como configurar o armazenamento em cache no Mountpoint nos exemplos a seguir.

Tópicos

- Cache local
- Cache compartilhado
- Cache local e compartilhado combinados

Cache local

Você pode optar por um cache local com a sinalização `--cache` *`CACHE_PATH`*. No exemplo a seguir, substitua *`CACHE_PATH`* pelo caminho de arquivo do diretório no qual você deseja armazenar os dados em cache. Substitua *`amzn-s3-demo-bucket`* pelo nome do bucket do Amazon S3 e substitua *`~/mnt`* pelo diretório no host em que você deseja montar o bucket do S3.

```
mkdir ~/mnt
mount-s3 --cache CACHE_PATH amzn-s3-demo-bucket ~/mnt
```

Quando você opta pelo armazenamento em cache local ao montar um bucket do Amazon S3, o Mountpoint cria um subdiretório vazio no local do cache configurado, caso esse subdiretório ainda não exista. Quando você monta um bucket pela primeira vez e quando desmonta, o Mountpoint exclui o conteúdo do cache local.

> **Important**
>
> Se você habilitar o armazenamento em cache local, o Mountpoint manterá o conteúdo de objeto não criptografado do bucket do Amazon S3 montado na localização do cache local indicada na montagem. Para proteger os dados, você deve restringir o acesso à localização do cache de dados usando mecanismos de controle de acesso ao sistema de arquivos.

Cache compartilhado

Se você lê repetidamente objetos pequenos (até 1 MB) de várias instâncias de computação ou se o tamanho do conjunto de dados que você lê repetidamente geralmente excede o tamanho do cache

local, use um cache compartilhado na classe S3 Express One Zone. Quando você lê os mesmos dados repetidamente de várias instâncias, isso melhora a latência ao evitar solicitações redundantes para o bucket do Amazon S3 montado.

Depois de optar pelo cache compartilhado, você paga pelos dados armazenados no bucket de diretório na classe S3 Express One Zone. Você também paga pelas solicitações feitas com relação aos seus dados no bucket de diretório na classe S3 Express One Zone. Para obter mais informações, consulte Preço do Amazon S3. O Mountpoint nunca exclui objetos em cache dos buckets de diretório. Para gerenciar os custos de armazenamento, você deve configurar uma política de ciclo de vida no bucket de diretório para que o Amazon S3 expire os dados em cache na classe S3 Express One Zone após um período especificado por você. Consulte mais informações em Mountpoint for Amazon S3 caching configuration no GitHub.

Para optar pelo armazenamento em cache na classe S3 Express One Zone ao montar um bucket do Amazon S3 na instância de computação, use a sinalização `--cache-xz` e especifique um bucket de diretório como a localização do cache. No exemplo a seguir, substitua os *espaços reservados de entrada do usuário*.

```
mount-s3 amzn-s3-demo-bucket ~/mnt --cache-xz amzn-s3-demo-bucket--usw2-az1--x-s3
```

Cache local e compartilhado combinados

Se você tem espaço não utilizado na instância, mas também quer usar um cache compartilhado em várias instâncias, pode optar por um cache local e um cache compartilhado. Com essa configuração de cache, você pode evitar solicitações de leitura redundantes da mesma instância para o cache compartilhado no bucket do diretório quando os dados necessários são armazenados em cache no armazenamento local. Isso pode reduzir os custos e melhorar o desempenho.

Para optar por um cache local e compartilhado ao montar um bucket do Amazon S3, especifique as localizações de ambos os caches usando os sinalizadores `--cache` e `--cache-xz`. Para usar o exemplo a seguir para optar por um cache local e compartilhado, substitua os *espaços reservados de entrada do usuário*.

```
mount -s3 amzn-s3-demo-bucket ~/mnt --cache /path/to/mountpoint/cache --cache -xz amzn-s3-demo-bucket--usw2-az1--x-s3
```

Consulte mais informações em Mountpoint for Amazon S3 caching configuration no GitHub.

> **Important**
>
> Se você habilitar o armazenamento em cache compartilhado, o Mountpoint copiará o conteúdo do objeto do bucket do Amazon S3 montado para o bucket do diretório do S3 que você fornece como a localização do cache compartilhado, tornando-o acessível a qualquer chamador com acesso ao bucket de diretório do S3. Para proteger os dados em cache, você deve seguir as Práticas recomendadas de segurança para o Amazon S3 para garantir que os buckets utilizem as políticas corretas e não sejam acessados publicamente. Você deve usar um bucket de diretório dedicado para o cache compartilhado do Mountpoint e conceder acesso somente aos clientes do Mountpoint.

Solução de problemas do Mountpoint

O Mountpoint para Amazon S3 conta com o suporte do Suporte. Se precisar de ajuda, entre em contato com o AWS Support Center.

Você também pode examinar e enviar Problemas do Mountpoint no GitHub.

Se você descobrir um possível problema de segurança nesse projeto, pedimos que você notifique a Segurança da AWS por meio de nossa página Relatório de vulnerabilidade. Não crie um problema público no GitHub.

Se a aplicação se comportar inesperadamente com o Mountpoint, você poderá inspecionar as informações de log para diagnosticar o problema.

Registro em log

Por padrão, o Mountpoint emite informações de log de alta gravidade para syslog.

Para visualizar os logs sobre as distribuições do Linux mais modernas, inclusive o Amazon Linux, execute o seguinte comando `journald`:

```
journalctl -e SYSLOG_IDENTIFIER=mount-s3
```

Em outros sistemas Linux, as entradas `syslog` provavelmente são gravadas em um arquivo como `/var/log/syslog`.

Você pode usar esses logs para solucionar problemas da aplicação. Por exemplo, se a aplicação tentar sobrescrever um arquivo existente, a operação falhará, e você verá uma linha semelhante à seguinte no log:

```
[WARN] open{req=12 ino=2}: mountpoint_s3::fuse: open failed: inode error: inode 2 (full
 key "README.md") is not writable
```

Para receber mais informações, consulte Registro em log do Mountpoint para Amazon S3 no GitHub.

Como trabalhar com o Navegador de Armazenamento para Amazon S3

O Navegador de Armazenamento para S3 é um componente de código aberto que você pode adicionar ao seu aplicativo web para fornecer aos usuários finais uma interface gráfica simples para dados armazenados no Amazon S3. Com o Navegador de Armazenamento para S3, você pode fornecer aos usuários finais autorizados acesso para navegar, baixar, carregar, copiar e excluir dados no S3 diretamente das próprias aplicações.

O Navegador de Armazenamento para S3 oferece suporte às seguintes operações para arquivos: `LIST`, `GET`, `PUT`, `COPY`, `UPLOAD` e `DELETE`. Para oferecer transferência de dados com alto throughput, o Navegador de Armazenamento para S3 exibe apenas os dados que os usuários finais estão autorizados a acessar e otimiza as solicitações de upload. O Navegador de Armazenamento também otimiza a performance para tempos de carregamento mais rápidos, calcula somas de verificação dos dados que os usuários finais carregam e aceita objetos após confirmar que a integridade dos dados foi mantida (em trânsito) pela internet pública. Você pode controlar o acesso aos dados com base na identidade do usuário final usando os serviços de segurança e identidade da AWS ou seus próprios serviços gerenciados. Também é possível personalizar o Navegador de Armazenamento de acordo com o design e a identidade de marca da sua aplicação existente.

O Navegador de Armazenamento para S3 só está disponível para aplicativos web e da intranet no framework React. Você pode usar o Navegador de Armazenamento para acessar objetos do Amazon S3 em todas as classes de armazenamento, exceto S3 Glacier Flexible Retrieval, S3 Glacier Deep Archive, S3 Intelligent-Tiering Archive Access e S3 Intelligent-Tiering Deep Archive Access.

O Navegador de Armazenamento para S3 está disponível para uso com aplicativos web na biblioteca AWS Amplify React. Para ter mais informações sobre o Navegador de Armazenamento, consulte Storage Browser para Amazon S3.

Tópicos

- Usar o Navegador de Armazenamento para S3
- Instalar o Navegador de Armazenamento para S3
- Configurar o Navegador de Armazenamento para S3
- Configurar o Navegador de Armazenamento para S3
- Solução de problemas do Navegador de Armazenamento para S3

Usar o Navegador de Armazenamento para S3

No Navegador de Armazenamento para S3, um local é um bucket de uso geral ou prefixo do S3 ao qual você concede acesso aos usuários finais usando a funcionalidade Concessão de Acesso do S3, políticas do IAM ou um serviço próprio de autorização gerenciado. Depois que você autorizar os usuários finais a acessar um local específico, eles poderão trabalhar com quaisquer dados dentro desse local.

A interface de usuário do Navegador de Armazenamento para S3 tem quatro exibições principais:

- Página inicial: a página inicial lista os locais do S3 que os usuários podem acessar, bem como as permissões que você concedeu a cada um. Essa é a exibição inicial para os usuários, mostrando os recursos do S3 de nível raiz aos quais os usuários finais têm acesso e as permissões (READ/WRITE/READWRITE) para cada local do S3.
- Detalhes do local: essa exibição permite que os usuários naveguem por arquivos e pastas no S3 e carreguem ou baixem arquivos. (Observe que, no Navegador de Armazenamento para S3, objetos são conhecidos como arquivos, e prefixos e buckets são conhecidos como pastas.)
- Ação de local: depois que um usuário escolhe uma ação (como Carregar) no Navegador de Armazenamento, é aberta outra exibição do local do arquivo.
- Elipse vertical: o ícone de elipse vertical abre a lista suspensa de ações.

Ao usar o Navegador de Armazenamento para S3, esteja ciente das seguintes limitações:

- Pastas que começam ou terminam com pontos (.) não são compatíveis.
- A funcionalidade Concessão de Acesso do S3 com permissão somente WRITE não é compatível.
- O Navegador de Armazenamento para S3 é compatível com a operação PUT para arquivos de até 160 GB.

- O Navegador de Armazenamento para S3 só é compatível com a operação `COPY` para arquivos menores que 5 GB. Se o tamanho do arquivo exceder 5 GB, o Navegador de Armazenamento falhará na solicitação.

Instalar o Navegador de Armazenamento para S3

A maneira mais rápida de começar a usar o Navegador de Armazenamento é clonar um dos projetos de exemplo no GitHub. Esses projetos de exemplo podem ajudar você a implantar aplicações web prontas para produção para o Navegador de Armazenamento com integrações predefinidas de serviços da AWS para o AWS Identity and Access Management. Dessa maneira, você pode conectar rapidamente usuários finais autorizados aos dados no S3.

Para ter mais informações, consulte Quick start no Amplify Dev Center.

Instalar o Navegador de Armazenamento para S3 por meio do GitHub

Como alternativa, você pode instalar o Navegador de Armazenamento para S3 usando a versão mais recente dos pacotes `aws-amplify/ui-react-storage` e `aws-amplify` no repositório `aws-amplify` do GitHub para começar a integrar o Navegador de Armazenamento à aplicação existente. Ao instalar o Navegador de Armazenamento para S3, adicione as seguintes dependências ao arquivo `package.json`:

```
"dependencies": {
    "aws-amplify/ui-react-storage": "latest",
    "aws-amplify": "latest",
  }
```

Você também pode adicionar as dependências usando o Node Package Manager (NPM):

```
npm i --save @aws-amplify/ui-react-storage aws-amplify
```

Configurar o Navegador de Armazenamento para S3

Para conectar usuários finais a locais do Amazon S3, primeiro é necessário configurar um método de autenticação e autorização. Há três métodos de configurar um método de autenticação e autorização com o Navegador de Armazenamento:

- Método 1: gerenciar o acesso aos dados para os clientes e parceiros terceiros

- Método 2: gerenciar o acesso aos dados para as entidades principais do IAM da sua conta da AWS
- Método 3: gerenciar o acesso aos dados em grande escala

Método 1: gerenciar o acesso aos dados para os clientes e parceiros terceiros

Com esse método, você pode usar o AWS Amplify Auth para gerenciar o controle de acesso e a segurança dos arquivos. Esse método é ideal quando você deseja conectar os clientes ou parceiros terceiros aos dados no S3. Com essa opção, os clientes podem se autenticar usando provedores de identidades sociais ou corporativas.

Forneça credenciais do IAM para os usuários finais e parceiros terceiros usando o AWS Amplify Auth com um bucket do S3 configurado para usar o armazenamento do Amplify. O AWS Amplify Auth é baseado no Amazon Cognito, um serviço de gerenciamento de identidades e acesso de clientes totalmente gerenciado, em que você pode autenticar e autorizar usuários de um diretório de usuários integrado ou de um diretório corporativo, ou também de provedores de identidades de consumidores. O modelo de autorização do Amplify define quais prefixos o usuário autenticado atual pode acessar. Para ter mais informações sobre como configurar a autorização para o AWS Amplify, consulte Set up storage.

Para inicializar o componente com os métodos de autenticação e armazenamento do Amplify, adicione o seguinte trecho de código ao aplicativo web:

```
import {
  createAmplifyAuthAdapter,
  createStorageBrowser,
} from '@aws-amplify/ui-react-storage/browser';
import "@aws-amplify/ui-react-storage/styles.css";

import config from './amplify_outputs.json';

Amplify.configure(config);

export const { StorageBrowser } = createStorageBrowser({
  config: createAmplifyAuthAdapter(),
});
```

Método 2: gerenciar o acesso aos dados para as entidades principais do IAM da sua conta da AWS

Se você quiser gerenciar o acesso das entidades principais do IAM ou da sua Conta da AWS diretamente, poderá criar um perfil do IAM que tenha permissões para invocar a operação de API GetDataAccess do S3. Para configurar isso, você deve criar uma instância da Concessão de Acesso do S3 e associar as permissões para buckets de uso geral e prefixos do S3 às identidades do IAM especificadas. O componente Navegador de Armazenamento (que deve ser chamado do lado do cliente após a obtenção das credenciais do IAM) invocará então a operação de API ListCallerAccessGrants do S3 para buscar as concessões disponíveis para o solicitante de identidade e preencher os locais no componente. Depois de conseguir a permissão `s3:GetDataAccess`, essas credenciais são usadas pelo componente Navegador de Armazenamento para solicitar acesso aos dados no S3.

```
import {
  createManagedAuthAdapter,
  createStorageBrowser,
} from '@aws-amplify/ui-react-storage/browser';
import "@aws-amplify/ui-react-storage/styles.css";

export const { StorageBrowser } = createStorageBrowser({
  config: createManagedAuthAdapter({
    credentialsProvider: async (options?: { forceRefresh?: boolean }) => {
      // return your credentials object
      return {
        credentials: {
          accessKeyId: 'my-access-key-id',
          secretAccessKey: 'my-secret-access-key',
          sessionToken: 'my-session-token',
          expiration: new Date()
        },
      }
    },
    // AWS `region` and `accountId`
    region: '',
    accountId: '',
    // call `onAuthStateChange` when end user auth state changes
    // to clear sensitive data from the `StorageBrowser` state
    registerAuthListener: (onAuthStateChange) => {},
  })
});
```

Método 3: gerenciar o acesso aos dados em grande escala

Se você quiser associar uma instância da funcionalidade Concessão de Acesso do S3 ao Centro de Identidade do IAM para conseguir uma solução mais escalável (como fornecer acesso aos dados para toda a empresa), poderá solicitar dados do Amazon S3 em nome do usuário autenticado atual. Por exemplo, você pode conceder aos grupos de usuários no seu diretório corporativo acesso aos dados no S3. Essa abordagem permite que você gerencie centralmente as permissões da funcionalidade Concessão de Acesso do S3 para os usuários e grupos, incluindo aqueles hospedados em provedores externos, como Microsoft Entra, Okta e outros.

Ao usar esse método, a integração com o Centro de Identidade do IAM permite que você use os diretórios de usuários existentes. Outro benefício da propagação de identidades confiáveis do Centro de Identidade do IAM é que cada evento de dados do AWS CloudTrail para o Amazon S3 contém uma referência direta à identidade do usuário final que acessou os dados do S3.

Se você tiver uma aplicação compatível com o OAuth 2.0 e os usuários precisarem de acesso aos serviços da AWS por meio dessa aplicação, recomendamos que use a propagação de identidades confiáveis. Com a propagação de identidades confiáveis, um usuário pode fazer login em uma aplicação e essa aplicação pode transmitir a identidade do usuário em todas as solicitações que acessam dados nos serviços da AWS. Essa aplicação interage com o Centro de Identidade do IAM em nome de qualquer usuário autenticado. Para ter mais informações, consulte Using trusted identity propagation with customer managed applications.

A propagação de identidade confiável é um recurso do AWS IAM Identity Center que os administradores de Serviços da AWS conectados podem usar para conceder e auditar o acesso aos dados do serviço. O acesso a esses dados é baseado em atributos do usuário, como associações de grupo. A configuração da propagação de identidade confiável requer a colaboração entre os administradores de Serviços da AWS conectados e os administradores do Centro de Identidade do IAM. Para ter mais informações, consulte Prerequisites and considerations.

Configuração

Para configurar a autenticação do Navegador de Armazenamento no AWS Management Console usando a funcionalidade Concessão de Acesso do S3 e a propagação de identidades confiáveis do Centro de Identidade do IAM, as aplicações devem solicitar dados do Amazon S3 em nome do usuário autenticado atual. Com essa abordagem, você pode conceder aos usuários ou grupos de usuários do seu diretório corporativo acesso direto aos buckets, prefixos ou objetos do S3. Isso significa que a aplicação não precisará mapear nenhum usuário para nenhuma entidade principal do IAM.

O fluxo de trabalho a seguir descreve as etapas para configurar o Navegador de Armazenamento para S3 usando o Centro de Identidade do IAM e a funcionalidade Concessão de Acesso do S3:

Etapas	Descrição
1	Habilitar o Centro de Identidade do IAM para o AWS Organizations
2	Configurar a federação do Centro de Identidade do AWS Identity and Access Management
3	Adicionar um emissor de tokens confiáveis no console do Centro de Identidade do AWS Identity and Access Management O emissor de tokens confiáveis representa o provedor de identidades (IdP) externo no Centro de Identidade do IAM, permitindo que ele reconheça tokens de identidade para os usuários autenticados da aplicação.
4	Criar um perfil do IAM para a aplicação `bootstrap` e para `identity bearer`
5	Criar e configurar uma aplicação no Centro de Identidade do IAM Essa aplicação interage com o Centro de Identidade do IAM em nome dos usuários autenticados.
6	Adicionar a funcionalidade Concessão de Acesso do S3 como uma aplicação confiável para propagação de identidades Esta etapa conecta a aplicação à funcionalidade Concessão de Acesso do S3, para que ela possa fazer solicitações a essa funcionalidade em nome de usuários autenticados.
7	Criar uma concessão para um usuário ou grupo Esta etapa sincroniza os usuários do Centro de Identidade do AWS Identity and Access Management com o System for Cross-domain Identity Management (SCIM). O SCIM mantém

Etapas	Descrição
	as identidades do Centro de Identidade do IAM sincronizadas com as identidades do provedor de identidades (IdP).
8	Criar o componente Navegador de Armazenamento para S3

Habilitar o Centro de Identidade do IAM para o AWS Organizations

Para habilitar o Centro de identidade do IAM para o AWS Organizations, execute as seguintes etapas:

1. Faça login no AWS Management Console usando um dos seguintes métodos:
    1. Iniciante na AWS (usuário-raiz): faça login como proprietário da conta, escolhendo a opção Usuário-raiz e inserindo o endereço de e-mail da Conta da AWS. Na próxima página, insira a senha.
    2. Já usa a AWS (credenciais do IAM): faça login usando as credenciais do IAM com permissões administrativas.
2. Abra o console do IAM Identity Center.
3. Em Habilitar o IAM Identity Center, escolha Habilitar.

> **Note**
>
> O Centro de Identidade do IAM exige a configuração do AWS Organizations. Se você não configurou uma organização, pode optar para que a AWS crie uma para você. Escolha Criar organização da AWS para concluir esse processo.

4. Selecione Habilitar com AWS Organizations.
5. Escolha Continuar.
6. (Opcional) Adicione as tags que deseja associar a essa instância de organização.
7. (Opcional) Configure a administração delegada.

> **Note**
>
> Se você estiver usando um ambiente com várias contas, recomendamos que configure a administração delegada. Com a administração delegada, você pode limitar o número

de pessoas que precisam de acesso à conta de gerenciamento no AWS Organizations. Para ter mais informações, consulte Delegated administration.

8. Escolha Salvar.

A AWS Organizations envia um e-mail de verificação automaticamente para o endereço associado à sua conta de gerenciamento. Talvez haja um atraso até você receber o e-mail de verificação. Verifique seu endereço de e-mail dentro de 24 horas, antes que o e-mail de verificação expire.

Configurar a federação do Centro de Identidade do AWS Identity and Access Management

Para usar o Navegador de Armazenamento para S3 com usuários do diretório corporativo, você deve configurar o Centro de Identidade do IAM para usar um provedor de identidades (IdP) externo. Você pode usar o provedor de identidades de sua escolha. No entanto, esteja ciente de que cada provedor de identidades usa configurações diferentes. Para tutoriais sobre como usar diferentes provedores de identidades externos, consulte IAM Identity Center source tutorials.

> **Note**
>
> Registre o URL do emissor e os atributos de público do provedor de identidades que você configurou, pois precisará consultá-los em etapas posteriores. Se você não tiver o acesso ou as permissões necessárias para configurar um IdP, talvez precise entrar em contato com o administrador do IdP externo para obtê-los.

Adicionar um emissor de tokens confiáveis no console do Centro de Identidade do AWS Identity and Access Management

O emissor de tokens confiáveis representa o provedor de identidades externo no Centro de Identidade do AWS Identity and Access Management e reconhece os tokens para os usuários autenticados da aplicação. O proprietário da conta da instância do Centro de Identidade do IAM no AWS Organizations deve executar essas etapas. Essas etapas podem ser executadas no console do Centro de Identidade do IAM ou de maneira programática.

Para adicionar um emissor de tokens confiáveis no console do Centro de Identidade do AWS Identity and Access Management, execute as seguintes etapas:

1. Abra o console do IAM Identity Center.

2. Escolha Settings.
3. Escolha a guia Autenticação.
4. Navegue até a seção Emissores de tokens confiáveis e preencha os seguintes detalhes:
    1. Em URL do emissor, insira o URL do IdP externo que serve como emissor de tokens confiáveis. Talvez seja necessário entrar em contato com o administrador do IdP externo para ter essas informações. Para ter mais informações, consulte Using applications with a trusted token issuer.
    2. Em Nome do emissor de tokens confiáveis, insira um nome para o emissor de tokens confiáveis. Esse nome aparecerá na lista de emissores de tokens confiáveis que você pode selecionar na Etapa 8, quando um recurso da aplicação for configurado para propagação de identidades.
5. Atualize os Atributos de mapeamento para o atributo de aplicação de sua preferência, em que o atributo de cada provedor de identidades é mapeado para um atributo do Centro de Identidade do IAM. Por exemplo, você pode mapear o atributo `email` da aplicação para o atributo `email` do usuário do Centro de Identidade do IAM. Para ver a lista de atributos de usuário permitidos no Centro de Identidade do IAM, consulte a tabela em Attribute mappings for AWS Managed Microsoft AD directory.
6. (Opcional) Se você quiser adicionar uma tag de recurso, insira o par de chave/valor. Para adicionar várias tags de recursos, escolha Adicionar nova tag para gerar uma nova entrada e inserir os pares de chave/valor.
7. Escolha Criar emissor de tokens confiáveis.
8. Depois de concluir a criação do emissor de tokens confiáveis, entre em contato com o administrador da aplicação para informar o nome do emissor de tokens confiáveis, para que ele possa confirmar que o emissor de tokens confiáveis está visível no console aplicável.
9. Garanta que o administrador da aplicação selecione esse emissor de tokens confiáveis no console aplicável para permitir o acesso do usuário à aplicação usando as aplicações configuradas para a propagação de identidades confiáveis.

Criar um perfil do IAM para a aplicação **`bootstrap`** e para **`identity bearer`**

Para garantir que a aplicação `bootstrap` e os usuários de `identity bearer` possam trabalhar adequadamente entre si, crie dois perfis do IAM. Um perfil do IAM é necessário para a aplicação `bootstrap` e o outro perfil do IAM deve ser usado para o portador da identidade ou para os usuários finais que estão acessando o aplicativo web que solicita acesso por meio da funcionalidade

Concessão de Acesso do S3. A aplicação `bootstrap` recebe o token emitido pelo provedor de identidades e invoca a API `CreateTokenWithIAM`, trocando esse token pelo token emitido pelo Centro de Identidade.

Crie um perfil do IAM, como `bootstrap-role`, com permissões como as mostradas a seguir. O seguinte exemplo de política do IAM concede permissões a `bootstrap-role` para realizar a troca de tokens:

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": [
            "sso-oauth:CreateTokenWithIAM",
        ],
        "Resource": "arn:${Partition}:sso::${AccountId}:application/${InstanceId}/
${ApplicationId}",
        "Effect": "Allow"
    },
    {
        "Action": [
            "sts:AssumeRole",
            "sts:SetContext"
        ],
        "Resource": "arn:aws:iam::${AccountId}:role/identity-bearer-role",
        "Effect": "Allow"
    }]
}
```

Depois, crie outro perfil do IAM (como `identity-bearer-role`) que o intermediador de identidades usa para gerar as credenciais do IAM. As credenciais do IAM retornadas do intermediador de identidades para o aplicativo web são usadas pelo componente Navegador de Armazenamento para S3 a fim de permitir o acesso aos dados do S3:

```
{
    "Action": [
        "s3:GetDataAccess",
        "s3:ListCallerAccessGrants",
    ],
    "Resource": "arn:${Partition}:s3:${Region}:${Account}:access-grants/default",
    "Effect": "Allow"
}
```

Esse perfil do IAM (`identity-bearer-role`) deve usar uma política de confiança com a seguinte instrução:

```
{
   "Effect": "Allow",
   "Principal": {
      "AWS": "arn:${Partition}:iam::${Account}:role/${RoleNameWithPath}"
   },
   "Action": [
       "sts:AssumeRole",
       "sts:SetContext"
   ]
}
```

Criar e configurar uma aplicação no Centro de Identidade do IAM

> **Note**
>
> Antes de começar, confirme que você criou os perfis do IAM necessários na etapa anterior. Você precisará especificar um desses perfis do IAM nesta etapa.

Para criar e configurar uma aplicação gerenciada pelo cliente no Centro de Identidade do AWS IAM, execute as seguintes etapas:

1. Abra o console do IAM Identity Center.
2. Selecione Aplicações.
3. Escolha a guia Gerenciada pelo cliente.
4. Escolha Adicionar aplicação.
5. Na página Selecionar tipo de aplicação, em Preferências de configuração, escolha Eu tenho uma aplicação que quero configurar.
6. Em Tipo de aplicação, escolha OAuth 2.0.
7. Escolha Próximo. A página Especificar aplicação é exibida.
8. Na seção Nome e descrição da aplicação, insira um Nome de exibição para a aplicação, como **`storage-browser-oauth`**.
9. Insira uma Descrição. A descrição da aplicação aparece somente no console do Centro de Identidade do IAM e nas solicitações de API, não no portal de acesso da AWS.

10. Em Método de atribuição de usuários e grupos, escolha Não exigir atribuições. Essa opção permita que todos os usuários e grupos autorizados do Centro de Identidade do IAM acessem essa aplicação.
11. Em Portal de acesso da AWS, insira um URL de aplicação onde os usuários possam acessar a aplicação.
12. (Opcional) Se você quiser adicionar uma tag de recurso, insira o par de chave/valor. Para adicionar várias tags de recursos, escolha Adicionar nova tag para gerar uma nova entrada e inserir os pares de chave/valor.
13. Escolha Próximo. A página Especificar autenticação é exibida.
14. Em Autenticação com emissor de tokens confiáveis, use a caixa de seleção para selecionar o emissor de tokens confiáveis que você criou anteriormente.
15. Em Configurar os emissores de tokens confiáveis selecionados, insira a declaração aud. A declaração aud identifica o público do token JSON da web (JWT) e é o nome pelo qual o emissor de tokens confiáveis identifica essa aplicação.

    > **Note**
    >
    > Talvez seja necessário entrar em contato com o administrador do IdP externo para ter essas informações.

16. Escolha Próximo. A página Especificar credenciais de autenticação é exibida.
17. Em Método de configuração, escolha Inserir um ou mais perfis do IAM.
18. Em Inserir perfis do IAM, adicione o perfil do IAM ou o nome do recurso da Amazon (ARN) para o token do portador da identidade. Você deve inserir o perfil do IAM que criou na etapa anterior para a aplicação do intermediador de identidades (por exemplo, **`bootstrap-role`**).
19. Escolha Próximo.
20. Na página Revisar e configurar, revise os detalhes da configuração da aplicação. Se você precisar modificar qualquer uma das configurações, escolha Editar para a seção que deseja editar e faça as alterações.
21. Selecione Enviar. É exibida a página de detalhes da aplicação que acabou de adicionar.

Depois que você configurou as aplicações, os usuários podem acessá-las no portal de acesso da AWS com base nos conjuntos de permissões que você criou e no acesso de usuário que você atribuiu.

Adicionar a funcionalidade Concessão de Acesso do S3 como uma aplicação confiável para propagação de identidades

Depois de configurar a aplicação gerenciada pelo cliente, você deve especificar a funcionalidade Concessão de Acesso do S3 para a propagação de identidades. A funcionalidade Concessão de Acesso do S3 fornece credenciais para que os usuários acessem os dados do Amazon S3. Quando você faz login na aplicação gerenciada pelo cliente, a funcionalidade Concessão de Acesso do S3 envia sua identidade de usuário para a aplicação confiável.

Pré-requisito: configure a funcionalidade Concessão de Acesso do S3 (como criar uma instância da funcionalidade Concessão de Acesso do S3 e registrar um local) antes de seguir estas etapas. Para ter mais informações, consulte Conceitos básicos da funcionalidade Concessões de Acesso do S3.

Para adicionar a funcionalidade Concessão de Acesso do S3 para propagação de identidades à aplicação gerenciada pelo cliente, execute as seguintes etapas:

1. Abra o console do IAM Identity Center.
2. Selecione Aplicações.
3. Escolha a guia Gerenciada pelo cliente.
4. Na lista Aplicações gerenciadas pelo cliente, selecione a aplicação OAuth 2.0 para a qual você deseja inicializar solicitações de acesso. Essa é a aplicação na qual os usuários farão login.
5. Na página Detalhes, em Aplicações confiáveis para a propagação de identidades, escolha Especificar aplicações confiáveis.
6. Em Tipo de configuração, selecione Aplicações individuais e especificar acesso e escolha Avançar.
7. Na página Selecionar serviço, escolha Concessão de Acesso do S3. A funcionalidade Concessão de Acesso do S3 tem aplicações que você pode usar para definir seu próprio aplicativo web para propagação de identidades confiáveis.
8. Escolha Próximo. Você selecionará as aplicações na próxima etapa.
9. Na página Selecionar aplicações, escolha Aplicações individuais, marque a caixa de seleção de cada aplicação que pode receber solicitações de acesso e escolha Avançar.
10. Na página Configurar acesso, em Método de configuração, escolha uma das seguintes opções:

    - Selecionar acesso por aplicação: selecione essa opção para configurar diferentes níveis de acesso para cada aplicação. Escolha a aplicação para a qual você deseja configurar o nível de acesso e depois escolha Editar acesso. Em Nível de acesso a ser aplicado, altere os níveis de acesso conforme necessário e escolha Salvar alterações.

- Aplicar o mesmo nível de acesso a todos as aplicações: selecione essa opção se você não precisar configurar níveis de acesso por aplicação.

11. Escolha Próximo.
12. Na página Revisar configuração, revise as escolhas que fez.

> **Note**
>
> Você deve garantir que a permissão `s3:access_grants:read_write` seja concedida aos usuários. Essa permissão possibilita que os usuários recuperem credenciais para acessar o Amazon S3. Use a política do IAM que você criou anteriormente ou a funcionalidade Concessão de Acesso do S3 para limitar o acesso às operações de gravação.

13. Para fazer alterações, escolha Editar para a seção de configuração que deseja alterar. Em seguida, faça as alterações necessárias e selecione Salvar alterações.
14. Escolha Aplicações confiáveis para adicionar a aplicação confiável para propagação de identidades.

Criar uma concessão para um usuário ou grupo

Nesta etapa, você usa o Centro de Identidade do IAM para provisionar os usuários. Você pode usar o SCIM para provisionamento de usuários e grupos de maneira automatizada ou manual. O SCIM mantém as identidades do Centro de Identidade do IAM sincronizadas com as identidades do provedor de identidades (IdP). Isso inclui qualquer provisionamento, atualizações e desprovisionamento de usuários entre seu IdP e o IAM Identity Center.

> **Note**
>
> Essa etapa é necessária porque, quando a funcionalidade Concessão de Acesso do S3 é usada com o Centro de Identidade do IAM, os usuários locais do Centro de Identidade do IAM não são usados. Em vez disso, os usuários devem ser sincronizados do provedor de identidades com o Centro de Identidade do IAM.

Para sincronizar usuários do seu provedor de identidades com o Centro de Identidade do IAM, execute as seguintes etapas:

1. Habilitar o provisionamento automático.
2. Gerar um token de acesso.

Para ver exemplos de como configurar o provedor de identidades com o Centro de Identidade do IAM para um caso de uso específico, consulte IAM Identity Center Identity source tutorials.

Criar o componente Navegador de Armazenamento para S3

Depois de configurar a instância do Centro de Identidade do IAM e criar concessões na funcionalidade Concessão de Acesso do S3, abra a aplicação React. Na aplicação React, use `createManagedAuthAdapter` para configurar as regras de autorização. Você deve fornecer um provedor de credenciais para retornar as credenciais obtidas do Centro de Identidade do IAM. Depois, você pode chamar `createStorageBrowser` para inicializar o componente Navegador de Armazenamento para S3:

```
import {
    createManagedAuthAdapter,
    createStorageBrowser,
} from '@aws-amplify/ui-react-storage/browser';
import '@aws-amplify/ui-react-storage/styles.css';

export const { StorageBrowser } = createStorageBrowser({
   config: createManagedAuthAdapter({
    credentialsProvider: async (options?: { forceRefresh?: boolean }) => {
      // return your credentials object
      return {
        credentials: {
          accessKeyId: 'my-access-key-id',
          secretAccessKey: 'my-secret-access-key',
          sessionToken: 'my-session-token',
          expiration: new Date(),
        },
      }
    },
    // AWS `region` and `accountId` of the S3 Access Grants Instance.
    region: '',
    accountId: '',
    // call `onAuthStateChange` when end user auth state changes
    // to clear sensitive data from the `StorageBrowser` state
    registerAuthListener: (onAuthStateChange) => {},
  })
```

```
});
```

Em seguida, crie um mecanismo para trocar os tokens JSON da web (JWTs) do aplicativo web com as credenciais do IAM do Centro de Identidade do IAM. Para ter mais informações sobre como trocar o JWT, consulte os seguintes recursos:

- Publicação How to develop a user-facing data application with IAM Identity Center and S3 Access Grants no AWS Storage Blog
- Publicação Scaling data access with S3 Access Grants no AWS Storage Blog
- S3 Access Grants workshop no AWS workshop studio
- S3 Access Grants workshop no GitHub

Depois, configure um endpoint de API para lidar com solicitações de busca de credenciais. Para validar a troca de tokens JSON da web (JWTs), execute as seguintes etapas:

1. Recupere o token JSON da web do cabeçalho de autorização para solicitações recebidas.
2. Valide o token usando as chaves públicas do URL do conjunto de chaves JSON da web (JWKS) especificado.
3. Verifique a expiração do token, o emissor, o assunto e as reivindicações de público.

Para trocar o token JSON da web do provedor de identidades por credenciais do AWS IAM, execute as seguintes etapas:

> **Tip**
>
> Evite evitar registrar qualquer informação confidencial. Recomendamos que você use controles de tratamento de erros para autorizações ausentes, tokens expirados e outras exceções. Para ter mais informações, consulte a publicação Implementing AWS Lambda error handling patterns no AWS Compute Blog.

1. Verifique se os parâmetros Permissão e Escopo necessários foram fornecidos na solicitação.
2. Use a API CreateTokenWithIAM para trocar o token JSON da web por um token do Centro de Identidade do IAM.

> **Note**
>
> Depois que o token JSON da web do IdP é usado, ele não pode ser usado novamente. Um novo token deve ser usado para troca com o Centro de Identidade do IAM.

3. Use a operação de API AssumeRole para assumir um perfil transitório usando o token do Centro de Identidade do IAM. Use o perfil do portador da identidade, também conhecido como perfil que carrega o contexto da identidade (por exemplo, **`identity-bearer-role`**) para solicitar as credenciais.
4. Retorne as credenciais do IAM para o aplicativo web.

> **Note**
>
> Confirme que você configurou um mecanismo de registro em log adequado. As respostas são retornadas em um formato JSON padronizado com um código de status HTTP apropriado.

Configurar o Navegador de Armazenamento para S3

Para permitir que o Navegador de Armazenamento para S3 acesse os buckets do S3, o componente Navegador de Armazenamento faz chamadas de API REST para o Amazon S3. Por padrão, o compartilhamento de recursos entre origens (CORS) não está habilitado nos buckets do S3. Como resultado, você deve habilitar o CORS para cada bucket do S3 do qual o Navegador de Armazenamento acessa dados.

Por exemplo, para habilitar o CORS no bucket do S3, você pode atualizar a política de CORS da seguinte forma:

```
[
    {
        "ID": "S3CORSRuleId1",
        "AllowedHeaders": [
            "*"
        ],
        "AllowedMethods": [
            "GET",
            "HEAD",
```

```
            "PUT",
            "POST",
            "DELETE"
        ],
        "AllowedOrigins": [
            "*"
        ],
        "ExposeHeaders": [
            "last-modified",
            "content-type",
            "content-length",
            "etag",
            "x-amz-version-id",
            "x-amz-request-id",
            "x-amz-id-2",
            "x-amz-cf-id",
            "x-amz-storage-class",
            "date",
            "access-control-expose-headers"
        ],
        "MaxAgeSeconds": 3000
    }
]
```

Solução de problemas do Navegador de Armazenamento para S3

Se você estiver enfrentando problemas com o Navegador de Armazenamento para S3, consulte as seguintes dicas de solução de problemas:

- Evite tentar usar o mesmo token (`idToken` ou `accessToken`) para várias solicitações. Os tokens não podem ser reutilizados. Isso resultará em falha na solicitação.
- Garanta que as credenciais do IAM que você fornece ao componente Navegador de Armazenamento incluam permissões para invocar a operação `s3:GetDataAccess`. Caso contrário, os usuários finais não poderão acessar os dados.

Como alternativa, você pode consultar os seguintes recursos:

- O Navegador de Armazenamento para S3 recebe suporte do AWS Support. Se precisar de ajuda, entre em contato com o AWS Support Center.

- Se você estiver tendo problemas com o Navegador de Armazenamento para S3 ou quiser enviar feedback, acesse a página do Amplify no GitHub.
- Se você descobrir um possível problema de segurança nesse projeto, pedimos que notifique a equipe de segurança da AWS por meio da página Relatório de vulnerabilidade da AWS.

Configurar transferências de arquivos rápidas e seguras usando o Amazon S3 Transfer Acceleration

A Aceleração de Transferências do Amazon S3 é um recurso em nível de bucket que possibilita transferências de arquivos rápidas, fáceis e seguras em longas distâncias entre o cliente e um bucket de uso geral do S3. A Aceleração de Transferências foi projetada para otimizar as velocidades de transferência ao redor do mundo para buckets de uso geral do S3. O Transfer Acceleration tira proveito dos pontos de presença distribuídos globalmente no Amazon CloudFront. Conforme os dados chegam em um ponto de presença, eles são roteados para o Amazon S3 por um caminho de rede otimizado.

Quando você usa o Transfer Acceleration, podem ser aplicadas cobranças adicionais de transferência de dados. Para obter mais informações sobre a definição de preços, consulte Definição de preços do Amazon S3.

Por que usar o Transfer Acceleration?

Você pode usar a Aceleração de Transferências em um bucket de uso geral por vários motivos:

- Seus clientes fazem upload em um bucket de uso geral centralizado do mundo todo.
- Você transfere gigabytes a terabytes de dados regularmente entre continentes.
- Não é possível utilizar toda a largura de banda disponível via Internet ao fazer upload para o Amazon S3.

Para obter mais informações sobre quando usar o Transfer Acceleration, consulte Perguntas frequentes do Amazon S3.

Requisitos para usar o Transfer Acceleration

Veja o que é necessário ao usar o Transfer Acceleration em um bucket do S3:

- O Transfer Acceleration só tem suporte em solicitações de estilo hospedadas virtualmente. Consulte mais informações sobre solicitações de estilo hospedadas virtualmente em Making requests using the REST API na Referência de API do Amazon S3.
- O nome do bucket usado para o Transfer Acceleration deve ser compatível com DNS e não deve conter pontos (“.”).
- O Transfer Acceleration deve estar ativado no bucket. Para obter mais informações, consulte Habilitar e usar o S3 Transfer Acceleration.

  Depois de habilitar o Transfer Acceleration em um bucket, pode levar até 20 minutos para que a velocidade da transferência de dados para o bucket aumente.

  > **Note**
  >
  > No momento, o Transfer Acceleration é compatível com buckets localizados nas seguintes regiões:
  >
  > - Ásia Pacific (Tóquio) (ap-northeast-1)
  > - Ásia-Pacífico (Seul) (ap-northeast-2)
  > - Ásia-Pacífico (Mumbai) (ap-south-1)
  > - Ásia-Pacífico (Singapura) (ap-southeast-1)
  > - Ásia-Pacífico (Sydney) (ap-southeast-2)
  > - Canadá (Central) (ca-central-1)
  > - Europa (Frankfurt) (eu-central-1)
  > - Europa (Irlanda) (eu-west-1)
  > - Europa (Londres) (eu-west-2)
  > - Europa (Paris) (eu-west-3)
  > - América do Sul (São Paulo) (sa-east-1)
  > - Leste dos EUA (Norte da Virgínia) (us-east-1)
  > - Leste dos EUA (Ohio) (us-east-2)
  > - Oeste dos EUA (Norte da Califórnia) (us-west-1)
  > - Oeste dos EUA (Oregon) (us-west-2)

- Para acessar o bucket que está habilitado para o Transfer Acceleration, você deve usar o endpoint *bucket-name*`.s3-accelerate.amazonaws.com`. Ou use o endpoint de pilha dupla *bucket-*

name.s3-accelerate.dualstack.amazonaws.com para se conectar ao bucket habilitado por IPv6. Você pode continuar usando os endpoints regulares para a transferência de dados padrão.

- Você deve ser o proprietário do bucket para configurar o estado de aceleração de transferência. O proprietário do bucket pode designar permissões para outros usuários para permitir que eles definam o estado de aceleração em um bucket. A permissão `s3:PutAccelerateConfiguration` autoriza os usuários a habilitarem ou desabilitarem o Transfer Acceleration em um bucket. A permissão `s3:GetAccelerateConfiguration` autoriza os usuários a retornar o estado do Transfer Acceleration de um bucket, que é `Enabled` ou `Suspended`.

As seções a seguir descrevem como começar a usar o Amazon S3 Transfer Acceleration para transferir dados.

Tópicos

- Conceitos básicos do Amazon S3 Transfer Acceleration
- Habilitar e usar o S3 Transfer Acceleration
- Usar a ferramenta de comparação de velocidade do Amazon S3 Transfer Acceleration

Conceitos básicos do Amazon S3 Transfer Acceleration

Você pode usar o Amazon S3 Transfer Acceleration para transferências de arquivos rápidas, fáceis e seguras em longas distâncias entre o seu cliente e um bucket do S3. O Transfer Acceleration usa os pontos de presença distribuídos globalmente no Amazon CloudFront. Conforme os dados chegam em um ponto de presença, eles são roteados para o Amazon S3 por um caminho de rede otimizado.

Para começar a usar o Amazon S3 Transfer Acceleration, execute as seguintes etapas:

1. Habilitar o Transfer Acceleration em um bucket

   Você pode ativar o Transfer Acceleration em um bucket de qualquer uma das seguintes maneiras:

   - Use o console do Amazon S3.
   - Use a operação PutBucketAccelerateConfiguration da API REST.
   - Use a AWS CLI e os AWS SDKs. Consulte mais informações em Developing with Amazon S3 using the AWS SDKs na Referência de API do Amazon S3.

   Para obter mais informações, consulte Habilitar e usar o S3 Transfer Acceleration.

> **Note**
>
> Para que o bucket funcione com a aceleração de transferência, o nome dele deve estar em conformidade com os requisitos de nomenclatura de DNS e não deve conter pontos (.).

2. Transferir dados de e para o bucket habilitado para aceleração

   Use um dos seguintes nomes de domínio de endpoint do `s3-accelerate`:

   - Para acessar um bucket habilitado para aceleração, use *`bucket-name`*`.s3-accelerate.amazonaws.com`.
   - Para acessar um bucket habilitado para aceleração por IPv6, use *`bucket-name`*`.s3-accelerate.dualstack.amazonaws.com`.

     Os endpoints de pilha dupla do Amazon S3 oferecem suporte para buckets do S3 por IPv6 e IPv4. O endpoint de pilha dupla do Transfer Acceleration usa somente o tipo virtual hospedado de nome do endpoint. Consulte mais informações em Making requests to Amazon S3 over IPv6 na Referência de API do Amazon S3 e em Using Amazon S3 dual-stack endpoints na Referência de API do Amazon S3.

   > **Note**
   >
   > A aplicação de transferência de dados deve usar um dos dois tipos de endpoints a seguir para acessar o bucket e agilizar a transferência de dados: `.s3-accelerate.amazonaws.com` ou `.s3-accelerate.dualstack.amazonaws.com` para o endpoint de pilha dupla. Se quiser usar a transferência de dados padrão, você poderá continuar usando os endpoints regulares.

Você pode apontar as solicitações de PUT object e GET object do Amazon S3 para o nome de domínio do endpoint do `s3-accelerate` depois de habilitar o recurso Aceleração de Transferências. Por exemplo, suponha que você tenha atualmente uma aplicação de API REST que esteja usando PutObject com o nome de host *`amzn-s3-demo-bucket`*`.s3.us-east-1.amazonaws.com` na solicitação PUT. Para acelerar o PUT, altere o nome do host em sua solicitação para *`amzn-s3-demo-bucket`*`.s3-accelerate.amazonaws.com`. Para

voltar a usar a velocidade de upload padrão, altere o nome de volta para *amzn-s3-demo-bucket*.s3.us-east-1.amazonaws.com.

Depois que o Transfer Acceleration é ativado, pode demorar 20 minutos para você perceber o benefício da performance. Contudo, o endpoint de aceleração estará disponível assim que você habilitar o Transfer Acceleration.

Você pode usar o endpoint de aceleração na AWS CLI, em AWS SDKs e em outras ferramentas que transferem dados para e do Amazon S3. Se você estiver usando AWS SDKs, algumas linguagens compatíveis usam uma sinalização de configuração de cliente do endpoint de aceleração para que você não precise definir explicitamente o endpoint do Transfer Acceleration como *bucket-name*.s3-accelerate.amazonaws.com. Para ver exemplos de como usar uma sinalização de configuração de cliente do endpoint de aceleração, consulte Habilitar e usar o S3 Transfer Acceleration.

Você pode usar todas as operações do Amazon S3 por meio dos endpoints de aceleração de transferência, exceto as seguintes:

- ListBuckets
- CreateBucket
- DeleteBucket

Além disso, a Aceleração de Transferências do Amazon S3 não permite o uso de CopyObject para cópias entre regiões.

Habilitar e usar o S3 Transfer Acceleration

É possível usar a Aceleração de Transferências do Amazon S3 para transferir arquivos com rapidez e segurança por longas distâncias entre o cliente e um bucket de uso geral do S3. Você pode habilitar a Aceleração de Transferências usando o console do S3, a AWS Command Line Interface (AWS CLI), a API ou os AWS SDKs.

Esta seção fornece exemplos de como ativar o Amazon S3 Transfer Acceleration em um bucket e usar o endpoint de aceleração para o bucket ativado.

Para obter mais informações sobre os requisitos do Transfer Acceleration, consulte Configurar transferências de arquivos rápidas e seguras usando o Amazon S3 Transfer Acceleration.

Usar o console do S3

> **Note**
>
> Se você quiser comparar velocidades de upload aceleradas e não aceleradas, abra a ferramenta Comparação de velocidade do Amazon S3 Transfer Acceleration.
> A ferramenta de Comparação de velocidade usa o carregamento fracionado para transferir um arquivo do seu navegador para várias Regiões da AWS com e sem o uso do Amazon S3 Transfer Acceleration. É possível comparar a velocidade de upload para uploads diretos e uploads de transferência acelerada por região.

Como habilitar a aceleração de transferência para um bucket de uso geral do S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets de uso geral.
3. Na lista Buckets de uso geral, escolha o nome do bucket no qual você deseja habilitar a aceleração de transferência.
4. Escolha Properties (Propriedades).
5. Em Transfer acceleration (Aceleração de transferência), escolha Edit (Editar).
6. Escolha Enable (Habilitar) e Save changes (Salvar alterações).

Para acessar transferências de dados aceleradas

1. Depois que o Amazon S3 habilitar a aceleração de transferência para seu bucket, visualize a guia Properties (Propriedades) do bucket.
2. Em Transfer acceleration (Aceleração de transferência), o Accelerated endpoint (Endpoint acelerado) exibe o endpoint de aceleração de transferência para o bucket. Use esse endpoint para acessar transferências de dados aceleradas do bucket e para ele.

   Se você suspender a Transfer Acceleration, o endpoint de aceleração não funcionará mais.

Como usar o AWS CLI

Veja a seguir exemplos de comandos da AWS CLI usados para o Transfer Acceleration. Consulte instruções sobre como configurar a AWS CLI em Developing with Amazon S3 using the AWS CLI na Referência de API do Amazon S3.

Habilitar o Transfer Acceleration em um bucket

Use o comando put-bucket-accelerate-configuration da AWS CLI para habilitar ou suspender a Aceleração de Transferências em um bucket.

O exemplo a seguir define `Status=Enabled` para habilitar a Aceleração de Transferências em um bucket chamado *`amzn-s3-demo-bucket`*. Para suspender a Aceleração de Transferências, use `Status=Suspended`.

Example

```
$ aws s3api put-bucket-accelerate-configuration --bucket amzn-s3-demo-bucket --
accelerate-configuration Status=Enabled
```

Habilitar o Transfer Acceleration

É possível direcionar todas as solicitações do Amazon S3 feitas pelos comandos `s3` e `s3api` da AWS CLI ao endpoint de aceleração: `s3-accelerate.amazonaws.com`. Para fazer isso, defina o valor de configuração de `use_accelerate_endpoint` como `true` em um perfil no arquivo do AWS Config. O Transfer Acceleration deve ser ativado em seu bucket para usar o endpoint de aceleração.

Todas as solicitações são enviadas usando o estilo virtual de endereçamento de bucket: *`amzn-s3-demo-bucket`*`.s3-accelerate.amazonaws.com`. Nenhuma solicitação `ListBuckets`, `CreateBucket` e `DeleteBucket` será enviada ao endpoint de aceleração porque esse endpoint não é compatível com essas operações.

Para obter mais informações sobre `use_accelerate_endpoint`, consulte Configuração do S3 com a AWS CLI na Referência de comandos da AWS CLI.

O exemplo a seguir define `use_accelerate_endpoint` como `true` no perfil padrão.

Example

```
$ aws configure set default.s3.use_accelerate_endpoint true
```

Se você quiser usar o endpoint de aceleração para alguns comandos da AWS CLI, mas não para outros, use qualquer um destes dois métodos:

- Use o endpoint de aceleração para qualquer comando `s3` ou `s3api` definindo o parâmetro `--endpoint-url` como `https://s3-accelerate.amazonaws.com`.
- Configure perfis separados no arquivo do AWS Config. Por exemplo, crie um perfil que defina `use_accelerate_endpoint` como `true` e um perfil que não defina `use_accelerate_endpoint`. Ao executar um comando, especifique qual perfil deseja usar, caso queira ou não usar o endpoint de aceleração.

Fazer upload de um objeto em um bucket habilitado para o Transfer Acceleration

O exemplo a seguir faz upload de um arquivo em um bucket chamado *amzn-s3-demo-bucket* que foi habilitado para a Aceleração de Transferências usando o perfil padrão configurado para usar o endpoint de aceleração.

Example

```
$ aws s3 cp file.txt s3://amzn-s3-demo-bucket/key-name --region region
```

O exemplo a seguir faz upload de um arquivo em um bucket habilitado para o Transfer Acceleration usando o parâmetro `--endpoint-url` para especificar o endpoint de aceleração.

Example

```
$ aws configure set s3.addressing_style virtual
$ aws s3 cp file.txt s3://amzn-s3-demo-bucket/key-name --region region --endpoint-url
 https://s3-accelerate.amazonaws.com
```

Uso dos SDKs da AWS

Veja a seguir exemplos de uso do Transfer Acceleration para fazer upload de objetos para o Amazon S3 usando o AWS SDK. Algumas linguagens compatíveis com o SDK da AWS (por exemplo, Java e .NET) usam uma sinalização de configuração de cliente do endpoint de aceleração para que você não precise definir explicitamente o endpoint da Aceleração de Transferências como *bucket-name*`.s3-accelerate.amazonaws.com`.

Java

Example

O exemplo a seguir mostra como usar um endpoint de aceleração para fazer upload de um objeto no Amazon S3. O exemplo faz o seguinte:

- Cria um `AmazonS3Client` que é configurado para usar endpoints de aceleração. Todos os buckets acessados pelo cliente devem ter o Transfer Acceleration habilitado.
- Habilita o Transfer Acceleration em um bucket especificado. Essa etapa é necessária somente se o bucket que você especificar não tiver o Transfer Acceleration habilitado ainda.
- Verifica se a aceleração da transferência está habilitada para o bucket especificado.
- Faz upload de um novo objeto para o bucket especificado usando o endpoint de aceleração do bucket.

Para obter mais informações sobre o Transfer Acceleration, consulte Conceitos básicos do Amazon S3 Transfer Acceleration. Consulte instruções sobre como criar e testar uma amostra funcional em Getting Started no Guia do desenvolvedor do AWS SDK para Java.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.BucketAccelerateConfiguration;
import com.amazonaws.services.s3.model.BucketAccelerateStatus;
import com.amazonaws.services.s3.model.GetBucketAccelerateConfigurationRequest;
import com.amazonaws.services.s3.model.SetBucketAccelerateConfigurationRequest;

public class TransferAcceleration {
    public static void main(String[] args) {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "*** Bucket name ***";
        String keyName = "*** Key name ***";

        try {
            // Create an Amazon S3 client that is configured to use the accelerate
 endpoint.
```

```
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withRegion(clientRegion)
                    .withCredentials(new ProfileCredentialsProvider())
                    .enableAccelerateMode()
                    .build();

            // Enable Transfer Acceleration for the specified bucket.
            s3Client.setBucketAccelerateConfiguration(
                    new SetBucketAccelerateConfigurationRequest(bucketName,
                            new BucketAccelerateConfiguration(
                                    BucketAccelerateStatus.Enabled)));

            // Verify that transfer acceleration is enabled for the bucket.
            String accelerateStatus = s3Client.getBucketAccelerateConfiguration(
                    new GetBucketAccelerateConfigurationRequest(bucketName))
                    .getStatus();
            System.out.println("Bucket accelerate status: " + accelerateStatus);

            // Upload a new object using the accelerate endpoint.
            s3Client.putObject(bucketName, keyName, "Test object for transfer
 acceleration");
            System.out.println("Object \"" + keyName + "\" uploaded with transfer
 acceleration.");
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

.NET

O exemplo a seguir mostra como usar o AWS SDK para .NET para habilitar o Transfer Acceleration em um bucket. Consulte informações sobre como configurar e executar exemplos de código, em Getting Started with the AWS SDK para .NET no Guia do desenvolvedor do AWS SDK para .NET.

Example

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class TransferAccelerationTest
    {
        private const string bucketName = "*** bucket name ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 s3Client;
        public static void Main()
        {
            s3Client = new AmazonS3Client(bucketRegion);
            EnableAccelerationAsync().Wait();
        }

        static async Task EnableAccelerationAsync()
        {
                try
                {
                    var putRequest = new PutBucketAccelerateConfigurationRequest
                    {
                        BucketName = bucketName,
                        AccelerateConfiguration = new AccelerateConfiguration
                        {
                            Status = BucketAccelerateStatus.Enabled
                        }
                    };
                    await
 s3Client.PutBucketAccelerateConfigurationAsync(putRequest);

                    var getRequest = new GetBucketAccelerateConfigurationRequest
                    {
                        BucketName = bucketName
                    };
                    var response = await
 s3Client.GetBucketAccelerateConfigurationAsync(getRequest);
```

```
                    Console.WriteLine("Acceleration state = '{0}' ",
 response.Status);
                }
                catch (AmazonS3Exception amazonS3Exception)
                {
                    Console.WriteLine(
                        "Error occurred. Message:'{0}' when setting transfer
 acceleration",
                        amazonS3Exception.Message);
                }
        }
    }
}
```

Ao fazer upload de um objeto a um bucket com Transfer Acceleration habilitado, especifique usando o endpoint de aceleração no momento da criação de um cliente.

```
var client = new AmazonS3Client(new AmazonS3Config
            {
                RegionEndpoint = TestRegionEndpoint,
                UseAccelerateEndpoint = true
            }
```

JavaScript

Para ver um exemplo sobre como habilitar a Aceleração de Transferências usando o AWS SDK para JavaScript, consulte o comando PutBucketAccelerateConfiguration na Referência de API do AWS SDK para JavaScript.

Python (Boto)

Consulte um exemplo sobre como habilitar a Aceleração de Transferências usando o SDK para Python em put_bucket_accelerate_configuration na Referência de API do AWS SDK para Python (Boto3).

Other

Para obter informações sobre como usar outros AWS SDKs, consulte Código de exemplo e bibliotecas.

Uso da API REST

Use a operação `PutBucketAccelerateConfiguration` da API REST para acelerar a configuração em um bucket existente.

Para obter mais informações, consulte PutBucketAccelerateConfiguration na Referência da API do Amazon Simple Storage Service.

Usar a ferramenta de comparação de velocidade do Amazon S3 Transfer Acceleration

É possível usar a usar a Ferramenta de comparação de velocidade da Aceleração de Transferências do Amazon S3 para comparar velocidades de upload aceleradas e não aceleradas em regiões do Amazon S3. A ferramenta de comparação de velocidade usa o multipart uploads para transferir um arquivo do seu navegador para várias regiões do Amazon S3 com e sem o uso do Transfer Acceleration.

Você pode acessar a ferramenta de comparação de velocidades usando qualquer um destes métodos:

- Copie o seguinte URL na janela do navegador, substituindo *`region`* pela Região da AWS que você está usando (por exemplo, `us-west-2`) e *`amzn-s3-demo-bucket`* pelo nome do bucket que deseja avaliar:

  `https://s3-accelerate-speedtest.s3-accelerate.amazonaws.com/en/accelerate-speed-comparsion.html?region=`*`region`*`&origBucketName=`*`amzn-s3-demo-bucket`*

  Para obter uma lista das regiões compatíveis com o Amazon S3, consulte Endpoints e cotas do Amazon S3 na Referência geral da AWS.
- Use o console do Amazon S3.

Utilizar buckets de uso geral com pagamento pelo solicitante para transferência e uso de armazenamento

Geralmente, proprietários de bucket pagam por todos os custos de armazenamento e transferência de dados do Amazon S3 associados ao bucket. Entretanto, você pode configurar um bucket

de uso geral para ser um bucket com pagamento pelo solicitante. Com buckets de Pagamento pelo solicitante, é o solicitante, em vez de o proprietário do bucket, quem paga pelo custo da solicitação e de download de dados do bucket. O proprietário do bucket sempre paga pelo custo de armazenamento de dados.

Normalmente, você configura buckets como Pagamento pelo solicitante quando quer compartilhar dados, mas não quer incorrer em cobranças associadas a outros que acessam os dados. Você pode, por exemplo, usar buckets de Pagamento pelo solicitante ao disponibilizar grandes conjuntos de dados, tais como diretórios de CEP, dados de referência, informações geoespaciais ou dados de crawling da Web.

> **Important**
>
> Se você habilitar o pagamento pelo solicitante em um bucket, de uso geral, o acesso anônimo a esse bucket não será permitido.

Você deve autenticar todas as solicitações que envolvem buckets de Pagamento pelo solicitante. A autenticação da solicitação permite que o Amazon S3 identifique e cobre o solicitante pelo uso do bucket de Pagamento pelo solicitante.

Quando o solicitante assume uma função do AWS Identity and Access Management (IAM) antes de fazer a solicitação, a conta à qual a função pertence é cobrada pela solicitação. Para obter mais informações sobre funções do IAM, consulte Funções do IAM no Manual do usuário do IAM.

Depois de configurar um bucket para ser um bucket de Pagamento pelo solicitante, os solicitantes devem mostrar que entendem que serão cobrados pela solicitação e pelo download dos dados. Para mostrar que aceitam as cobranças, os solicitantes devem incluir `x-amz-request-payer` como um cabeçalho na solicitação de API para as solicitações DELETE, GET, HEAD, POST e PUT, ou adicionar o parâmetro `RequestPayer` na solicitação REST. Para solicitações da CLI, os solicitantes podem usar o parâmetro `--request-payer`.

Example : usar a opção Pagamento pelo solicitante ao excluir um objeto

Para usar o exemplo de API DeleteObjectVersion a seguir, substitua *`user input placeholders`* por suas próprias informações.

```
DELETE /Key+?versionId=VersionId HTTP/1.1
```

```
Host: Bucket.s3.amazonaws.com
x-amz-mfa: MFA
x-amz-request-payer: RequestPayer
x-amz-bypass-governance-retention: BypassGovernanceRetention
x-amz-expected-bucket-owner: ExpectedBucketOwner
```

Se o solicitante restaurar objetos usando a API RestoreObject, a opção Pagamento pelo solicitante será compatível desde que o cabeçalho `x-amz-request-payer` ou o parâmetro `RequestPayer` estejam na solicitação. No entanto, o solicitante paga apenas pelo custo da solicitação. O proprietário do bucket paga pelas cobranças de recuperação.

Os buckets de Pagamento pelo solicitante não oferecem suporte aos itens a seguir.

- Solicitações anônimas
- Solicitações de SOAP
- Usando um bucket Pagamento pelo solicitante como bucket de destino para log de usuário final ou vice-versa. No entanto, você pode ativar o log do usuário final em um bucket Pagamento pelo solicitante no qual o bucket de destino não é um bucket Pagamento pelo solicitante.

Como funcionam as cobranças de Pagamento pelo solicitante

A cobrança por solicitações de Pagamento pelo solicitante bem-sucedidas é direta: o solicitante paga pela transferência de dados e pela solicitação; o proprietário do bucket paga pelo armazenamento de dados. Contudo, o proprietário do bucket é cobrado pela solicitação nas seguintes condições:

- A solicitação retorna um erro `AccessDenied` (HTTP `403 Forbidden`) e a solicitação é iniciada dentro da conta da AWS individual ou da organização da AWS do proprietário do bucket.
- A solicitação é uma solicitação SOAP.

Para obter mais informações sobre pagamentos pelo solicitante, consulte os tópicos abaixo.

Tópicos

- Configurar Pagamento pelo solicitante em um bucket
- Recuperar a configuração requestPayment usando a API REST
- Fazer download de objetos de buckets de Pagamento pelo solicitante

Configurar Pagamento pelo solicitante em um bucket

Você pode configurar um bucket do Amazon S3 para ser um bucket de Pagamento pelo solicitante, de modo que o solicitante pague o custo da solicitação e do download de dados em vez do proprietário do bucket.

Esta seção fornece exemplos de como configurar o pagamento pelo solicitante em um bucket do Amazon S3 usando o console e a API REST.

Uso do console do S3

Como habilitar o pagamento pelo solicitante para um bucket de uso geral do S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets de uso geral.
3. Na lista Buckets de uso geral escolha o nome do bucket para o qual você deseja habilitar o pagamento pelo solicitante.
4. Escolha Properties (Propriedades).
5. Em Requester pays (Pagamento pelo solicitante), escolha Edit (Editar).
6. Escolha Enable (Habilitar) e Save changes (Salvar alterações).

   O Amazon S3 habilitará o Pagamento pelo solicitante para o bucket e exibirá a Bucket overview (Visão geral do bucket). Em Requester pays (Pagamento pelo solicitante), você verá a opção Enabled (Habilitado).

Uso dos REST API

Somente o proprietário do bucket pode definir o valor de configuração `RequestPaymentConfiguration.payer` de um bucket como `BucketOwner` (o padrão) ou `Requester`. A definição do recurso `requestPayment` é opcional. Por padrão, o bucket não é um bucket de Pagamento pelo solicitante.

Para reverter um bucket de Pagamento pelo solicitante para um bucket regular, use o valor `BucketOwner`. Normalmente, você usaria `BucketOwner` ao fazer upload de dados para o bucket do Amazon S3 e definiria o valor como `Requester` antes da publicação de objetos no bucket.

Para definir requestPayment

- Use uma solicitação PUT para definir o valor `Payer` como `Requester` em um bucket especificado.

```
PUT ?requestPayment HTTP/1.1
Host: [BucketName].s3.amazonaws.com
Content-Length: 173
Date: Wed, 01 Mar 2009 12:00:00 GMT
Authorization: AWS [Signature]

<RequestPaymentConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
<Payer>Requester</Payer>
</RequestPaymentConfiguration>
```

Se houver êxito na solicitação, o Amazon S3 retornará uma resposta similar ao seguinte:

```
HTTP/1.1 200 OK
x-amz-id-2: [id]
x-amz-request-id: [request_id]
Date: Wed, 01 Mar 2009 12:00:00 GMT
Content-Length: 0
Connection: close
Server: AmazonS3
x-amz-request-charged:requester
```

Você pode definir pagamentos do solicitante somente no nível de bucket. Você não pode definir pagamentos pelo solicitante para objetos específicos dentro do bucket.

Você pode configurar um bucket para ser `BucketOwner` ou `Requester` a qualquer momento. No entanto, pode haver alguns minutos antes que o novo valor de configuração entre em vigor.

> **Note**
>
> Proprietários de bucket que abrem mão de URLs pré-assinadas devem pensar duas vezes antes de configurar um bucket para ser de pagamento pelo solicitante, especialmente se o URL tiver um ciclo de vida bem longo. O proprietário do bucket é cobrado cada vez que o solicitante usa um pre-signed URL que usa as credenciais do proprietário do bucket.

Recuperar a configuração requestPayment usando a API REST

Você pode determinar o `Payer` valor que é definido em um bucket solicitando o recurso `requestPayment`.

Para retornar o recurso requestPayment

- Use uma solicitação GET para obter o recurso `requestPayment`, conforme exibido na seguinte solicitação.

```
GET ?requestPayment HTTP/1.1
Host: [BucketName].s3.amazonaws.com
Date: Wed, 01 Mar 2009 12:00:00 GMT
Authorization: AWS [Signature]
```

Se houver êxito na solicitação, o Amazon S3 retornará uma resposta similar ao seguinte:

```
HTTP/1.1 200 OK
x-amz-id-2: [id]
x-amz-request-id: [request_id]
Date: Wed, 01 Mar 2009 12:00:00 GMT
Content-Type: [type]
Content-Length: [length]
Connection: close
Server: AmazonS3

<?xml version="1.0" encoding="UTF-8"?>
<RequestPaymentConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
<Payer>Requester</Payer>
</RequestPaymentConfiguration>
```

Esta resposta mostra que o valor `payer` é definido como `Requester`.

Fazer download de objetos de buckets de Pagamento pelo solicitante

Como os solicitantes serão cobrados pelo download de dados dos buckets de Pagamento pelo solicitante, as solicitações deverão conter um parâmetro especial, `x-amz-request-payer`, que confirma que o solicitante sabe que será cobrado pelo download. Para acessar objetos em buckets de Pagamento pelo solicitante, as solicitações devem incluir um dos seguintes.

- Para solicitações DELETE, GET, HEAD, POST e PUT, inclua `x-amz-request-payer : requester` no cabeçalho
- Para URLs assinados, inclua `x-amz-request-payer=requester` na solicitação

Se a solicitação for bem-sucedida e o solicitante for cobrado, a resposta incluirá o cabeçalho `x-amz-request-charged:requester`. Se `x-amz-request-payer` não estiver na solicitação, o Amazon S3 retornará um erro 403 e cobrará o proprietário do bucket pela solicitação.

> **Note**
>
> Proprietários de bucket não precisam adicionar `x-amz-request-payer` às suas solicitações.
> Certifique-se de que você tenha incluído `x-amz-request-payer` e seu valor no cálculo da assinatura. Consulte mais informações em Using an Authorization Header na Referência de API do Amazon S3.

Uso da API REST

Para fazer download de objetos em um bucket de Pagamento pelo solicitante

- Use uma solicitação `GET` para fazer download de um objeto em um bucket de Pagamento pelo solicitante, conforme exibido na seguinte solicitação.

```
GET / [destinationObject] HTTP/1.1
Host: [BucketName].s3.amazonaws.com
x-amz-request-payer : requester
Date: Wed, 01 Mar 2009 12:00:00 GMT
Authorization: AWS [Signature]
```

Se a solicitação GET for bem-sucedida e o solicitante for cobrado, a resposta incluirá `x-amz-request-charged:requester`.

O Amazon S3 poderá retornar um erro `Access Denied` para solicitações que tentarem obter objetos de um bucket de Pagamento pelo solicitante. Para obter informações, consulte Erros Responses (Respostas com erro) na Referência de APIs do Amazon Simple Storage Service.

Usar a AWS CLI

Para fazer download de objetos de um bucket de pagamento a cargo do solicitante usando a AWS CLI, especifique `--request-payer requester` como parte da sua solicitação `get-object`. Para obter mais informações, consulte get-object na Referência da AWS CLI.

Trabalhar com objetos no Amazon S3

Para armazenar seus dados no Amazon S3, você trabalha com recursos conhecidos como buckets e objetos. Um bucket é um contêiner de objetos. Um objeto é um arquivo e qualquer metadado que descreva esse arquivo.

Para armazenar um objeto no Amazon S3, crie um bucket e faça upload do objeto em um bucket. Quando o objeto estiver no bucket, você poderá abri-lo, baixá-lo e copiá-lo. Quando você não precisa mais de um objeto ou um bucket, você pode limpar esses recursos.

> **Note**
>
> Para obter mais informações sobre o uso da classe de armazenamento Amazon S3 Express One Zone com buckets de diretório, consulte S3 Express One Zone e Trabalhar com buckets de diretório.

> **Important**
>
> No console do Amazon S3, quando você escolhe Open (Abrir) ou Download As (Baixar como) para um objeto, essas operações criam URLs pré-assinados. Durante cinco minutos, seu objeto estará acessível a qualquer pessoa que tenha acesso a esses URLs pré-assinados. Para obter mais informações sobre URLs pré-assinados, consulte Usar URLs pré-assinados.

Com o Amazon S3, você paga somente pelo que for usado. Para obter mais informações sobre os recursos e a definição de preço do Amazon S3, consulte Amazon S3. Se você for um novo cliente do Amazon S3, você pode começar a usar o Amazon S3 gratuitamente. Para obter mais informações, consulte Nível gratuito da AWS.

Tópicos

- Visão geral de objetos Amazon S3
- Nomear objetos do Amazon S3
- Trabalhar com metadados de objeto
- Fazer upload de objetos

- Adicionar condições prévias às operações do S3 com solicitações condicionais
- Copiar, mover e renomear objetos
- Baixar objetos
- Verificar a integridade do objeto no Amazon S3
- Excluir objetos do Amazon S3
- Organizar, listar e trabalhar com seus objetos
- Baixar e fazer upload de objetos com URLs pré-assinados
- Transformar objetos com o S3 Object Lambda
- Executar operações de objetos em massa com o Operações em Lote
- Consultar dados no local com o Amazon S3 Select

Visão geral de objetos Amazon S3

O Amazon S3 é um depósito de objetos que usa valores de chave exclusivos para armazenar quantos objetos você quiser. Esses objetos são armazenados em um ou mais buckets e cada objeto pode ter até 5 TB de tamanho. Um objeto consiste no seguinte:

Chave

O nome que você atribui a um objeto. Você usa a chave de objeto para recuperar o objeto. Para obter mais informações, consulte Trabalhar com metadados de objetos.

ID da versão

Em um bucket, uma chave e um ID de versão identificam um objeto de maneira exclusiva. O ID de versão é uma string que o Amazon S3 gera quando você adiciona um objeto a um bucket. Para obter mais informações, consulte Reter várias versões de objetos com o Versionamento do S3.

Valor

O conteúdo que você está armazenando.

Um valor de objeto pode ser qualquer sequência de bytes. Objetos podem variar em tamanho de zero a 5 TB. Para obter mais informações, consulte Fazer upload de objetos.

Metadados

Um conjunto de pares de nome-valor com o qual é possível armazenar informações relacionadas ao objeto. Você pode atribuir os metadados, referidos como metadados definidos pelo usuário, a seus objetos no Amazon S3. O Amazon S3 também atribui metadados de sistema a esses objetos, os quais o sistema usa para gerenciar objetos. Para obter mais informações, consulte Trabalhar com metadados de objetos.

Sub-recursos

O Amazon S3 usa o mecanismo de sub-recursos para armazenar informações adicionais específicas do objeto. Como os sub-recursos são subordinados aos objetos, eles estão sempre associados com qualquer outra entidade, tal como um objeto ou um bucket. Para obter mais informações, consulte Sub-recursos do objeto.

Informações de controle de acesso

Você pode controlar o acesso aos objetos armazenados no Amazon S3. O Amazon S3 e compatível com o controle de acesso baseado em recursos, como uma lista de controle de acesso (ACL) e políticas de bucket, e com o controle de acesso de dados baseados no usuário. Para obter mais informações sobre controle de acesso, consulte:

- Controle de acesso no Amazon S3
- Gerenciamento de identidade e acesso para o Amazon S3
- Configurar ACLs

Seus recursos do Amazon S3 (por exemplo, buckets e objetos) são privados por padrão. É necessário conceder permissão expressa para que outras pessoas acessem esses recursos. Para obter mais informações sobre compartilhamento de objetos, consulte Compartilhar objetos com URLs pré-assinados.

Tags

Para categorizar objetos armazenados para a finalidade de controle de acesso ou alocação de custos, você pode usar tags. Para obter mais informações, consulte Categorizar seu armazenamento usando tags.

Sub-recursos do objeto

O Amazon S3 define um conjunto de sub-recursos associados a buckets e objetos. Os subrecursos são subordinados aos objetos. Isso significa que os subrecursos não existem por conta própria. Eles são sempre associados a alguma outra entidade, como um objeto ou um bucket.

A tabela a seguir lista os sub-recursos associados a objetos do Amazon S3.

Sub-recurso	Descrição
acl	Contém uma lista de concessões que identifica os concessionários e permissões concedidas. Quando você cria um objeto, o `acl` identifica o proprietário do objeto como tendo total controle sobre o objeto. Você pode recuperar a ACL de um objeto ou substituí-la por uma lista atualizada de concessões. Qualquer atualização para um ACL requer que você substitua o ACL existente. Para obter mais informações sobre ACLs, consulte Visão geral da lista de controle de acesso (ACL).

Nomear objetos do Amazon S3

A chave de objeto (ou nome da chave) identifica o objeto em um bucket do Amazon S3 de maneira exclusiva. Ao criar um objeto, você especifica o nome da chave. Por exemplo, no console do Amazon S3, quando você seleciona um bucket, é exibida uma lista de objetos no bucket. Esses nomes são as chaves de objeto.

O nome da chave do objeto é uma sequência de caracteres Unicode com codificação UTF-8 e até 1.024 bytes de extensão ou em torno de 1.024 caracteres latinos. Em algumas localidades, um único caractere pode precisar de 2 bytes para codificação. Ao nomear objetos, esteja ciente do seguinte:

- Os nomes das chaves de objeto diferenciam letras maiúsculas de minúsculas.
- Os nomes das chaves de objeto incluem quaisquer prefixos (conhecidos como pastas no console). Por exemplo, `Development/Projects.xls` é o nome completo da chave do objeto `Projects.xls` localizado dentro do prefixo (ou pasta) `Development`. O prefixo, o delimitador (`/`) e o nome do objeto estão incluídos na limitação de 1.024 bytes para o nome da chave do objeto. Para ter mais informações sobre prefixos e pastas, consulte the section called “Escolher nomes de chave de objeto”.

- Certos caracteres podem exigir tratamento especial quando usados em nomes de chaves de objeto. Para obter mais informações, consulte the section called “Diretrizes de nomeação de chave de objeto”.

> **Note**
>
> Os nomes de chaves de objeto com o valor `"soap"` não são compatíveis com solicitações de estilo de hospedagem virtual. Quanto a valores de nome de chave de objeto em que se usa `"soap"`, deve-se usar, em vez disso, um URL de estilo de caminho.

Escolher nomes de chave de objeto

O modelo de dados do Amazon S3 é uma estrutura plana: você cria um bucket e o bucket armazena objetos. Não há hierarquia de sub-buckets ou de subpastas. No entanto, é possível pressupor a hierarquia lógica usando prefixos e delimitadores de nome de chave como faz o console do Amazon S3. O console do Amazon S3 é compatível com o conceito de pastas. Para obter mais informações sobre como editar metadados do console do Amazon S3, consulte Editar metadados de objeto no console do Amazon S3.

Vamos supor que seu bucket (`admin-created`) tenha quatro objetos com as seguintes chaves de objeto:

`Development/Projects.xls`

`Finance/statement1.pdf`

`Private/taxdocument.pdf`

`s3-dg.pdf`

O console usa prefixos de nome de chave (`Development/`, `Finance/` e `Private/`) e o delimitador (`/`) para apresentar uma estrutura de pastas. A chave `s3-dg.pdf` não contém um prefixo delimitado por barra, por isso seu objeto aparece diretamente no nível da raiz do bucket. Ao abrir a pasta `Development/`, o objeto `Projects.xlsx` é exibido.

- O Amazon S3 é compatível com buckets e objetos e não há nenhuma hierarquia. No entanto, ao usar prefixos e delimitadores em um nome de chave de objeto, o console do Amazon S3 e os AWS SDKs podem pressupor uma hierarquia e apresentar o conceito de pastas.

- O console do Amazon S3 implementa a criação de objetos de pasta criando objetos de zero bytes com o valor de prefixo e do delimitador da pasta como a chave. Esses objetos de pasta não aparecem no console. Caso contrário, eles se comportam como qualquer outro objeto e podem ser visualizados e manipulados por meio da API REST, AWS CLI e AWS SDKs.

Diretrizes de nomeação de chave de objeto

Você pode usar qualquer caractere UTF-8 em um nome de chave de objeto. No entanto, o uso de determinados caracteres em nomes de chave pode causar problemas com algumas aplicações e protocolos. As seguintes diretrizes ajudam você a maximizar a conformidade com DNS, caracteres seguros da web, parsers de XML e outras APIs.

Caracteres seguros

Os seguintes conjuntos de caracteres são, geralmente, confiáveis para uso em nomes de chave:

Alphanumeric characters	• 0-9 • a-z • A-Z
Special characters	• Ponto de exclamação (!) • Hífen (-) • Sublinhado (_) • Ponto final (.) • Asterisco (*) • Aspas simples (') • Parêntese de abertura (() • Parêntese de fechamento ())

Os seguintes são exemplos de nomes de chave válidos:

- `4my-organization`
- `my.great_photos-2014/jan/myvacation.jpg`
- `videos/2014/birthday/video1.wmv`

Note

Se você usar o console do Amazon S3 para fazer download de objetos com nomes de chave que terminam com pontos (`.`), os pontos serão removidos do final dos nomes de chave dos objetos baixados. Para manter os pontos no final dos nomes de chave nos objetos baixados, você deve usar a AWS Command Line Interface (AWS CLI), os AWS SDKs ou a API REST do Amazon S3.
Além disso, saiba das seguintes limitações do prefixo:

- Objetos com um prefixo de `./` devem ser carregados ou baixados com a AWS CLI, os AWS SDKs ou a API REST. Não é possível usar o console do Amazon S3 para fazer upload desses objetos.
- As chaves de objeto que contêm elementos de caminho relativo (por exemplo, `../`) são válidas se, quando analisadas da esquerda para a direita, a contagem cumulativa de segmentos de caminho relativo nunca exceder o número de elementos de caminho não relativos encontrados. Essa regra se aplica a todas as solicitações feitas usando o console do Amazon S3, a API REST do Amazon S3, a AWS CLI e os AWS SDKs.

  Por exemplo:

  - `videos/2014/../../video1.wmv` é válido.
  - `videos/../../video1.wmv` não é válido.
  - `videos/../../2014/video1.wmv` não é válido.

Caracteres que podem exigir tratamento especial

Os caracteres a seguir em um nome de chave podem exigir tratamento adicional do código e, provavelmente, precisarão ser criptografados em URL ou referenciados como HEX. Alguns desses caracteres não são imprimíveis, e seu navegador pode não reconhecê-los, o que também exigirá tratamento especial:

- E comercial (&)
- Sinal de dólar ($)
- Caracteres ASCII variam de 00-1F em hexadecimal (0-31 decimal) e 7F (127 decimal)
- Símbolo de arroba (@)
- Sinal de igual (=)

- Ponto e vírgula (;)
- Barra (/)
- Dois pontos (:)
- Sinal de adição (+)
- Espaço: sequências significativas de espaços podem ser perdidas em alguns casos (especialmente múltiplos espaços)
- Vírgula (,)
- Ponto de interrogação (?)

Caracteres a serem evitados

Recomendamos não usar os seguintes caracteres no nome de uma chave devido ao tratamento significativo de caracteres especiais, que não é consistente em todas as aplicações:

- Barra invertida (\)
- Chave esquerda ({)
- Caracteres ASCII não imprimíveis (128-255 caracteres decimais)
- Acento circunflexo (^)
- Chave direita (})
- Caractere de porcentagem (%)
- Acento grave ou crase (`)
- Colchete direito (])
- Aspas (")
- Sinal maior que (>)
- Colchete esquerdo ([)
- Til (~)
- Sinal menor que (<)
- Sinal de libra (#)
- Barra vertical (|)

Restrições de chave de objeto relacionadas a XML

Conforme especificado pelo padrão XML no processamento de fim de linha, todo o texto XML é normalizado de modo que os retornos de carro simples (código ASCII 13) e os retornos de carro imediatamente seguidos por uma nova linha (código ASCII 10), também conhecidos como caracteres de quebra de linha, sejam substituídos por um único caractere de nova linha. Para garantir a análise correta de chaves de objeto em solicitações XML, retornos de carro e outros caracteres especiais devem ser substituídos por seu código de entidade XML equivalente quando forem inseridos em tags XML.

A seguinte lista mostra os tais caracteres especiais e seus códigos de entidade XML equivalentes:

- O apóstrofo (') deve ser substituído por `'`.
- As aspas (") devem ser substituídas por `"`.
- O e comercial (&) deve ser substituído por `&`.
- O sinal menor que (<) deve ser substituído por `<`.
- O sinal maior que (>) deve ser substituído por `>`.
- O retorno de carro (`\r`) deve ser substituído por `
` ou `
`.
- A quebra de linha (`\n`) deve ser substituída por `
` ou `
`.

Example

O exemplo a seguir ilustra o uso de um código de entidade XML como uma substituição para um retorno de carro. Esta solicitação `DeleteObjects` exclui um objeto com o parâmetro `key` `/some/prefix/objectwith\rcarriagereturn` (em que `\r` é o retorno de carro).

```
<Delete xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Object>
    <Key>/some/prefix/objectwith&#13;carriagereturn</Key>
  </Object>
</Delete>
```

Trabalhar com metadados de objeto

Há dois tipos de metadados de objeto no Amazon S3: metadados definidos pelo sistema e metadados definidos pelo usuário. Os metadados definidos pelo sistema incluem a data de criação, o tamanho e a classe de armazenamento do objeto, entre outros. Os metadados definidos pelo

usuário são metadados que você pode optar por definir no momento do upload de um objeto. Esses metadados definidos pelo usuário são um conjunto de pares de nome/valor. Para obter mais informações, consulte the section called “Metadados do objeto definidos pelo sistema” e the section called “Metadados do objeto definidos pelo usuário”.

Ao criar um objeto, você especifica a chave do objeto (ou nome da chave), que identifica exclusivamente o objeto em um bucket do Amazon S3. Para obter mais informações, consulte Nomear objetos do Amazon S3. Você também pode definir metadados definidos pelo usuário no Amazon S3 no momento do upload do objeto.

Após fazer upload do objeto, você não pode mais modificar esses metadados definidos pelo usuário. A única forma de modificar esses metadados é fazer uma cópia do objeto e definir os metadados. Para ter mais informações sobre como editar metadados usando o console do Amazon S3, consulte Editar metadados de objeto no console do Amazon S3.

Consultar os metadados e acelerar a descoberta de dados com o S3 Metadata

Para encontrar, armazenar e consultar facilmente os metadados dos objetos do S3, você pode usar o S3 Metadata. Com o S3 Metadata, você pode preparar dados rapidamente para uso em analytics de negócios, recuperação de conteúdo, treinamento de modelos de inteligência artificial e machine learning (IA/ML) e muito mais.

O S3 Metadata acelera a descoberta de dados ao capturar automaticamente os metadados dos objetos nos buckets de uso geral e armazená-los em tabelas do Apache Iceberg totalmente gerenciadas e somente leitura que você pode consultar. Essas tabelas somente leitura são chamadas de tabelas de metadados. À medida que objetos são adicionados, atualizados e removidos dos buckets de uso geral, o S3 Metadata atualiza automaticamente as tabelas de metadados correspondentes para refletir as alterações mais recentes.

Por padrão, o S3 Metadata fornece metadados de objetos definidos pelo sistema, como o horário de criação e a classe de armazenamento de um objeto, e metadados personalizados, como tags e metadados definidos pelo usuário que foram incluídos durante o upload do objeto. O S3 Metadata também fornece metadados de eventos, como quando um objeto é atualizado ou excluído, e a Conta da AWS que fez a solicitação.

As tabelas de metadados são armazenadas em buckets de tabela do S3, que fornecem armazenamento otimizado para dados tabulares. Para consultar os metadados, você pode integrar o bucket de tabela a serviços de analytics da AWS, como Amazon Athena, Amazon Redshift e Amazon QuickSight.

Para ter mais informações sobre o S3 Metadata, consulte the section called “Acelerar a descoberta de dados”.

Metadados do objeto definidos pelo sistema

Para cada objeto armazenado em um bucket, o Amazon S3 mantém um conjunto de metadados do sistema. O Amazon S3 processa estes metadados do sistema conforme necessário. Por exemplo, o Amazon S3 mantém a data de criação e o tamanho dos metadados, usando essas informações como parte do gerenciamento de objetos.

Existem duas categorias de metadados de sistema:

- Controlados pelo sistema: os metadados, como a data de criação do objeto, são controlados pelo sistema, o que significa que somente o Amazon S3 pode modificar o valor da data.
- Controlados pelo usuário: outros metadados de sistema, como a classe de armazenamento configurada para o objeto e se o objeto tem criptografia habilitada no lado do servidor, são exemplos cujos valores são controlados por você. Se o bucket está configurado como um site, você pode querer redirecionar uma solicitação de página para outra página ou para um URL externo. Nesse caso, uma página é um objeto no bucket. O Amazon S3 armazena o valor do redirecionamento da página como metadados do sistema, que você pode controlar.

  Ao criar objetos, você pode configurar os valores desses itens de metadados de sistema ou atualizar os valores quando necessário. Para obter mais informações sobre classes de armazenamento, consulte Compreender e gerenciar classes de armazenamento do Amazon S3.

  O Amazon S3 usa chaves AWS KMS para criptografar seus objetos do Amazon S3. O AWS KMS criptografa apenas os dados do objeto. A soma de verificação e o algoritmo especificado são armazenados como parte dos metadados do objeto. Se a criptografia no lado do servidor for solicitada para o objeto, a soma de verificação será armazenada em formato criptografado. Para obter mais informações sobre criptografia no lado do servidor, consulte Proteger dados com criptografia.

> **Note**
>
> O cabeçalho da solicitação PUT é limitado a 8 KB. No cabeçalho da solicitação PUT, os metadados definidos pelo sistema são limitados a 2 KB. O tamanho de metadados definidos

pelo sistema é medido pela soma do número de bytes na codificação US-ASCII de cada chave e valor.

A tabela a seguir fornece uma lista dos metadados definidos por sistema e se você pode atualizá-los.

Nome	Descrição	O usuário pode modificar o valor?
`Date`	A data e hora atual.	Não
`Cache-Control`	Um campo de cabeçalho geral usado para especificar políticas de armazenamento em cache.	Sim
`Content-Disposition`	Informações de apresentação do objeto.	Sim
`Content-Length`	O tamanho do objeto em bytes.	Não
`Content-Type`	O tipo do objeto.	Sim
`Last-Modified`	A data de criação do objeto ou data da última modificação, o que aconteceu por último. Para carregamentos fracionados, a data de criação do objeto é a data de início do respectivo carregamento.	Não
`ETag`	Uma tag de entidade (ETag) que representa uma versão específica de um objeto. Para objetos que não são carregados como um carregamento fracionado e não são criptografados ou são criptografados por criptografia no servidor com chaves gerenciadas pelo Simple Storage Service (Amazon S3) (SSE-S3), a ETag é um resumo MD5 dos dados.	Não
`x-amz-server-side-encryption`	Um cabeçalho que indica se a criptografia do lado do servidor está ativada para o objeto e se essa criptografia está usando as chaves do AWS Key Management	Sim

Nome	Descrição	O usuário pode modificar o valor?
	Service (AWS KMS) (SSE-KMS) ou usando as chaves de criptografia gerenciadas pelo Amazon S3 (SSE-S3). Para obter mais informações, consulte Proteger os dados usando criptografia do lado do servidor.	
`x-amz-checksum-crc64nvme` , `x-amz-checksum-crc32` , `x-amz-checksum-crc32c` , `x-amz-checksum-sha1` , `x-amz-checksum-sha256`	Cabeçalhos que contêm a soma de verificação ou o resumo do objeto. No máximo um desses cabeçalhos será definido por vez, dependendo do algoritmo de soma de verificação que você instruir o Amazon S3 a usar. Para obter mais informações sobre a escolha do algoritmo de soma de verificação, consulte Verificar a integridade do objeto no Amazon S3.	Não
`x-amz-checksum-type`	O tipo de soma de verificação, que determina como as somas de verificação em nível de parte são combinadas para criar uma soma de verificação em nível de objeto para objetos fracionados.	Sim
`x-amz-version-id`	A versão do objeto. Quando você ativa o versionamento em um bucket, o Amazon S3 atribui um ID de versão aos objetos adicionados ao bucket. Para obter mais informações, consulte Reter várias versões de objetos com o Versionamento do S3.	Não
`x-amz-delete-marker`	Um marcador booliano que indica se o objeto é um marcador de exclusão. Esse marcador é usado somente em buckets com versionamento ativado.	Não

Nome	Descrição	O usuário pode modificar o valor?
`x-amz-storage-class`	A classe de armazenamento usada para armazenar o objeto. Para obter mais informações, consulte Compreender e gerenciar classes de armazenamento do Amazon S3.	Sim
`x-amz-website-redirect-location`	Um cabeçalho que redireciona solicitações do objeto associado para outro objeto no mesmo bucket ou para um URL externo. Para obter mais informações, consulte (Opcional) Configurar um redirecionamento de uma página da Web.	Sim
`x-amz-server-side-encryption-aws-kms-key-id`	Um cabeçalho que indica o ID da chave do KMS de criptografia simétrica do AWS KMS que foi usada para criptografar o objeto. Esse cabeçalho é usado somente quando o cabeçalho `x-amz-server-side-encryption` está presente e tem o valor de `aws:kms`.	Sim
`x-amz-server-side-encryption-customer-algorithm`	Um cabeçalho que indica se a criptografia do lado do servidor com as chaves de criptografia fornecidas pelo cliente (SSE-C) está ativada. Para obter mais informações, consulte Como usar criptografia do lado do servidor com chaves fornecidas pelo cliente (SSE-C).	Sim
`x-amz-tagging`	O conjunto de etiquetas do objeto. O conjunto de etiquetas deve ser codificado como parâmetros de consulta de URL.	Sim

Metadados do objeto definidos pelo usuário

Ao fazer upload de um objeto, você também pode atribuir metadados ao objeto. Você fornece essas informações opcionais como um par de nome-valor (valor-chave) quando envia uma solicitação

PUT ou POST para criar o objeto. Ao fazer upload de objetos usando a API REST, os nomes de metadados opcionais definidos pelo usuário devem começar com `x-amz-meta-`, para diferenciá-los de outros cabeçalhos HTTP. Quando você recupera o objeto usando a API REST, o prefixo é retornado. Ao fazer upload de objetos usando a API SOAP, o prefixo não é obrigatório. Quando você recupera o objeto usando SOAP API, o prefixo é removido, independentemente da API que você usou para fazer upload do objeto.

> **Note**
>
> As APIs SOAP não estão disponíveis para novos clientes e chegam ao fim da vida útil (EOL) em 31 de agosto de 2025. Recomendamos usar a API REST ou os AWS SDKs.

Quando os metadados são recuperados por meio da API REST, o Amazon S3 combina os cabeçalhos que têm o mesmo nome (sem distinção entre letras maiúsculas e minúsculas) em uma lista delimitada por vírgulas. Se alguns metadados contêm caracteres não imprimíveis, eles não são retornados. Em vez disso, o cabeçalho `x-amz-missing-meta` é retornado com o valor do número de entradas de metadados não imprimíveis. A ação `HeadObject` recupera metadados de um objeto sem retornar o próprio objeto. Essa operação é útil se você estiver interessado apenas nos metadados de um objeto. Para usar `HEAD`, você deve ter acesso `READ` ao objeto. Para obter mais informações, consulte HeadObject na Referência de API do Amazon Simple Storage Service.

Metadados definidos pelo usuário são um conjunto de pares chave-valor. O Amazon S3 armazena chaves de metadados definidas pelo usuário em minúsculas.

O Amazon S3 permite caracteres Unicode arbitrários em seus valores de metadados.

Para evitar problemas relacionados à apresentação desses valores de metadados, é necessário estar em conformidade com o uso de caracteres US-ASCII ao usar REST e UTF-8 ao usar SOAP ou uploads baseados em navegador via `POST`.

Ao usar caracteres não US-ASCII nos valores de metadados, a string Unicode fornecida é examinada quanto a caracteres não US-ASCII. Os caracteres desses cabeçalhos são decodificados conforme o RFC 2047 antes do armazenamento e codificados de acordo com o RFC 2047 antes de retornar para garantir que eles possam ser enviados por e-mail com segurança. Se a string contiver apenas caracteres US-ASCII, ela será apresentada como está.

Veja um exemplo a seguir.

```
PUT /Key HTTP/1.1
Host: amzn-s3-demo-bucket.s3.amazonaws.com
x-amz-meta-nonascii: ÄMÄZÕÑ S3

HEAD /Key HTTP/1.1
Host: amzn-s3-demo-bucket.s3.amazonaws.com
x-amz-meta-nonascii: =?UTF-8?B?w4PChE3Dg8KEWsODwpXDg8KRIFMz?=

PUT /Key HTTP/1.1
Host: amzn-s3-demo-bucket.s3.amazonaws.com
x-amz-meta-ascii: AMAZONS3

HEAD /Key HTTP/1.1
Host: amzn-s3-demo-bucket.s3.amazonaws.com
x-amz-meta-ascii: AMAZONS3
```

> **Note**
>
> O cabeçalho da solicitação PUT é limitado a 8 KB. No cabeçalho da solicitação PUT, os metadados definidos pelo usuário são limitados a 2 KB. O tamanho de metadados definidos pelo usuário é medido pela soma do número de bytes na codificação UTF-8 de cada chave e valor.

Para obter informações sobre como alterar os metadados do objeto depois do upload criando uma cópia, modificando e substituindo o objeto antigo ou criando outra versão dele, consulte Editar metadados de objeto no console do Amazon S3.

Editar metadados de objeto no console do Amazon S3

Você pode usar o console do Amazon S3 para editar metadados de objetos do S3 existentes por meio da ação Copiar. Para editar metadados, você copia objetos para o mesmo destino e especifica os novos metadados que deseja aplicar, os quais substituem os metadados antigos do objeto. Alguns metadados são definidos pelo Amazon S3 quando você faz upload do objeto. Por exemplo, `Content-Length` e `Last-Modified` são campos de metadados de objetos definidos pelo sistema que não podem ser modificados por um usuário.

Você também pode definir metadados definidos pelo usuário ao carregar o objeto e depois substituí-lo conforme suas necessidades mudarem. Por exemplo, você pode ter um conjunto de objetos que

você armazena inicialmente na classe de armazenamento `STANDARD`. Com o tempo, pode ser que você não precise mais que esses dados estejam altamente disponíveis. Desse modo, você pode alterar a classe de armazenamento para `GLACIER` substituindo o valor da chave `x-amz-storage-class` de `STANDARD` para `GLACIER`.

> **Note**
>
> Considere o seguinte ao substituir metadados de objeto no Amazon S3:
>
> - É necessário especificar os metadados existentes que deseja reter, os que deseja adicionar e os que deseja editar.
> - Se o objeto tiver menos de 5 GB, você poderá usar a ação Copiar no console do S3 para substituir os metadados do objeto. Se o objeto tiver mais de 5 GB, você poderá substituir os metadados do objeto ao copiá-lo com carregamento fracionado usando a AWS CLI ou os SDKs da AWS. Para obter mais informações, consulte Copiar um objeto usando multipart upload.
> - Para obter uma lista das permissões adicionais necessárias para substituir metadados, consulte the section called “Permissões obrigatórias para operações de API do S3”. Para ver exemplos das políticas que concedem essas permissões, consulte the section called “Exemplos de políticas baseadas em identidade”.
> - Essa ação cria uma cópia do objeto com configurações atualizadas e a data da última modificação. Se o versionamento do S3 estiver habilitado, uma nova versão do objeto será criada e o objeto existente se tornará uma versão mais antiga. Se a funcionalidade Versionamento do S3 não estiver habilitada, uma nova cópia do objeto substituirá o original. A Conta da AWS associada ao perfil do IAM que altera a propriedade também se torna a proprietária do novo objeto ou (versão do objeto).
> - Ao editar os metadados, os valores referentes a nomes de chave existentes são substituídos.
> - Objetos criptografados com chaves de criptografia fornecidas pelo cliente (SSE-C) não podem ser copiados usando o console. Você deve usar a AWS CLI, o AWS SDK ou a API REST do Amazon S3.
> - Ao copiar um objeto usando o console do Amazon S3, você pode receber a seguinte mensagem de erro: “Não é possível verificar os metadados copiados.” O console usa cabeçalhos para recuperar e definir metadados para o objeto. Se a configuração da rede ou do navegador modificar as solicitações de rede, esse comportamento poderá fazer com que metadados não intencionais (como cabeçalhos `Cache-Control` modificados)

sejam gravados no objeto copiado. O Amazon S3 não pode verificar esses metadados não intencionais.

Para resolver esse problema, verifique a configuração da rede e do navegador para garantir que não modifique cabeçalhos, como `Cache-Control`. Para ter mais informações, consulte o Modelo de Responsabilidade Compartilhada.

⚠ Warning

Ao substituir metadados referentes a pastas, aguarde a conclusão da ação Copiar antes de adicionar novos objetos à pasta. Caso contrário, novos objetos também podem ser editados.

Os tópicos a seguir descrevem como substituir metadados de um objeto usando a ação Copiar no console do Amazon S3.

Substituir metadados definidos pelo sistema

Você pode configurar alguns metadados definidos pelo sistema para um objeto do S3. Para ter uma lista de metadados definidos pelo sistema e de valores que você pode modificar, consulte Metadados do objeto definidos pelo sistema.

Como substituir metadados definidos pelo sistema de um objeto

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets de uso geral ou Buckets de diretórios.
3. Na lista de buckets, escolha o nome do bucket que contém os objetos que você deseja alterar.
4. Marque a caixa de seleção referente aos objetos que você quer alterar.
5. No menu Ações, escolha Copiar na lista de opções exibida.
6. Para especificar o caminho de destino, escolha Procurar S3, navegue até o mesmo destino dos objetos de origem e marque a caixa de seleção do destino. Escolha Choose destination (Escolher destino) no canto inferior direito.

   Outra alternativa é inserir o caminho de destino.
7. Se o versionamento de bucket não estiver habilitado, você verá um aviso recomendando que o habilite para ajudar a impedir a substituição ou exclusão involuntária de objetos. Se você quiser

manter todas as versões de objetos neste bucket, selecione Enable Bucket Versioning (Ativar versionamento de bucket). Você também pode atualizar as propriedades de criptografia padrão e do Bloqueio de Objetos em Detalhes do destino.

8. Em Configurações adicionais de cópia, escolha Especificar configurações para especificar configurações para Metadados.
9. Role até a seção Metadados e escolha Substituir todos os metadados.
10. Escolha Add Metadata (Adicionar metadados).
11. Para Type (Tipo) de metadados, selecione System-defined (Definidos pelo sistema).
12. Especifique uma key (chave) exclusiva e o value (valor) dos metadados.
13. Para editar metadados adicionais, escolha Add metadata (Adicionar metadados). Você também pode escolher Remove (Remover) para remover um conjunto de valores de chave de tipo.
14. Escolha Copiar. O Amazon S3 salva as alterações feitas nos metadados.

Substituir metadados definidos pelo usuário

Você pode substituir metadados definidos pelo usuário de um objeto usando o prefixo de metadados, `x-amz-meta-`, e um nome escolhido para criar uma chave personalizada. Por exemplo, se você adicionar o nome personalizado `alt-name`, a chave de metadados será `x-amz-meta-alt-name`.

Metadados definidos pelo usuário podem ter até 2 KB no total. Para calcular o tamanho total dos metadados definidos pelo usuário, some o número de bytes na codificação UTF-8 referente a cada chave e valor. As duas chaves e seus valores devem estar em conformidade com os padrões US-ASCII. Para obter mais informações, consulte Metadados do objeto definidos pelo usuário.

Como substituir metadados definidos pelo usuário de um objeto

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação, escolha Buckets e selecione a guia Buckets de uso geral ou Buckets de diretório. Acesse o bucket ou pasta do Amazon S3 que contém os objetos que você quer alterar.
3. Marque a caixa de seleção referente aos objetos que você quer alterar.
4. No menu Ações, escolha Copiar na lista de opções exibida.
5. Para especificar o caminho de destino, escolha Procurar S3, navegue até o mesmo destino dos objetos de origem e marque a caixa de seleção do destino. Escolha Choose destination (Escolher destino).

Outra alternativa é inserir o caminho de destino.

6. Se o versionamento de bucket não estiver habilitado, você verá um aviso recomendando que o habilite para ajudar a impedir a substituição ou exclusão involuntária de objetos. Se você quiser manter todas as versões de objetos neste bucket, selecione Enable Bucket Versioning (Ativar versionamento de bucket). Você também pode atualizar as propriedades de criptografia padrão e do Bloqueio de Objetos em Detalhes do destino.
7. Em Configurações adicionais de cópia, escolha Especificar configurações para especificar configurações para Metadados.
8. Role até a seção Metadados e escolha Substituir todos os metadados.
9. Escolha Add Metadata (Adicionar metadados).
10. Para Type (Tipo) de metadados, escolha User-defined (Definido pelo usuário).
11. Insira uma Key (Chave) personalizada única após `x-amz-meta-`. Insira também um value (valor) dos metadados.
12. Para adicionar metadados extras, escolha Add metadata (Adicionar metadados). Você também pode escolher Remove (Remover) para remover um conjunto de valores de chave de tipo.
13. Escolha Copiar. O Amazon S3 salva as alterações feitas nos metadados.

Acelerar a descoberta de dados com o S3 Metadata

O Amazon S3 Metadata acelera a descoberta de dados ao capturar automaticamente os metadados dos objetos nos buckets de uso geral e armazená-los em tabelas do Apache Iceberg totalmente gerenciadas e somente leitura que você pode consultar. Essas tabelas somente leitura são chamadas de tabelas de metadados. À medida que objetos são adicionados, atualizados e removidos dos buckets de uso geral, o S3 Metadata atualiza automaticamente as tabelas de metadados correspondentes para refletir as alterações mais recentes.

Por padrão, o S3 Metadata fornece três tipos de metadados:

- Metadados definidos pelo sistema, como o horário de criação e a classe de armazenamento de um objeto.
- Metadados personalizados, como tags e metadados definidos pelo usuário que foram incluídos durante o upload do objeto.
- Metadados de eventos, como quando um objeto é atualizado ou excluído, e a Conta da AWS que fez a solicitação.

Para conferir detalhes sobre quais dados são armazenados nas tabelas de metadados, consulte the section called “Esquema de tabelas do Metadata”.

Com o S3 Metadata, você pode facilmente encontrar, armazenar e consultar metadados para os objetos do S3, para que possa preparar dados rapidamente para uso em analytics de negócios, recuperação de conteúdo, treinamento de modelos de inteligência artificial e machine learning (IA/ML) e muito mais.

As tabelas de metadados são armazenadas em buckets de tabela do S3, que fornecem armazenamento otimizado para dados tabulares. Para consultar metadados com facilidade, você pode integrar o bucket de tabela ao AWS Glue Data Catalog. Depois que o bucket de tabela for integrado ao AWS Glue Data Catalog, você poderá consultar diretamente as tabelas de metadados com mecanismos de consulta, como Amazon Athena, Amazon EMR, Amazon Redshift, Apache Spark e Trino. Você também pode consultar tabelas de metadados com qualquer outra aplicação que seja compatível com o formato Apache Iceberg. Para criar painéis das tabelas de metadados, use o Amazon QuickSight.

Para ter informações sobre os preços do S3 Metadata, consulte Definição de preço do Amazon S3.

Como funcionam as tabelas de metadados

As tabelas de metadados são gerenciadas pelo Amazon S3 e não podem ser modificadas por nenhuma entidade principal do IAM fora do próprio Amazon S3. (No entanto, você pode excluir as tabelas de metadados.) Como resultado, as tabelas de metadados são somente leitura, o que ajuda a garantir que elas reflitam corretamente o conteúdo do bucket.

Para manter as tabelas de metadados do Apache Iceberg com a melhor performance, o Amazon S3 realiza atividades de manutenção periódicas nas tabelas, como compactação e remoção de arquivos sem referência. Essas atividades de manutenção ajudam a minimizar o custo de armazenamento das tabelas de metadados e a otimizar a performance das consultas. Essa manutenção das tabelas ocorre automaticamente, não exigindo adesão nem gerenciamento contínuo da sua parte. No entanto, se necessário, você pode configurar essas atividades de manutenção das tabelas. Para ter mais informações, consulte Table bucket maintenance.

> **Note**
>
> O S3 Metadata foi projetado para anexar continuamente à tabela de metadados conforme você faz alterações no bucket de uso geral. Cada atualização cria um snapshot, que é uma nova versão da tabela de metadados. Devido à natureza somente leitura da tabela de metadados, não é possível excluir registros da tabela de metadados. Você também não pode

usar o recurso de expiração de snapshots da funcionalidade Tabelas do S3 para expirar snapshots antigos da tabela de metadados.
Para ajudar a minimizar os custos, você pode excluir periodicamente a configuração de tabelas de metadados e as tabelas de metadados, depois recriá-las. Para obter mais informações, consulte the section called “Excluir configurações de tabelas de metadados” e the section called “Excluir tabelas de metadados”.

Para gerar e armazenar metadados de objetos em uma tabela de metadados gerenciada pelo S3, crie uma configuração de tabelas de metadados para o bucket de uso geral. O Amazon S3 foi projetado para atualizar continuamente a tabela de metadados a fim de refletir as alterações mais recentes nos dados, desde que a configuração esteja ativa no bucket.

Para criar uma configuração de tabelas de metadados, você deve garantir que tenha as permissões do AWS Identity and Access Management (IAM) necessárias para criar e gerenciar tabelas de metadados. Para obter mais informações, consulte the section called “Permissões para tabelas de metadados”. Você também deve criar ou especificar um bucket de tabela do S3 para armazenar a tabela de metadados. Esse bucket de tabela deve estar na mesma conta e Região da AWS que o bucket de uso geral. Para ter mais informações sobre como criar buckets de tabela, consulte Creating table buckets.

Note

O S3 Metadata não se aplica a nenhum objeto que já existia no bucket de uso geral antes de você criar a configuração de tabelas de metadados. Em outras palavras, o S3 Metadata captura apenas metadados de eventos de alteração (como uploads, atualizações e exclusões) que acontecem depois que você cria a configuração de tabelas de metadados.

Para monitorar as atualizações na configuração de tabelas de metadados, você pode usar o AWS CloudTrail. Para obter mais informações, consulte the section called “Ações de buckets do Amazon S3 rastreadas pelo registro em log do CloudTrail”.

Tópicos

- Limitações e restrições das tabelas de metadados
- Esquema de tabelas do S3 Metadata
- Configurar tabelas de metadados

- Consultar tabelas de metadados

Limitações e restrições das tabelas de metadados

Antes de criar uma configuração de tabelas de metadados, esteja ciente das seguintes limitações e restrições:

- No momento, o S3 Metadata só está disponível nas regiões Leste dos EUA (Norte da Virgínia), Leste dos EUA (Ohio) e Oeste dos EUA (Oregon).
- O S3 Metadata é compatível com todas as classes de armazenamento, exceto as seguintes:
  - A classe de armazenamento S3 Express One Zone
  - A classe de armazenamento S3 One Zone-Infrequent Access (S3 One Zone-IA; Z-IA) em buckets de diretório em zonas locais

> **Note**
>
> Para a classe de armazenamento S3 Intelligent-Tiering, o nível específico não é mostrado na tabela de metadados.

- Para criar uma configuração de tabelas de metadados, é necessário criar ou especificar um bucket de tabela do S3 para armazenar a tabela de metadados. Esse bucket de tabela deve estar na mesma Região da AWS e Conta da AWS que o bucket de uso geral.
- O S3 Metadata não é compatível com buckets de diretório ou buckets de tabela. Você pode criar configurações de tabelas de metadados somente para buckets de uso geral.
- O S3 Metadata não se aplica a nenhum objeto que já existia no bucket de uso geral antes de você criar a configuração de tabelas de metadados. Em outras palavras, o S3 Metadata captura apenas metadados de eventos de alteração (como uploads, atualizações e exclusões) que acontecem depois que você cria a configuração de tabelas de metadados.
- O S3 Metadata foi projetado para anexar continuamente à tabela de metadados conforme você faz alterações no bucket de uso geral. Cada atualização cria um snapshot, que é uma nova versão da tabela de metadados. Devido à natureza somente leitura da tabela de metadados, não é possível excluir registros da tabela de metadados. Você também não pode usar o recurso de expiração de snapshots da funcionalidade Tabelas do S3 para expirar snapshots antigos da tabela de metadados.

Para ajudar a minimizar os custos, você pode excluir periodicamente a configuração de tabelas de metadados e as tabelas de metadados, depois recriá-las. Para obter mais informações, consulte the section called “Excluir configurações de tabelas de metadados” e the section called “Excluir tabelas de metadados”.

- Ao criar ou atualizar políticas de bucket de tabela ou de tabela, não impeça que o Amazon S3 grave no bucket de tabela ou na tabela de metadados. Se o Amazon S3 não conseguir gravar no bucket de tabela ou na tabela de metadados, você deverá criar outra tabela de metadados excluindo a configuração de tabelas de metadados e a tabela de metadados e criando outra configuração.
- Antes de excluir uma tabela de metadados, primeiro é necessário excluir a configuração de tabelas de metadados associada no bucket de uso geral.
- Só é possível criar uma configuração de tabelas de metadados para um bucket de uso geral inteiro. Não é possível aplicar uma configuração de tabelas de metadados ao nível do prefixo.
- Você não pode pausar e retomar as atualizações em uma tabela de metadados. Em vez disso, você pode impedir a atualização de uma tabela de metadados excluindo a configuração de tabelas de metadados associada. Para voltar a receber atualizações, você deverá criar outra configuração de tabelas de metadados, o que criará outra tabela de metadados.
- As tabelas de metadados não contêm os mesmos metadados que estão disponíveis por meio da funcionalidade Inventário S3 ou da API REST do Amazon S3. Por exemplo, as seguintes informações não estão disponíveis nas tabelas de metadados:
  - Status de expiração ou transição da funcionalidade Ciclo de Vida do S3
  - Período de retenção ou modo de governança da funcionalidade Bloqueio de Objetos
  - Informações da lista de controle de acesso (ACL) do objeto
  - Status de replicação
- Não é possível ajustar o particionamento ou a classificação das tabelas de metadados. Como resultado, algumas consultas podem exigir varreduras de tabela e, portanto, podem ser menos eficientes.

Esquema de tabelas do S3 Metadata

As tabelas de metadados do Amazon S3 contêm linhas e colunas. Cada linha representa um evento de mutação que criou, atualizou ou excluiu um objeto no bucket de uso geral. A maioria desses eventos é o resultado de várias ações de usuários, mas alguns desses eventos são o resultado de

ações tomadas pelo Amazon S3 em seu nome, como expirações da funcionalidade Ciclo de Vida do S3 ou transições de classes de armazenamento.

O S3 Metadata é um pipeline de processamento de eventos projetado para manter a tabela de metadados final consistente com as alterações que ocorreram no bucket de uso geral. Esteja ciente de que, quando o S3 Metadata for notificado de que um objeto foi criado ou atualizado, esse objeto poderá já ter sido sobrescrito ou excluído do bucket. Por padrão, uma linha de tabela é criada para cada operação de bucket do S3. No entanto, se algum metadado do objeto for excluído ou sobrescrito, ou se os objetos não puderem mais ser recuperados, algumas colunas poderão mostrar um valor NULL para indicar qualquer esquema de metadados ausente.

O seguinte exemplo mostra uma tabela de metadados para um bucket de uso geral chamado `amzn-s3-demo-bucket`:

```
bucket                key                          sequence_number
                                                                    record_type
 record_timestamp           version_id   is_delete_marker   size   last_modified_date
   e_tag                           storage_class  is_multipart   encryption_status
 is_bucket_key_enabled   kms_key_arn
               checksum_algorithm   object_tags   user_metadata

    requester      source_ip_address   request_id
amzn-s3-demo-bucket   Finance/statement1.pdf
 80e737d8b4d82f776afffffffffffffff006737d8b4d82f776a00000000000000000000000000000000000000000000
   CREATE        2024-11-15 23:26:44.899                 FALSE
 6223   11/15/2024 23:26     e131b86632dda753aac4018f72192b83    STANDARD
 FALSE          SSE-KMS             FALSE                   arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890df   SSECRC32             {}
            {count -> Asia, customs -> false, family -> true, location -> Mary, name ->
 football, user -> United States}                      111122223333   192.0.2.1
    CVK8FWYRW0M9JW65
amzn-s3-demo-bucket   s3-dg.pdf
 80e737d8b4e39f1dbdfffffffffffffff006737d8b4e39f1dbd00000000000000000000000000000000000000000000
   CREATE        2024-11-15 23:26:44.942                 FALSE
 3554   11/15/2024 23:26     9bb49efc2d92c05558ddffbbde8636d5    STANDARD
 FALSE          DSSE-KMS            FALSE                   arn:aws:kms:us-
east-1:936810216292:key/0dcebce6-49fd-4cae-b2e2-5512ad281afd   SSESHA1              {}
           {}
                                                    111122223333   192.0.2.1
   CVKAQDRAZEG7KXAY
amzn-s3-demo-bucket   Development/Projects.xls
 80e737d8b4ed9ac5c6fffffffffffffff006737d8b4ed9ac5c60000000000000000000000000000000000000000000
```

```
  CREATE        2024-11-15 23:26:44.966                FALSE              7746
11/15/2024 23:26     729a6863e47fb9955b31bfabce984908    STANDARD   FALSE
SSE-S3              FALSE                    NULL
                                    SSECRC32             {}            {count -> Asia,
customs -> Canada, family -> Billiards, filter -> true, location -> Europe, name ->
Asia, user -> United States}   111122223333   192.0.2.1           CVK7Z6XQTQ90BSRV
```

As tabelas de metadados têm o seguinte esquema:

Nome da coluna	Obrigatório?	Tipo de dados	
`bucket`	Sim	String	O nome do bucket de uso geral. Para obter mais informações, consulte the section called “Regras de nomenclatura”.
`key`	Sim	String	O nome da chave de objeto (ou chave) que identifica o objeto no bucket de maneira única. Para obter mais informações, consulte the section called “Nomear objetos”.
`sequence_number`	Sim	String	O número de sequência, que é um ordinal incluído nos registros de determinado objeto. Para ordenar registros do mesmo bucket e chave, você pode classificar por `sequence_`

Nome da coluna	Obrigatório?	Tipo de dados	
			`number` . Para um bucket e uma chave específicos, um valor `sequence_number` maior em ordem lexicográfica implica que o registro foi introduzido no bucket mais recentemente.

Nome da coluna	Obrigatório?	Tipo de dados	
`record_type`	Sim	String	O tipo desse registro, que pode ser `CREATE`, `UPDATE_METADATA` ou `DELETE`. Registros `CREATE` indicam que um novo objeto (ou uma nova versão do objeto) foi gravado no bucket. Registros `UPDATE_METADATA` capturam alterações nos metadados mutáveis de um objeto existente, como a classe de armazenamento ou as tags. Registros `DELETE` indicam que esse objeto (ou essa versão do objeto) foi excluído. Quando o versionamento está habilitado, os registros `DELETE` representam um marcador de exclusão ou uma exclusão permanente. Os marcadores de exclusão têm um valor `DELETE` para

Nome da coluna	Obrigatório?	Tipo de dados	
			`record_type` e um valor `True` para `is_delete_marker` . Os registros de exclusão permanente têm valores nulos em todas as outras colunas, exceto `bucket`, `key`, `sequence_number` , `record_type` , `record_timestamp` e `version_id` . Para obter mais informações, consulte the section called “Excluir versões de objeto”.
`record_timestamp`	Sim	Carimbo de data/hora NTZ (sem fuso horário)	O carimbo de data/hora associado a esse registro.

Nome da coluna	Obrigatório?	Tipo de dados	
`version_id`	Não	String	O ID da versão do objeto. Quando você habilita o versionamento em um bucket, o Amazon S3 atribui um número de versão aos objetos adicionados ao bucket. Para obter mais informações, consulte the section called “Reter várias versões de objetos”. Os objetos que são armazenados no bucket antes da habilitação do versionamento têm um ID de versão nulo.

Nome da coluna	Obrigatório?	Tipo de dados	
`is_delete_marker`	Não	Booleano	O status do marcador de exclusão do objeto. Se o objeto for um marcador de exclusão, esse valor será `True`. Caso contrário, será `False`. Para obter mais informações, consulte the section called “Trabalhar com marcadores de exclusão”. **Note** As linhas adicionadas para marcadores de exclusão têm um valor `DELETE` para `record_type` , não `UPDATE_METADATA` . Se o marcador de exclusão for criado como resultado de uma expiração da funcionalidade Ciclo

Nome da coluna	Obrigatório?	Tipo de dados	
			de Vida do S3, o valor de `requester` será `s3.amazonaws.com`.
`size`	Não	Longo	O tamanho do objeto em bytes, sem incluir o tamanho de uploads fracionados incompletos ou metadados de objetos. Se `is_delete_marker` for `True`, o tamanho será `0`. Para obter mais informações, consulte the section called "Metadados do objeto definidos pelo sistema".

Nome da coluna	Obrigatório?	Tipo de dados	
`last_modified_date`	Não	Carimbo de data/hora NTZ (sem fuso horário)	A data de criação do objeto ou data da última modificação, o que aconteceu por último. Para uploads fracionados, a data de criação do objeto é a data em que o upload fracionado foi inicializado. Para obter mais informações, consulte the section called “Metadados do objeto definidos pelo sistema”.

Nome da coluna	Obrigatório?	Tipo de dados	
`e_tag`	Não	String	A tag de entidade (ETag), que é um hash do objeto. O ETag reflete as alterações apenas no conteúdo de um objeto, não em seus metadados. A ETag pode ser um resumo MD5 dos dados do objeto. O fato de a ETag ser um resumo MD5 depende de como o objeto foi criado e de como ele é criptografado. Para obter mais informaçõ es, consulte Object na Referência da API do Amazon S3.

Nome da coluna	Obrigatório?	Tipo de dados	
`storage_class`	Não	String	A classe de armazenamento usada para armazenar o objeto. Uma destas opções: `STANDARD`, `REDUCED_REDUNDANCY`, `STANDARD_IA`, `ONEZONE_IA`, `INTELLIGENT_TIERING`, `GLACIER`, `DEEP_ARCHIVE` ou `GLACIER_IR`. Para obter mais informações, consulte the section called "Compreender e gerenciar classes de armazenamento".
`is_multipart`	Não	Booleano	O tipo de upload do objeto. Se o objeto foi carregado como um upload fracionado, esse valor será `True`. Caso contrário, será `False`. Para obter mais informações, consulte the section called "Usar multipart upload".

Nome da coluna	Obrigatório?	Tipo de dados	
`encryption_status`	Não	String	O status da criptografia do lado do servidor, dependendo do tipo de chave de criptografia usada: criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3), criptografia do lado do servidor com chaves do AWS Key Management Service (AWS KMS) (SSE-KMS), criptografia de camada dupla do lado do servidor com AWS KMS keys (DSSE-KMS) ou criptografia do lado do servidor com chaves fornecidas pelo cliente (SSE-C). Se o objeto não estiver criptografado, esse valor será nulo. Os valores possíveis são `SSE-S3`, `SSE-KMS`, `DSSE-KMS`, `SSE-C` ou nulo. Para obter mais informações, consulte the section called “Criptografia de dados”.

Nome da coluna	Obrigatório?	Tipo de dados	
`is_bucket_key_enabled`	Não	Booleano	O status de habilitação da chave de bucket do S3 do objeto. Se o objeto usar uma chave de bucket do S3 para SSE-KMS, esse valor será `True`. Caso contrário, será `False`. Para obter mais informações, consulte the section called "Configuração de uma chave de bucket do S3 para um objeto".

Nome da coluna	Obrigatório?	Tipo de dados	
`kms_key_arn`	Não	String	O nome do recurso da Amazon (ARN) para a chave do KMS com a qual o objeto é criptografado, para linhas em que `encryption_status` é `SSE-KMS` ou `DSSE-KMS`. Se o objeto não estiver criptografado com SSE-KMS ou DSSE-KMS, o valor será nulo. Para obter mais informações, consulte the section called “Chaves do KMS armazenadas no AWS KMS (SSE-KMS)” e the section called “Criptografia de camada dupla do lado do servidor (DSSE-KMS)”. **Note** Se uma linha representa uma versão do objeto que não existia mais no momento em que um

Nome da coluna	Obrigatório?	Tipo de dados	
			evento de exclusão ou substituição foi processado, `kms_key_arn` conterá um valor nulo, mesmo que o valor da coluna `encryption_status` seja `SSE-KMS` ou `DSSE-KMS`.
`checksum_algorithm`	Não	String	O algoritmo usado para criar a soma de verificação do objeto, podendo ser `CRC64NVME` , `CRC32`, `CRC32C`, `SHA1` ou `SHA256`. Se nenhuma soma de verificação estiver presente, esse valor será nulo. Para obter mais informações, consulte the section called "Usar algoritmos de soma de verificação compatíveis".

Nome da coluna	Obrigatório?	Tipo de dados	
`object_tags`	Não	Mapa <String, String>	As tags que estão associadas ao objeto. As tags de objeto são armazenadas como um mapa de pares de chave/valor. Se um objeto não tiver nenhum tag, um mapa vazio ({}) será armazenado. Para obter mais informações, consulte the section called "Categorizar objetos com tags".

> **Note**
>
> Se o valor de `record_type` for `DELETE`, a coluna `object_tags` conterá um valor nulo. Se o valor de `record_type` for `CREATE` ou `UPDATE_METADATA`, as linhas que representam versões

Nome da coluna	Obrigatório?	Tipo de dados	
			de objetos que não existiam mais no momento em que um evento de exclusão ou substituição foi processado conterão um valor nulo na coluna `object_tags` .

Nome da coluna	Obrigatório?	Tipo de dados	
`user_metadata`	Não	Mapa <String, String>	Os metadados de usuários associados ao objeto. Os metadados de usuários são armazenados como um mapa de pares de chave/valor. Se um objeto não tiver nenhum metadado de usuário, um mapa vazio (`{}`) será armazenado. Para obter mais informações, consulte the section called "Metadados do objeto definidos pelo usuário". **Note** Se o valor de `record_type` for `DELETE`, a coluna `user_metadata` conterá um valor nulo. Se o valor de `record_type` for `CREATE` ou

Nome da coluna	Obrigatório?	Tipo de dados	
			`UPDATE_METADATA` , as linhas que representam versões de objetos que não existiam mais no momento em que um evento de exclusão ou substituição foi processado conterão um valor nulo na coluna `user_metadata` .
`requester`	Não	String	O ID da Conta da AWS do solicitante ou da entidade principal do AWS service (Serviço da AWS) que fez a solicitação.

Nome da coluna	Obrigatório?	Tipo de dados	
`source_ip_address`	Não	String	O endereço IP de origem da solicitação. Para registros gerados por uma solicitação de usuário, esta coluna contém o endereço IP de origem da solicitação. Para ações realizadas pelo Amazon S3 ou outro AWS service (Serviço da AWS) em nome do usuário, esta coluna contém um valor nulo.
`request_id`	Não	String	O ID associado à solicitação.

Configurar tabelas de metadados

O Amazon S3 Metadata acelera a descoberta de dados ao capturar automaticamente os metadados dos objetos nos buckets de uso geral e armazená-los em tabelas do Apache Iceberg totalmente gerenciadas e somente leitura que você pode consultar. Essas tabelas somente leitura são chamadas de tabelas de metadados. À medida que objetos são adicionados, atualizados e removidos dos buckets de uso geral, o S3 Metadata atualiza automaticamente as tabelas de metadados correspondentes para refletir as alterações mais recentes.

Com o S3 Metadata, você pode facilmente encontrar, armazenar e consultar metadados para os objetos do S3, para que possa preparar dados rapidamente para uso em analytics de negócios, treinamento de modelos de inteligência artificial e machine learning (IA/ML) e muito mais.

Para gerar e armazenar metadados de objetos em uma tabela de metadados gerenciada pelo S3, crie uma configuração de tabelas de metadados para o bucket de uso geral. O Amazon S3 foi projetado para atualizar continuamente a tabela de metadados a fim de refletir as alterações mais

recentes nos dados, desde que a configuração esteja ativa no bucket. Além disso, o Amazon S3 otimiza continuamente as tabelas de metadados para ajudar a reduzir os custos de armazenamento e melhorar a performance das consultas de analytics.

Para criar uma configuração de tabelas de metadados, garanta que você tenha as permissões do AWS Identity and Access Management (IAM) necessárias para criar e gerenciar tabelas de metadados. Você também deve criar ou especificar um bucket de tabela do S3 para armazenar a tabela de metadados. Esse bucket de tabela deve estar na mesma Região da AWS e Conta da AWS que o bucket de uso geral.

Para monitorar as atualizações na configuração de tabelas de metadados, você pode usar o AWS CloudTrail. Para obter mais informações, consulte the section called “Ações de buckets do Amazon S3 rastreadas pelo registro em log do CloudTrail”.

Tópicos

- Definir permissões para configurar tabelas de metadados
- Criar configurações de tabelas de metadados
- Controlar o acesso às tabelas de metadados
- Excluir configurações de tabelas de metadados
- Excluir tabelas de metadados

Definir permissões para configurar tabelas de metadados

Para criar uma configuração de tabelas de metadados, é necessário ter as permissões do AWS Identity and Access Management (IAM) necessárias para criar e gerenciar essa configuração de tabelas de metadados e para criar e gerenciar a tabela de metadados e o bucket de tabela em que a tabela de metadados está armazenada.

Para criar e gerenciar a configuração de tabelas de metadados, você deve ter as seguintes permissões:

- `s3:CreateBucketMetadataTableConfiguration`: essa permissão possibilita criar uma configuração de tabelas de metadados para o bucket de uso geral.
- `s3:GetBucketMetadataTableConfiguration`: essa permissão possibilita recuperar informações sobre a configuração de tabelas de metadados.
- `s3:DeleteBucketMetadataTableConfiguration`: essa permissão possibilita excluir a configuração de tabelas de metadados.

Para criar e trabalhar com tabelas e buckets de tabela, é necessário ter determinadas permissões `s3tables`. No mínimo, para criar uma configuração de tabelas de metadados, você deve ter as seguintes permissões `s3tables`:

- `s3tables:CreateNamespace`: essa permissão possibilita criar um namespace em um bucket de tabela. As tabelas de metadados usam o namespace padrão `aws_s3_metadata`.
- `s3tables:GetTable`: essa permissão possibilita recuperar informações sobre a tabela de metadados.
- `s3tables:CreateTable`: essa permissão possibilita criar a tabela de metadados.
- `s3tables:PutTablePolicy`: essa permissão possibilita adicionar ou atualizar a política da tabela de metadados.

Para ter informações detalhadas sobre todas as permissões de tabelas e de buckets de tabela, consulte Access management for S3 Tables.

> **Important**
>
> Se você também quiser integrar o bucket de tabela com os serviços de analytics da AWS para poder consultar a tabela de metadados, precisará de permissões adicionais. Para ter mais informações, consulte Integrating Amazon S3 Tables with AWS analytics services.

Permissões para SSE-KMS

Para acessar buckets de tabela do S3 ou tabelas do S3 que estão usando criptografia do lado do servidor com chaves do AWS Key Management Service (AWS KMS) (SSE-KMS), você precisa incluir outras permissões.

1. O usuário ou o perfil do IAM precisa das permissões a seguir. Você pode conceder essas permissões no console do IAM, em https://console.aws.amazon.com/iam/.
   a. `s3tables:PutTableEncryption` para configurar a criptografia de tabelas.
   b. `s3tables:PutTableBucketEncryption` para configurar a criptografia do bucket de tabela.
   c. `kms:DescribeKey` na chave usada do AWS KMS.
2. Na política de recursos para a chave do KMS, você precisa das permissões a seguir. Você pode conceder essas permissões usando o console do KMS, em https://console.aws.amazon.com/kms.

a. Permissão `kms:GenerateDataKey` para `metadata.s3.amazonaws.com` e `maintenance.s3tables.amazonaws.com`.

b. Permissão `kms:Decrypt` para `metadata.s3.amazonaws.com` e `maintenance.s3tables.amazonaws.com`.

c. Permissão `kms:DescribeKey` para a entidade principal AWS invocadora.

Para ter mais informações sobre como conceder as permissões necessárias ao serviço S3 Metadata, consulte a documentação em Conceder permissões à entidade principal do serviço S3 Metadata para usar sua chave do KMS.

Exemplo de política

Para criar e trabalhar com tabelas de metadados e buckets de tabela, você pode usar o exemplo de política a seguir. Nesta política, o bucket de uso geral ao qual você está aplicando a configuração de tabelas de metadados é chamado de *amzn-s3-demo-source-bucket*. O bucket de tabela em que você está armazenando a tabela de metadados é chamado de *amzn-s3-demo-bucket*. Para usar essa política, substitua esses nomes de bucket e os *user input placeholders* por suas próprias informações:

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"PermissionsToWorkWithMetadataTables",
         "Effect":"Allow",
         "Action":[
            "s3:CreateBucketMetadataTableConfiguration",
            "s3:GetBucketMetadataTableConfiguration",
            "s3:DeleteBucketMetadataTableConfiguration",
            "s3tables:*"
         ],
         "Resource":[
            "arn:aws:s3:::bucket/amzn-s3-demo-source-bucket",
            "arn:aws:s3tables:region:account_id:bucket/amzn-s3-demo-bucket",
            "arn:aws:s3tables:region:account_id:bucket/amzn-s3-demo-bucket/table/*"
         ]
      }
   ]
}
```

Criar configurações de tabelas de metadados

Para gerar e armazenar o Amazon S3 Metadata em uma tabela de metadados do Apache Iceberg totalmente gerenciada, crie uma configuração de tabelas de metadados para o bucket de uso geral. O Amazon S3 foi projetado para atualizar continuamente a tabela de metadados a fim de refletir as alterações mais recentes nos dados, desde que a configuração esteja ativa no bucket. Além disso, o Amazon S3 otimiza continuamente a tabela de metadados para ajudar a reduzir os custos de armazenamento e melhorar a performance das consultas de analytics.

As tabelas de metadados têm o seguinte formato de nome do recurso da Amazon (ARN):

`arn:aws:s3tables:`*`region-code`*`:`*`account-id`*`:bucket/`*`table-bucket-name`*`/table/`*`metadata_table_name`*

As tabelas de metadados totalmente gerenciadas pelo Amazon S3 são armazenadas no namespace `aws_s3_metadata` do bucket de tabela. Para ter mais informações sobre os namespaces em buckets de tabela, consulte Table namespaces.

Você pode criar uma configuração de tabelas de metadados usando o console do Amazon S3, a AWS Command Line Interface (AWS CLI), os AWS SDKs ou a API REST do Amazon S3.

Pré-requisitos

Para criar uma configuração de tabelas de metadados, primeiro é necessário fazer o seguinte:

- Garanta que você tenha as permissões do AWS Identity and Access Management (IAM) necessárias para criar e gerenciar tabelas de metadados. Para obter mais informações, consulte the section called “Permissões para tabelas de metadados”.
- Crie um bucket de tabela do S3 para armazenar a tabela de metadados. Esse bucket de tabela deve estar na mesma Região da AWS e Conta da AWS que o bucket de uso geral. Para ter mais informações sobre como criar buckets de tabela, consulte Creating table buckets. Se estiver usando o console do Amazon S3 para criar a configuração, você poderá executar essa etapa como parte desse processo.
- Integre o bucket de tabela ao AWS Glue Data Catalog para que você possa consultar diretamente as tabelas de metadados com mecanismos de consulta, como Amazon Athena, Amazon EMR, Amazon Redshift, Apache Spark, Apache Trino e qualquer outra aplicação compatível com o formato Apache Iceberg. Para obter mais informações, consulte the section called “Consultar tabelas de metadados com serviços de analytics da AWS”.

Criar uma configuração de tabelas de metadados

Usar o console do S3

Como criar uma configuração de tabelas de metadados

Antes de criar uma configuração de tabelas de metadados, revise e cumpra os pré-requisitos e revise the section called “Limitações e restrições”.

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets de uso geral.
3. Escolha o bucket de uso geral para o qual você deseja criar uma configuração de tabelas de metadados.

   > **Note**
   >
   > Garanta que esse bucket de uso geral esteja em uma Região da AWS onde os buckets de tabela estejam disponíveis. Os buckets de tabela só estão disponíveis nas regiões Leste dos EUA (Norte da Virgínia), Leste dos EUA (Ohio) e Oeste dos EUA (Oregon).

4. Na página de detalhes dos buckets, escolha a guia Metadados.
5. Na guia Metadados, escolha Criar configuração de metadados.
6. Na página Criar configuração de metadados, em Bucket de tabela de destino, especifique um bucket de tabela para armazenar a tabela de metadados. O bucket de tabela deve estar na mesma Conta da AWS e Região da AWS que o bucket de uso geral.

   Se você ainda não tiver um bucket de tabela, escolha Criar bucket de tabela. Os nomes de buckets de tabela devem ter entre 3 e 63 caracteres e ser exclusivos dentro da Conta da AWS na Região da AWS escolhida. Os caracteres válidos são a–z, 0–9 e hifens (-). Para ter mais informações sobre como criar um bucket de tabela, consulte Creating table buckets.

   Ao criar o bucket de tabela, integre-o ao AWS Glue Data Catalog. Para obter mais informações, consulte the section called “Consultar tabelas de metadados com serviços de analytics da AWS”.
7. Em Nome da tabela de metadados, especifique o nome que você deseja que a tabela tenha. O nome da tabela de metadados deve ter entre 1 e 255 caracteres e ser exclusivo no namespace `aws_s3_metadata` do bucket de tabela. Os caracteres válidos são letras minúsculas, números e sublinhados (_).

8. Escolha Criar configuração de tabelas de metadados.

Se a configuração de tabelas de metadados for bem-sucedida, o ARN da tabela de metadados será exibido na guia Metadados com o bucket de tabela especificado e o nome da tabela de metadados.

Para monitorar as atualizações na configuração de tabelas de metadados, você pode usar o AWS CloudTrail. Para obter mais informações, consulte the section called “Ações de buckets do Amazon S3 rastreadas pelo registro em log do CloudTrail”.

Usar a AWS CLI

Para executar os comandos a seguir, você deve ter a AWS CLI instalada e configurada. Se ainda não tiver a AWS CLI instalada, consulte Instalar ou atualizar a versão mais recente da AWS CLI no Guia do usuário da AWS Command Line Interface.

Também é possível executar comandos da AWS CLI pelo console usando o AWS CloudShell. O AWS CloudShell é um shell pré-autenticado e baseado em navegador que você pode iniciar diretamente do AWS Management Console. Para ter mais informações, consulte What is CloudShell? e Getting started with AWS CloudShell no Guia do usuário do AWS CloudShell.

Como criar uma configuração de tabelas de metadados usando a AWS CLI

Antes de criar uma configuração de tabelas de metadados, revise e cumpra os pré-requisitos e revise the section called “Limitações e restrições”.

Para usar os comandos a seguir, substitua os *`user input placeholders`* por suas próprias informações.

1. Se você ainda não tiver um bucket de tabela, use o comando a seguir para criar um bucket de tabela a fim de armazenar a tabela de metadados. Garanta que o bucket de tabela esteja na mesma Região da AWS que o bucket de uso geral para o qual você deseja criar uma configuração de tabelas de metadados.

```
aws s3tables create-table-bucket --name amzn-s3-demo-bucket --region us-east-2
```

2. Para verificar se o bucket de tabela foi criado, use o seguinte comando:

```
aws s3tables list-table-buckets --region us-east-2
```

3. Crie um arquivo JSON que contenha a configuração de tabelas de metadados e salve-o (por exemplo, `metadata-config.json`). Veja a seguir uma configuração de amostra.

Os nomes de buckets de tabela devem ter entre 3 e 63 caracteres e ser exclusivos dentro da Conta da AWS na Região da AWS escolhida. Os caracteres válidos são a–z, 0–9 e hifens (-). Para ter mais informações sobre como criar um bucket de tabela, consulte Creating table buckets.

O nome da tabela de metadados deve ter entre 1 e 255 caracteres e ser exclusivo no namespace `aws_s3_metadata` do bucket de tabela. Os caracteres válidos são letras minúsculas, números e sublinhados (_).

```
{
  "S3TablesDestination": {
    "TableBucketArn": "arn:aws:s3tables:us-east-2:111122223333:bucket/amzn-s3-demo-bucket",
    "TableName": "test_metadata_table"
  }
}
```

4. Use o comando a seguir para aplicar a configuração de tabelas de metadados ao bucket de uso geral (por exemplo, *amzn-s3-demo-source-bucket*):

```
aws s3api create-bucket-metadata-table-configuration \
--bucket amzn-s3-demo-source-bucket \
--metadata-table-configuration  file://./metadata-config.json \
--region us-east-2
```

5. Para verificar se a configuração foi criada, execute o seguinte comando:

```
aws s3api get-bucket-metadata-table-configuration \
--bucket amzn-s3-demo-source-bucket \
--region us-east-2
```

Para monitorar as atualizações na configuração de tabelas de metadados, você pode usar o AWS CloudTrail. Para obter mais informações, consulte the section called “Ações de buckets do Amazon S3 rastreadas pelo registro em log do CloudTrail”.

Uso da API REST

Você pode enviar solicitações REST para criar uma configuração de tabelas de metadados. Para obter mais informações, consulte CreateBucketMetadataTableConfiguration na Referência da API do Amazon S3.

Uso dos SDKs da AWS

Você pode usar os AWS SDKs para criar uma configuração de tabelas de metadados no Amazon S3. Para ter mais informações, consulte a lista de SDKs compatíveis na Referência de API do Amazon S3.

Controlar o acesso às tabelas de metadados

Para controlar o acesso às tabelas de metadados do Amazon S3, você pode usar políticas baseadas em recurso do AWS Identity and Access Management (IAM) anexadas ao bucket de tabela e à tabela de metadados. Em outras palavras, você pode controlar o acesso às tabelas de metadados tanto ao nível do bucket de tabela quanto ao nível da tabela.

Para ter mais informações sobre como controlar o acesso aos buckets e às tabelas, consulte Access management for S3 Tables.

> **Important**
>
> Não impeça que o Amazon S3 grave no bucket de tabela ou na tabela de metadados. Se o Amazon S3 não conseguir gravar no bucket de tabela ou na tabela de metadados, você deverá criar outra tabela de metadados excluindo a configuração de tabelas de metadados e criando outra configuração.

Você também pode controlar o acesso às linhas e colunas da tabela de metadados por meio do AWS Lake Formation. Para ter mais informações, consulte Managing Lake Formation permissions e Data filtering and cell-level security in Lake Formation no Guia do desenvolvedor do AWS Lake Formation.

Excluir configurações de tabelas de metadados

Se você quiser interromper a atualização de uma configuração de tabelas de metadados para um bucket de uso geral do Amazon S3, poderá excluir a configuração de tabelas de metadados que está anexada ao bucket. A exclusão de uma configuração de tabelas de metadados exclui apenas a

configuração. O bucket de tabela e a tabela de metadados continuarão existindo, mesmo que você exclua a configuração de tabelas de metadados. No entanto, a tabela de metadados não será mais atualizada.

Para excluir a tabela de metadados, consulte the section called “Excluir uma tabela de metadados”. Para excluir o bucket de tabela, consulte Deleting table buckets e DeleteTableBucket na Referência de API do Amazon S3.

Você pode excluir uma configuração de tabelas de metadados usando o console do Amazon S3, a AWS Command Line Interface (AWS CLI), os AWS SDKs ou a API REST do Amazon S3.

Excluir uma configuração de tabelas de metadados

Usar o console do S3

Como excluir uma configuração de tabelas de metadados

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets de uso geral.
3. Escolha o bucket de uso geral do qual você deseja remover uma configuração de tabelas de metadados.
4. Na página de detalhes dos buckets, escolha a guia Metadados.
5. Na guia Metadados, escolha Excluir.
6. Na caixa de diálogo Excluir configuração de metadados, insira **`confirm`** para confirmar que deseja excluir a configuração. Escolha Excluir.

Como usar o AWS CLI

Para executar os comandos a seguir, você deve ter a AWS CLI instalada e configurada. Se ainda não tiver a AWS CLI instalada, consulte Instalar ou atualizar a versão mais recente da AWS CLI no Guia do usuário da AWS Command Line Interface.

Também é possível executar comandos da AWS CLI pelo console usando o AWS CloudShell. O AWS CloudShell é um shell pré-autenticado e baseado em navegador que você pode iniciar diretamente do AWS Management Console. Para ter mais informações, consulte What is CloudShell? e Getting started with AWS CloudShell no Guia do usuário do AWS CloudShell.

Como excluir uma configuração de tabelas de metadados usando a AWS CLI

Para usar os comandos a seguir, substitua os *user input placeholders* por suas próprias informações.

1. Use o comando a seguir para excluir a configuração de tabelas de metadados do bucket de uso geral (por exemplo, *amzn-s3-demo-source-bucket*):

```
aws s3api delete-bucket-metadata-table-configuration \
--bucket amzn-s3-demo-source-bucket \
--region us-east-2
```

2. Para verificar se a configuração foi excluída, execute o seguinte comando:

```
aws s3api get-bucket-metadata-table-configuration \
--bucket amzn-s3-demo-source-bucket \
--region us-east-2
```

Uso da API REST

Você pode enviar solicitações REST para excluir uma configuração de tabelas de metadados. Para obter mais informações, consulte DeleteBucketMetadataTableConfiguration.

Uso da SDKs AWS

Você pode usar os AWS SDKs para excluir uma configuração de tabelas de metadados no Amazon S3. Para ter mais informações, consulte a lista de SDKs compatíveis.

Excluir tabelas de metadados

Se você quiser excluir a tabela de metadados que criou para um bucket de uso geral do Amazon S3, poderá excluir essa tabela de metadados do bucket de tabela.

> **Note**
>
> Antes de excluir uma tabela de metadados, recomendamos primeiro excluir a configuração de tabelas de metadados associada no bucket de uso geral. Para obter mais informações, consulte the section called “Excluir configurações de tabelas de metadados”.

Para excluir o bucket de tabela, consulte Deleting table buckets e DeleteTableBucket na Referência de API do Amazon S3.

Você pode excluir uma tabela de metadados usando a AWS Command Line Interface (AWS CLI), os AWS SDKs ou a API REST do Amazon S3.

Excluir uma tabela de metadados

Como usar o AWS CLI

Para executar os comandos a seguir, você deve ter a AWS CLI instalada e configurada. Se ainda não tiver a AWS CLI instalada, consulte Instalar ou atualizar a versão mais recente da AWS CLI no Guia do usuário da AWS Command Line Interface.

Também é possível executar comandos da AWS CLI pelo console usando o AWS CloudShell. O AWS CloudShell é um shell pré-autenticado e baseado em navegador que você pode iniciar diretamente do AWS Management Console. Para ter mais informações, consulte What is CloudShell? e Getting started with AWS CloudShell no Guia do usuário do AWS CloudShell.

Como excluir uma configuração de tabelas de metadados usando a AWS CLI

Para usar os comandos a seguir, substitua os *`user input placeholders`* por suas próprias informações.

1. Use o comando a seguir para excluir a tabela de metadados do bucket de tabela (por exemplo, *`amzn-s3-demo-bucket`*):

```
aws s3tables delete-table \
--table-bucket-arn arn:aws:s3tables:us-east-2:111122223333:bucket/amzn-s3-demo-bucket \
--namespace aws_s3_metadata \
--name test_metadata_table \
--region us-east-2
```

2. Para verificar se a tabela foi excluída, execute o seguinte comando:

```
aws s3tables get-table \
--table-bucket-arn arn:aws:s3tables:us-east-2:111122223333:bucket/amzn-s3-demo-bucket \
--namespace aws_s3_metadata \
--name test_metadata_table \
--region us-east-2
```

Uso da API REST

Você pode enviar solicitações REST para excluir uma configuração de tabelas de metadados. Para obter mais informações, consulte DeleteTable na Referência da API do Amazon S3.

Uso dos SDKs da AWS

Você pode usar os AWS SDKs para excluir uma configuração de tabelas de metadados no Amazon S3. Para ter mais informações, consulte a lista de SDKs compatíveis na Referência de API do Amazon S3.

Consultar tabelas de metadados

O Amazon S3 Metadata permite que você analise tabelas de metadados gerenciadas pelo S3 com qualquer mecanismo de consulta compatível com o formato Apache Iceberg. Ao integrar buckets de tabela do S3 a serviços de analytics da AWS, você pode usar alguns serviços, como Amazon Athena, Amazon Redshift e outros, para ajudar a fazer o seguinte com as tabelas de metadados:

- Descobrir padrões e tendências de uso do armazenamento.
- Auditar o uso de chaves de criptografia do AWS Key Management Service (AWS KMS) nos objetos.
- Pesquisar objetos por metadados definidos pelo usuário e tags de objeto.
- Entender as alterações nos metadados de objetos ao longo do tempo.
- Saber quando os objetos são atualizados ou excluídos, incluindo o ID da Conta da AWS ou o endereço IP que fez a solicitação.

Depois que os buckets de tabela forem integrados aos serviços de analytics da AWS, você poderá consultar as tabelas de metadados. Isso inclui unir tabelas de metadados gerenciadas pelo S3 e tabelas de metadados personalizadas, permitindo que você consulte vários conjuntos de dados, desde que as tabelas de metadados estejam armazenadas no mesmo bucket de tabela.

A partir daí, você pode criar painéis interativos com os dados de consulta usando o Amazon QuickSight.

Considerações sobre os preços de consultas

Há preços adicionais para a execução de consultas nas tabelas de metadados. Saiba mais nas informações sobre os preços do mecanismo de consulta que você está usando.

Para ter mais informações sobre como tornar as consultas mais econômicas, consulte Otimizar a performance das consultas de tabelas de metadados.

Tópicos

- Consultar tabelas de metadados com serviços de analytics da AWS
- Consultar tabelas de metadados com mecanismos de consulta de código aberto
- Otimizar a performance das consultas de tabelas de metadados
- Exemplos de consultas a tabelas de metadados
- Unir metadados personalizados com tabelas de metadados do S3
- Visualizar dados de tabelas de metadados com o Amazon QuickSight

Consultar tabelas de metadados com serviços de analytics da AWS

Você pode consultar as tabelas de metadados gerenciadas pelo S3 usando os serviços de analytics da AWS, como Amazon Athena, Amazon Redshift e Amazon EMR.

Antes de executar consultas, primeiro é necessário integrar os buckets de tabela do S3 na região e Conta da AWS aos serviços de analytics da AWS.

Consultar tabelas de metadados com o Amazon Athena

Depois de integrar os buckets de tabela do S3 aos serviços de analytics da AWS, você pode começar a consultar as tabelas de metadados no Athena. Nas consultas, especifique o catálogo como `s3tablescatalog` e o banco de dados como `aws_s3_metadata` (que é o namespace para as tabelas de metadados). Para ter mais informações, consulte Querying Amazon S3 tables with Athena.

Consultar tabelas de metadados com o Amazon Redshift

Depois de integrar os buckets de tabela do S3 aos serviços de analytics da AWS, crie um link de recurso para o namespace da tabela de metadados (`aws_s3_metadata`). Feito isso, você pode começar a consultar as tabelas de metadados no console do Amazon Redshift. Para ter mais informações, consulte Accessing Amazon S3 tables with Amazon Redshift.

Consultar tabelas de metadados com o Amazon EMR

Para consultar as tabelas de metadados usando o Amazon EMR, crie um cluster do Amazon EMR configurado para Apache Iceberg e estabeleça conexão com as tabelas de metadados usando o

Apache Spark. Você pode configurar isso integrando os buckets de tabela do S3 aos serviços de analytics da AWS ou usando o catálogo de cliente de código aberto Amazon S3 Tables Catalog for Iceberg.

Para ter mais informações, consulte Accessing Amazon S3 tables with Amazon EMR.

Consultar tabelas de metadados com mecanismos de consulta de código aberto

Você pode consultar as tabelas de metadados gerenciadas pelo S3 usando mecanismos de consulta de código aberto, como o Apache Spark. Para consultar as tabelas de metadados, você precisa do catálogo de cliente Amazon S3 Tables Catalog for Apache Iceberg (uma biblioteca de código aberto hospedada pelo AWS Labs).

Para ter mais informações, consulte Querying Amazon S3 tables with Apache Spark.

Otimizar a performance das consultas de tabelas de metadados

Como o S3 Metadata é baseado no formato de tabela Apache Iceberg, você pode otimizar a performance e o custo das consultas a tabelas de metadados usando intervalos de tempo específicos.

Por exemplo, a consulta SQL a seguir fornece o nível de sensibilidade de novos objetos em um bucket de uso geral do S3:

```
SELECT key, object_tags['SensitivityLevel']
FROM aws_s3_metadata.my_metadata_table
WHERE record_type = 'CREATE'
GROUP BY object_tags['SensitivityLevel']
```

Essa consulta examina toda a tabela de metadados, podendo levar muito tempo para ser executada. Para melhorar a performance, você pode incluir a coluna `record_timestamp` para enfocar um intervalo de tempo específico. Aqui está uma versão atualizada da consulta anterior que analisa novos objetos do mês passado:

```
SELECT key, object_tags['SensitivityLevel']
FROM aws_s3_metadata.my_metadata_table
WHERE record_type = 'CREATE'
AND record_timestamp > (CURRENT_TIMESTAMP - interval '1' month)
GROUP BY object_tags['SensitivityLevel']
```

Exemplos de consultas a tabelas de metadados

Os exemplos a seguir mostram como você pode obter diferentes tipos de informações das tabelas do S3 Metadata usando consultas SQL padrão.

Lembre-se do seguinte ao usar esses exemplos:

- Os exemplos foram escritos para funcionar com o Amazon Athena. Talvez seja necessário modificar os exemplos para trabalhar com um mecanismo de consulta diferente.
- Entenda como otimizar as consultas.
- Substitua *amzn-s3-demo-bucket* pelo nome do bucket de tabela do S3 que está armazenando a tabela de metadados.
- Substitua *my_metadata_table* pelo nome da tabela de metadados que você está consultando.
- Para conferir uma lista de colunas compatíveis, consulte Esquema de tabelas do S3 Metadata.

Encontrar objetos por extensão de arquivo

A consulta a seguir retorna objetos com uma extensão de arquivo específica (`.jpg` neste caso).

```
SELECT key FROM "s3tablescatalog/amzn-s3-demo-
bucket"."aws_s3_metadata"."my_metadata_table"
WHERE key LIKE '%.jpg'
AND record_type = 'CREATE'
```

Listar exclusões de objetos

A consulta a seguir retorna eventos de exclusão de objetos, incluindo o ID da Conta da AWS ou a entidade principal do serviço da AWS que fez a solicitação.

```
SELECT DISTINCT bucket, key, sequence_number, record_type, record_timestamp, requester,
 source_ip_address, version_id
FROM "s3tablescatalog/amzn-s3-demo-bucket"."aws_s3_metadata"."my_metadata_table"
WHERE record_type = 'DELETE';
```

Listar as chaves de criptografia do AWS KMS usadas pelos objetos

A consulta a seguir retorna os ARNs das chaves do AWS Key Management Service (AWS KMS) que criptografam os objetos.

```
SELECT DISTINCT kms_key_arn
```

```
FROM "s3tablescatalog/amzn-s3-demo-bucket"."aws_s3_metadata"."my_metadata_table";
```

Listar objetos que não usam chaves do KMS

A consulta a seguir retorna objetos que não estão criptografados com chaves do AWS KMS.

```
SELECT DISTINCT kms_key_arn
FROM "s3tablescatalog/amzn-s3-demo-bucket"."aws_s3_metadata"."my_metadata_table"
WHERE encryption_status NOT IN ('SSE-KMS', 'DSSE-KMS')
AND record_type = 'CREATE';
```

Visualizar metadados fornecidos pelo Amazon Bedrock

Alguns serviços da AWS (como o Amazon Bedrock) fazem upload de objetos no Amazon S3. Você pode consultar os metadados de objetos fornecidos por esses serviços. Por exemplo, a consulta a seguir inclui a coluna `user_metadata` para determinar se há objetos carregados pelo Amazon Bedrock em um bucket de uso geral.

```
SELECT DISTINCT bucket, key, sequence_number, record_type, record_timestamp,
 user_metadata
FROM "s3tablescatalog/amzn-s3-demo-bucket"."aws_s3_metadata"."my_metadata_table"
WHERE record_type = 'CREATE'
AND user_metadata['content-source'] = 'AmazonBedrock';
```

Se o Amazon Bedrock tiver feito upload de um objeto no bucket, a coluna `user_metadata` exibirá os seguintes metadados associados ao objeto no resultado da consulta:

```
user_metadata
{content-additional-params -> requestid="CVK8FWYRW0M9JW65",
 signedContentSHA384="38b060a751ac96384cd9327eb1b1e36a21fdb71114be07434c0cc7bf63f6e1da274edebfe
 content-model-id -> bedrock-model-arn, content-source -> AmazonBedrock}
```

Noções básicas sobre o estado atual dos objetos

A consulta a seguir pode ajudar você a determinar o estado atual dos objetos. A consulta identifica a versão mais recente de cada objeto, filtra para eliminar os objetos excluídos e marca a versão mais recente de cada objeto com base nos números de sequência. Os resultados são ordenados pelas colunas `bucket`, `key` e `sequence_number`.

```
WITH records_of_interest as (
   -- Start with a query that can narrow down the records of interest.
```

```
    SELECT * from "s3tablescatalog/amzn-s3-demo-
bucket"."aws_s3_metadata"."my_metadata_table"
),

version_stacks as (
   SELECT *,
          -- Introduce a column called 'next_sequence_number', which is the next larger
          -- sequence_number for the same key version_id in sorted order.
          LEAD(sequence_number, 1) over (partition by (bucket, key,
 coalesce(version_id, '')) order by sequence_number ASC) as next_sequence_number
   from records_of_interest
),

-- Pick the 'tip' of each version stack triple: (bucket, key, version_id).
-- The tip of the version stack is the row of that triple with the largest sequencer.
-- Selecting only the tip filters out any row duplicates.
-- This isn't typical, but some events can be delivered more than once to the table
-- and include rows that might no longer exist in the bucket (since the
-- table contains rows for both extant and extinct objects).
-- In the next subquery, eliminate the rows that contain deleted objects.
current_versions as (
    SELECT * from version_stacks where next_sequence_number is NULL
),

-- Eliminate the rows that are extinct from the bucket by filtering with
-- record_type. An object version has been deleted from the bucket if its tip is
-- record_type==DELETE.
existing_current_versions as (
    SELECT * from current_versions where not (record_type = 'DELETE' and
 is_delete_marker = FALSE)
),

-- Optionally, to determine which of several object versions is the 'latest',
-- you can compare their sequence numbers. A version_id is the latest if its
-- tip's sequencer is the largest among all other tips in the same key.
with_is_latest as (
    SELECT *,
           -- Determine if the sequence_number of this row is the same as the largest
 sequencer for the key that still exists.
           sequence_number = (MAX(sequence_number) over (partition by (bucket, key)))
 as is_latest_version
    FROM existing_current_versions
)
```

```
SELECT * from with_is_latest
ORDER BY bucket, key, sequence_number;
```

Unir metadados personalizados com tabelas de metadados do S3

Você pode analisar dados nas tabelas de metadados gerenciadas pelo S3 e nas tabelas de metadados de clientes (autogerenciadas). Usando um operador SQL `JOIN` padrão, você pode consultar dados dessas várias fontes.

O exemplo de consulta SQL a seguir encontra registros correspondentes entre uma tabela de metadados gerenciada pelo S3 (*`my_s3_metadata_table`*) e uma tabela de metadados autogerenciada (*`my_self_managed_metadata_table`*). A consulta também filtra as informações com base em eventos `CREATE`, que indicam que um novo objeto (ou uma nova versão do objeto) foi gravado no bucket. (Para obter mais informações, consulte Esquema de tabelas do S3 Metadata.)

```
SELECT *
FROM aws_s3_metadata.my_s3_metadata_table a
JOIN my_namespace.my_self_managed_metadata_table b
ON a.bucket = b.bucket AND a.key = b.key AND a.version_id = b.version_id
WHERE a.record_type = 'CREATE';
```

Visualizar dados de tabelas de metadados com o Amazon QuickSight

Com o Amazon QuickSight, você pode criar painéis interativos para analisar e visualizar resultados de consultas SQL sobre as tabelas de metadados gerenciadas pelo S3. Os painéis do QuickSight podem ajudar você a monitorar estatísticas, rastrear alterações e obter insights operacionais sobre as tabelas de metadados.

Um painel sobre as tabelas de metadados pode mostrar:

- Quantos objetos estão em diferentes classes de armazenamento.
- Qual porcentagem dos dados de armazenamento são objetos pequenos em comparação com objetos grandes.
- Quais tipos de objetos estão no bucket.
- Qual é a porcentagem de uploads de objetos em relação às exclusões.

Depois de integrar os buckets de tabela do S3 aos serviços de analytics da AWS, você pode criar conjuntos de dados com base nas tabelas de metadados e trabalhar com eles no Amazon

QuickSight usando consultas SPICE ou SQL direto do mecanismo de consulta. O QuickSight oferece suporte ao Amazon Athena e ao Amazon Redshift como fontes de dados.

Para ter mais informações, consulte Visualizing table data with Amazon QuickSight.

Fazer upload de objetos

Quando você faz upload de um arquivo no Amazon S3, ele é armazenado como um objeto do S3. Os objetos consistem em dados e metadados de arquivo que descrevem o objeto. Você pode ter um número ilimitado de objetos em um bucket. Antes de fazer upload de arquivos em um bucket do Amazon S3, você precisa escrever permissões para o bucket. Para obter mais informações sobre permissões de acesso, consulte Gerenciamento de identidade e acesso para o Amazon S3.

Você pode fazer upload de qualquer tipo de arquivo (imagens, backups, dados, filmes etc.) para um bucket do S3. O tamanho máximo de arquivo que você pode carregar usando o console do Amazon S3 é de 160 GB. Para fazer upload de um arquivo com mais de 160 GB, use a AWS Command Line Interface (AWS CLI), AWS SDKs ou a API REST do Amazon S3.

Se você fizer upload de um objeto com um nome de chave que já existe em um bucket com versionamento habilitado, o Amazon S3 criará outra versão de objeto em vez de substituir o objeto existente. Para ter mais informações sobre como habilitar o versionamento, consulte Habilitar o versionamento em buckets.

Dependendo do tamanho de dados enviados por upload, o Amazon S3 oferece as seguintes opções:

- Fazer upload de um objeto em uma única operação usando AWS SDKs, a API REST ou a AWS CLI: com uma única operação PUT, você pode fazer upload de um único objeto com até 5 GB.
- Fazer upload de um único objeto usando o console do Amazon S3: com o console do Amazon S3, é possível fazer upload de um único objeto com até 160 GB de tamanho.
- Fazer upload de um objeto em partes usando AWS SDKs, a API REST ou a AWS CLI: com a operação de API de upload de várias partes, é possível fazer upload de um único objeto grande, com até 5 TB.

  A operação de API de upload de várias partes foi projetada para melhorar a experiência de upload de objetos maiores. É possível fazer upload de um objeto em partes. O upload dessas partes de objetos pode ser feito independentemente, em qualquer ordem, e em paralelo. Você pode usar um multipart upload de objetos de 5 MB a 5 TB. Para obter mais informações, consulte Carregar e copiar objetos usando upload fracionado no Amazon S3.

Quando você faz upload de um objeto, ele é automaticamente criptografado usando criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3) por padrão. Quando você faz download, o objeto é descriptografado. Para obter mais informações, consulte Definir o comportamento padrão da criptografia para os buckets do Amazon S3 e Proteger dados com criptografia.

Ao fazer upload de um objeto, se quiser usar um tipo diferente de criptografia padrão, você também pode especificar a criptografia do lado do servidor com chaves do AWS Key Management Service (AWS KMS) (SSE-KMS) nas solicitações PUT do S3 ou definir a configuração de criptografia padrão no bucket de destino para usar o SSE-KMS para criptografar os dados. Para obter mais informações sobre SSE-KMS, consulte Especificando criptografia no lado do servidor com o AWS KMS (SSE-KMS). Se quiser usar uma chave do KMS que seja de propriedade de outra conta, você deverá ter permissão para usar a chave. Para obter mais informações sobre permissões entre contas para chaves do KMS, consulte Criar chaves do KMS que outras contas podem usar no Guia do desenvolvedor do AWS Key Management Service.

Se você encontrar um erro de Acesso negado (403 Proibido) no Amazon S3, consulte Solucionar erros de acesso negado (403 Forbidden) no Amazon S3 para saber mais sobre as causas comuns.

Fazer upload de um objeto

Usar o console do S3

Este procedimento explica como fazer upload de objetos e pastas para um bucket do Amazon S3 usando o console.

Quando você faz upload de um objeto, o nome da chave de objeto é o nome do arquivo e quaisquer prefixos opcionais. No console do Amazon S3, você pode criar pastas para organizar seus objetos. No Amazon S3, as pastas são representadas como prefixos que aparecem no nome da chave de objeto. Se você fizer upload um objeto individual para uma pasta no console do Amazon S3, o nome da pasta será incluído no nome da chave do objeto.

Por exemplo, se você carregar um objeto chamado `sample1.jpg` para uma pasta chamada `backup`, o nome da chave será `backup/sample1.jpg`. Contudo, o objeto é exibido no console como `sample1.jpg` na pasta `backup`. Para obter mais informações sobre nomes de chave, consulte Trabalhar com metadados de objeto.

> **Note**
>
> Se você renomear um objeto ou alterar qualquer uma das propriedades no console do Amazon S3, por exemplo Classe de armazenamento, Criptografia ou Metadados, será criado outro objeto para substituir o antigo. Se o versionamento do S3 estiver habilitado, uma nova versão do objeto será criada e o objeto existente se tornará uma versão mais antiga. O perfil que altera a propriedade também se torna o proprietário do novo objeto (ou versão do objeto).

Quando você faz upload de uma pasta, o Amazon S3 faz upload de todos os arquivos e subpastas da pasta especificada em seu bucket. Ele então atribui um nome de chave de objeto que é uma combinação do nome de arquivo carregado com o nome da pasta. Por exemplo, se você fizer upload de uma pasta chamada `/images` que contém dois arquivos, `sample1.jpg` e `sample2.jpg`, o Amazon S3 fará upload dos arquivos e atribuirá a eles os nomes de chave correspondentes, `images/sample1.jpg` e `images/sample2.jpg`. Os nomes de chave incluem o nome da pasta como um prefixo. O console do Amazon S3 exibe somente a parte do nome de chave que vem depois da última `/`. Por exemplo, em uma pasta `images`, os objetos `images/sample1.jpg` e `images/sample2.jpg` são exibidos como `sample1.jpg` e `sample2.jpg`.

Para fazer upload de pastas e arquivos para um bucket do S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets.
3. Na lista Buckets, escolha o nome do bucket no qual você deseja carregar suas pastas ou arquivos.
4. Escolha Upload (Fazer upload).
5. Na janela Upload (Fazer upload), siga um destes procedimentos:
   - Arraste e solte arquivos e pastas para a janela Upload (Fazer upload) .
   - Escolha Adicionar arquivo ou Adicionar pasta, escolha arquivos ou pastas para fazer upload e depois escolha Abrir.
6. Para habilitar o versionamento, em Destination (Destino), escolha Enable Bucket Versioning (Ativar versionamento de bucket).

7. Para fazer upload dos arquivos e pastas listados sem configurar opções de upload adicionais, na parte inferior da página, escolha Upload (Fazer upload).

   O Amazon S3 faz o upload de seus objetos e pastas. Quando o upload for concluído, você verá uma mensagem de sucesso na página Upload: status.

Para configurar propriedades de objeto adicionais

1. Para alterar as permissões da lista de controle de acesso, escolha Permissions (Permissões).
2. Em Access control list (ACL) (Lista de controle de acesso (ACL)), edite as permissões.

   Para informações sobre permissões de acesso a objeto, consulte Usar o console do S3 para definir permissões de ACL para um objeto. Você pode conceder acesso de leitura aos seus objetos ao público (todos no mundo), para todos os arquivos que você está carregando. No entanto, recomendamos não alterar a configuração padrão para acesso de leitura público. Conceder acesso público de leitura é aplicável a um pequeno subconjunto de casos de uso, como quando buckets são usados para sites. Você sempre pode alterar as permissões de objeto depois de carregar o objeto.
3. Para configurar outras propriedades, escolha Properties (Propriedades).
4. Na seção Classe de armazenamento escolha a classe de armazenamento para os arquivos que você está carregando.

   Para obter mais informações sobre classes de armazenamento, consulte Compreender e gerenciar classes de armazenamento do Amazon S3.
5. Para atualizar as configurações de criptografia para seus objetos, em Server-side encryption settings (Configurações de criptografia do lado do servidor), faça o seguinte.

   a. Escolha Specify an encryption key (Especificar uma chave de criptografia).

   b. Em Configurações de criptografia, escolha Usar configurações de bucket para criptografia padrão ou Substituir configurações de bucket para criptografia padrão.

   c. Se você escolher Substituir configurações do bucket para criptografia padrão, deverá definir as configurações de criptografia a seguir.

      - Para criptografar os arquivos carregados usando chaves gerenciadas pelo Amazon S3, escolha Chave gerenciada pelo Amazon S3 (SSE-S3).

Para obter mais informações, consulte Usar a criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3).

- Para criptografar os arquivos carregados usando chaves armazenadas no AWS Key Management Service (AWS KMS), selecione Chave do AWS Key Management Service (SSE-KMS). Depois, escolha uma das seguintes opções para a chave do AWS KMS:
  - Para escolher entre uma lista de chaves do KMS disponíveis, selecione Escolher de sua AWS KMS keys e escolha a chave do KMS na lista de chaves disponíveis.

    As chaves Chave gerenciada pela AWS (`aws/s3`) e as chaves gerenciadas pelo cliente são exibidas nessa lista. Para ter mais informações sobre chaves gerenciadas pelo cliente, consulte Chaves de clientes e chaves da AWS no Guia do desenvolvedor do AWS Key Management Service.
  - Para inserir o ARN da chave do KMS, selecione Inserir ARN da AWS KMS key e insira o ARN da chave do KMS no campo exibido.
  - Para criar uma chave gerenciada pelo cliente no console do AWS KMS, selecione Criar uma chave do KMS.

    Para ter mais informações sobre como criar uma AWS KMS key, consulte Criação de chaves no Guia do desenvolvedor do AWS Key Management Service.

    > **Important**
    >
    > Você só pode usar chaves do KMS disponíveis na mesma Região da AWS que o bucket. O console do Amazon S3 lista somente as primeiras 100 chaves do KMS na mesma região que o bucket. Para usar uma chave do KMS que não esteja listada, você deve inserir o ARN da chave do KMS. Se quiser usar uma chave do KMS que seja de propriedade de outra conta, primeiro você deverá ter permissão para usar a chave e, depois, inserir o ARN da chave do KMS.
    > O Amazon S3 só é compatível com chaves do KMS de criptografia simétrica, e não com chaves assimétricas do KMS. Para ter mais informações, consulte Identificar chaves do KMS simétricas e assimétricas no Guia do desenvolvedor do AWS Key Management Service.

6. Para usar somas de verificação adicionais, escolha On (Ativar). Em seguida, em Checksum function (Função de soma de verificação), escolha a função que você gostaria de usar. O Amazon S3 calcula e armazena o valor da soma de verificação depois de receber o objeto

inteiro. Você pode usar a caixa Precalculated value (Valor pré-calculado) para fornecer esse valor. Se fizer isso, o Amazon S3 vai comparar o valor que você forneceu com o valor calculado. Se os dois valores não corresponderem, o Amazon S3 gerará um erro.

As somas de verificação adicionais permitem que você especifique o algoritmo de soma de verificação que gostaria de usar para verificar seus dados. Para obter mais informações sobre somas de verificação adicionais, consulte Verificar a integridade do objeto no Amazon S3.

7. Para adicionar tags a todos os objetos que você está carregando, escolha Add tag (Adicionar tag). Insira um nome de tag no campo Chave. Insira um valor para a tag.

   A marcação de objetos é uma forma de categorizar o armazenamento. Cada tag é um par de chave-valor. Os valores de chave e tag diferenciam maiúsculas de minúsculas. É possível ter até dez tags por objeto. Uma chave de tag pode ter até 128 caracteres Unicode e os valores de tag podem ter até 255 caracteres Unicode. Para obter mais informações sobre tags de objeto, consulte Categorizar seu armazenamento usando tags.

8. Para adicionar metadados, escolha Add metadata (Adicionar metadados).

   a. Em Type (Tipo), escolha System defined (Definido pelo sistema) ou User defined (Definido pelo usuário).

      Para metadados definidos pelo sistema, você pode selecionar cabeçalhos HTTP comuns, como Content-Type e Content-Disposition. Para obter uma lista de metadados definidos pelo sistema e informações sobre a possibilidade de adicionar o valor, consulte Metadados do objeto definidos pelo sistema. Todos os metadados que começam com o prefixo `x-amz-meta-` são tratados como metadados definidos pelo usuário. Os metadados definidos pelo usuário são armazenados com o objeto e retornados quando você baixa o objeto. As chaves e seus valores devem estar em conformidade com os padrões US-ASCII. Metadados definidos pelo usuário podem ter até 2 KB. Para obter mais informações sobre metadados definidos pelo sistema e pelo usuário, consulte Trabalhar com metadados de objeto.

   b. Para Key (Chave), escolha uma chave.

   c. Digite um valor para a chave.

9. Para carregar seus objetos, escolha Upload (Fazer upload).

   O Amazon S3 faz o upload do objeto. Quando o upload for concluído, você pode ver uma mensagem de sucesso na página de Upload: status.

10. Selecione Exit (Sair).

Como usar o AWS CLI

Você pode enviar uma solicitação PUT para fazer upload de um objeto de até 5 GB em uma única operação. Para obter mais informações, consulte o exemplo de `PutObject` na Referência de comandos da AWS CLI.

Uso da API REST

Você pode enviar solicitações REST para fazer upload de um objeto. Você pode enviar uma solicitação PUT para carregar dados em uma única operação. Para obter mais informações, consulte Objeto PUT.

Uso dos SDKs da AWS

Você pode usar os AWS SDKs para fazer upload de objetos no Amazon S3. Os SDKs fornecem bibliotecas wrapper para você para fazer upload de dados com facilidade. Para obter informações, consulte a Lista de SDKs compatíveis.

Aqui estão alguns exemplos com alguns SDKs selecionados:

.NET

O exemplo de código C# a seguir cria dois objetos com as duas solicitações `PutObjectRequest`:

- A primeira solicitação `PutObjectRequest` salva uma sequência de texto como exemplo de dados do objeto. Ela também especifica os nomes do bucket e da chave de objeto.
- A segunda solicitação `PutObjectRequest` faz upload de um arquivo especificando o nome do arquivo. Essa solicitação também especifica o cabeçalho `ContentType` e os metadados opcionais de objeto (título).

Para obter informações sobre como configurar e executar exemplos de código, consulte Conceitos básicos do AWS SDK for .NET no Guia do desenvolvedor do AWS SDK for .NET.

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
```

```
{
    class UploadObjectTest
    {
        private const string bucketName = "*** bucket name ***";
        // For simplicity the example creates two objects from the same file.
        // You specify key names for these objects.
        private const string keyName1 = "*** key name for first object created ***";
        private const string keyName2 = "*** key name for second object created
 ***";
        private const string filePath = @"*** file path ***";
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.EUWest1;

        private static IAmazonS3 client;

        public static void Main()
        {
            client = new AmazonS3Client(bucketRegion);
            WritingAnObjectAsync().Wait();
        }

        static async Task WritingAnObjectAsync()
        {
            try
            {
                // 1. Put object-specify only key name for the new object.
                var putRequest1 = new PutObjectRequest
                {
                    BucketName = bucketName,
                    Key = keyName1,
                    ContentBody = "sample text"
                };

                PutObjectResponse response1 = await
 client.PutObjectAsync(putRequest1);

                // 2. Put the object-set ContentType and add metadata.
                var putRequest2 = new PutObjectRequest
                {
                    BucketName = bucketName,
                    Key = keyName2,
                    FilePath = filePath,
                    ContentType = "text/plain"
                };
```

```
                putRequest2.Metadata.Add("x-amz-meta-title", "someTitle");
                PutObjectResponse response2 = await
 client.PutObjectAsync(putRequest2);
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine(
                        "Error encountered ***. Message:'{0}' when writing an
 object"
                        , e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine(
                    "Unknown encountered on server. Message:'{0}' when writing an
 object"
                    , e.Message);
            }
        }
    }
}
```

Java

O exemplo a seguir cria dois objetos. O primeiro objeto tem uma sequência de texto como dados, e o segundo objeto é um arquivo. O exemplo cria o primeiro objeto especificando o nome de bucket, a chave de objeto, e os dados de texto diretamente em uma chamada para `AmazonS3Client.putObject()`. O exemplo cria um segundo objeto usando um `PutObjectRequest` que especifica o nome de bucket, a chave de objeto, e o caminho do arquivo. O `PutObjectRequest` também especifica o cabeçalho de `ContentType` e os metadados do título.

Consulte instruções sobre como criar e testar uma amostra funcional em Getting Started no Guia do desenvolvedor do AWS SDK para Java.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
```

```
import com.amazonaws.services.s3.model.ObjectMetadata;
import com.amazonaws.services.s3.model.PutObjectRequest;

import java.io.File;
import java.io.IOException;

public class UploadObject {

    public static void main(String[] args) throws IOException {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "*** Bucket name ***";
        String stringObjKeyName = "*** String object key name ***";
        String fileObjKeyName = "*** File object key name ***";
        String fileName = "*** Path to file to upload ***";

        try {
            // This code expects that you have AWS credentials set up per:
            // https://docs.aws.amazon.com/sdk-for-java/v1/developer-guide/setup-
credentials.html
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withRegion(clientRegion)
                    .build();

            // Upload a text string as a new object.
            s3Client.putObject(bucketName, stringObjKeyName, "Uploaded String
 Object");

            // Upload a file as a new object with ContentType and title specified.
            PutObjectRequest request = new PutObjectRequest(bucketName,
 fileObjKeyName, new File(fileName));
            ObjectMetadata metadata = new ObjectMetadata();
            metadata.setContentType("plain/text");
            metadata.addUserMetadata("title", "someTitle");
            request.setMetadata(metadata);
            s3Client.putObject(request);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
```

```
    }
}
```

JavaScript

O exemplo a seguir carrega um arquivo existente para um bucket do Amazon S3 em uma região específica.

```
import { readFile } from "node:fs/promises";

import {
  PutObjectCommand,
  S3Client,
  S3ServiceException,
} from "@aws-sdk/client-s3";

/**
 * Upload a file to an S3 bucket.
 * @param {{ bucketName: string, key: string, filePath: string }}
 */
export const main = async ({ bucketName, key, filePath }) => {
  const client = new S3Client({});
  const command = new PutObjectCommand({
    Bucket: bucketName,
    Key: key,
    Body: await readFile(filePath),
  });

  try {
    const response = await client.send(command);
    console.log(response);
  } catch (caught) {
    if (
      caught instanceof S3ServiceException &&
      caught.name === "EntityTooLarge"
    ) {
      console.error(
        `Error from S3 while uploading object to ${bucketName}. \
The object was too large. To upload objects larger than 5GB, use the S3 console
 (160GB max) \
or the multipart upload API (5TB max).`,
      );
```

```
    } else if (caught instanceof S3ServiceException) {
      console.error(
        `Error from S3 while uploading object to ${bucketName}.  ${caught.name}:
 ${caught.message}`,
      );
    } else {
      throw caught;
    }
  }
};
```

PHP

Este exemplo orienta você quanto ao uso de classes do AWS SDK para PHP para fazer upload de um objeto de até 5 GB. Para arquivos maiores, você deve usar a operação de API de upload de várias partes. Para obter mais informações, consulte Carregar e copiar objetos usando upload fracionado no Amazon S3.

Para obter mais informações sobre a API do AWS SDK for Ruby, acesse AWS SDK for Ruby Version 2.

Example Criar um objeto em um bucket do Amazon S3 fazendo upload dos dados

O exemplo PHP a seguir cria um objeto em um bucket especificado pelo upload de dados usando o método `putObject()`.

```
 require 'vendor/autoload.php';

use Aws\S3\Exception\S3Exception;
use Aws\S3\S3Client;

$bucket = '*** Your Bucket Name ***';
$keyname = '*** Your Object Key ***';

$s3 = new S3Client([
    'version' => 'latest',
    'region'  => 'us-east-1'
]);

try {
    // Upload data.
    $result = $s3->putObject([
        'Bucket' => $bucket,
```

```
        'Key'    => $keyname,
        'Body'   => 'Hello, world!',
        'ACL'    => 'public-read'
    ]);

    // Print the URL to the object.
    echo $result['ObjectURL'] . PHP_EOL;
} catch (S3Exception $e) {
    echo $e->getMessage() . PHP_EOL;
}
```

Ruby

O AWS SDK para Ruby versão 3 oferece duas maneiras de fazer upload de um objeto para o Amazon S3. O primeiro usa um upload gerenciado de arquivo, que facilita o upload de arquivos de qualquer tamanho para disco. Usar o método de upload gerenciado de arquivo:

1. Crie uma instância da classe `Aws::S3::Resource`.
2. Faça referência ao objeto de destino pelo nome e chave do bucket. Os objetos residem em um bucket e têm chaves exclusivas que identificam cada objeto.
3. Chame `#upload_file` no objeto.

Example

```
require 'aws-sdk-s3'

# Wraps Amazon S3 object actions.
class ObjectUploadFileWrapper
  attr_reader :object

  # @param object [Aws::S3::Object] An existing Amazon S3 object.
  def initialize(object)
    @object = object
  end

  # Uploads a file to an Amazon S3 object by using a managed uploader.
  #
  # @param file_path [String] The path to the file to upload.
  # @return [Boolean] True when the file is uploaded; otherwise false.
  def upload_file(file_path)
```

```
    @object.upload_file(file_path)
    true
  rescue Aws::Errors::ServiceError => e
    puts "Couldn't upload file #{file_path} to #{@object.key}. Here's why:
 #{e.message}"
    false
  end
end

# Example usage:
def run_demo
  bucket_name = "amzn-s3-demo-bucket"
  object_key = "my-uploaded-file"
  file_path = "object_upload_file.rb"

  wrapper = ObjectUploadFileWrapper.new(Aws::S3::Object.new(bucket_name,
 object_key))
  return unless wrapper.upload_file(file_path)

  puts "File #{file_path} successfully uploaded to #{bucket_name}:#{object_key}."
end

run_demo if $PROGRAM_NAME == __FILE__
```

A segunda forma que o AWS SDK para Ruby – Versão 3 pode fazer upload de um objeto usa o método `#put` do `Aws::S3::Object`. Isso é útil se o objeto for uma string ou um objeto de E/S que não seja um arquivo em disco. Para usar este método:

1. Crie uma instância da classe `Aws::S3::Resource`.
2. Faça referência ao objeto de destino pelo nome e chave do bucket.
3. Chame`#put`, passando a sequência ou objeto de E/S.

Example

```
require 'aws-sdk-s3'

# Wraps Amazon S3 object actions.
class ObjectPutWrapper
  attr_reader :object

  # @param object [Aws::S3::Object] An existing Amazon S3 object.
```

```
  def initialize(object)
    @object = object
  end

  def put_object(source_file_path)
    File.open(source_file_path, 'rb') do |file|
      @object.put(body: file)
    end
    true
  rescue Aws::Errors::ServiceError => e
    puts "Couldn't put #{source_file_path} to #{object.key}. Here's why:
 #{e.message}"
    false
  end
end

# Example usage:
def run_demo
  bucket_name = "amzn-s3-demo-bucket"
  object_key = "my-object-key"
  file_path = "my-local-file.txt"

  wrapper = ObjectPutWrapper.new(Aws::S3::Object.new(bucket_name, object_key))
  success = wrapper.put_object(file_path)
  return unless success

  puts "Put file #{file_path} into #{object_key} in #{bucket_name}."
end

run_demo if $PROGRAM_NAME == __FILE__
```

Impedir o upload de objetos com nomes de chave idênticos

É possível conferir a existência de um objeto no bucket antes de criá-lo usando uma gravação condicional nas operações de upload. Isso pode evitar a substituição de dados existentes. As gravações condicionais confirmarão que não há nenhum objeto com o mesmo nome de chave no bucket durante o upload.

É possível usar gravações condicionais para solicitações PutObject ou CompleteMultipartUpload.

Para ter mais informações sobre solicitações condicionais, consulte Adicionar condições prévias às operações do S3 com solicitações condicionais.

Carregar e copiar objetos usando upload fracionado no Amazon S3

O upload fracionado permite que você faça upload de um único objeto no Amazon S3 como um conjunto de partes. Cada parte é uma parte contígua de dados do objeto. O upload dessas partes de objetos pode ser feito de maneira independente e em qualquer ordem. Para uploads, o cliente da AWS atualizado calcula automaticamente uma soma de verificação do objeto e a envia para o Amazon S3 com o tamanho do objeto como parte da solicitação. Se a transmissão de alguma parte falhar, você poderá retransmitir essa parte sem afetar outras partes. Depois que todas as partes do objeto forem carregadas, o Amazon S3 montará as partes e criará o objeto. É uma prática recomendada usar o upload fracionado para objetos com 100 MB ou mais, em vez de carregá-los em uma única operação.

Usar o multipart upload fornece as seguintes vantagens:

- Improved throughput (Throughput aprimorada): você pode carregar as partes em paralelo para melhorar o throughput.
- Quick recovery from any network issues (Recuperação rápida de qualquer problema de rede): o tamanho menor das partes minimiza o impacto de reiniciar um carregamento que falhou devido a um erro de rede.
- Pause and resume object uploads (Pausar e retomar carregamentos de objetos): você pode carregar as partes do objeto ao longo do tempo. Após ser iniciado um carregamento fracionado, ele não expira; você deve concluir ou interromper explicitamente o carregamento fracionado.
- Iniciar um upload antes de saber o tamanho final do objeto você pode fazer upload de um objeto ao criá-lo.

Recomendamos que você use o carregamento fracionado das seguintes maneiras:

- Se você fizer upload de objetos grandes em uma rede de banda larga estável, use o upload fracionado para maximizar o uso da largura de banda disponível, fazendo upload de partes do objeto em paralelo para performance com vários threads.
- Se fizer upload em uma rede lenta, use o upload fracionado para aumentar a resiliência contra erros de rede, evitando reinicializações de uploads. Ao usar o upload fracionado, tente carregar novamente apenas as partes que foram interrompidas durante o carregamento. Você não precisa reiniciar o upload do seu objeto do começo.

> **Note**
>
> Para obter mais informações sobre o uso da classe de armazenamento Amazon S3 Express One Zone com buckets de diretório, consulte S3 Express One Zone e Trabalhar com buckets de diretório. Para obter mais informações sobre como usar multipart upload com a classe S3 Express One Zone e buckets de diretório, consulte Usar uploads multiparte com buckets de diretório.

Processo de carregamento fracionado

O upload fracionado é um processo de três etapas: você inicia o upload, faz upload de partes do objeto e, depois de fazer upload de todas as partes, conclui o upload fracionado. Ao receber a solicitação de conclusão do upload fracionado, o Amazon S3 cria o objeto com base nas partes carregadas, e você poderá acessar o objeto como qualquer outro objeto no bucket.

Você pode listar todos os seus multipart uploads em andamento ou obter uma lista das partes que carregou para um multipart upload específico. Cada uma dessas operações é explicada nesta seção.

Iniciação de carregamento fracionado

Ao enviar uma solicitação para iniciar um upload fracionado, especifique um tipo de soma de verificação. Depois, o Amazon S3 retornará uma resposta com um ID de upload, que é um identificador exclusivo para o upload fracionado. Esse ID de upload é necessário ao fazer upload de partes, listar as partes, concluir um upload ou interromper um upload. Se você quiser fornecer metadados que descrevam o objeto que está sendo carregado, deverá fornecê-los na solicitação para iniciar o upload fracionado. Usuários anônimos não podem iniciar carregamentos fracionados.

Carregamento de partes

Ao fazer upload de uma parte, além do ID de upload, é necessário especificar um número de parte. Você pode escolher qualquer número de parte entre 1 e 10.000. Um número de parte identifica com exclusividade a parte e sua posição no objeto do qual você está fazendo upload. O número de parte que você escolheu não precisa estar em uma sequência consecutiva (por exemplo, pode ser 1, 5 e 14). Saiba que, se você fizer upload de uma nova parte usando o mesmo número da parte anteriormente carregada, a parte anteriormente carregada será substituída.

Quando você faz upload de uma parte, o Amazon S3 retorna o tipo de algoritmo de soma de verificação com o valor da soma para cada parte como cabeçalho na resposta. Para cada upload de parte, você deve registrar o número de parte e o valor de ETag. Você tem que incluir esses valores

na solicitação subsequente para concluir o multipart upload. Cada parte terá sua própria ETag no momento do upload. No entanto, quando o upload fracionado estiver concluído e todas as partes estiverem consolidadas, todas as partes pertencerão a uma ETag como uma soma de verificação das somas de verificação.

> **Important**
>
> Depois de inicializar um upload fracionado e fazer upload de uma ou mais partes, será necessário concluir ou interromper o upload fracionado para interromper a cobrança pelo armazenamento das partes carregadas. Somente depois que você concluir ou interromper um upload fracionado é que o Amazon S3 liberará o armazenamento das partes e deixará de cobrar pelo armazenamento das partes.
>
> Depois de interromper um upload fracionado, você não poderá fazer upload de nenhuma parte usando esse ID de upload novamente. Se havia uploads de partes em andamento, eles ainda poderão ser bem-sucedidos ou falhar mesmo depois da interrupção. Para liberar todo o armazenamento consumido por todas as partes, você deve interromper um upload fracionado somente depois que todos os uploads de partes forem concluídos.

Conclusão de carregamento fracionado

Quando você concluir um multipart upload, o Amazon S3 criará um objeto concatenando as partes em ordem crescente com base no número da parte. Se algum metadado de objeto for fornecido na solicitação iniciar multipart upload, o Amazon S3 associará esses metadados ao objeto. Depois de uma solicitação de conclusão bem-sucedida, as partes não existem mais.

Sua solicitação de conclusão do upload fracionado deve incluir o ID de upload e uma lista dos números das partes e dos valores de ETag correspondentes. A resposta do Amazon S3 inclui um ETag que identifica exclusivamente os dados do objeto combinados. Esse ETag não é necessariamente um hash MD5 dos dados do objeto.

Ao fornecer uma soma de verificação de objeto inteiro durante um upload fracionado, o AWS SDK envia a soma de verificação para o Amazon S3, e o S3 valida a integridade do objeto do lado do servidor, comparando-a com o valor recebido. Depois, o S3 armazena o objeto se os valores corresponderem. Se os dois valores não corresponderem, o Amazon S3 reprovará a solicitação com um erro `BadDigest`. A soma de verificação do objeto também é armazenada nos metadados do objeto que você usará posteriormente para validar a integridade dos dados do objeto.

Exemplos de chamada de carregamento fracionado

Para este exemplo, suponha que você esteja gerando um upload fracionado para um arquivo de 100 GB. Nesse caso, você teria as seguintes chamadas de API para todo o processo. Haveria um total de 1.002 chamadas de API.

- Uma chamada `CreateMultipartUpload` para iniciar o processo.
- Mil chamadas `UploadPart` individuais, cada uma fazendo upload de uma parte de 100 MB, para um tamanho total de 100 GB.
- Uma chamada `CompleteMultipartUpload` para concluir o processo.

Listagens de carregamento fracionado

Você pode listar as partes de um multipart upload específico ou de todos os multipart uploads em andamento. A operação de listagem de partes retorna as informações das partes que você carregou em um upload fracionado específico. Para cada solicitação de listagem de partes, o Amazon S3 retorna informações das partes do multipart upload especificado, até no máximo 1.000 partes. Se houver mais de 1.000 partes no upload fracionado, você deverá enviar uma série de solicitações de listagem para recuperar todas as partes. Observe que a lista de partes retornada não inclui aquelas cujo carregamento não foi concluído. Usando a operação list multipart uploads (listar carregamentos fracionados), você pode obter uma lista daqueles que estão em andamento.

Um multipart upload em andamento é um upload que você iniciou, mas que ainda não concluiu nem interrompeu. Cada solicitação retorna no máximo 1.000 multipart uploads. Se houver mais de 1.000 carregamento fracionados em andamento, você precisará enviar solicitações adicionais para recuperar os carregamento fracionados restantes. Use a listagem retornada apenas para verificação.

> **Important**
>
> Não use o resultado dessa listagem ao enviar uma solicitação complete multipart upload (concluir carregamento fracionado). Em vez disso, mantenha sua própria lista de números de parte que você especificou ao carregar as partes e os valores correspondentes de ETag que o Amazon S3 retorna.

Somas de verificação com operações de carregamento fracionado

Ao carregar um objeto no Amazon S3, você pode especificar um algoritmo de soma de verificação a ser usado pelo Amazon S3. Por padrão, o AWS SDK e o console do S3 usam um algoritmo

para todos os uploads de objetos, que você pode substituir. Se você estiver usando um SDK mais antigo e o objeto carregado não tiver uma soma de verificação especificada, o Amazon S3 usará automaticamente o algoritmo de soma de verificação CRC-64/NVME (`CRC64NVME`). (Essa também é a opção recomendada para uma verificação eficiente da integridade dos dados.) Ao usar o CRC-64/NVME, o Amazon S3 calcula a soma de verificação do objeto inteiro após a conclusão do upload fracionado ou de parte única. O algoritmo de soma de verificação CRC-64/NVME é usado para calcular uma soma de verificação direta do objeto inteiro ou uma soma de verificação das somas de verificação de cada parte.

Depois que você faz upload de um objeto no S3 usando o upload fracionado, o Amazon S3 calcula o valor da soma de verificação de cada parte ou do objeto inteiro e armazena os valores. Você pode usar a API do S3 ou o AWS SDK para recuperar o valor da soma de verificação das seguintes maneiras:

- Para partes individuais, você pode usar `GetObject` ou `HeadObject`. Se quiser recuperar os valores da soma de verificação para partes individuais de uploads fracionados enquanto ainda estão em andamento, você pode usar `ListParts`.
- Para o objeto inteiro, você pode usar `PutObject`. Se você quiser realizar um upload fracionado com uma soma de verificação de objeto inteiro, use `CreateMultipartUpload` e `CompleteMultipartUpload` especificando o tipo de soma de verificação do objeto inteiro. Para validar o valor da soma de verificação do objeto inteiro ou para confirmar qual tipo de soma de verificação está sendo usado no upload fracionado, use `ListParts`.

> **Important**
>
> Se você estiver usando um upload fracionado com somas de verificação, os números de cada parte do upload (no upload fracionado) deverão ser consecutivos e começar com 1. Ao usar Checksums, se tentar concluir uma solicitação de upload fracionado com números de parte não consecutivos, o Amazon S3 gerará um erro `HTTP 500 Internal Server`.

Consulte mais informações sobre como as somas de verificação funcionam com objetos de carregamento fracionado em Verificar a integridade do objeto no Amazon S3.

Para conferir um procedimento completo que demonstra como fazer upload de um objeto usando o upload fracionado com uma soma de verificação adicional, consulte Tutorial: Fazer upload de um objeto por meio do carregamento fracionado e conferir a integridade dos dados.

Operações simultâneas de multipart upload

Em um ambiente de desenvolvimento distribuído, é possível que sua aplicação inicie várias atualizações no mesmo objeto ao mesmo tempo. Seu aplicativo pode iniciar vários multipart uploads usando a mesma chave de objeto. Para cada um desses uploads, sua aplicação pode fazer upload das partes e enviar uma solicitação de conclusão de upload ao Amazon S3 para criar o objeto. Quando os buckets têm o versionamento do S3 habilitado, a conclusão de um carregamento fracionado sempre criará uma versão. Ao iniciar vários uploads multiparte que usam a mesma chave de objeto em um bucket habilitado para versionamento, a versão atual do objeto é determinada pelo upload iniciado mais recentemente (`createdDate`).

Por exemplo, você inicia uma solicitação `CreateMultipartUpload` para um objeto às 10h. Depois, você envia uma segunda solicitação `CreateMultipartUpload` para o mesmo objeto às 11h. Como a segunda solicitação foi enviada mais recentemente, o objeto carregado pela solicitação das 11h se torna a versão atual, mesmo que o primeiro upload seja concluído após o segundo. Para os buckets que não têm o versionamento habilitado, é possível que qualquer outra solicitação recebida entre o momento em que um upload fracionado é inicializado e sua conclusão tenha precedência.

Outro exemplo de quando uma solicitação de upload fracionado simultânea pode ter precedência é se outra operação excluir uma chave depois que você iniciar um upload fracionado com essa chave. Antes de concluir a operação, a resposta do upload fracionado concluído poderá indicar a criação bem-sucedida de um objeto sem você nunca ter visto o objeto.

Impedir o upload de objetos com nomes de chave idênticos durante carregamentos fracionados

É possível conferir a existência de um objeto no bucket antes de criá-lo usando uma gravação condicional nas operações de upload. Isso pode evitar a substituição de dados existentes. As gravações condicionais confirmarão que não há nenhum objeto com o mesmo nome de chave no bucket durante o upload.

É possível usar gravações condicionais para solicitações PutObject ou CompleteMultipartUpload.

Para ter mais informações sobre solicitações condicionais, consulte Adicionar condições prévias às operações do S3 com solicitações condicionais.

Multipart upload e definição de preço

Depois que você iniciar um multipart upload, o Amazon S3 reterá todas as partes até você concluir ou interromper o upload. Durante todo o ciclo de vida, você será cobrado por armazenamento, largura de banda e solicitações desse multipart upload e das partes associadas.

Essas partes são cobradas de acordo com a classe de armazenamento especificada no upload das partes. No entanto, você não receberá cobrança por essas partes se elas forem carregadas nas classes S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive. As partes fracionadas em andamento para uma solicitação PUT na classe de armazenamento S3 Glacier Flexible Retrieval são cobradas como armazenamento de preparação da classe S3 Glacier Flexible Retrieval de acordo com as taxas de armazenamento da classe S3 Standard até que o upload seja concluído. Além disso, tanto `CreateMultipartUpload` quanto `UploadPart` são cobradas de acordo com as taxas da classe S3 Standard. Somente a solicitação `CompleteMultipartUpload` é cobrada de acordo com a taxa da classe S3 Glacier Flexible Retrieval. De maneira semelhante, as partes fracionadas em andamento para uma PUT na classe de armazenamento S3 Glacier Deep Archive são cobradas como armazenamento de preparação da classe S3 Glacier Flexible Retrieval de acordo com as taxas de armazenamento da classe S3 Standard até que o upload seja concluído. Apenas a solicitação `CompleteMultipartUpload` é cobrada de acordo com as taxas da classe S3 Glacier Deep Archive.

Se você interromper o upload fracionado, o Amazon S3 excluirá os artefatos de upload e todas as partes carregadas. Você não receberá cobrança por esses artefatos. Não há cobrança de exclusão antecipada pela exclusão de carregamentos fracionados incompletos, independentemente da classe de armazenamento especificada. Para obter mais informações sobre a definição de preços, consulte Definição de preços do Amazon S3.

> **Note**
>
> Para minimizar os custos de armazenamento, recomendamos que você configure uma regra de ciclo de vida para excluir uploads incompletos de várias partes após um determinado número de dias usando a ação `AbortIncompleteMultipartUpload`. Para obter mais informações sobre como criar uma regra de ciclo de vida para excluir uploads incompletos de várias partes, consulte Configurando uma política de ciclo de vida de bucket para anular multipart uploads incompletos.

Suporte de API para multipart upload

As seções a seguir na Referência de APIs do Amazon Simple Storage Service descrevem a API REST para multipart upload.

Para conferir um passo a passo sobre upload multiparte que utiliza funções do AWS Lambda, consulte Uploading large objects to Amazon S3 using multipart upload and transfer acceleration.

- Criar carregamento fracionado
- Carregar parte
- Carregar parte (copiar)
- Concluir carregamento fracionado
- Anular carregamento fracionado
- Listar partes
- Listar carregamentos fracionados

Suporte da AWS Command Line Interface para carregamento fracionado

Os tópicos a seguir na AWS Command Line Interface descrevem as operações de carregamento fracionado.

- Iniciar multipart upload
- Carregar parte
- Carregar parte (copiar)
- Concluir carregamento fracionado
- Anular carregamento fracionado
- Listar partes
- Listar carregamentos fracionados

Suporte do AWS SDK para upload fracionado

Você pode usar AWS SDKs para fazer upload de um objeto em partes. Para obter uma lista dos AWS SDKs compatíveis com a ação da API, consulte:

- Criar carregamento fracionado
- Carregar parte
- Carregar parte (copiar)
- Concluir carregamento fracionado
- Anular carregamento fracionado
- Listar partes
- Listar carregamentos fracionados

API de multipart upload e permissões

Você deve ter as permissões necessárias para usar as operações do multipart upload. É possível usar listas de controle de acesso (ACLs), a política de bucket ou a política de usuário para conceder permissões às pessoas para realizar essas operações. A tabela a seguir lista as permissões necessárias para várias operações de multipart upload ao usar ACLs, uma política de bucket ou uma política de usuário.

Ação	Permissões obrigatórias
Criar carregamento fracionado	Você deve ter permissão para realizar a ação `s3:PutObject` em um objeto a fim de criar uma solicitação de upload fracionado. O proprietário do bucket pode permitir que outros principais realizem a ação `s3:PutObject` .
Iniciar multipart upload	Você deve ter permissão para realizar a ação `s3:PutObject` em um objeto a fim de inicializar um upload fracionado. O proprietário do bucket pode permitir que outros principais realizem a ação `s3:PutObject` .
Iniciador	O elemento de contêiner que identifica quem iniciou o multipart upload. Se o iniciador for uma Conta da AWS, esse elemento fornecerá as mesmas informaçõ es que o elemento Owner (Proprietário). Se o iniciador for um usuário do IAM, esse elemento fornecerá o ARN e o nome da exibição do usuário.
Carregar parte	Você deve ter permissão para realizar a ação `s3:PutObject` em um objeto para fazer upload de uma parte.

Ação	Permissões obrigatórias
	O proprietário do bucket deve permitir que o iniciador realize a ação `s3:PutObject` em um objeto para que o iniciador possa fazer upload de uma parte desse objeto.
Carregar parte (Copiar)	Você deve ter permissão para realizar a ação `s3:PutObject` em um objeto para fazer upload de uma parte. Como você está fazendo upload de uma parte a partir de um objeto existente, deverá ter permissão `s3:GetObject` no objeto de origem. Para iniciador fazer upload de uma parte para um objeto, o proprietário do bucket deve permitir que o iniciador realize a ação `s3:PutObject` no objeto.
Concluir carregamento fracionado	Você deve ter permissão para realizar a ação `s3:PutObject` em um objeto para concluir o multipart upload. O proprietário do bucket deve permitir que o iniciador realize a ação `s3:PutObject` em um objeto para que o iniciador possa concluir um multipart upload desse objeto.
Parar o multipart upload	Você deve ter permissão para realizar a ação `s3:AbortMultipartUpload` em um objeto para interromper um multipart upload. Por padrão, o proprietário do bucket e o inicializador do upload fracionado têm permissão para executar essa ação como parte das políticas do IAM e de buckets do S3. Se o iniciador for um usuário do IAM, a Conta da AWS desse usuário também terá permissão para interromper o carregamento fracionado. Com as políticas de endpoint da VPC, o inicializador do upload fracionado não recebe automaticamente a permissão para executar a ação `s3:AbortMultipartUpload` . Além desses padrões, o proprietário do bucket pode permitir que outras entidades principais executem a ação `s3:AbortMultipartUpload` em um objeto. O proprietário do bucket pode negar que qualquer principal realize a ação `s3:AbortMultipartUpload` .

Ação	Permissões obrigatórias
Listar partes	Você deve ter permissão para realizar a ação `s3:ListMultipartUploadParts` para listar partes em um multipart upload. Por padrão, o proprietário do bucket tem permissão para listar as partes de qualquer multipart upload para o bucket. O iniciador do multipart upload tem permissão para listar partes do multipart upload específico. Se o iniciador do carregamento fracionado for um usuário do IAM, a Conta da AWS que controla o usuário do IAM também terá permissão para listar partes desse carregamento. Além desses padrões, o proprietário do bucket pode permitir que outras entidades principais executem a ação `s3:ListMultipartUploadParts` em um objeto. O proprietário do bucket também pode negar que qualquer principal realize a ação `s3:ListMultipartUploadParts` .
Listar multipart uploads	Você deve ter permissão para realizar a ação `s3:ListBucketMultipartUploads` em um bucket para listar multipart uploads em andamento no bucket. Além desse padrão, o proprietário do bucket pode permitir que outros principais executem a ação `s3:ListBucketMultipartUploads` no bucket.

Ação	Permissões obrigatórias
Permissões relacionadas a criptografia e descriptografia do AWS KMS	Para executar um upload fracionado com criptografia usando uma chave do AWS Key Management Service (AWS KMS), o solicitante deve ter as seguintes permissões: • As ações `kms:Decrypt` e `kms:GenerateDataKey` na chave. • A ação `kms:GenerateDataKey` para a API CreateMultipartUpload. • A ação `kms:Decrypt` nas APIs UploadPart e UploadPartCopy. Essas permissões são necessárias porque o Amazon S3 precisa descriptografar e ler os dados de partes de arquivos criptografados antes de concluir o multipart upload. A permissão `kms:Decrypt` e a criptografia do lado do servidor com chaves de criptografia fornecidas pelo cliente também são necessárias para obter o valor da soma de verificação de um objeto. Se você não tiver essas permissões necessárias ao usar a API CompleteMultipartUpload, o objeto será criado sem um valor de soma de verificação. Se o seu usuário ou perfil do IAM estiver na mesma Conta da AWS que a chave do KMS, valide que você tem permissões nas políticas de chave e do IAM. Se o seu usuário ou a sua função do IAM pertencer a uma conta diferente da chave do KMS, será necessário ter as permissões na política da chave e no usuário ou na função do IAM.
SSE-C (criptografia do lado do servidor com chaves fornecidas pelo cliente)	Ao usar a API CompleteMultipartUpload, você deve fornecer a SSE-C (criptografia do lado do servidor com chaves de criptografia fornecidas pelo cliente), ou seu objeto será criado sem uma soma de verificação e nenhum valor de soma de verificação será retornado.

Para obter informações sobre a relação entre permissões de ACL e permissões em políticas de acesso, consulte Mapeamento das permissões da ACL e das permissões da política de acesso. Para obter informações sobre os usuários do IAM e as práticas recomendadas, consulte Identidades do IAM (usuários, grupos de usuários e perfis) no Guia do usuário do IAM.

Somas de verificação com operações de carregamento fracionado

Há três APIs do Amazon S3 que são usadas para realizar o upload fracionado: `CreateMultipartUpload`, `UploadPart` e `CompleteMultipartUpload`. A tabela a seguir indica quais cabeçalhos e valores de soma de verificação devem ser fornecidos para cada uma das APIs:

Algoritmo da soma de verificação	Tipo de soma de verificação	**CreateMultipartUpload**	**UploadPart**	**CompleteMultipartUpload**

CRC-64/NVME (`CRC64NVME`)	Objeto inteiro	Cabeçalhos obrigatórios:
		`x-amz-checksum-algorithm`
			Cabeçalhos opcionais:
			`x-amz-checksum-crc64nvme`
				Cabeçalhos opcionais:
				`x-amz-checksum-algorithm`
				`x-amz-crc64`

CRC-32 (`CRC32`)
CRC 32-C (`CRC32C`)
	Objeto inteiro	Cabeçalhos obrigatórios:
		`x-amz-checksum-algorithm`
		`x-amz-checksum-type`
			Cabeçalhos opcionais:
			`x-amz-checksum-crc64nvme`
				Cabeçalhos opcionais:
				`x-amz-checksum-algorithm`
				`x-amz-crc32`
				`x-amz-crc32c`

CRC-32 (`CRC32`) CRC-32C (`CRC32C`) SHA-1 (`SHA1`)	Composto	Cabeçalhos obrigatórios: `x-amz-checksum-algorithm`	Cabeçalhos obrigatórios: `x-amz-checksum-crc32`	Cabeçalhos obrigatórios: Todas as somas de verificação ao nível da parte precisam

Algoritmo da soma de verificação	Tipo de soma de verificação	**CreateMultipartUpload**	**UploadPart**	**CompleteMultipartUpload**

SHA-256 (SHA256)			`x-amz-checksum-crc32c`
			
			`x-amz-checksum-sha1`
			
			`x-amz-checksum-sha256`
				ser incluídas na solicitação `CompleteMultiPartUpload` .
				
				Cabeçalhos opcionais:
				
				`x-amz-crc32`
				
				`x-amz-crc32c`
				
				`x-amz-sha1`
				
				`x-amz-sha256`

Tópicos

- Configurar uma política de ciclo de vida de bucket para anular uploads incompletos de várias partes
- Fazer upload de um objeto usando multipart upload
- Carregar um diretório usando a classe TransferUtility .NET de alto nível
- Listar multipart uploads
- Monitorar um carregamento fracionado com os SDKs da AWS
- Abortar um multipart upload
- Copiar um objeto usando multipart upload
- Tutorial: Fazer upload de um objeto por meio do carregamento fracionado e conferir a integridade dos dados
- Limites do multipart upload do Amazon S3

Configurar uma política de ciclo de vida de bucket para anular uploads incompletos de várias partes

Recomendamos que você configure uma regra de ciclo de vida usando a ação `AbortIncompleteMultipartUpload` para minimizar os custos de armazenamento. Para obter mais informações sobre como anular um multipart upload, consulte Abortar um multipart upload.

O Amazon S3 é compatível com uma regra de ciclo de vida de bucket que pode ser usada para fazer com que o Amazon S3 interrompa multipart uploads que não forem concluídos dentro de um número especificado de dias após a inicialização. Quando um multipart upload não é concluído dentro do prazo especificado, ele se torna elegível para uma operação de anulação. O Amazon S3 interrompe o multipart upload e exclui todas as partes associadas a ele. Essa regra se aplica tanto aos uploads multiparte existentes quanto aos que você criar posteriormente.

Veja a seguir um exemplo de configuração de ciclo de vida que especifica uma regra com a ação `AbortIncompleteMultipartUpload`.

```
<LifecycleConfiguration>
    <Rule>
        <ID>sample-rule</ID>
        <Prefix></Prefix>
        <Status>Enabled</Status>
        <AbortIncompleteMultipartUpload>
          <DaysAfterInitiation>7</DaysAfterInitiation>
        </AbortIncompleteMultipartUpload>
    </Rule>
</LifecycleConfiguration>
```

No exemplo, a regra não especifica um valor para o elemento `Prefix` (o prefixo do nome da chave de objeto). Portanto, a regra se aplica a todos os objetos no bucket para o qual você iniciou multipart uploads. Multipart uploads que foram iniciados e não concluídos dentro de sete dias tornam-se elegíveis para uma operação de anulação. A ação de anulação não tem efeito em multipart uploads concluídos.

Para obter mais informações sobre a configuração do ciclo de vida de bucket, consulte Gerenciar o ciclo de vida dos objetos.

> **Note**
>
> Se o multipart upload for concluído durante o período de dias especificado na regra, a ação de ciclo de vida `AbortIncompleteMultipartUpload` não se aplicará (ou seja, o Amazon S3 não executará nenhuma ação). Além disso, essa ação não se aplica a objetos. Nenhum objeto é excluído por essa ação do ciclo de vida. Além disso, você não incorrerá em cobranças de exclusão antecipada do ciclo de vida do S3 ao remover qualquer parte incompleta do upload de várias partes.

Usar o console do S3

Para gerenciar multipart uploads incompletos automaticamente, use o console do S3 para criar uma regra de ciclo de vida para expirar bytes de multipart uploads incompletos em um bucket após determinado número de dias. O procedimento a seguir mostra como adicionar uma regra de ciclo de vida para excluir multipart uploads incompletos depois de 7 dias. Para obter mais informações sobre como adicionar regras de ciclo de vida, consulte Definir uma configuração do Ciclo de Vida do S3 em um bucket.

Como adicionar uma regra de ciclo de vida para anular multipart uploads incompletos há mais de 7 dias

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Na lista Buckets, escolha o nome do bucket para o qual você deseja criar uma regra de ciclo de vida.
3. Escolha a guia Management (Gerenciamento) e escolha Create lifecycle rule (Criar regra de ciclo de vida).
4. Em Lifecycle rule name (Nome da regra do ciclo de vida), insira um nome para sua regra.

   O nome deve ser exclusivo dentro do bucket.
5. Escolha o escopo da regra do ciclo de vida:

   - Para criar uma regra de ciclo de vida para todos os objetos com um prefixo específico, escolha Limit the scope of this rule using one or more filters (Limitar o escopo desta regra usando um ou mais filtros) e insira o prefixo no campo Prefix (Prefixo).

- Para criar uma regra de ciclo de vida para todos os objetos no bucket, escolha This rule applies to all objects in the bucket (Esta regra se aplica a todos os objetos no bucket) e escolha I acknowledge that this rule applies to all objects in the bucket (Eu reconheço que essa regra se aplica a todos os objetos no bucket).

6. Em Lifecycle rule actions (Ações da regra de ciclo de vida), selecione Delete expired object delete markers or incomplete multipart uploads (Excluir marcadores de exclusão de objetos expirados ou multipart uploads incompletos).
7. Em Delete expired object delete markers or incomplete multipart uploads (Excluir marcadores de exclusão de objetos expirados ou multipart uploads incompletos), escolha Delete incomplete multipart uploads (Excluir multipart uploads incompletos).
8. No campo Number of days (Número de dias), insira o número de dias depois dos quais os multipart uploads incompletos devem ser excluídos (por exemplo, 7 dias).
9. Escolha Criar regra.

Como usar o AWS CLI

O comando `put-bucket-lifecycle-configuration` da AWS Command Line Interface (AWS CLI) a seguir adiciona a configuração de ciclo de vida para o bucket especificado. Para usar esse comando, substitua *`user input placeholders`* por suas informações.

```
aws s3api put-bucket-lifecycle-configuration  \
        --bucket amzn-s3-demo-bucket  \
        --lifecycle-configuration filename-containing-lifecycle-configuration
```

O exemplo a seguir mostra como adicionar uma regra de ciclo de vida para anular multipart uploads incompletos usando a AWS CLI. Ele inclui um exemplo de configuração de ciclo de vida JSON para anular multipart uploads incompletos há mais de 7 dias.

Para usar os comandos da CLI neste exemplo, substitua *`user input placeholders`* pelas suas informações.

Como adicionar uma regra de ciclo de vida para anular multipart uploads incompletos

1. Configure o AWS CLI. Consulte instruções em Developing with Amazon S3 using the AWS CLI na Referência de API do Amazon S3.
2. Salve o seguinte exemplo de configuração de ciclo de vida em um arquivo (por exemplo, *`lifecycle.json`*). Esse exemplo de configuração especifica um prefixo vazio, portanto aplica-

se a todos os objetos no bucket. Para restringir a configuração a um subconjunto de objetos, especifique um prefixo.

```
{
    "Rules": [
        {
            "ID": "Test Rule",
            "Status": "Enabled",
            "Filter": {
                "Prefix": ""
            },
            "AbortIncompleteMultipartUpload": {
                "DaysAfterInitiation": 7
            }
        }
    ]
}
```

3. Execute o comando da CLI a seguir para definir essa configuração de ciclo de vida em seu bucket.

```
aws s3api put-bucket-lifecycle-configuration   \
--bucket amzn-s3-demo-bucket  \
--lifecycle-configuration file://lifecycle.json
```

4. Para verificar se a configuração de ciclo de vida foi definida no bucket, recupere a configuração de ciclo de vida usando o comando `get-bucket-lifecycle` a seguir.

```
aws s3api get-bucket-lifecycle  \
--bucket amzn-s3-demo-bucket
```

5. Para excluir a configuração de ciclo de vida, use o comando `delete-bucket-lifecycle` a seguir.

```
aws s3api delete-bucket-lifecycle \
--bucket amzn-s3-demo-bucket
```

Fazer upload de um objeto usando multipart upload

Você pode usar o multipart upload para fazer upload programático de um único objeto para o Amazon S3. Cada objeto é carregado como um conjunto de partes. Cada parte é uma parte contígua de dados do objeto. O upload dessas partes de objetos pode ser feito de maneira independente e em qualquer ordem. Se a transmissão de alguma parte falhar, você poderá retransmitir essa parte sem afetar outras partes. Depois que todas as partes do objeto forem carregadas, o Amazon S3 montará essas partes e criará o objeto. Usuários anônimos não podem iniciar carregamentos fracionados.

Consulte um procedimento completo sobre o upload de um objeto com carregamento fracionado e com uma soma de verificação adicional em Tutorial: Fazer upload de um objeto por meio do carregamento fracionado e conferir a integridade dos dados.

A seção a seguir mostra como usar o carregamento fracionado com a AWS Command Line Interface e os SDKs da AWS.

Usar o console do S3

Você pode fazer upload de qualquer tipo de arquivo (imagens, backups, dados, filmes etc.) para um bucket do S3. O tamanho máximo de arquivo que você pode carregar usando o console do Amazon S3 é de 160 GB. Para fazer upload de um arquivo com mais de 160 GB, use a AWS Command Line Interface (AWS CLI), AWS SDKs ou a API REST do Amazon S3.

Para obter instruções sobre como fazer upload de um objeto pelo AWS Management Console, consulte Fazer upload de objetos.

Como usar o AWS CLI

O conteúdo a seguir descreve as operações do Amazon S3 para carregamento fracionado usando a AWS CLI.

- Iniciar multipart upload
- Carregar parte
- Carregar parte (copiar)
- Concluir carregamento fracionado
- Anular carregamento fracionado
- Listar partes
- Listar carregamentos fracionados

Uso da API REST

As seções a seguir na Referência de APIs do Amazon Simple Storage Service descrevem a API REST para multipart upload.

- Iniciar multipart upload
- Carregar parte
- Concluir carregamento fracionado
- Parar o multipart upload
- Listar partes
- Listar carregamentos fracionados

Usar os AWS SDKs (API de alto nível)

Alguns AWS SDKs expõem uma API de alto nível que simplifica o upload de várias partes combinando as diferentes operações de API necessárias para concluir um upload de várias partes em uma única operação. Para obter mais informações, consulte Carregar e copiar objetos usando upload fracionado no Amazon S3.

Se precisar pausar e retomar uploads de várias partes, variar os tamanhos das partes durante o upload ou se você não souber o tamanho necessário dos dados com antecedência, use os métodos da API de baixo nível. Os métodos de API de baixo nível para uploads de várias partes oferecem funcionalidades adicionais. Consulte mais informações em Usar os AWS SDKs (API de baixo nível).

.NET

Para fazer upload de um arquivo para um bucket do S3, use a classe `TransferUtility`. Ao fazer o upload de dados de um arquivo, você deve fornecer o nome da chave do objeto. Caso contrário, a API usará o nome do arquivo no lugar do nome da chave. Ao fazer o upload de dados de um fluxo, você deve fornecer o nome da chave do objeto.

Para definir opções de upload avançadas, como o tamanho da parte, o número de threads ao fazer upload das partes simultaneamente, os metadados, a classe de armazenamento, ou ACL, use a classe `TransferUtilityUploadRequest`.

> **Note**
>
> Quando você está usando um streaming na fonte dos dados, a classe `TransferUtility` não faz uploads simultâneos.

O exemplo de C# a seguir faz upload de um arquivo em um bucket do Amazon S3 em várias partes. Ele mostra como usar várias sobrecargas de `TransferUtility.Upload` para fazer upload de um arquivo. Cada chamada sucessiva para upload substitui o upload anterior. Para obter informações sobre como configurar e executar exemplos de código, consulte Conceitos básicos do AWS SDK for .NET no Guia do desenvolvedor do AWS SDK for .NET.

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Transfer;
using System;
using System.IO;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class UploadFileMPUHighLevelAPITest
    {
        private const string bucketName = "*** provide bucket name ***";
        private const string keyName = "*** provide a name for the uploaded object
 ***";
        private const string filePath = "*** provide the full path name of the file
 to upload ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 s3Client;

        public static void Main()
        {
            s3Client = new AmazonS3Client(bucketRegion);
            UploadFileAsync().Wait();
        }

        private static async Task UploadFileAsync()
        {
            try
```

```
            {
                var fileTransferUtility =
                    new TransferUtility(s3Client);

                // Option 1. Upload a file. The file name is used as the object key
name.
                await fileTransferUtility.UploadAsync(filePath, bucketName);
                Console.WriteLine("Upload 1 completed");

                // Option 2. Specify object key name explicitly.
                await fileTransferUtility.UploadAsync(filePath, bucketName,
keyName);
                Console.WriteLine("Upload 2 completed");

                // Option 3. Upload data from a type of System.IO.Stream.
                using (var fileToUpload =
                    new FileStream(filePath, FileMode.Open, FileAccess.Read))
                {
                    await fileTransferUtility.UploadAsync(fileToUpload,
                                               bucketName, keyName);
                }
                Console.WriteLine("Upload 3 completed");

                // Option 4. Specify advanced settings.
                var fileTransferUtilityRequest = new TransferUtilityUploadRequest
                {
                    BucketName = bucketName,
                    FilePath = filePath,
                    StorageClass = S3StorageClass.StandardInfrequentAccess,
                    PartSize = 6291456, // 6 MB.
                    Key = keyName,
                    CannedACL = S3CannedACL.PublicRead
                };
                fileTransferUtilityRequest.Metadata.Add("param1", "Value1");
                fileTransferUtilityRequest.Metadata.Add("param2", "Value2");

                await fileTransferUtility.UploadAsync(fileTransferUtilityRequest);
                Console.WriteLine("Upload 4 completed");
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered on server. Message:'{0}' when
writing an object", e.Message);
            }
```

```
            catch (Exception e)
            {
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
 writing an object", e.Message);
            }

        }
    }
}
```

JavaScript

Example

Faça upload de um arquivo grande.

```
import { S3Client } from "@aws-sdk/client-s3";
import { Upload } from "@aws-sdk/lib-storage";

import {
  ProgressBar,
  logger,
} from "@aws-doc-sdk-examples/lib/utils/util-log.js";

const twentyFiveMB = 25 * 1024 * 1024;

export const createString = (size = twentyFiveMB) => {
  return "x".repeat(size);
};

/**
 * Create a 25MB file and upload it in parts to the specified
 * Amazon S3 bucket.
 * @param {{ bucketName: string, key: string }}
 */
export const main = async ({ bucketName, key }) => {
  const str = createString();
  const buffer = Buffer.from(str, "utf8");
  const progressBar = new ProgressBar({
    description: `Uploading "${key}" to "${bucketName}"`,
    barLength: 30,
  });

  try {
```

```
    const upload = new Upload({
      client: new S3Client({}),
      params: {
        Bucket: bucketName,
        Key: key,
        Body: buffer,
      },
    });

    upload.on("httpUploadProgress", ({ loaded, total }) => {
      progressBar.update({ current: loaded, total });
    });

    await upload.done();
  } catch (caught) {
    if (caught instanceof Error && caught.name === "AbortError") {
      logger.error(`Multipart upload was aborted. ${caught.message}`);
    } else {
      throw caught;
    }
  }
};
```

Example

Baixe um arquivo grande.

```
import { fileURLToPath } from "node:url";
import { GetObjectCommand, NoSuchKey, S3Client } from "@aws-sdk/client-s3";
import { createWriteStream, rmSync } from "node:fs";

const s3Client = new S3Client({});
const oneMB = 1024 * 1024;

export const getObjectRange = ({ bucket, key, start, end }) => {
  const command = new GetObjectCommand({
    Bucket: bucket,
    Key: key,
    Range: `bytes=${start}-${end}`,
  });

  return s3Client.send(command);
};
```

```
/**
 * @param {string | undefined} contentRange
 */
export const getRangeAndLength = (contentRange) => {
  const [range, length] = contentRange.split("/");
  const [start, end] = range.split("-");
  return {
    start: Number.parseInt(start),
    end: Number.parseInt(end),
    length: Number.parseInt(length),
  };
};

export const isComplete = ({ end, length }) => end === length - 1;

const downloadInChunks = async ({ bucket, key }) => {
  const writeStream = createWriteStream(
    fileURLToPath(new URL(`./${key}`, import.meta.url)),
  ).on("error", (err) => console.error(err));

  let rangeAndLength = { start: -1, end: -1, length: -1 };

  while (!isComplete(rangeAndLength)) {
    const { end } = rangeAndLength;
    const nextRange = { start: end + 1, end: end + oneMB };

    const { ContentRange, Body } = await getObjectRange({
      bucket,
      key,
      ...nextRange,
    });
    console.log(`Downloaded bytes ${nextRange.start} to ${nextRange.end}`);

    writeStream.write(await Body.transformToByteArray());
    rangeAndLength = getRangeAndLength(ContentRange);
  }
};

/**
 * Download a large object from and Amazon S3 bucket.
 *
 * When downloading a large file, you might want to break it down into
 * smaller pieces. Amazon S3 accepts a Range header to specify the start
```

```
 * and end of the byte range to be downloaded.
 *
 * @param {{ bucketName: string, key: string }}
 */
export const main = async ({ bucketName, key }) => {
  try {
    await downloadInChunks({
      bucket: bucketName,
      key: key,
    });
  } catch (caught) {
    if (caught instanceof NoSuchKey) {
      console.error(`Failed to download object. No such key "${key}".`);
      rmSync(key);
    }
  }
};
```

Go

Se quiser ter mais informações sobre o exemplo de código Go para carregamento fracionado, consulte Carregue ou baixe arquivos grandes de e para o Amazon S3 usando um AWS SDK.

Example

Faça upload de um objeto grande usando um gerenciador de uploads para dividir os dados em partes e fazer upload delas simultaneamente.

```
import (
 "bytes"
 "context"
 "errors"
 "fmt"
 "io"
 "log"
 "os"
 "time"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/feature/s3/manager"
 "github.com/aws/aws-sdk-go-v2/service/s3"
 "github.com/aws/aws-sdk-go-v2/service/s3/types"
```

```
 "github.com/aws/smithy-go"
)

// BucketBasics encapsulates the Amazon Simple Storage Service (Amazon S3) actions
// used in the examples.
// It contains S3Client, an Amazon S3 service client that is used to perform bucket
// and object actions.
type BucketBasics struct {
 S3Client *s3.Client
}
```

```
// UploadLargeObject uses an upload manager to upload data to an object in a bucket.
// The upload manager breaks large data into parts and uploads the parts
 concurrently.
func (basics BucketBasics) UploadLargeObject(ctx context.Context, bucketName string,
 objectKey string, largeObject []byte) error {
 largeBuffer := bytes.NewReader(largeObject)
 var partMiBs int64 = 10
 uploader := manager.NewUploader(basics.S3Client, func(u *manager.Uploader) {
  u.PartSize = partMiBs * 1024 * 1024
 })
 _, err := uploader.Upload(ctx, &s3.PutObjectInput{
  Bucket: aws.String(bucketName),
  Key:    aws.String(objectKey),
  Body:   largeBuffer,
 })
 if err != nil {
  var apiErr smithy.APIError
  if errors.As(err, &apiErr) && apiErr.ErrorCode() == "EntityTooLarge" {
   log.Printf("Error while uploading object to %s. The object is too large.\n"+
    "The maximum size for a multipart upload is 5TB.", bucketName)
  } else {
   log.Printf("Couldn't upload large object to %v:%v. Here's why: %v\n",
    bucketName, objectKey, err)
  }
 } else {
  err = s3.NewObjectExistsWaiter(basics.S3Client).Wait(
   ctx, &s3.HeadObjectInput{Bucket: aws.String(bucketName), Key:
 aws.String(objectKey)}, time.Minute)
  if err != nil {
   log.Printf("Failed attempt to wait for object %s to exist.\n", objectKey)
```

```
  }
 }

 return err
}
```

Example

Faça download de um objeto grande usando um gerenciador de downloads para obter os dados em partes e baixá-las simultaneamente.

```
// DownloadLargeObject uses a download manager to download an object from a bucket.
// The download manager gets the data in parts and writes them to a buffer until all
 of
// the data has been downloaded.
func (basics BucketBasics) DownloadLargeObject(ctx context.Context, bucketName
 string, objectKey string) ([]byte, error) {
 var partMiBs int64 = 10
 downloader := manager.NewDownloader(basics.S3Client, func(d *manager.Downloader) {
  d.PartSize = partMiBs * 1024 * 1024
 })
 buffer := manager.NewWriteAtBuffer([]byte{})
 _, err := downloader.Download(ctx, buffer, &s3.GetObjectInput{
  Bucket: aws.String(bucketName),
  Key:    aws.String(objectKey),
 })
 if err != nil {
  log.Printf("Couldn't download large object from %v:%v. Here's why: %v\n",
   bucketName, objectKey, err)
 }
 return buffer.Bytes(), err
}
```

PHP

Este tópico explica como usar a classe `Aws\S3\Model\MultipartUpload\UploadBuilder` de alto nível do AWS SDK para PHP para multipart uploads de arquivos. Para obter mais informações sobre a API do AWS SDK for Ruby, acesse AWS SDK for Ruby Version 2.

O exemplo de PHP a seguir faz upload de um arquivo em um bucket do Amazon S3. O exemplo demonstra como definir parâmetros para o objeto `MultipartUploader`.

```
 require 'vendor/autoload.php';

use Aws\Exception\MultipartUploadException;
use Aws\S3\MultipartUploader;
use Aws\S3\S3Client;

$bucket = '*** Your Bucket Name ***';
$keyname = '*** Your Object Key ***';

$s3 = new S3Client([
    'version' => 'latest',
    'region'  => 'us-east-1'
]);

// Prepare the upload parameters.
$uploader = new MultipartUploader($s3, '/path/to/large/file.zip', [
    'bucket' => $bucket,
    'key'    => $keyname
]);

// Perform the upload.
try {
    $result = $uploader->upload();
    echo "Upload complete: {$result['ObjectURL']}" . PHP_EOL;
} catch (MultipartUploadException $e) {
    echo $e->getMessage() . PHP_EOL;
}
```

Python

O exemplo a seguir carrega um objeto usando a API do Python de multipart upload de alto nível (a classe `TransferManager`).

```
import sys
import threading

import boto3
from boto3.s3.transfer import TransferConfig
```

```
MB = 1024 * 1024
s3 = boto3.resource("s3")


class TransferCallback:
    """
    Handle callbacks from the transfer manager.

    The transfer manager periodically calls the __call__ method throughout
    the upload and download process so that it can take action, such as
    displaying progress to the user and collecting data about the transfer.
    """

    def __init__(self, target_size):
        self._target_size = target_size
        self._total_transferred = 0
        self._lock = threading.Lock()
        self.thread_info = {}

    def __call__(self, bytes_transferred):
        """
        The callback method that is called by the transfer manager.

        Display progress during file transfer and collect per-thread transfer
        data. This method can be called by multiple threads, so shared instance
        data is protected by a thread lock.
        """
        thread = threading.current_thread()
        with self._lock:
            self._total_transferred += bytes_transferred
            if thread.ident not in self.thread_info.keys():
                self.thread_info[thread.ident] = bytes_transferred
            else:
                self.thread_info[thread.ident] += bytes_transferred

            target = self._target_size * MB
            sys.stdout.write(
                f"\r{self._total_transferred} of {target} transferred "
                f"({(self._total_transferred / target) * 100:.2f}%)."
            )
            sys.stdout.flush()
```

```
def upload_with_default_configuration(
    local_file_path, bucket_name, object_key, file_size_mb
):
    """
    Upload a file from a local folder to an Amazon S3 bucket, using the default
    configuration.
    """
    transfer_callback = TransferCallback(file_size_mb)
    s3.Bucket(bucket_name).upload_file(
        local_file_path, object_key, Callback=transfer_callback
    )
    return transfer_callback.thread_info


def upload_with_chunksize_and_meta(
    local_file_path, bucket_name, object_key, file_size_mb, metadata=None
):
    """
    Upload a file from a local folder to an Amazon S3 bucket, setting a
    multipart chunk size and adding metadata to the Amazon S3 object.

    The multipart chunk size controls the size of the chunks of data that are
    sent in the request. A smaller chunk size typically results in the transfer
    manager using more threads for the upload.

    The metadata is a set of key-value pairs that are stored with the object
    in Amazon S3.
    """
    transfer_callback = TransferCallback(file_size_mb)

    config = TransferConfig(multipart_chunksize=1 * MB)
    extra_args = {"Metadata": metadata} if metadata else None
    s3.Bucket(bucket_name).upload_file(
        local_file_path,
        object_key,
        Config=config,
        ExtraArgs=extra_args,
        Callback=transfer_callback,
    )
    return transfer_callback.thread_info


def upload_with_high_threshold(local_file_path, bucket_name, object_key,
 file_size_mb):
```

```
    """
    Upload a file from a local folder to an Amazon S3 bucket, setting a
    multipart threshold larger than the size of the file.

    Setting a multipart threshold larger than the size of the file results
    in the transfer manager sending the file as a standard upload instead of
    a multipart upload.
    """
    transfer_callback = TransferCallback(file_size_mb)
    config = TransferConfig(multipart_threshold=file_size_mb * 2 * MB)
    s3.Bucket(bucket_name).upload_file(
        local_file_path, object_key, Config=config, Callback=transfer_callback
    )
    return transfer_callback.thread_info


def upload_with_sse(
    local_file_path, bucket_name, object_key, file_size_mb, sse_key=None
):
    """
    Upload a file from a local folder to an Amazon S3 bucket, adding server-side
    encryption with customer-provided encryption keys to the object.

    When this kind of encryption is specified, Amazon S3 encrypts the object
    at rest and allows downloads only when the expected encryption key is
    provided in the download request.
    """
    transfer_callback = TransferCallback(file_size_mb)
    if sse_key:
        extra_args = {"SSECustomerAlgorithm": "AES256", "SSECustomerKey": sse_key}
    else:
        extra_args = None
    s3.Bucket(bucket_name).upload_file(
        local_file_path, object_key, ExtraArgs=extra_args,
 Callback=transfer_callback
    )
    return transfer_callback.thread_info


def download_with_default_configuration(
    bucket_name, object_key, download_file_path, file_size_mb
):
    """
    Download a file from an Amazon S3 bucket to a local folder, using the
```

```
    default configuration.
    """
    transfer_callback = TransferCallback(file_size_mb)
    s3.Bucket(bucket_name).Object(object_key).download_file(
        download_file_path, Callback=transfer_callback
    )
    return transfer_callback.thread_info


def download_with_single_thread(
    bucket_name, object_key, download_file_path, file_size_mb
):
    """
    Download a file from an Amazon S3 bucket to a local folder, using a
    single thread.
    """
    transfer_callback = TransferCallback(file_size_mb)
    config = TransferConfig(use_threads=False)
    s3.Bucket(bucket_name).Object(object_key).download_file(
        download_file_path, Config=config, Callback=transfer_callback
    )
    return transfer_callback.thread_info


def download_with_high_threshold(
    bucket_name, object_key, download_file_path, file_size_mb
):
    """
    Download a file from an Amazon S3 bucket to a local folder, setting a
    multipart threshold larger than the size of the file.

    Setting a multipart threshold larger than the size of the file results
    in the transfer manager sending the file as a standard download instead
    of a multipart download.
    """
    transfer_callback = TransferCallback(file_size_mb)
    config = TransferConfig(multipart_threshold=file_size_mb * 2 * MB)
    s3.Bucket(bucket_name).Object(object_key).download_file(
        download_file_path, Config=config, Callback=transfer_callback
    )
    return transfer_callback.thread_info


def download_with_sse(
```

```
    bucket_name, object_key, download_file_path, file_size_mb, sse_key
):
    """
    Download a file from an Amazon S3 bucket to a local folder, adding a
    customer-provided encryption key to the request.

    When this kind of encryption is specified, Amazon S3 encrypts the object
    at rest and allows downloads only when the expected encryption key is
    provided in the download request.
    """
    transfer_callback = TransferCallback(file_size_mb)

    if sse_key:
        extra_args = {"SSECustomerAlgorithm": "AES256", "SSECustomerKey": sse_key}
    else:
        extra_args = None
    s3.Bucket(bucket_name).Object(object_key).download_file(
        download_file_path, ExtraArgs=extra_args, Callback=transfer_callback
    )
    return transfer_callback.thread_info
```

Usar os AWS SDKs (API de baixo nível)

O AWS SDK expõe uma API de baixo nível que se assemelha à API REST do Amazon S3 para carregamentos fracionados (consulte Carregar e copiar objetos usando upload fracionado no Amazon S3). Use a API de baixo nível quando precisar pausar e retomar carregamentos fracionados, variar os tamanhos das partes durante o carregamento ou não souber o tamanho dos dados com antecedência. Quando esses requisitos não existirem, use a API de alto nível (consulte Usar os AWS SDKs (API de alto nível)).

Java

O exemplo a seguir mostra como usar as classes Java de baixo nível para fazer upload de um arquivo. Ele realiza as seguintes etapas:

- Inicia um multipart upload usando o método `AmazonS3Client.initiateMultipartUpload()`, e transmite a um objeto `InitiateMultipartUploadRequest`.

- Salva o ID de upload retornado pelo método `AmazonS3Client.initiateMultipartUpload()`. Você fornece esse ID de upload para cada operação de multipart upload subsequente.
- Faz upload das partes do objeto. Para cada parte, chame o método `AmazonS3Client.uploadPart()`. Você fornece informações sobre o upload da parte usando um objeto `UploadPartRequest`.
- Para cada parte, você salva a ETag da resposta do método `AmazonS3Client.uploadPart()` em uma lista. Você usa os valores de ETag para concluir o multipart upload.
- Chama o método `AmazonS3Client.completeMultipartUpload()` para concluir o multipart upload.

Example

Consulte instruções sobre como criar e testar uma amostra funcional em Getting Started no Guia do desenvolvedor do AWS SDK para Java.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.*;

import java.io.File;
import java.io.IOException;
import java.util.ArrayList;
import java.util.List;

public class LowLevelMultipartUpload {

    public static void main(String[] args) throws IOException {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "*** Bucket name ***";
        String keyName = "*** Key name ***";
        String filePath = "*** Path to file to upload ***";

        File file = new File(filePath);
```

```
        long contentLength = file.length();
        long partSize = 5 * 1024 * 1024; // Set part size to 5 MB.

        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withRegion(clientRegion)
                    .withCredentials(new ProfileCredentialsProvider())
                    .build();

            // Create a list of ETag objects. You retrieve ETags for each object
part
            // uploaded,
            // then, after each individual part has been uploaded, pass the list of
ETags to
            // the request to complete the upload.
            List<PartETag> partETags = new ArrayList<PartETag>();

            // Initiate the multipart upload.
            InitiateMultipartUploadRequest initRequest = new
InitiateMultipartUploadRequest(bucketName, keyName);
            InitiateMultipartUploadResult initResponse =
s3Client.initiateMultipartUpload(initRequest);

            // Upload the file parts.
            long filePosition = 0;
            for (int i = 1; filePosition < contentLength; i++) {
                // Because the last part could be less than 5 MB, adjust the part
size as
                // needed.
                partSize = Math.min(partSize, (contentLength - filePosition));

                // Create the request to upload a part.
                UploadPartRequest uploadRequest = new UploadPartRequest()
                        .withBucketName(bucketName)
                        .withKey(keyName)
                        .withUploadId(initResponse.getUploadId())
                        .withPartNumber(i)
                        .withFileOffset(filePosition)
                        .withFile(file)
                        .withPartSize(partSize);

                // Upload the part and add the response's ETag to our list.
                UploadPartResult uploadResult = s3Client.uploadPart(uploadRequest);
                partETags.add(uploadResult.getPartETag());
```

```
                filePosition += partSize;
            }

            // Complete the multipart upload.
            CompleteMultipartUploadRequest compRequest = new
 CompleteMultipartUploadRequest(bucketName, keyName,
                    initResponse.getUploadId(), partETags);
            s3Client.completeMultipartUpload(compRequest);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

.NET

O exemplo do C# a seguir mostra como usar a API de multipart upload do SDK para .NET de nível baixo para fazer upload de um arquivo para um bucket do S3. Para obter informações sobre multipart uploads do Amazon S3, consulte Carregar e copiar objetos usando upload fracionado no Amazon S3.

> **Note**
>
> Ao usar a SDK para .NET API para fazer upload de objetos grandes, um tempo limite pode ocorrer mesmo quando os dados são gravados para o fluxo de solicitação. Você pode definir um tempo limite explícito usando o `UploadPartRequest`.

O exemplo do C# a seguir faz upload de um arquivo para um bucket do S3 usando a API de multipart upload de nível baixo. Para obter informações sobre como configurar e executar exemplos de código, consulte Conceitos básicos do AWS SDK for .NET no Guia do desenvolvedor do AWS SDK for .NET.

```
using Amazon;
using Amazon.Runtime;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Collections.Generic;
using System.IO;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class UploadFileMPULowLevelAPITest
    {
        private const string bucketName = "*** provide bucket name ***";
        private const string keyName = "*** provide a name for the uploaded object
 ***";
        private const string filePath = "*** provide the full path name of the file
 to upload ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 s3Client;

        public static void Main()
        {
            s3Client = new AmazonS3Client(bucketRegion);
            Console.WriteLine("Uploading an object");
            UploadObjectAsync().Wait();
        }

        private static async Task UploadObjectAsync()
        {
            // Create list to store upload part responses.
            List<UploadPartResponse> uploadResponses = new
 List<UploadPartResponse>();

            // Setup information required to initiate the multipart upload.
            InitiateMultipartUploadRequest initiateRequest = new
 InitiateMultipartUploadRequest
            {
                BucketName = bucketName,
                Key = keyName
            };
```

```
            // Initiate the upload.
            InitiateMultipartUploadResponse initResponse =
                await s3Client.InitiateMultipartUploadAsync(initiateRequest);

            // Upload parts.
            long contentLength = new FileInfo(filePath).Length;
            long partSize = 5 * (long)Math.Pow(2, 20); // 5 MB

            try
            {
                Console.WriteLine("Uploading parts");

                long filePosition = 0;
                for (int i = 1; filePosition < contentLength; i++)
                {
                    UploadPartRequest uploadRequest = new UploadPartRequest
                        {
                            BucketName = bucketName,
                            Key = keyName,
                            UploadId = initResponse.UploadId,
                            PartNumber = i,
                            PartSize = partSize,
                            FilePosition = filePosition,
                            FilePath = filePath
                        };

                    // Track upload progress.
                    uploadRequest.StreamTransferProgress +=
                        new
EventHandler<StreamTransferProgressArgs>(UploadPartProgressEventCallback);

                    // Upload a part and add the response to our list.
                    uploadResponses.Add(await
s3Client.UploadPartAsync(uploadRequest));

                    filePosition += partSize;
                }

                // Setup to complete the upload.
                CompleteMultipartUploadRequest completeRequest = new
CompleteMultipartUploadRequest
                    {
                        BucketName = bucketName,
```

```
                        Key = keyName,
                        UploadId = initResponse.UploadId
                    };
                completeRequest.AddPartETags(uploadResponses);

                // Complete the upload.
                CompleteMultipartUploadResponse completeUploadResponse =
                    await s3Client.CompleteMultipartUploadAsync(completeRequest);
            }
            catch (Exception exception)
            {
                Console.WriteLine("An AmazonS3Exception was thrown: { 0}",
 exception.Message);

                // Abort the upload.
                AbortMultipartUploadRequest abortMPURequest = new
 AbortMultipartUploadRequest
                {
                    BucketName = bucketName,
                    Key = keyName,
                    UploadId = initResponse.UploadId
                };
               await s3Client.AbortMultipartUploadAsync(abortMPURequest);
            }
        }
        public static void UploadPartProgressEventCallback(object sender,
 StreamTransferProgressArgs e)
        {
            // Process event.
            Console.WriteLine("{0}/{1}", e.TransferredBytes, e.TotalBytes);
        }
    }
}
```

PHP

Este tópico mostra como usar o método de baixo nível `uploadPart`, da versão 3 do AWS SDK para PHP, para carregar um arquivo em várias partes. Para obter mais informações sobre a API do AWS SDK for Ruby, acesse AWS SDK for Ruby Version 2.

O exemplo de PHP a seguir faz upload de um arquivo para um bucket do Amazon S3 usando o multipart upload da API de baixo nível do PHP.

```
 require 'vendor/autoload.php';

use Aws\S3\Exception\S3Exception;
use Aws\S3\S3Client;

$bucket = '*** Your Bucket Name ***';
$keyname = '*** Your Object Key ***';
$filename = '*** Path to and Name of the File to Upload ***';

$s3 = new S3Client([
    'version' => 'latest',
    'region'  => 'us-east-1'
]);

$result = $s3->createMultipartUpload([
    'Bucket'       => $bucket,
    'Key'          => $keyname,
    'StorageClass' => 'REDUCED_REDUNDANCY',
    'Metadata'     => [
        'param1' => 'value 1',
        'param2' => 'value 2',
        'param3' => 'value 3'
    ]
]);
$uploadId = $result['UploadId'];

// Upload the file in parts.
try {
    $file = fopen($filename, 'r');
    $partNumber = 1;
    while (!feof($file)) {
        $result = $s3->uploadPart([
            'Bucket'     => $bucket,
            'Key'        => $keyname,
            'UploadId'   => $uploadId,
            'PartNumber' => $partNumber,
            'Body'       => fread($file, 5 * 1024 * 1024),
        ]);
        $parts['Parts'][$partNumber] = [
            'PartNumber' => $partNumber,
            'ETag' => $result['ETag'],
        ];
        $partNumber++;
```

```
        echo "Uploading part $partNumber of $filename." . PHP_EOL;
    }
    fclose($file);
} catch (S3Exception $e) {
    $result = $s3->abortMultipartUpload([
        'Bucket'   => $bucket,
        'Key'      => $keyname,
        'UploadId' => $uploadId
    ]);

    echo "Upload of $filename failed." . PHP_EOL;
}

// Complete the multipart upload.
$result = $s3->completeMultipartUpload([
    'Bucket'   => $bucket,
    'Key'      => $keyname,
    'UploadId' => $uploadId,
    'MultipartUpload'    => $parts,
]);
$url = $result['Location'];

echo "Uploaded $filename to $url." . PHP_EOL;
```

Como usar o AWS SDK para Ruby

O AWS SDK para Ruby versão 3 é compatível com carregamentos fracionados do Amazon S3 de duas formas. Para a primeira opção, é possível usar uploads de arquivos gerenciados. Para obter mais informações, consulte Uploading Files to Amazon S3 no Blog do desenvolvedor da AWS. O upload de arquivos gerenciado é o método recomendado para fazer upload de arquivos em um bucket. Eles fornecem os seguintes benefícios:

- Gerenciam multipart uploads para objetos com mais de 15 MB.
- Abrem corretamente arquivos em modo binário para evitar problemas de codificação.
- Usam vários threads para upload de partes de grandes objetos em paralelo.

Como alternativa, você pode usar as seguintes operações de cliente do multipart upload diretamente:

- create_multipart_upload: inicia um multipart upload e retorna um ID de upload.

- upload_part: faz upload de uma parte em um multipart upload.
- upload_part_copy:f az upload de uma parte copiando dados de um objeto existente como a fonte de dados.
- complete_multipart_upload: conclui um multipart upload montando as partes obtidas por upload anteriormente.
- abort_multipart_upload: interrompe um multipart upload.

Carregar um diretório usando a classe TransferUtility .NET de alto nível

Você pode usar a classe `TransferUtility` para fazer upload de um diretório inteiro. Por padrão, a API faz upload somente dos arquivos na raiz do diretório especificado. No entanto, você pode especificar um upload recursivo dos arquivos em todos os subdiretórios.

Para selecionar arquivos no diretório especificado, com base nos critérios de filtragem, especifique expressões de filtragem. Por exemplo, para fazer upload somente dos arquivos PDF de um diretório, especifique a expressão de filtragem `"*.pdf"`.

Ao fazer upload de arquivos de um diretório, você não especifica os nomes da chave para os objetos resultantes. O Amazon S3 cria os nomes de chave usando o caminho original do arquivo. Por exemplo, suponha que você tem um diretório denominado `c:\myfolder` com a seguinte estrutura:

Example

```
C:\myfolder
      \a.txt
      \b.pdf
      \media\
             An.mp3
```

quando você faz upload desse diretório, o Amazon S3 usa os seguintes nomes de chave:

Example

```
a.txt
b.pdf
media/An.mp3
```

Example

O exemplo de C# a seguir faz upload de um diretório em um bucket do Amazon S3. Ele mostra como usar várias sobrecargas de `TransferUtility.UploadDirectory` para fazer upload do diretório. Cada chamada sucessiva para upload substitui o upload anterior. Para obter informações sobre como configurar e executar exemplos de código, consulte Conceitos básicos do AWS SDK for .NET no Guia do desenvolvedor do AWS SDK for .NET.

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Transfer;
using System;
using System.IO;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class UploadDirMPUHighLevelAPITest
    {
        private const string existingBucketName = "*** bucket name ***";
        private const string directoryPath = @"*** directory path ***";
        // The example uploads only .txt files.
        private const string wildCard = "*.txt";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion = RegionEndpoint.USWest2;
        private static IAmazonS3 s3Client;
        static void Main()
        {
            s3Client = new AmazonS3Client(bucketRegion);
            UploadDirAsync().Wait();
        }

        private static async Task UploadDirAsync()
        {
            try
            {
                var directoryTransferUtility =
                    new TransferUtility(s3Client);

                // 1. Upload a directory.
                await directoryTransferUtility.UploadDirectoryAsync(directoryPath,
                    existingBucketName);
                Console.WriteLine("Upload statement 1 completed");
```

```
                // 2. Upload only the .txt files from a directory
                //    and search recursively.
                await directoryTransferUtility.UploadDirectoryAsync(
                                                directoryPath,
                                                existingBucketName,
                                                wildCard,
                                                SearchOption.AllDirectories);
                Console.WriteLine("Upload statement 2 completed");

                // 3. The same as Step 2 and some optional configuration.
                //    Search recursively for .txt files to upload.
                var request = new TransferUtilityUploadDirectoryRequest
                {
                    BucketName = existingBucketName,
                    Directory = directoryPath,
                    SearchOption = SearchOption.AllDirectories,
                    SearchPattern = wildCard
                };

                await directoryTransferUtility.UploadDirectoryAsync(request);
                Console.WriteLine("Upload statement 3 completed");
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine(
                        "Error encountered ***. Message:'{0}' when writing an object",
 e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine(
                    "Unknown encountered on server. Message:'{0}' when writing an
 object", e.Message);
            }
        }
    }
}
```

Listar multipart uploads

É possível usar a AWS CLI, a API REST ou os SDKs da AWS para recuperar uma lista de carregamentos fracionados em andamento no Amazon S3. Você pode usar o multipart upload para

fazer upload programático de um único objeto para o Amazon S3. Carregamentos fracionados movem objetos para o Amazon S3 movendo uma parte dos dados de um objeto por vez. Consulte mais informações gerais sobre carregamentos fracionados em Carregar e copiar objetos usando upload fracionado no Amazon S3.

Consulte um procedimento completo sobre o upload de um objeto com carregamento fracionado e com uma soma de verificação adicional em Tutorial: Fazer upload de um objeto por meio do carregamento fracionado e conferir a integridade dos dados.

A seção a seguir mostra como listar carregamentos fracionados em andamento com a AWS Command Line Interface, a API REST do Amazon S3 e os SDKs da AWS.

Listagem de carregamentos fracionados usando a AWS CLI

As seções a seguir na AWS Command Line Interface descrevem as operações de listagem de carregamentos fracionados.

- list-parts: liste as partes enviadas por upload de um multipart upload específico.
- list-multipart-uploads: liste multipart uploads em andamento.

Listar multipart uploads usando a API REST

As seções a seguir na Referência de APIs do Amazon Simple Storage Service descrevem a API REST para listagem de multipart uploads:

- ListParts-lista as partes enviadas por upload de um multipart upload específico.
- ListMultipartUploads lista multipart uploads em andamento.

Listar uploads fracionados usando o AWS SDK (API de baixo nível)

Java

As tarefas a seguir fornecem orientações para usar as classes Java de baixo nível para listar todos os multipart uploads em andamento em um bucket.

Processo de listagem de multipart uploads da API de baixo nível

1	Crie uma instância da classe `ListMultipartUploadsRequest` e forneça o nome do bucket.

2	Execute o método `AmazonS3Client.listMultipartUploads` . O método retorna uma instância da classe `MultipartUploadListing` que fornece informações sobre os multipart uploads em andamento.

O exemplo de código Java a seguir demonstra as tarefas anteriores.

Example

```
ListMultipartUploadsRequest allMultpartUploadsRequest =
     new ListMultipartUploadsRequest(existingBucketName);
MultipartUploadListing multipartUploadListing =
     s3Client.listMultipartUploads(allMultpartUploadsRequest);
```

.NET

Para listar todos os multipart uploads em andamento em um bucket específico, use a classe `ListMultipartUploadsRequest` da API de multipart upload do SDK para .NET de nível baixo. O `AmazonS3Client.ListMultipartUploads` método retorna uma instância da classe `ListMultipartUploadsResponse` que fornece informações sobre multipart uploads em andamento.

Um multipart upload em andamento é um multipart upload que foi iniciado com o uso da solicitação para iniciar o multipart upload, mas que ainda não foi concluído ou parado. Para obter mais informações sobre multipart uploads do Amazon S3, consulte Carregar e copiar objetos usando upload fracionado no Amazon S3.

O exemplo do C# a seguir mostra como usar o SDK para .NET para listar todos os multipart uploads em andamento em um bucket. Para obter informações sobre como configurar e executar exemplos de código, consulte Conceitos básicos do AWS SDK for .NET no Guia do desenvolvedor do AWS SDK for .NET.

```
ListMultipartUploadsRequest request = new ListMultipartUploadsRequest
{
  BucketName = bucketName // Bucket receiving the uploads.
};

ListMultipartUploadsResponse response = await
 AmazonS3Client.ListMultipartUploadsAsync(request);
```

PHP

Este tópico mostra como usar as classes da API de baixo nível da versão 3 do AWS SDK para PHP para listar todos os multipart uploads em andamento em um bucket. Para obter mais informações sobre a API do AWS SDK for Ruby, acesse AWS SDK for Ruby Version 2.

O exemplo de PHP a seguir demonstra a listagem de todos os multipart uploads em andamento em um bucket.

```
 require 'vendor/autoload.php';

use Aws\S3\S3Client;

$bucket = '*** Your Bucket Name ***';

$s3 = new S3Client([
    'version' => 'latest',
    'region'  => 'us-east-1'
]);

// Retrieve a list of the current multipart uploads.
$result = $s3->listMultipartUploads([
    'Bucket' => $bucket
]);

// Write the list of uploads to the page.
print_r($result->toArray());
```

Monitorar um carregamento fracionado com os SDKs da AWS

É possível monitorar o progresso do upload de um objeto para o Amazon S3 com uma interface de escuta. A API de carregamento fracionado de alto nível fornece essa interface de escuta, chamada `ProgressListener`. Os eventos de progresso ocorrem periodicamente e notificam o listener que os bytes foram transferidos. Consulte mais informações gerais sobre carregamentos fracionados em Carregar e copiar objetos usando upload fracionado no Amazon S3.

Consulte um procedimento completo sobre o upload de um objeto com carregamento fracionado e com uma soma de verificação adicional em Tutorial: Fazer upload de um objeto por meio do carregamento fracionado e conferir a integridade dos dados.

A seção a seguir mostra como monitorar um carregamento fracionado com os SDKs da AWS.

Java

Example

```
TransferManager tm = new TransferManager(new ProfileCredentialsProvider());

PutObjectRequest request = new PutObjectRequest(
    existingBucketName, keyName, new File(filePath));

// Subscribe to the event and provide event handler.
request.setProgressListener(new ProgressListener() {
   public void progressChanged(ProgressEvent event) {
    System.out.println("Transferred bytes: " +
      event.getBytesTransfered());
            }
});
```

Example

O código Java a seguir faz upload de um arquivo e usa `ProgressListener` para rastrear o progresso do upload. Consulte instruções sobre como criar e testar uma amostra funcional em Getting Started no Guia do desenvolvedor do AWS SDK para Java.

```
import java.io.File;

import com.amazonaws.AmazonClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.event.ProgressEvent;
import com.amazonaws.event.ProgressListener;
import com.amazonaws.services.s3.model.PutObjectRequest;
import com.amazonaws.services.s3.transfer.TransferManager;
import com.amazonaws.services.s3.transfer.Upload;

public class TrackMPUProgressUsingHighLevelAPI {

    public static void main(String[] args) throws Exception {
        String existingBucketName = "*** Provide bucket name ***";
        String keyName            = "*** Provide object key ***";
        String filePath           = "*** file to upload ***";
```

```
        TransferManager tm = new TransferManager(new ProfileCredentialsProvider());


        // For more advanced uploads, you can create a request object
        // and supply additional request parameters (ex: progress listeners,
        // canned ACLs, etc.)
        PutObjectRequest request = new PutObjectRequest(
          existingBucketName, keyName, new File(filePath));

        // You can ask the upload for its progress, or you can
        // add a ProgressListener to your request to receive notifications
        // when bytes are transferred.
        request.setGeneralProgressListener(new ProgressListener() {
   @Override
   public void progressChanged(ProgressEvent progressEvent) {
    System.out.println("Transferred bytes: " +
      progressEvent.getBytesTransferred());
   }
  });

        // TransferManager processes all transfers asynchronously,
        // so this call will return immediately.
        Upload upload = tm.upload(request);

        try {
         // You can block and wait for the upload to finish
         upload.waitForCompletion();
        } catch (AmazonClientException amazonClientException) {
         System.out.println("Unable to upload file, upload aborted.");
         amazonClientException.printStackTrace();
        }
    }
}
```

.NET

O seguinte exemplo do C# faz upload de um arquivo em um bucket do S3 usando a classe `TransferUtility` e monitora o andamento do upload. Para obter informações sobre como configurar e executar exemplos de código, consulte Conceitos básicos do AWS SDK for .NET no Guia do desenvolvedor do AWS SDK for .NET.

```
using Amazon;
using Amazon.S3;
```

```
using Amazon.S3.Transfer;
using System;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class TrackMPUUsingHighLevelAPITest
    {
        private const string bucketName = "*** provide the bucket name ***";
        private const string keyName = "*** provide the name for the uploaded object
 ***";
        private const string filePath = " *** provide the full path name of the file
 to upload **";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 s3Client;


        public static void Main()
        {
            s3Client = new AmazonS3Client(bucketRegion);
            TrackMPUAsync().Wait();
        }

        private static async Task TrackMPUAsync()
        {
            try
            {
                var fileTransferUtility = new TransferUtility(s3Client);

                // Use TransferUtilityUploadRequest to configure options.
                // In this example we subscribe to an event.
                var uploadRequest =
                    new TransferUtilityUploadRequest
                    {
                        BucketName = bucketName,
                        FilePath = filePath,
                        Key = keyName
                    };

                uploadRequest.UploadProgressEvent +=
                    new EventHandler<UploadProgressArgs>
                        (uploadRequest_UploadPartProgressEvent);
```

```
                await fileTransferUtility.UploadAsync(uploadRequest);
                Console.WriteLine("Upload completed");
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered on server. Message:'{0}' when
 writing an object", e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
 writing an object", e.Message);
            }
        }

        static void uploadRequest_UploadPartProgressEvent(object sender,
 UploadProgressArgs e)
        {
            // Process event.
            Console.WriteLine("{0}/{1}", e.TransferredBytes, e.TotalBytes);
        }
    }
}
```

Abortar um multipart upload

Após iniciar um multipart upload, você começa a fazer upload de partes. O Amazon S3 armazena essas partes, cria o objeto somente após o carregamento de todas as partes e envia uma solicitação para concluir o carregamento fracionado. Ao receber a solicitação para concluir o multipart upload, o Amazon S3 monta as partes e cria um objeto. Se você não enviar a solicitação de conclusão do carregamento fracionado, o S3 não montará as partes e não criará nenhum objeto. Se você não quiser concluir um carregamento fracionado após o upload das partes, anule o carregamento fracionado.

Você é cobrado por todo o armazenamento associado a partes enviadas por upload. É recomendável sempre concluir ou interromper o carregamento fracionado para remover todas as partes carregadas. Para obter mais informações sobre a definição de preços, consulte Multipart upload e definição de preço.

Você também pode interromper um upload incompleto de várias partes usando uma configuração de ciclo de vida do bucket. Para obter mais informações, consulte Configurar uma política de ciclo de vida de bucket para anular uploads incompletos de várias partes.

A seção a seguir mostra como interromper um carregamento fracionado em andamento no Amazon S3 usando a AWS Command Line Interface, a API REST ou os SDKs da AWS.

Como usar o AWS CLI

Para obter mais informações sobre o uso da AWS CLI para interromper um upload fracionado, consulte abort-multipart-upload na Referência de comandos da AWS CLI.

Uso da API REST

Para obter mais informações sobre o uso da API REST para interromper um multipart upload, consulte AbortMultipartUpload na Referência da API do Amazon Simple Storage Service.

Usar os AWS SDKs (API de alto nível)

Java

A classe `TransferManager` fornece o método `abortMultipartUploads` para interromper multipart uploads em andamento. Um upload é considerado como em andamento depois que você o inicia até ser concluído ou parado. Você fornece um valor `Date` e essa API interrompe todos os multipart uploads, naquele bucket, que foram iniciados antes da `Date` especificada e que ainda estão em andamento.

As tarefas a seguir orientam sobre a utilização de classes Java de alto nível para interromper multipart uploads.

Processo de interrupção de multipart uploads com API de alto nível

1	Crie uma instância da classe `TransferManager` .
2	Execute o método `TransferManager.abortMultipartUploads` passando o nome do bucket e um valor de `Date`.

O código Java a seguir interrompe todos os multipart uploads em andamento que foram iniciados em um bucket específico uma semana atrás. Consulte instruções sobre como criar e testar uma amostra funcional em Getting Started no Guia do desenvolvedor do AWS SDK para Java.

```
import java.util.Date;

import com.amazonaws.AmazonClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3.transfer.TransferManager;

public class AbortMPUUsingHighLevelAPI {

    public static void main(String[] args) throws Exception {
        String existingBucketName = "*** Provide existing bucket name ***";

        TransferManager tm = new TransferManager(new ProfileCredentialsProvider());


        int sevenDays = 1000 * 60 * 60 * 24 * 7;
  Date oneWeekAgo = new Date(System.currentTimeMillis() - sevenDays);

        try {
         tm.abortMultipartUploads(existingBucketName, oneWeekAgo);
        } catch (AmazonClientException amazonClientException) {
         System.out.println("Unable to upload file, upload was aborted.");
         amazonClientException.printStackTrace();
        }
    }
}
```

> **Note**
>
> Você também pode parar um multipart upload específico. Para obter mais informações, consulte Usar os AWS SDKs (API de baixo nível).

.NET

O exemplo do C# a seguir interrompe todos os multipart uploads em andamento que foram iniciados em um bucket específico há uma semana. Para obter informações sobre como configurar e executar exemplos de código, consulte Conceitos básicos do AWS SDK for .NET no Guia do desenvolvedor do AWS SDK for .NET.

```
using Amazon;
using Amazon.S3;
```

```
using Amazon.S3.Transfer;
using System;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class AbortMPUUsingHighLevelAPITest
    {
        private const string bucketName = "*** provide bucket name ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 s3Client;

        public static void Main()
        {
            s3Client = new AmazonS3Client(bucketRegion);
            AbortMPUAsync().Wait();
        }

        private static async Task AbortMPUAsync()
        {
            try
            {
                var transferUtility = new TransferUtility(s3Client);

                // Abort all in-progress uploads initiated before the specified
 date.
                await transferUtility.AbortMultipartUploadsAsync(
                    bucketName, DateTime.Now.AddDays(-7));
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered on server. Message:'{0}' when
 writing an object", e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
 writing an object", e.Message);
            }
        }
    }
```

```
}
```

> **Note**
>
> Você também pode parar um multipart upload específico. Para obter mais informações, consulte Usar os AWS SDKs (API de baixo nível).

Usar os AWS SDKs (API de baixo nível)

É possível interromper um multipart upload em andamento chamando o método `AmazonS3.abortMultipartUpload`. Esse método exclui todas as partes que foram carregadas no Amazon S3 e libera os recursos. Você deve fornecer o ID do upload, o nome do bucket e o nome da chave. O código Java de exemplo a seguir demonstra como interromper um multipart upload em andamento.

Para parar um multipart upload, é preciso fornecer o ID de upload e nomes do bucket e da chave usados no upload. Após parar um multipart upload, não é possível usar o ID de upload para fazer upload de partes adicionais. Para obter mais informações sobre multipart uploads do Amazon S3, consulte Carregar e copiar objetos usando upload fracionado no Amazon S3.

Java

O exemplo de código Java a seguir interrompe um multipart upload em andamento.

Example

```
InitiateMultipartUploadRequest initRequest =
    new InitiateMultipartUploadRequest(existingBucketName, keyName);
InitiateMultipartUploadResult initResponse =
               s3Client.initiateMultipartUpload(initRequest);

AmazonS3 s3Client = new AmazonS3Client(new ProfileCredentialsProvider());
s3Client.abortMultipartUpload(new AbortMultipartUploadRequest(
            existingBucketName, keyName, initResponse.getUploadId()));
```

> **Note**
>
> Em vez de um multipart upload específico, você pode interromper todos os multipart iniciados antes de uma determinada hora que ainda estiverem em andamento. Essa

operação de limpeza é útil para interromper multipart uploads antigos que você iniciou, mas não concluiu ou parou. Para obter mais informações, consulte Usar os AWS SDKs (API de alto nível).

.NET

O exemplo do C# a seguir mostra como parar um multipart upload. Para um exemplo do C# completo que inclui o código seguinte, consulte Usar os AWS SDKs (API de baixo nível).

```
AbortMultipartUploadRequest abortMPURequest = new AbortMultipartUploadRequest
{
    BucketName = existingBucketName,
    Key = keyName,
    UploadId = initResponse.UploadId
};
await AmazonS3Client.AbortMultipartUploadAsync(abortMPURequest);
```

Você também pode anular todos os multipart uploads em andamento que foram iniciados antes de um horário específico. Essa operação de limpeza é útil para anular os multipart uploads que não foram concluídos nem anulados. Para obter mais informações, consulte Usar os AWS SDKs (API de alto nível).

PHP

Este exemplo descreve como usar uma classe da versão 3 do AWS SDK para PHP para anular um carregamento fracionado que está em andamento. Para obter mais informações sobre a API do AWS SDK for Ruby, acesse AWS SDK for Ruby Version 2. O exemplo do método `abortMultipartUpload()`.

Para obter mais informações sobre a API do AWS SDK for Ruby, acesse AWS SDK for Ruby Version 2.

```
 require 'vendor/autoload.php';

use Aws\S3\S3Client;

$bucket = '*** Your Bucket Name ***';
$keyname = '*** Your Object Key ***';
$uploadId = '*** Upload ID of upload to Abort ***';

$s3 = new S3Client([
```

```
    'version' => 'latest',
    'region'  => 'us-east-1'
]);

// Abort the multipart upload.
$s3->abortMultipartUpload([
    'Bucket'   => $bucket,
    'Key'      => $keyname,
    'UploadId' => $uploadId,
]);
```

Copiar um objeto usando multipart upload

O carregamento fracionado permite copiar objetos como um conjunto de partes. Os exemplos nesta seção mostram como copiar objetos maiores que 5 GB usando a API de multipart upload. Consulte informações sobre carregamentos fracionados em Carregar e copiar objetos usando upload fracionado no Amazon S3.

É possível copiar objetos com menos de 5 GB em uma única operação sem usar a API de carregamento fracionado. É possível copiar objetos com menos de 5 GB usando o AWS Management Console, a AWS CLI, a API REST ou SDKs da AWS. Para obter mais informações, consulte Copiar, mover e renomear objetos.

Consulte um procedimento completo sobre o upload de um objeto com carregamento fracionado e com uma soma de verificação adicional em Tutorial: Fazer upload de um objeto por meio do carregamento fracionado e conferir a integridade dos dados.

A seção a seguir mostra como copiar um objeto com carregamento fracionado usando a API REST ou SDKs da AWS.

Uso da API REST

As seções a seguir na Referência de APIs do Amazon Simple Storage Service descrevem a API REST para multipart upload. Para copiar um objeto existente, use a API para upload de parte (cópia) e especifique o objeto de origem adicionando o cabeçalho de solicitação `x-amz-copy-source` na solicitação.

- Iniciar multipart upload
- Carregar parte
- Carregar parte (copiar)

- Concluir carregamento fracionado
- Anular carregamento fracionado
- Listar partes
- Listar carregamentos fracionados

Use essas APIs para fazer suas próprias solicitações REST ou use um dos SDKs que fornecemos. Para obter mais informações sobre como usar o multipart upload com a AWS CLI, consulte Como usar o AWS CLI. Para obter mais informações sobre os SDKs, consulte Suporte do AWS SDK para upload fracionado.

Uso dos SDKs da AWS

Para copiar um objeto usando a API de baixo nível, faça o seguinte:

- Inicie um multipart upload chamando o método `AmazonS3Client.initiateMultipartUpload()`.
- Salve o ID de upload do objeto de resposta retornado pelo método `AmazonS3Client.initiateMultipartUpload()`. Você fornece esse ID de upload para cada operação do upload de parte.
- Copie todas as partes. Para cada parte que você precisar copiar, crie uma nova instância da classe `CopyPartRequest`. Forneça as informações da parte, incluindo a origem e os nomes do bucket de destino, as chaves de objeto de origem e de destino, o ID de upload, os locais dos primeiros e últimos bytes da parte, e o número da parte.
- Salve as respostas das chamadas de método `AmazonS3Client.copyPart()`. Cada resposta inclui o valor `ETag` e o número da parte para a parte cujo upload foi feito. Você precisa dessas informações para concluir o multipart upload.
- Chame o método `AmazonS3Client.completeMultipartUpload()` para concluir a operação de cópia.

Java

Example

O exemplo a seguir mostra como usar a API Java de baixo nível do Amazon S3 para realizar uma cópia multipart. Consulte instruções sobre como criar e testar uma amostra funcional em Getting Started no Guia do desenvolvedor do AWS SDK para Java.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.*;

import java.io.IOException;
import java.util.ArrayList;
import java.util.List;

public class LowLevelMultipartCopy {

    public static void main(String[] args) throws IOException {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String sourceBucketName = "*** Source bucket name ***";
        String sourceObjectKey = "*** Source object key ***";
        String destBucketName = "*** Target bucket name ***";
        String destObjectKey = "*** Target object key ***";

        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(clientRegion)
                    .build();

            // Initiate the multipart upload.
            InitiateMultipartUploadRequest initRequest = new
 InitiateMultipartUploadRequest(destBucketName,
                    destObjectKey);
            InitiateMultipartUploadResult initResult =
 s3Client.initiateMultipartUpload(initRequest);

            // Get the object size to track the end of the copy operation.
            GetObjectMetadataRequest metadataRequest = new
 GetObjectMetadataRequest(sourceBucketName, sourceObjectKey);
            ObjectMetadata metadataResult =
 s3Client.getObjectMetadata(metadataRequest);
            long objectSize = metadataResult.getContentLength();

            // Copy the object using 5 MB parts.
```

```
            long partSize = 5 * 1024 * 1024;
            long bytePosition = 0;
            int partNum = 1;
            List<CopyPartResult> copyResponses = new ArrayList<CopyPartResult>();
            while (bytePosition < objectSize) {
                // The last part might be smaller than partSize, so check to make
sure
                // that lastByte isn't beyond the end of the object.
                long lastByte = Math.min(bytePosition + partSize - 1, objectSize -
1);

                // Copy this part.
                CopyPartRequest copyRequest = new CopyPartRequest()
                        .withSourceBucketName(sourceBucketName)
                        .withSourceKey(sourceObjectKey)
                        .withDestinationBucketName(destBucketName)
                        .withDestinationKey(destObjectKey)
                        .withUploadId(initResult.getUploadId())
                        .withFirstByte(bytePosition)
                        .withLastByte(lastByte)
                        .withPartNumber(partNum++);
                copyResponses.add(s3Client.copyPart(copyRequest));
                bytePosition += partSize;
            }

            // Complete the upload request to concatenate all uploaded parts and
make the
            // copied object available.
            CompleteMultipartUploadRequest completeRequest = new
CompleteMultipartUploadRequest(
                    destBucketName,
                    destObjectKey,
                    initResult.getUploadId(),
                    getETags(copyResponses));
            s3Client.completeMultipartUpload(completeRequest);
            System.out.println("Multipart copy complete.");
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
```

```
        }
    }

    // This is a helper function to construct a list of ETags.
    private static List<PartETag> getETags(List<CopyPartResult> responses) {
        List<PartETag> etags = new ArrayList<PartETag>();
        for (CopyPartResult response : responses) {
            etags.add(new PartETag(response.getPartNumber(), response.getETag()));
        }
        return etags;
    }
}
```

.NET

O exemplo em C# a seguir mostra como usar o SDK para .NET para copiar um objeto do Amazon S3 com mais de 5 GB de um local de origem para outro, como de um bucket para outro. Para copiar objetos menores que 5 GB, use um procedimento de cópia de operação única descrita em Uso dos SDKs da AWS. Para obter mais informações sobre multipart uploads do Amazon S3, consulte Carregar e copiar objetos usando upload fracionado no Amazon S3.

Este exemplo mostra como copiar um objeto do Amazon S3 com mais de 5 GB de um bucket do S3 para outro usando a API de carregamento fracionado do SDK para .NET.

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Collections.Generic;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class CopyObjectUsingMPUapiTest
    {
        private const string sourceBucket = "*** provide the name of the bucket with
 source object ***";
        private const string targetBucket = "*** provide the name of the bucket to
 copy the object to ***";
        private const string sourceObjectKey = "*** provide the name of object to
 copy ***";
```

```
        private const string targetObjectKey = "*** provide the name of the object
copy ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
RegionEndpoint.USWest2;
        private static IAmazonS3 s3Client;

        public static void Main()
        {
            s3Client = new AmazonS3Client(bucketRegion);
            Console.WriteLine("Copying an object");
            MPUCopyObjectAsync().Wait();
        }
        private static async Task MPUCopyObjectAsync()
        {
            // Create a list to store the upload part responses.
            List<UploadPartResponse> uploadResponses = new
List<UploadPartResponse>();
            List<CopyPartResponse> copyResponses = new List<CopyPartResponse>();

            // Setup information required to initiate the multipart upload.
            InitiateMultipartUploadRequest initiateRequest =
                new InitiateMultipartUploadRequest
                {
                    BucketName = targetBucket,
                    Key = targetObjectKey
                };

            // Initiate the upload.
            InitiateMultipartUploadResponse initResponse =
                await s3Client.InitiateMultipartUploadAsync(initiateRequest);

            // Save the upload ID.
            String uploadId = initResponse.UploadId;

            try
            {
                // Get the size of the object.
                GetObjectMetadataRequest metadataRequest = new
GetObjectMetadataRequest
                {
                    BucketName = sourceBucket,
                    Key = sourceObjectKey
                };
```

```
                GetObjectMetadataResponse metadataResponse =
                    await s3Client.GetObjectMetadataAsync(metadataRequest);
                long objectSize = metadataResponse.ContentLength; // Length in
bytes.

                // Copy the parts.
                long partSize = 5 * (long)Math.Pow(2, 20); // Part size is 5 MB.

                long bytePosition = 0;
                for (int i = 1; bytePosition < objectSize; i++)
                {
                    CopyPartRequest copyRequest = new CopyPartRequest
                    {
                        DestinationBucket = targetBucket,
                        DestinationKey = targetObjectKey,
                        SourceBucket = sourceBucket,
                        SourceKey = sourceObjectKey,
                        UploadId = uploadId,
                        FirstByte = bytePosition,
                        LastByte = bytePosition + partSize - 1 >= objectSize ?
objectSize - 1 : bytePosition + partSize - 1,
                        PartNumber = i
                    };

                    copyResponses.Add(await s3Client.CopyPartAsync(copyRequest));

                    bytePosition += partSize;
                }

                // Set up to complete the copy.
                CompleteMultipartUploadRequest completeRequest =
                new CompleteMultipartUploadRequest
                {
                    BucketName = targetBucket,
                    Key = targetObjectKey,
                    UploadId = initResponse.UploadId
                };
                completeRequest.AddPartETags(copyResponses);

                // Complete the copy.
                CompleteMultipartUploadResponse completeUploadResponse =
                    await s3Client.CompleteMultipartUploadAsync(completeRequest);
            }
```

```
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered on server. Message:'{0}' when
 writing an object", e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
 writing an object", e.Message);
            }
        }
    }
}
```

Tutorial: Fazer upload de um objeto por meio do carregamento fracionado e conferir a integridade dos dados

O multipart upload permite que você faça upload de um único objeto como um conjunto de partes. Cada parte é uma parte contígua de dados do objeto. O upload dessas partes de objetos pode ser feito de maneira independente e em qualquer ordem. Se a transmissão de alguma parte falhar, você poderá retransmitir essa parte sem afetar outras partes. Depois que todas as partes do objeto forem carregadas, o Amazon S3 montará essas partes e criará o objeto. Geralmente, quando seu objeto alcança 100 MB de tamanho, você deve considerar o uso de multipart uploads em vez de fazer upload do objeto em uma única operação. Para obter mais informações sobre multipart uploads, consulte Carregar e copiar objetos usando upload fracionado no Amazon S3. Para ver os limites relacionados a carregamentos fracionados, consulte Limites do multipart upload do Amazon S3.

É possível usar somas de verificação para verificar se os ativos não são alterados quando copiados. A execução de uma soma de verificação consiste em usar um algoritmo para iterar sequencialmente sobre cada byte em um arquivo. O Amazon S3 oferece várias opções de soma de verificação para conferir a integridade dos dados. Recomendamos que você execute essas verificações de integridade como prática recomendada de durabilidade e para garantir que cada byte seja transferido sem alteração. O Amazon S3 também é compatível com os seguintes algoritmos: SHA-1, SHA-256, CRC32 e CRC32C. O Amazon S3 usa um ou mais desses algoritmos para calcular um valor de soma de verificação adicional e armazená-lo como parte dos metadados do objeto. Para ter mais informações sobre somas de verificação, consulte Verificar a integridade do objeto no Amazon S3.

Objetivo

Neste tutorial, você aprenderá a fazer upload de um objeto no Amazon S3 usando um carregamento fracionado e uma soma de verificação SHA-256 adicional por meio da AWS Command Line Interface (AWS CLI). Você também aprenderá a conferir a integridade dos dados do objeto calculando o hash MD5 e a soma de verificação SHA-256 do objeto carregado.

Tópicos

- Pré-requisitos
- Etapa 1: criar um arquivo grande
- Etapa 2: dividir o arquivo em vários arquivos
- Etapa 3: criar o carregamento fracionado com uma soma de verificação adicional
- Etapa 4: fazer upload das partes do carregamento fracionado
- Etapa 5: listar todas as partes do carregamento fracionado
- Etapa 6: concluir o carregamento fracionado
- Etapa 7: confirmar se o objeto foi carregado no bucket
- Etapa 8: verificar a integridade do objeto com uma soma de verificação MD5
- Etapa 9: verificar a integridade do objeto com uma soma de verificação adicional
- Etapa 10: Limpar os recursos

Pré-requisitos

- Antes de iniciar este tutorial, confira se você tem acesso a um bucket do Amazon S3 para o qual possa fazer upload. Para obter mais informações, consulte Criar um bucket de uso geral.
- É necessário ter a AWS CLI instalada e configurada. Se você ainda não tiver a AWS CLI instalada, consulte Install or update to the latest version of the AWS CLI no Guia do usuário da AWS Command Line Interface.
- Também é possível executar comandos da AWS CLI pelo console usando o AWS CloudShell. O AWS CloudShell é um shell pré-autenticado e baseado em navegador que você pode iniciar diretamente do AWS Management Console. Para ter mais informações, consulte What is CloudShell? e Getting started with AWS CloudShell no Guia do usuário do AWS CloudShell.

Etapa 1: criar um arquivo grande

Se você já tiver um arquivo pronto para upload, poderá usá-lo para este tutorial. Caso contrário, crie um arquivo de 15 MB usando as etapas a seguir. Para ver os limites relacionados a carregamentos fracionados, consulte Limites do multipart upload do Amazon S3.

Como criar um arquivo grande

Use um dos seguintes comandos para criar o arquivo, dependendo do sistema operacional que estiver usando.

Linux ou macOS

Para criar um arquivo de 15 MB, abra o terminal local e execute o seguinte comando:

```
dd if=/dev/urandom of=census-data.bin bs=1M count=15
```

Esse comando cria um arquivo de 15 MB denominado `census-data.bin` preenchido com bytes aleatórios.

Windows

Para criar um arquivo de 15 MB, abra o terminal local e execute o seguinte comando:

```
fsutil file createnew census-data.bin 15728640
```

Esse comando cria um arquivo denominado `census-data.bin` com um tamanho de 15 MB de dados arbitrários (15.728.640 bytes).

Etapa 2: dividir o arquivo em vários arquivos

Para realizar o carregamento fracionado, é necessário dividir o arquivo grande em partes menores. Depois, é possível fazer upload das partes menores usando o processo de carregamento fracionado. Esta etapa demonstra como dividir em partes menores o arquivo grande criado na Etapa 1. O exemplo a seguir usa um arquivo de 15 MB denominado `census-data.bin`.

Como dividir um arquivo grande em partes

Linux ou macOS

Para dividir o arquivo grande em partes de 5 MB, use o comando `split`. Abra o terminal e execute o seguinte:

```
split -b 5M -d census-data.bin census-part
```

Esse comando divide `census-data.bin` em partes de 5 MB denominadas `census-part**`, em que `**` é um sufixo numérico de `00`.

Windows

Para dividir o arquivo grande, use o PowerShell. Abra o PowerShell e execute o seguinte script:

```
$inputFile = "census-data.bin"
$outputFilePrefix = "census-part"
$chunkSize = 5MB

$fs = [System.IO.File]::OpenRead($inputFile)
$buffer = New-Object byte[] $chunkSize
$fileNumber = 0

while ($fs.Position -lt $fs.Length) {
$bytesRead = $fs.Read($buffer, 0, $chunkSize)
$outputFile = "{0}{1:D2}" -f $outputFilePrefix, $fileNumber
$fileStream = [System.IO.File]::Create($outputFile)
$fileStream.Write($buffer, 0, $bytesRead)
$fileStream.Close()
$fileNumber++
}

$fs.Close()
```

O script do PowerShell lê o arquivo grande em partes de 5 MB e grava cada uma em um novo arquivo com um sufixo numérico.

Depois de executar o comando apropriado, você deverá ver as partes no diretório no qual executou o comando. Cada parte terá um sufixo correspondente ao número da parte, por exemplo:

```
census-part00 census-part01 census-part02
```

Etapa 3: criar o carregamento fracionado com uma soma de verificação adicional

Para iniciar o processo de carregamento fracionado, é necessário criar a solicitação de carregamento fracionado. Essa etapa envolve iniciar o carregamento fracionado e especificar uma soma de

verificação adicional para a integridade dos dados. O exemplo a seguir usa a soma de verificação SHA-256. Se você quiser fornecer metadados que descrevam o objeto que está sendo carregado, deverá fornecê-los na solicitação para iniciar o carregamento fracionado.

> **Note**
>
> Nesta etapa e nas etapas subsequentes, este tutorial usa o algoritmo adicional SHA-256. Também é possível usar outra soma de verificação adicional para essas etapas, como CRC32, CRC32C ou SHA-1. Se você usar um algoritmo diferente, deverá usá-lo em todas as etapas do tutorial.

Como iniciar o carregamento fracionado

No terminal, use o comando `create-multipart-upload` a seguir para iniciar um carregamento fracionado para o bucket. Substitua *amzn-s3-demo-bucket1* pelo nome do bucket real. Além disso, substitua o `census_data_file` pelo nome do arquivo escolhido. Esse nome de arquivo torna-se a chave do objeto quando o upload é concluído.

```
aws s3api create-multipart-upload --bucket amzn-s3-demo-bucket1 --key
 'census_data_file' --checksum-algorithm sha256
```

Se a solicitação for bem-sucedida, você verá uma saída JSON como a seguinte:

```
{
    "ServerSideEncryption": "AES256",
    "ChecksumAlgorithm": "SHA256",
    "Bucket": "amzn-s3-demo-bucket1",
    "Key": "census_data_file",
    "UploadId":
 "cNV6KCSNANFZapz1LUGPC5XwUVi1n6yUoIeSP138sNOKPeMhpKQRrbT9k0ePmgoOTCj9K83T4e2Gb5hQvNoNpCKqyb8m3
}
```

> **Note**
>
> Quando você envia uma solicitação para iniciar um multipart upload, o Amazon S3 retorna uma resposta com um ID de upload, que é um identificador exclusivo do seu multipart upload. É necessário incluir esse ID de upload sempre que fizer upload de partes, listar

as partes, concluir um upload ou interromper um upload. Será necessário usar os valores `UploadId`, `Key` e `Bucket` para as etapas posteriores; portanto, lembre-se de salvá-los. Além disso, se você estiver usando um carregamento fracionado com somas de verificação adicionais, os números das partes deverão ser consecutivos. Se você usar números de parte não consecutivos, a solicitação `complete-multipart-upload` poderá gerar um HTTP `500 Internal Server Error`.

Etapa 4: fazer upload das partes do carregamento fracionado

Nesta etapa, você fará upload das partes do carregamento fracionado no bucket do S3. Use o comando `upload-part` para fazer upload de cada parte individualmente. Esse processo requer a especificação do ID do upload, do número da parte e do arquivo a ser carregado para cada parte.

Como fazer upload das partes

1. Ao fazer upload de uma parte, além do ID do upload, é necessário especificar o número da parte usando o argumento `--part-number`. Você pode escolher qualquer número de parte entre 1 e 10.000. Um número de parte identifica com exclusividade a parte e sua posição no objeto do qual você está fazendo upload. O número da parte que você escolher não precisa estar em uma sequência consecutiva (por exemplo, pode ser 1, 2 ou 3). Se você fizer upload de uma nova parte usando o mesmo número da parte anteriormente carregada, a parte anteriormente carregada será substituída.
2. Use o comando `upload-part` para fazer upload de cada parte do carregamento fracionado. O `--upload-id` é o mesmo que estava na saída criada pelo comando `create-multipart-upload` na Etapa 3. Para fazer upload da primeira parte dos dados, use o seguinte comando:

```
aws s3api upload-part --bucket amzn-s3-demo-bucket1 --key
 'census_data_file' --part-number 1 --body census-part00 --upload-id
 "cNV6KCSNANFZapz1LUGPC5XwUVi1n6yUoIeSP138sNOKPeMhpKQRrbT9k0ePmgoOTCj9K83T4e2Gb5hQvNoNpCKqy
 --checksum-algorithm SHA256
```

Após a conclusão de cada comando `upload-part`, você deverá ver uma saída como a seguinte:

```
{
    "ServerSideEncryption": "AES256",
    "ETag": "\"e611693805e812ef37f96c9937605e69\"",
```

```
    "ChecksumSHA256": "QLl8R4i4+SaJlrl8ZIcutc5TbZtwt2NwB8lTXkd3GH0="
}
```

3. Para as partes subsequentes, aumente o número da parte apropriadamente:

```
aws s3api upload-part --bucket amzn-s3-demo-bucket1 --key 'census_data_file' --
part-number <part-number> --body <file-path> --upload-id "<your-upload-id>" --
checksum-algorithm SHA256
```

Por exemplo, use o seguinte comando para fazer upload da segunda parte:

```
aws s3api upload-part --bucket amzn-s3-demo-bucket1 --key
 'census_data_file' --part-number 2 --body census-part01 --upload-id
 "cNV6KCSNANFZapz1LUGPC5XwUVi1n6yUoIeSP138sNOKPeMhpKQRrbT9k0ePmgoOTCj9K83T4e2Gb5hQvNoNpCKqy
 --checksum-algorithm SHA256
```

O Amazon S3 exibe uma tag de entidade (ETag) e somas de verificação adicionais para cada parte carregada como cabeçalho na resposta.

4. Continue usando o comando `upload-part` até fazer upload de todas as partes do objeto.

Etapa 5: listar todas as partes do carregamento fracionado

Para concluir o carregamento fracionado, você precisará de uma lista de todas as partes que foram carregadas para esse carregamento fracionado específico. A saída do comando `list-parts` fornece algumas informações, como nome do bucket, chave, ID do upload, número da parte, ETag, somas de verificação adicionais etc. É útil salvar essa saída em um arquivo para que você possa usá-la na próxima etapa ao concluir o processo de carregamento fracionado. É possível criar um arquivo de saída JSON chamado `parts.json` usando o método a seguir.

Como criar um arquivo que liste todas as partes

1. Para gerar um arquivo JSON com os detalhes de todas as partes carregadas, use o comando `list-parts` a seguir. Substitua ***amzn-s3-demo-bucket1*** pelo nome real do bucket e **<your-upload-id>** pelo ID de upload recebido na Etapa 3. Para ter mais informações sobre o comando `list-parts`, consulte list-parts no Guia do usuário da AWS Command Line Interface.

```
aws s3api list-parts --bucket amzn-s3-demo-bucket1 --key 'census_data_file' --
upload-id <your-upload-id> --query '{Parts: Parts[*].{PartNumber: PartNumber, ETag:
 ETag, ChecksumSHA256: ChecksumSHA256}}' --output json > parts.json
```

Um novo arquivo chamado `parts.json` é gerado. O arquivo contém as informações em formato JSON de todas as partes carregadas. O arquivo `parts.json` inclui informações essenciais para cada parte do carregamento fracionado, como os números de parte e os valores de ETag correspondentes, os quais são necessários para concluir o processo de carregamento fracionado.

2. Abra `parts.json` usando qualquer editor de texto ou pelo terminal. Veja a saída de exemplo:

```
{
    "Parts": [
        {
            "PartNumber": 1,
            "ETag": "\"3c3097f89e2a2fece47ac54b243c9d97\"",
            "ChecksumSHA256": "fTPVHfyNHdv5VkR4S3EewdyioXECv7JBxN+d4FXYYTw="
        },
        {
            "PartNumber": 2,
            "ETag": "\"03c71cc160261b20ab74f6d2c476b450\"",
            "ChecksumSHA256": "VDWTa8enjOvULBAO3W2a6C+5/7ZnNjrnLApa1QVc3FE="
        },
        {
            "PartNumber": 3,
            "ETag": "\"81ae0937404429a97967dffa7eb4affb\"",
            "ChecksumSHA256": "cVVkXehUlzcwrBrXgPIM+EKQXPUvWist8mlUTCs4bg8="
        }
    ]
}
```

Etapa 6: concluir o carregamento fracionado

Depois de fazer upload de todas as partes do carregamento fracionado e listá-las, a etapa final é concluir o carregamento fracionado. Essa etapa mescla todas as partes carregadas em um único objeto no bucket do S3.

> **Note**
>
> É possível calcular a soma de verificação do objeto antes de chamar `complete-multipart-upload` incluindo `--checksum-sha256` na solicitação. Se as somas de verificação não coincidirem, o Amazon S3 rejeitará a solicitação. Consulte mais informações em complete-multipart-upload no Guia de Usuário AWS Command Line Interface.

Como concluir o carregamento fracionado

Para finalizar o carregamento fracionado, use o comando `complete-multipart-upload`. Esse comando requer o arquivo `parts.json` criado na Etapa 5, o nome do bucket e o ID do upload. Substitua **<*amzn-s3-demo-bucket1*>** pelo nome do bucket e **<your-upload-id>** pelo ID do upload de `parts.json`.

```
aws s3api complete-multipart-upload --multipart-upload file://parts.json --bucket amzn-s3-demo-bucket1 --key 'census_data_file' --upload-id <your-upload-id>
```

Veja a saída de exemplo:

```
{
    "ServerSideEncryption": "AES256",
    "Location": "https://amzn-s3-demo-bucket1.s3.us-east-2.amazonaws.com/census_data_file",
    "Bucket": "amzn-s3-demo-bucket1",
    "Key": "census_data_file",
    "ETag": "\"f453c6dccca969c457efdf9b1361e291-3\"",
    "ChecksumSHA256": "aI8EoktCdotjU8Bq46DrPCxQCGuGcPIhJ51noWs6hvk=-3"
}
```

> **Note**
>
> Não exclua ainda os arquivos de parte individuais. Você precisará das partes individuais para poder realizar somas de verificação e conferir a integridade do objeto mesclado.

Etapa 7: confirmar se o objeto foi carregado no bucket

Depois de concluir o carregamento fracionado, você poderá verificar se o objeto foi carregado com êxito no bucket do S3. Para listar os objetos no bucket e confirmar a presença do arquivo recém-carregado, use o comando `list-objects-v2`

Como listar o objeto carregado

Para listar os objetos no bucket, use o bucket de comando `list-objects-v2`. Substitua ***amzn-s3-demo-bucket1*** pelo nome do bucket real.

```
aws s3api list-objects-v2 --bucket amzn-s3-demo-bucket1
```

Esse comando exibe uma lista de objetos no bucket. Procure o arquivo carregado (por exemplo, `census_data_file`) na lista de objetos.

Para ter mais informações, consulte a seção Examples do comando `list-objects-v2` no Guia do usuário do AWS Command Line Interface.

Etapa 8: verificar a integridade do objeto com uma soma de verificação MD5

Ao fazer upload de um objeto, é possível especificar um algoritmo de soma de verificação a ser usado pelo Amazon S3. Por padrão, o Amazon S3 armazena o resumo MD5 de bytes como ETag do objeto. Para carregamentos fracionados, a ETag não é a soma de verificação do objeto completo, mas um composto de somas de verificação de cada parte.

Como verificar a integridade do objeto usando uma soma de verificação MD5

1. Para recuperar a ETag do objeto carregado, faça uma solicitação `head-object`:

   ```
   aws s3api head-object --bucket amzn-s3-demo-bucket1 --key census_data_file
   ```

   Veja a saída de exemplo:

   ```
   {
       "AcceptRanges": "bytes",
       "LastModified": "2024-07-26T19:04:13+00:00",
       "ContentLength": 16106127360,
       "ETag": "\"f453c6dccca969c457efdf9b1361e291-3\"",
       "ContentType": "binary/octet-stream",
       "ServerSideEncryption": "AES256",
   ```

```
    "Metadata": {}
}
```

Essa ETag tem “-3” anexado ao final. Isso indica que o objeto foi carregado em três partes usando o carregamento fracionado.

2. Depois, calcule a soma de verificação MD5 de cada parte usando o comando `md5sum`. Forneça o caminho correto para os arquivos de parte:

```
md5sum census-part*
```

Veja a saída de exemplo:

```
e611693805e812ef37f96c9937605e69 census-part00
63d2d5da159178785bfd6b6a5c635854 census-part01
95b87c7db852451bb38b3b44a4e6d310 census-part02
```

3. Para esta etapa, combine manualmente os hashes MD5 em uma string. Depois, execute o comando a seguir para converter a string em binário e calcular a soma de verificação MD5 do valor binário:

```
echo
 "e611693805e812ef37f96c9937605e6963d2d5da159178785bfd6b6a5c63585495b87c7db852451bb38b3b44a
 | xxd -r -p | md5sum
```

Veja a saída de exemplo:

```
f453c6dccca969c457efdf9b1361e291 -
```

Esse valor de hash deve corresponder ao valor de hash do valor da ETag original na Etapa 1, que valida a integridade do objeto `census_data_file`.

Quando você instrui o Amazon S3 a usar somas de verificação adicionais, ele calcula o respectivo valor para cada parte e armazena os valores. Se você quiser recuperar os valores da soma de verificação para partes individuais de carregamentos fracionados ainda em andamento, poderá usar `list-parts`.

Consulte mais informações sobre como as somas de verificação funcionam com objetos de carregamento fracionado em Verificar a integridade do objeto no Amazon S3.

Etapa 9: verificar a integridade do objeto com uma soma de verificação adicional

Nesta etapa, este tutorial usa o SHA-256 como uma soma de verificação adicional para validar a integridade do objeto. Se você usou uma soma de verificação adicional diferente, use esse valor de soma de verificação.

Como verificar a integridade do objeto com SHA256

1. Execute o seguinte comando no terminal, incluindo o argumento `--checksum-mode enabled`, para exibir o valor `ChecksumSHA256` do objeto:

```
aws s3api head-object --bucket amzn-s3-demo-bucket1 --key census_data_file --
checksum-mode enabled
```

   Veja a saída de exemplo:

```
{
    "AcceptRanges": "bytes",
    "LastModified": "2024-07-26T19:04:13+00:00",
    "ContentLength": 16106127360,
    "ChecksumSHA256": "aI8EoktCdotjU8Bq46DrPCxQCGuGcPIhJ51noWs6hvk=-3",
    "ETag": "\"f453c6dccca969c457efdf9b1361e291-3\"",
    "ContentType": "binary/octet-stream",
    "ServerSideEncryption": "AES256",
    "Metadata": {}
}
```

2. Use os comandos a seguir para decodificar os valores `ChecksumSHA256` das partes individuais em base64 e salvá-los em um arquivo binário chamado `outfile`. Esses valores podem ser encontrados no arquivo `parts.json`. Substitua as strings base64 de exemplo pelos valores `ChecksumSHA256` reais.

```
echo "QLl8R4i4+SaJlrl8ZIcutc5TbZtwt2NwB8lTXkd3GH0=" | base64 --decode >> outfile
echo "xCdgs1K5Bm4jWETYw/CmGYr+m6O2DcGfpckx5NVokvE=" | base64 --decode >> outfile
echo "f5wsfsa5bB+yXuwzqG1Bst91uYneqGD3CCidpb54mAo=" | base64 --decode >> outfile
```

3. Execute o seguinte comando para calcular a soma de verificação SHA256 do `outfile`:

```
sha256sum outfile
```

Veja a saída de exemplo:

```
688f04a24b42768b6353c06ae3a0eb3c2c50086b8670f221279d67a16b3a86f9 outfile
```

Na próxima etapa, converta o valor do hash em um valor binário. Esse valor binário deve corresponder ao valor `ChecksumSHA256` da Etapa 1.

4. Converta a soma de verificação SHA256 da Etapa 3 em um valor binário e, depois, codifique-o em base64 para verificar se ele corresponde ao valor `ChecksumSHA256` da Etapa 1:

```
echo "688f04a24b42768b6353c06ae3a0eb3c2c50086b8670f221279d67a16b3a86f9" | xxd -r -p
 | base64
```

Veja a saída de exemplo:

```
aI8EoktCdotjU8Bq46DrPCxQCGuGcPIhJ51noWs6hvk=
```

Essa saída deve confirmar se a saída base64 corresponde ao valor `ChecksumSHA256` da saída do comando `head-object`. Se a saída corresponder ao valor da soma de verificação, o objeto será válido.

Important

- Quando você instrui o Amazon S3 a usar somas de verificação adicionais, ele calcula os respectivos valores para cada parte e armazena esses valores.
- Se você quiser recuperar os valores da soma de verificação para partes individuais de carregamentos fracionados ainda em andamento, poderá usar o comando `list-parts`.

Etapa 10: Limpar os recursos

Se você quiser limpar os arquivos criados neste tutorial, use o método a seguir. Para obter instruções sobre como excluir os arquivos carregados no bucket do S3, consulte Excluir objetos do Amazon S3.

Exclua os arquivos locais criados na Etapa 1:

Para remover os arquivos criados para o carregamento fracionado, execute o seguinte comando no diretório de trabalho:

```
rm census-data.bin census-part* outfile parts.json
```

Limites do multipart upload do Amazon S3

O multipart upload permite que você faça upload de um único objeto como um conjunto de partes. Cada parte é uma parte contígua de dados do objeto. Depois que todas as partes do objeto forem carregadas, o Amazon S3 montará essas partes e criará o objeto. Geralmente, quando seu objeto alcança 100 MB de tamanho, você deve considerar o uso de multipart uploads em vez de fazer upload do objeto em uma única operação. Para obter mais informações sobre multipart uploads, consulte Carregar e copiar objetos usando upload fracionado no Amazon S3.

A tabela a seguir fornece especificações básicas do multipart upload. Isso inclui tamanho máximo do objeto, número máximo de partes, tamanho máximo das partes etc. Não há limite de tamanho mínimo na última parte do carregamento fracionado.

Item	Especificação
Tamanho máximo do objeto	5 TiB
Número máximo de partes por upload	10.000
Números de parte	1 a 10.000 (inclusive)
Tamanho da parte	5 MiB a 5 GiB. Não há limite de tamanho mínimo na última parte do carregamento fracionado.
Número máximo de partes retornadas em uma solicitação de listagem de partes	1000

Item	Especificação
Número máximo de multipart uploads retornados em uma solicitação de listagem de multipart uploads	1000

Adicionar condições prévias às operações do S3 com solicitações condicionais

É possível usar solicitações condicionais para adicionar condições prévias às operações do S3. Para usar solicitações condicionais, é necessário adicionar outro cabeçalho à operação de API do Amazon S3. Esse cabeçalho especifica uma condição que, se não for atendida, provocará uma falha na operação do S3.

As leituras condicionais comportam solicitações `GET`, `HEAD` e `COPY`. É possível adicionar condições prévias para exibir ou copiar um objeto com base na tag de entidade (ETag) ou na data da última modificação. Isso pode limitar uma operação do S3 a objetos atualizados desde uma data especificada. Também é possível limitar uma operação do S3 a uma ETag específica. Isso pode garantir que você exiba ou copie somente uma versão específica do objeto. Para obter mais informações sobre metadados de objeto, consulte Trabalhar com metadados de objeto.

As gravações condicionais podem garantir que não exista nenhum objeto com o mesmo nome de chave no bucket durante as operações `PUT`. Isso evita a substituição de objetos existentes por nomes de chave idênticos. Da mesma forma, você pode usar gravações condicionais para verificar se a ETag de um objeto está inalterada antes de atualizar o objeto. Isso evita substituições não intencionais em um objeto sem conhecer o estado do conteúdo dele. É possível usar gravações condicionais para solicitações PutObject ou CompleteMultipartUpload. Para obter mais informações sobre nomes de chave, consulte Nomear objetos do Amazon S3.

Não há custo adicional para leituras ou gravações condicionais. Você só paga as taxas existentes para as solicitações aplicáveis, inclusive para solicitações malsucedidas. Para obter informações sobre os recursos e a definição de preço do Amazon S3, consulte a definição de preço do Amazon S3.

Tópicos

- Como recuperar ou copiar objetos com base em metadados com leituras condicionais
- Como evitar substituições de objeto com gravações condicionais

Como recuperar ou copiar objetos com base em metadados com leituras condicionais

Com as leituras condicionais, é possível adicionar um cabeçalho extra à solicitação de leitura para adicionar condições prévias à operação do S3. Se essas condições prévias não forem atendidas, a solicitação de leitura falhará.

É possível usar leituras condicionais em solicitações `GET`, `HEAD` ou `COPY` para exibir apenas um objeto com base nos metadados.

Ao fazer upload de um objeto, o Amazon S3 cria metadados controlados pelo sistema que só podem ser modificados pelo S3. Tags de entidade (ETags) e Last-Modified são exemplos de metadados controlados pelo sistema. ETag de um objeto é uma string que representa uma versão específica de um objeto. A data Last-Modified corresponde a metadados que representam a data de criação de um objeto ou a data da última modificação, a mais recente entre as duas.

Com leituras condicionais, é possível exibir um objeto com base na ETag ou na data da última modificação do objeto. É possível especificar um valor de ETag com sua solicitação e exibir o objeto somente se o valor da ETag coincidir. Isso pode garantir que você exiba ou copie apenas uma versão específica de um objeto. É possível especificar um valor de Last-Modified com sua solicitação de leitura e exibir um objeto somente se ele tiver sido modificado desde a data fornecida.

APIs aceitas do :

As seguintes APIs do S3 são compatíveis com o uso de leituras condicionais:

- GetObject
- HeadObject
- CopyObject

É possível usar os cabeçalhos a seguir para exibir um objeto dependente da tag da entidade (ETag) ou da data da última modificação. Para ter mais informações sobre metadados de objetos, como ETags e Last-Modified, consulte the section called “Metadados do objeto definidos pelo sistema”.

GetObject

- `If-Match`: exibirá o objeto somente se a ETag corresponder à fornecida.

- `If-Modified-Since`: exibirá o objeto somente se ele tiver sido modificado desde o horário especificado.
- `If-None-Match`: exibirá o objeto somente se a ETag não corresponder à fornecida.
- `If-Unmodified-Since`: exibirá o objeto somente se ele não tiver sido modificado desde o horário especificado.

Para ter mais informações sobre esses cabeçalhos, erros exibidos e a ordem em que o S3 processa vários cabeçalhos condicionais em uma única solicitação, consulte GetObject na Referência da API do Amazon Simple Storage Service.

HeadObject

- `If-Match`: exibirá o objeto somente se a ETag corresponder à fornecida.
- `If-Modified-Since`: exibirá o objeto somente se ele tiver sido modificado desde o horário especificado.
- `If-None-Match`: exibirá o objeto somente se a ETag não corresponder à fornecida.
- `If-Unmodified-Since`: exibirá o objeto somente se ele não tiver sido modificado desde o horário especificado.

Para ter mais informações sobre esses cabeçalhos, erros exibidos e a ordem em que o S3 processa vários cabeçalhos condicionais em uma única solicitação, consulte HeadObject na Referência da API do Amazon Simple Storage Service.

CopyObject

- `x-amz-copy-source-if-match`: copiará o objeto de origem somente se a ETag corresponder à fornecida.
- `x-amz-copy-source-if-modified-since`: copiará o objeto de origem somente se ele tiver sido modificado desde o horário especificado.
- `x-amz-copy-source-if-none-match`: copiará o objeto de origem somente se a ETag não corresponder à fornecida.
- `x-amz-copy-source-if-unmodified-since`: copiará o objeto de origem somente se ele não tiver sido modificado desde o horário especificado.

Para ter mais informações sobre esses cabeçalhos, erros exibidos e a ordem em que o S3 processa vários cabeçalhos condicionais em uma única solicitação, consulte CopyObject na Referência da API do Amazon Simple Storage Service.

Como evitar substituições de objeto com gravações condicionais

Ao usar as gravações condicionais, é possível adicionar outro cabeçalho às solicitações `WRITE` a fim de especificar condições prévias para a operação do Amazon S3. Para gravar objetos condicionalmente, adicione o cabeçalho HTTP `If-None-Match` ou `If-Match`.

O cabeçalho `If-None-Match` evita a substituição de dados existentes, validando que não há um objeto com o mesmo nome de chave já existente no bucket.

Como alternativa, você pode adicionar o cabeçalho `If-Match` para verificar a tag de entidade (ETag) de um objeto antes de gravá-lo. Com esse cabeçalho, o Amazon S3 compara o valor da ETag fornecido com o valor da ETag do objeto no S3. Se esses valores de ETag não forem correspondentes, a operação vai falhar.

Os proprietários de buckets podem usar políticas de bucket para impor gravações condicionais para objetos carregados. Para obter mais informações, consulte the section called “Impor gravações condicionais”.

> **Note**
>
> Para usar gravações condicionais, é necessário fazer as solicitações por HTTPS (TLS) ou usar o AWS Signature Version 4 para assinar a solicitação.

Tópicos

- Como evitar substituições de objeto com base em nomes de chave
- Como evitar substituições se o objeto tiver sido alterado
- Comportamento de uma gravação condicional
- Cenários de gravação condicional
- Impor gravações condicionais em buckets do Amazon S3

Como evitar substituições de objeto com base em nomes de chave

Você pode usar o cabeçalho condicional HTTP `If-None-Match` para verificar se um objeto já existe no bucket especificado com base no nome da chave antes de criá-lo. Ao fazer upload de um objeto no Amazon S3, especifique o nome da chave: um identificador exclusivo de um objeto em um bucket, com diferenciação entre maiúsculas e minúsculas. Sem o cabeçalho HTTP `If-None-Match`, se você fizer upload de um objeto com um nome de chave idêntico em um bucket sem versionamento ou com versionamento suspenso, o objeto será substituído. Em um bucket com versionamento, o objeto cujo upload foi feito mais recentemente se torna a versão atual do objeto. As gravações condicionais com o cabeçalho HTTP `If-None-Match` verificam a existência de um objeto durante a operação `WRITE`. Se um nome de chave idêntico for encontrado no bucket, a operação falhará. Para ter mais informações sobre como usar nomes de chave, consulte the section called “Nomear objetos”.

Para realizar gravações condicionais com o cabeçalho HTTP `If-None-Match`, é necessário ter a permissão `s3:PutObject`. Isso possibilita que o chamador confira a presença de objetos no bucket. O cabeçalho `If-None-Match` espera o valor * (asterisco).

É possível usar o cabeçalho `If-None-Match` com as seguintes APIs:

- PutObject
- CompleteMultipartUpload

Como usar o AWS CLI

O exemplo de comando `put-object` a seguir tenta realizar uma gravação condicional para um objeto com o nome da chave `dir-1/my_images.tar.bz2`.

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key dir-1/my_images.tar.bz2 --body
 my_images.tar.bz2 --if-none-match "*"
```

Para obter mais informações, consulte put-object na Referência de comandos da AWS CLI.

Para obter informações sobre o AWS CLI, consulte O que é AWS Command Line Interface? no Guia do usuário do AWS Command Line Interface.

Como evitar substituições se o objeto tiver sido alterado

A ETag de um objeto é uma string exclusiva do objeto, que reflete uma alteração no conteúdo do objeto. Você pode usar o cabeçalho `If-Match` para comparar o valor da ETag de um objeto em um

bucket do Amazon S3 com aquele que você fornece durante a operação `WRITE`. Se esses valores de ETag não forem correspondentes, a operação vai falhar. Para ter mais informações sobre as ETags, consulte the section called “Usar Content-MD5 e a ETag para verificar objetos carregados”.

Para realizar gravações condicionais com o cabeçalho HTTP `If-Match`, é necessário ter as permissões `s3:PutObject` e `s3:GetObject`. Isso possibilita que o chamador verifique a ETag e o estado dos objetos no bucket. O cabeçalho `If-Match` espera o valor da ETag como uma string.

É possível usar o cabeçalho `If-Match` com as seguintes APIs:

- PutObject
- CompleteMultipartUpload

Como usar o AWS CLI

O exemplo de comando `put-object` a seguir tenta realizar uma gravação condicional com o valor de ETag fornecido `6805f2cfc46c0f04559748bb039d69ae`.

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key dir-1/my_images.tar.bz2 --body
 my_images.tar.bz2 --if-match "6805f2cfc46c0f04559748bb039d69ae"
```

Para obter mais informações, consulte put-object na Referência de comandos da AWS CLI.

Para obter informações sobre o AWS CLI, consulte O que é AWS Command Line Interface? no Guia do usuário do AWS Command Line Interface.

Comportamento de uma gravação condicional

Gravações condicionais com cabeçalho **`If-None-Match`**

As gravações condicionais com o cabeçalho `If-None-Match` são avaliadas em relação aos objetos existentes em um bucket. Se não houver nenhum objeto existente com o mesmo nome de chave no bucket, a operação de gravação será bem-sucedida, resultando em uma resposta `200 OK`. Se houver um objeto existente, a operação de gravação falhará, resultando em uma resposta `412 Precondition Failed`.

Para buckets com o versionamento habilitado, se não houver nenhuma versão atual do objeto com o mesmo nome, ou se a versão atual do objeto for um marcador de exclusão, a operação de gravação será bem-sucedida. Caso contrário, isso resultará em uma resposta `412 Precondition Failed`, que indica uma falha na operação de gravação.

Se ocorrerem várias gravações condicionais para o mesmo nome de objeto, a primeira operação de gravação que for concluída será bem-sucedida. O Amazon S3 rejeitará as gravações subsequentes com uma resposta `412 Precondition Failed`.

Também é possível receber uma resposta `409 Conflict` no caso de solicitações simultâneas se uma solicitação de exclusão de um objeto for bem-sucedida antes que uma operação de gravação condicional nesse objeto seja concluída. Ao usar gravações condicionais com `PutObject`, os uploads podem ser repetidos após o recebimento de um erro `409 Conflict`. Ao usar `CompleteMultipartUpload`, o upload fracionado deve ser reinicializado com `CreateMultipartUpload` para que o objeto seja carregado novamente após o recebimento de um erro `409 Conflict`.

Gravações condicionais com cabeçalho **`If-Match`**

O cabeçalho `If-Match` é avaliado em relação aos objetos existentes em um bucket. Se já houver um objeto com o mesmo nome de chave e um ETag correspondente, a operação de gravação será bem-sucedida, resultando em uma resposta `200 OK`. Se a ETag não corresponder, a operação de gravação falhará com uma resposta `412 Precondition Failed`.

Você também pode receber uma resposta `409 Conflict` no caso de solicitações simultâneas.

Você receberá uma resposta `404 Not Found` se uma solicitação simultânea de exclusão de um objeto for bem-sucedida antes que uma operação de gravação condicional nesse objeto seja concluída, já que a chave do objeto não existe mais. Você deve fazer upload do objeto novamente ao receber uma `404 Not Found` resposta.

Se não houver uma versão atual do objeto com o mesmo nome ou se a versão atual do objeto for um marcador de exclusão, a operação falhará com um erro `404 Not Found`.

Cenários de gravação condicional

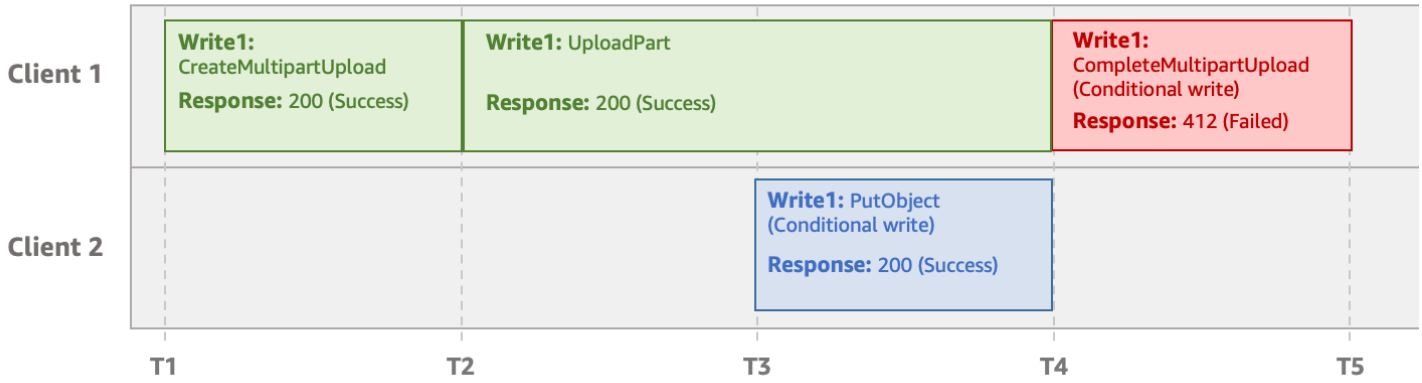
Considere os casos a seguir, em que dois clientes estão executando operações no mesmo bucket.

Gravações condicionais durante uploads fracionados

As gravações condicionais não levam em conta nenhuma solicitação de carregamento fracionado em andamento, pois nesse caso os objetos ainda não foram totalmente gravados. Considere o exemplo a seguir, em que o Cliente 1 está fazendo upload de um objeto usando o carregamento fracionado. Durante o carregamento fracionado, o Cliente 2 consegue gravar com êxito o mesmo objeto com

a operação de gravação condicional. Posteriormente, quando o Cliente 1 tenta concluir o upload fracionado usando uma gravação condicional, o upload falha.

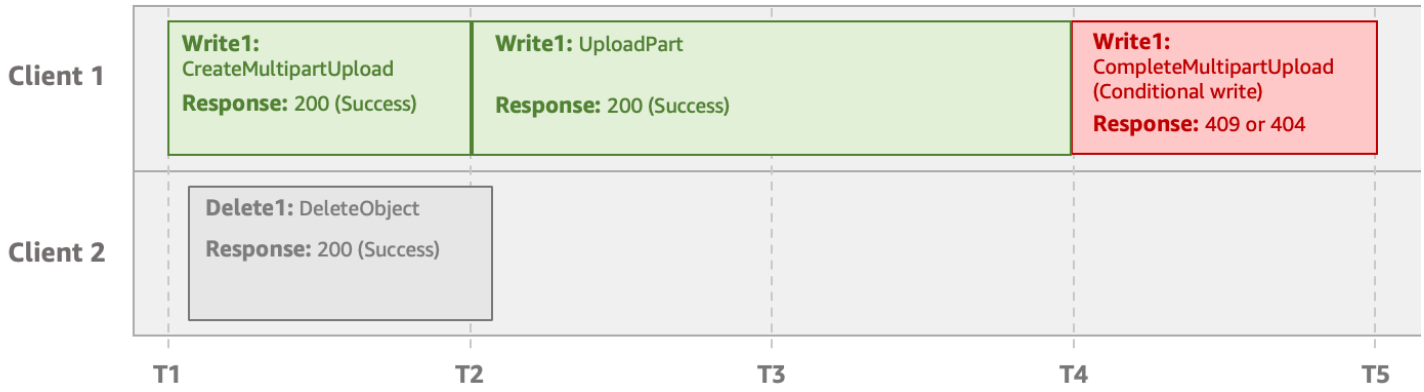
> **Note**
>
> Esse cenário resultará em uma resposta `412 Precondition Failed` para os cabeçalhos `If-None-Match` e `If-Match`.



Exclusões simultâneas durante uploads fracionados

Se uma solicitação de exclusão for bem-sucedida antes que uma solicitação de gravação condicional possa ser concluída, o Amazon S3 exibirá uma resposta `409 Conflict` ou `404 Not Found` para a operação de gravação. Isso ocorre porque a solicitação de exclusão iniciada anteriormente tem precedência sobre a operação de gravação condicional. Nesses casos, é necessário iniciar um novo carregamento fracionado.

> **Note**
>
> Esse cenário resultará em uma resposta `409 Conflict` para um cabeçalho `If-None-Match` e em uma resposta `404 Not Found` para um cabeçalho `If-Match`.



> **Note**
>
> Para minimizar os custos de armazenamento, recomendamos que você configure uma regra de ciclo de vida para excluir uploads incompletos de várias partes após um determinado número de dias usando a ação `AbortIncompleteMultipartUpload`. Para obter mais informações sobre como criar uma regra de ciclo de vida para excluir uploads incompletos de várias partes, consulte Configurando uma política de ciclo de vida de bucket para anular multipart uploads incompletos.

Impor gravações condicionais em buckets do Amazon S3

Ao usar as políticas de bucket do Amazon S3, você pode impor gravações condicionais para uploads de objetos em buckets de uso geral.

Uma política de bucket é uma política baseada em recursos que você pode usar para conceder permissões de acesso ao bucket do Amazon S3 e aos objetos contidos nele. Só o proprietário do bucket pode associar uma política a um bucket. Para obter mais informações sobre políticas de bucket, consulte the section called “Políticas de buckets”.

Você pode usar as chaves de condição `s3:if-match` ou `s3:if-none-match` como elemento `Condition` opcional ou o bloco `Condition` para especificar quando uma política está em vigor. Para uploads fracionados, você deve especificar a chave de condição `s3:ObjectCreationOperation` para isentar as operações `CreateMultipartUpload`, `UploadPart` e `UploadPartCopy`, pois essas APIs não aceitam cabeçalhos condicionais. Para ter mais informações sobre como usar condições em políticas de bucket, consulte the section called “Exemplos de chave de condição”.

> **Note**
>
> Se você usar uma política de bucket para impor gravações condicionais, não poderá realizar operações de cópia no bucket ou no prefixo especificado na política de bucket. As solicitações `CopyObject` sem um cabeçalho HTTP `If-None-Match` ou `If-Match` falham com um erro `403 Access Denied`. As solicitações `CopyObject` feitas com esses cabeçalhos HTTP falham com uma resposta `501 Not Implemented`.

Os exemplos a seguir mostram como usar condições em uma política de bucket para forçar os clientes a usar o cabeçalho HTTP `If-None-Match` ou `If-Match`.

Tópicos

- Exemplo 1: permitir somente uploads de objetos usando solicitações PutObject e CompleteMultipartUpload que incluam o cabeçalho if-none-match
- Exemplo 2: permitir somente uploads de objetos usando solicitações PutObject e CompleteMultipartUpload que incluam o cabeçalho if-match
- Exemplo 3: permitir somente solicitações de upload de objetos que incluam o cabeçalho if-none-match ou if-match

Exemplo 1: permitir somente uploads de objetos usando solicitações **`PutObject`** e **`CompleteMultipartUpload`** que incluam o cabeçalho **`if-none-match`**

Essa política permite que a conta 111122223333, usuária Alice, grave no bucket *`amzn-s3-demo-bucket1`* se a solicitação incluir o cabeçalho `if-none-match`, garantindo que a chave de objeto ainda não exista no bucket. Todas as solicitações `PutObject` e `CompleteMultipartUpload` ao bucket especificado devem incluir o cabeçalho `if-none-match` para serem bem-sucedidas. Usando esse cabeçalho, os clientes só poderão gravar nesse bucket se a chave de objeto não existir no bucket.

> **Note**
>
> Essa política também define a chave de condição `s3:ObjectCreationOperation` que permite uploads fracionados usando as APIs `CreateMultipartUpload`, `UploadPart` e `UploadPartCopy`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowConditionalPut",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:user/Alice"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*",
            "Condition": {
                "Null": {
                    "s3:if-none-match": "false"
                }
            }
        },
        {
            "Sid": "AllowConditionalPutwithMPUs",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:user/Alice"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*",
            "Condition": {
                "Bool": {
                    "s3:ObjectCreationOperation": "false"
                }
            }
        }
    ]
}
```

Exemplo 2: permitir somente uploads de objetos usando solicitações **`PutObject`** e **`CompleteMultipartUpload`** que incluam o cabeçalho **`if-match`**

Essa política permite que a conta 111122223333, usuário Alice, grave em *amzn-s3-demo-bucket1* somente se a solicitação incluir o cabeçalho `if-match`. Esse cabeçalho compara o valor da ETag de um objeto no S3 com o valor fornecido durante a operação `WRITE`. Se esses valores de ETag não forem correspondentes, a operação vai falhar. Todas as solicitações `PutObject` e

`CompleteMultipartUpload` ao bucket especificado devem incluir o cabeçalho `if-match` para serem bem-sucedidas.

> **Note**
>
> Essa política também define a chave de condição `s3:ObjectCreationOperation` que permite uploads fracionados usando as APIs `CreateMultipartUpload`, `UploadPart` e `UploadPartCopy`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowPutObject",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:user/Alice"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*",
        },
        {
            "Sid": "BlockNonConditionalObjectCreation",
            "Effect": "Deny",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:user/Alice"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*",
            "Condition": {
                "Null": {
                    "s3:if-match": "true"
                },
                "Bool": {
                    "s3:ObjectCreationOperation": "true"
                }
            }
        },
        {
            "Sid": "AllowGetObjectBecauseConditionalPutIfMatchETag",
            "Effect": "Allow",
```

```
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:user/Alice"
            },
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*"
        }
    ]
}
```

Exemplo 3: permitir somente solicitações de upload de objetos que incluam o cabeçalho **`if-none-match`** ou **`if-match`**

Essa política permite que a conta 111122223333, usuário Alice, grave em *amzn-s3-demo-bucket1* se as solicitações incluírem o cabeçalho `if-none-match` ou `if-match`. Isso permite que Alice faça upload de um objeto se o nome de chave não existir no bucket. Se o nome de chave existir, Alice poderá sobrescrever o objeto se a ETag do objeto corresponder à ETag fornecida na solicitação PUT.

> **Note**
>
> Essa política também define a chave de condição `s3:ObjectCreationOperation` que permite uploads fracionados usando as APIs `CreateMultipartUpload`, `UploadPart` e `UploadPartCopy`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": " AllowConditionalPutifAbsent",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:user/Alice"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*",
            "Condition": {
                "Null": {
                    "s3:if-none-match": "false"
                }
            }
        },
```

```
        {
            "Sid": "AllowConditionalPutIfMatchEtag",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:user/Alice"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*",
            "Condition": {
                "Null": {
                    "s3:if-match": "false"
                }
            }
        },
        {
            "Sid": "AllowConditionalObjectCreation",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:user/Alice"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*",
            "Condition": {
                "Bool": {
                    "s3:ObjectCreationOperation": "false"
                }
            }
        },
        {
            "Sid": " AllowGetObjectBecauseConditionalPutIfMatchETag",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:user/Alice"
            },
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*"
        }
    ]
}
```

Copiar, mover e renomear objetos

A operação `CopyObject` cria uma cópia de um objeto que já está armazenado no Amazon S3.

Você pode criar uma cópia do objeto de até 5 GB em uma única operação atômica. No entanto, para copiar um objeto com mais de 5 GB, você deve usar um upload fracionado com a AWS CLI ou AWS SDKs. Para obter mais informações, consulte Copiar um objeto usando multipart upload.

> **Note**
>
> Para manter o benefício de performance de um objeto que você carregou usando o upload fracionado, é necessário copiar o objeto usando o upload fracionado com a AWS CLI ou um AWS SDK em vez do console do S3. Para obter mais informações, consulte Copiar um objeto usando multipart upload.

Usando a operação `CopyObject` você pode:

- Criar cópias adicionais de objetos.
- Renomear objetos copiando-os e excluindo os originais.
- Copiar ou mover objetos de um bucket para outro, inclusive entre Regiões da AWS (por exemplo, de `us-west-1` para `eu-west-2`). Ao mover um objeto, o Amazon S3 o copia para o destino especificado e, em seguida, exclui o objeto de origem.

  > **Note**
  >
  > A cópia ou movimentação de objetos entre Regiões da AWS gera cobranças de largura de banda. Para obter mais informações, consulte Preços do Amazon S3.

- Alterar metadados do objeto. Cada objeto do Amazon S3 tem metadados. Esses metadados são um conjunto de pares de nome-valor. Você pode definir metadados de objeto no momento em que carregar um objeto. Depois de fazer upload do objeto, você não poderá modificar os metadados dele. A única forma de modificar metadados de objeto é fazer uma cópia do objeto e definir os metadados. Para isso, na operação de cópia, defina o mesmo objeto como origem e destino.

  Alguns metadados de objeto são metadados de sistema e outros são definidos pelo usuário. É possível controlar alguns dos metadados do sistema. Por exemplo, é possível controlar a classe de armazenamento e o tipo de criptografia do lado do servidor a ser usado para o objeto. Quando você copia um objeto, os metadados de sistema controlados pelo usuário e os metadados definidos pelo usuário também são copiados. O Amazon S3 redefine os metadados controlados pelo sistema. Por exemplo, quando você copia um objeto, o Amazon S3 redefine a data de criação

do objeto copiado. Você não precisa definir nenhum desses valores de metadados controlados pelo sistema na sua solicitação de cópia.

Ao copiar um objeto, você pode decidir atualizar alguns dos valores de metadados. Por exemplo, se o objeto de origem for configurado para usar o armazenamento padrão do S3, você poderá optar por usar o S3 Intelligent-Tiering para a cópia de objeto. Você também pode modificar os valores de metadados definidos pelo usuário presentes no objeto de origem. Se optar por atualizar metadados configuráveis pelo usuário do objeto (definidos pelo sistema ou pelo usuário) durante a cópia, você deverá especificar explicitamente todos os metadados configuráveis pelo usuário presentes no objeto de origem na solicitação, mesmo se estiver apenas alterando um dos valores de metadados.

> **Note**
>
> Ao copiar um objeto usando o console do Amazon S3, você pode receber a seguinte mensagem de erro: “Não é possível verificar os metadados copiados.” O console usa cabeçalhos para recuperar e definir metadados para o objeto. Se a configuração da rede ou do navegador modificar as solicitações de rede, esse comportamento poderá fazer com que metadados não intencionais (como cabeçalhos `Cache-Control` modificados) sejam gravados no objeto copiado. O Amazon S3 não pode verificar esses metadados não intencionais.
> Para resolver esse problema, verifique a configuração da rede e do navegador para garantir que não modifique cabeçalhos, como `Cache-Control`. Para ter mais informações, consulte o Modelo de Responsabilidade Compartilhada.

Para obter mais informações sobre metadados de objeto, consulte Trabalhar com metadados de objeto.

Copiar objetos arquivados e restaurados

Se o objeto de origem estiver arquivado em S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive, será necessário primeiramente restaurar uma cópia temporária antes de copiar o objeto para outro bucket. Para obter informações sobre objetos de arquivo, consulte Trabalhando com objetos arquivados.

No console do Amazon S3, não é possível usar a operação Copiar para objetos restaurados nas classes de armazenamento S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive. Para copiar

esses objetos restaurados, use a AWS Command Line Interface (AWS CLI), os SDKs da AWS ou a API REST do Amazon S3.

Copiar objetos criptografados

O Amazon S3 criptografa automaticamente todos os novos objetos que são copiados para um bucket do S3. Se você não especificar informações de criptografia na solicitação de cópia, a configuração de criptografia do objeto de destino será definida como a configuração de criptografia padrão do bucket de destino. Por padrão, todos os buckets têm um nível básico de configuração de criptografia que usa criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3). Se o bucket de destino tiver uma configuração de criptografia padrão que usa criptografia do lado do servidor com uma chave do AWS Key Management Service (AWS KMS) (SSE-KMS) ou uma chave de criptografia fornecida pelo cliente (SSE-C), o Amazon S3 usará a chave do KMS correspondente ou uma chave fornecida pelo cliente para criptografar a cópia do objeto de destino.

Ao copiar um objeto, se quiser usar um tipo diferente de configuração de criptografia para o objeto de destino, você poderá solicitar que o Amazon S3 criptografe o objeto de destino com uma chave do KMS, uma chave gerenciada pelo Amazon S3 ou uma chave fornecida pelo cliente. Se a configuração de criptografia na solicitação for diferente da configuração de criptografia padrão do bucket de destino, a configuração de criptografia na solicitação terá precedência. Se o objeto de origem da cópia for criptografado com SSE-C, você deverá fornecer as informações de criptografia necessárias na solicitação, de maneira que o Amazon S3 possa descriptografar o objeto para a cópia. Para obter mais informações, consulte Proteger dados com criptografia.

Usar somas de verificação ao copiar objetos

Ao copiar objetos, você pode optar por usar um algoritmo de soma de verificação diferente para eles. Se optar por usar o mesmo algoritmo ou um novo, o Amazon S3 calculará um novo valor de soma de verificação depois que o objeto for copiado. O Amazon S3 não copia diretamente o valor da soma de verificação. Todos os objetos copiados sem somas de verificação e algoritmos de soma de verificação de destino especificados ganham automaticamente um algoritmo de soma de verificação `CRC-64NVME`. Para obter mais informações sobre como essa soma de verificação é calculada, consulte Carregar e copiar objetos usando upload fracionado no Amazon S3.

Copiar vários objetos em uma única solicitação

Para copiar mais de um objeto do Amazon S3 com uma única solicitação, você pode usar Operações em Lote do Amazon S3. Você fornece às operações em lote do S3 uma lista de objetos nos quais operar. O S3 Batch Operations chama a respectiva operação de API para executar a operação

especificada. Um único trabalho de operações em lote pode realizar a operação especificada em bilhões de objetos contendo exabytes de dados.

O recurso S3 Batch Operations rastreia o progresso, envia notificações e armazena um relatório de conclusão detalhado de todas as ações, fornecendo uma experiência totalmente gerenciada, auditável e sem servidor. É possível usar as operações em lote do S3 por meio do console do Amazon S3, da AWS CLI, de AWS SDKs ou da API REST. Para obter mais informações, consulte the section called “Conceitos básicos do Batch Operations”.

Copiar objetos para buckets de diretório

Para obter informações sobre como copiar um objeto em um bucket de diretório, consulte Copiar objetos de ou para um bucket de diretório. Para obter informações sobre o uso da classe de armazenamento Amazon S3 Express One Zone com buckets de diretório, consulte S3 Express One Zone e Trabalhar com buckets de diretório.

Para copiar um objeto

Para copiar um objeto, use os métodos a seguir.

Usar o console do S3

> **Note**
>
> As restrições e limitações ao copiar um objeto com o console são as seguintes:
>
> - Você pode copiar um objeto se ele tiver menos de 5 GB. Se o objeto tiver mais de 5 GB, você deve usar a AWS CLI ou SDKs da AWS para copiá-lo.
> - Para obter uma lista das permissões adicionais necessárias para copiar objetos, consulte the section called “Permissões obrigatórias para operações de API do S3”. Para ver exemplos das políticas que concedem essas permissões, consulte the section called “Exemplos de políticas baseadas em identidade”.
> - A ação `Copy` se aplica a todos os objetos nas pastas especificadas (prefixos). Os objetos adicionados a essas pastas enquanto a ação estiver em andamento também poderão ser afetados.
> - O console do Amazon S3 não permite a cópia entre regiões de objetos criptografados com SSE-KMS. Para copiar objetos criptografados com SSE-KMS, use a AWS CLI, o SDK da AWS ou a API REST do Amazon S3.

- Objetos criptografados com chaves de criptografia fornecidas pelo cliente (SSE-C) não podem ser copiados usando o console do S3. Para copiar objetos criptografados com SSE-C, use a AWS CLI, o SDK da AWS ou a API REST do Amazon S3.
- Os objetos copiados não manterão as configurações do Bloqueio de Objetos dos objetos originais.
- Se o bucket do qual você está copiando os objetos usar a configuração aplicada pelo proprietário do bucket em Propriedade de objetos do S3, as ACLs de objeto não serão copiadas para o destino especificado.
- Se você quiser copiar objetos para um bucket que usa a configuração aplicada pelo proprietário do bucket em Propriedade de objetos do S3, o bucket de origem também deve usar a configuração aplicada pelo proprietário do bucket ou você deve remover qualquer objeto concedido pela ACL a outras contas e grupos da AWS.

Para copiar um objeto

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets de uso geral ou Buckets de diretórios.
3. Na lista de buckets, escolha o nome do bucket que contém os objetos que você deseja copiar.
4. Marque a caixa de seleção à esquerda dos nomes dos objetos que você deseja copiar.
5. No menu Ações, escolha Copiar na lista de opções exibida.
6. Selecione o tipo de destino e a conta de destino. Para especificar o caminho de destino, escolha Browse S3 (Procurar S3), navegue até o destino e marque a caixa de seleção à esquerda do destino. Escolha Choose destination (Escolher destino) no canto inferior direito.

   Outra alternativa é inserir o caminho de destino.
7. Se o versionamento de bucket não estiver habilitado, você verá um aviso recomendando que o habilite para ajudar a impedir a substituição ou exclusão involuntária de objetos. Se você quiser manter todas as versões de objetos neste bucket, selecione Enable Bucket Versioning (Ativar versionamento de bucket). Você também pode atualizar as propriedades de criptografia padrão e do Bloqueio de Objetos do S3 em Detalhes do destino.
8. Em Configurações adicionais de cópia, escolha se você quer Copiar configurações de origem, Não especificar configurações ou Especificar configurações. Copiar configurações de origem é a opção padrão. Se você quiser copiar o objeto somente sem os atributos das configurações

de origem, escolha Não especificar configurações. Escolha Especificar configurações para especificar configurações referentes a classes de armazenamento, ACLs, tags de objeto, metadados, criptografia do lado do servidor e somas de verificação adicionais.

9. Escolha Copy (Copiar) no canto inferior direito. O Amazon S3 copia o objeto no destino.

Uso dos SDKs da AWS

O exemplo nesta seção mostra como copiar objetos de até 5 GB em uma única operação. Para copiar objetos maiores do que 5 GB, você deve usar um carregamento fracionado. Para obter mais informações, consulte Copiar um objeto usando multipart upload.

Java

Example

O exemplo a seguir copia um objeto no Amazon S3 usando o AWS SDK para Java. Consulte instruções sobre como criar e testar uma amostra funcional em Getting Started no Guia do desenvolvedor do AWS SDK para Java.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.CopyObjectRequest;

import java.io.IOException;

public class CopyObjectSingleOperation {

    public static void main(String[] args) throws IOException {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "*** Bucket name ***";
        String sourceKey = "*** Source object key *** ";
        String destinationKey = "*** Destination object key ***";

        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(clientRegion)
```

```
                    .build();

            // Copy the object into a new object in the same bucket.
            CopyObjectRequest copyObjRequest = new CopyObjectRequest(bucketName,
 sourceKey, bucketName, destinationKey);
            s3Client.copyObject(copyObjRequest);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

.NET

O exemplo em C# a seguir usa o SDK para .NET de alto nível para copiar objetos de até 5 GB em uma única operação. Para objetos maiores do que 5 GB, use o exemplo de cópia do multipart upload descrito em Copiar um objeto usando multipart upload.

Esse exemplo faz a cópia de um objeto de até 5 GB. Para obter informações sobre como configurar e executar exemplos de código, consulte Conceitos básicos do AWS SDK for .NET no Guia do desenvolvedor do AWS SDK for .NET.

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class CopyObjectTest
    {
        private const string sourceBucket = "*** provide the name of the bucket with
 source object ***";
        private const string destinationBucket = "*** provide the name of the bucket
 to copy the object to ***";
```

```
        private const string objectKey = "*** provide the name of object to copy
***";
        private const string destObjectKey = "*** provide the destination object key
name ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
RegionEndpoint.USWest2;
        private static IAmazonS3 s3Client;

        public static void Main()
        {
            s3Client = new AmazonS3Client(bucketRegion);
            Console.WriteLine("Copying an object");
            CopyingObjectAsync().Wait();
        }

        private static async Task CopyingObjectAsync()
        {
            try
            {
                CopyObjectRequest request = new CopyObjectRequest
                {
                    SourceBucket = sourceBucket,
                    SourceKey = objectKey,
                    DestinationBucket = destinationBucket,
                    DestinationKey = destObjectKey
                };
                CopyObjectResponse response = await
s3Client.CopyObjectAsync(request);
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered on server. Message:'{0}' when
writing an object", e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
writing an object", e.Message);
            }
        }
    }
}
```

PHP

Este tópico fornece orientações sobre como usar classes da versão 3 do AWS SDK para PHP para copiar um ou múltiplos objetos no Amazon S3 de um bucket para outro ou no mesmo bucket.

Para obter mais informações sobre a API do AWS SDK for Ruby, acesse AWS SDK for Ruby Version 2.

O exemplo do PHP a seguir mostra o uso do método `copyObject()` para copiar um único objeto no Amazon S3. Ele também demonstra como fazer várias cópias de um objeto usando um lote de chamadas para `CopyObject` com o método `getcommand()`.

Cópia de objetos

1	Crie uma instância de um cliente do Amazon S3 usando o construtor da classe `Aws\S3\S3Client` .
2	Para fazer várias cópias de um objeto, execute um lote de chamadas para o método getCommand() do cliente do Amazon S3, que é herdado da classe Aws\CommandInterface. Você fornece o comando `CopyObject` como o primeiro argumento e uma matriz contendo o bucket de origem, o nome de uma chave de origem, o bucket de destino e o nome do destino como segundo argumento.

```
 require 'vendor/autoload.php';

use Aws\CommandPool;
use Aws\Exception\AwsException;
use Aws\ResultInterface;
use Aws\S3\S3Client;

$sourceBucket = '*** Your Source Bucket Name ***';
$sourceKeyname = '*** Your Source Object Key ***';
$targetBucket = '*** Your Target Bucket Name ***';

$s3 = new S3Client([
    'version' => 'latest',
    'region' => 'us-east-1'
]);
```

```
// Copy an object.
$s3->copyObject([
    'Bucket' => $targetBucket,
    'Key' => "$sourceKeyname-copy",
    'CopySource' => "$sourceBucket/$sourceKeyname",
]);

// Perform a batch of CopyObject operations.
$batch = array();
for ($i = 1; $i <= 3; $i++) {
    $batch[] = $s3->getCommand('CopyObject', [
        'Bucket' => $targetBucket,
        'Key' => "{targetKeyname}-$i",
        'CopySource' => "$sourceBucket/$sourceKeyname",
    ]);
}
try {
    $results = CommandPool::batch($s3, $batch);
    foreach ($results as $result) {
        if ($result instanceof ResultInterface) {
            // Result handling here
        }
        if ($result instanceof AwsException) {
            // AwsException handling here
        }
    }
} catch (Exception $e) {
    // General error handling here
}
```

Python

```
class ObjectWrapper:
    """Encapsulates S3 object actions."""

    def __init__(self, s3_object):
        """
        :param s3_object: A Boto3 Object resource. This is a high-level resource in
 Boto3
                          that wraps object actions in a class-like structure.
        """
        self.object = s3_object
```

```
        self.key = self.object.key
```

```
   def copy(self, dest_object):
        """
        Copies the object to another bucket.

        :param dest_object: The destination object initialized with a bucket and
key.
                            This is a Boto3 Object resource.
        """
        try:
            dest_object.copy_from(
                CopySource={"Bucket": self.object.bucket_name, "Key":
self.object.key}
            )
            dest_object.wait_until_exists()
            logger.info(
                "Copied object from %s:%s to %s:%s.",
                self.object.bucket_name,
                self.object.key,
                dest_object.bucket_name,
                dest_object.key,
            )
        except ClientError:
            logger.exception(
                "Couldn't copy object from %s/%s to %s/%s.",
                self.object.bucket_name,
                self.object.key,
                dest_object.bucket_name,
                dest_object.key,
            )
            raise
```

Ruby

As tarefas a seguir orientam como usar classes Ruby para copiar um objeto no Amazon S3 de um bucket para outro ou no mesmo bucket.

Cópia de objetos

1	Use o gem modularizado do Amazon S3 da versão 3 do AWS SDK para Ruby, exija `aws-sdk-s3` e forneça suas credenciais da AWS. Consulte mais informaçõ es sobre como fornecer credenciais em Making requests using AWS account or IAM user credentials na Referência de API do Amazon S3.
2	Forneça as informações da solicitação, como o nome do bucket de origem, o nome da chave de origem, o nome do bucket de destino e a chave de destino.

O exemplo de código Ruby a seguir demonstra as tarefas precedentes usando o método `#copy_object` para copiar um objeto de um bucket para outro.

```
require 'aws-sdk-s3'

# Wraps Amazon S3 object actions.
class ObjectCopyWrapper
  attr_reader :source_object

  # @param source_object [Aws::S3::Object] An existing Amazon S3 object. This is
 used as the source object for
  #                                        copy actions.
  def initialize(source_object)
    @source_object = source_object
  end

  # Copy the source object to the specified target bucket and rename it with the
 target key.
  #
  # @param target_bucket [Aws::S3::Bucket] An existing Amazon S3 bucket where the
 object is copied.
  # @param target_object_key [String] The key to give the copy of the object.
  # @return [Aws::S3::Object, nil] The copied object when successful; otherwise,
 nil.
  def copy_object(target_bucket, target_object_key)
    @source_object.copy_to(bucket: target_bucket.name, key: target_object_key)
    target_bucket.object(target_object_key)
  rescue Aws::Errors::ServiceError => e
    puts "Couldn't copy #{@source_object.key} to #{target_object_key}. Here's why:
 #{e.message}"
  end
```

```
end

# Example usage:
def run_demo
  source_bucket_name = "amzn-s3-demo-bucket1"
  source_key = "my-source-file.txt"
  target_bucket_name = "amzn-s3-demo-bucket2"
  target_key = "my-target-file.txt"

  source_bucket = Aws::S3::Bucket.new(source_bucket_name)
  wrapper = ObjectCopyWrapper.new(source_bucket.object(source_key))
  target_bucket = Aws::S3::Bucket.new(target_bucket_name)
  target_object = wrapper.copy_object(target_bucket, target_key)
  return unless target_object

  puts "Copied #{source_key} from #{source_bucket_name} to
 #{target_object.bucket_name}:#{target_object.key}."
end

run_demo if $PROGRAM_NAME == __FILE__
```

Uso da API REST

Este exemplo descreve como copiar um objeto usando a API REST do S3. Para obter mais informações sobre a API REST, consulte CopyObject.

Este exemplo copia o objeto `flotsam` do bucket *amzn-s3-demo-bucket1* para o objeto `jetsam` do bucket *amzn-s3-demo-bucket2*, preservando seus metadados.

```
PUT /jetsam HTTP/1.1
Host: amzn-s3-demo-bucket2.s3.amazonaws.com
x-amz-copy-source: /amzn-s3-demo-bucket1/flotsam
Authorization: AWS AKIAIOSFODNN7EXAMPLE:ENoSbxYByFA0UGLZUqJN5EUnLDg=
Date: Wed, 20 Feb 2008 22:12:21 +0000
```

A assinatura foi gerada a partir das informações a seguir.

```
PUT\r\n
\r\n
\r\n
Wed, 20 Feb 2008 22:12:21 +0000\r\n
```

```
x-amz-copy-source:/amzn-s3-demo-bucket1/flotsam\r\n
/amzn-s3-demo-bucket2/jetsam
```

O Amazon S3 retorna a resposta a seguir, que especifica a ETag do objeto e quando ele foi modificado pela última vez.

```
HTTP/1.1 200 OK
x-amz-id-2: Vyaxt7qEbzv34BnSu5hctyyNSlHTYZFMWK4FtzO+iX8JQNyaLdTshL0KxatbaOZt
x-amz-request-id: 6B13C3C5B34AF333
Date: Wed, 20 Feb 2008 22:13:01 +0000

Content-Type: application/xml
Transfer-Encoding: chunked
Connection: close
Server: AmazonS3
<?xml version="1.0" encoding="UTF-8"?>

<CopyObjectResult>
   <LastModified>2008-02-20T22:13:01</LastModified>
   <ETag>"7e9c608af58950deeb370c98608ed097"</ETag>
</CopyObjectResult>
```

Como usar o AWS CLI

Você também pode usar a AWS Command Line Interface (AWS CLI) para copiar um objeto do S3. Para obter mais informações, consulte copy-object na Referência de comandos da AWS CLI.

Para obter informações sobre o AWS CLI, consulte O que é AWS Command Line Interface? no Guia do usuário do AWS Command Line Interface.

Como mover um objeto

Para mover um objeto, use os métodos a seguir.

Usar o console do S3

> **Note**
>
> - Você pode mover um objeto se ele tiver menos de 5 GB. Se o objeto tiver mais de 5 GB, você deve usar a AWS CLI ou SDKs da AWS para movê-lo.

- Para obter uma lista das permissões adicionais necessárias para mover objetos, consulte the section called “Permissões obrigatórias para operações de API do S3”. Para ver exemplos das políticas que concedem essas permissões, consulte the section called “Exemplos de políticas baseadas em identidade”.
- Objetos criptografados com chaves de criptografia fornecidas pelo cliente (SSE-C) não podem ser movidos usando o console do Amazon S3. Para mover objetos criptografados com SSE-C, use a AWS CLI, SDKs da AWS ou a API REST do Amazon S3.
- Ao mover pastas, aguarde a conclusão da operação Mover antes de fazer alterações adicionais nas pastas.
- No console do Amazon S3, não é possível usar aliases de ponto de acesso do S3 como origem ou destino para operações Mover.

Como mover um objeto

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets. Navegue até o bucket ou pasta do Amazon S3 que contém os objetos que você deseja mover.
3. Marque a caixa de seleção referente aos objetos que você quer mover.
4. No menu Ações, escolha Mover.
5. Para especificar o caminho de destino, escolha Procurar S3, navegue até o destino e marque a caixa de seleção do destino. Escolha Choose destination (Escolher destino).

   Outra alternativa é inserir o caminho de destino.
6. Se o versionamento de bucket não estiver habilitado, você verá um aviso recomendando que o habilite para ajudar a impedir a substituição ou exclusão involuntária de objetos. Se você quiser manter todas as versões de objetos neste bucket, selecione Enable Bucket Versioning (Ativar versionamento de bucket). Você também pode atualizar as propriedades de criptografia padrão e do Bloqueio de Objetos em Detalhes do destino.
7. Em Configurações adicionais de cópia, escolha se você quer Copiar configurações de origem, Não especificar configurações ou Especificar configurações. Copiar configurações de origem é a opção padrão. Se você quiser copiar o objeto somente sem os atributos das configurações de origem, escolha Não especificar configurações. Escolha Especificar configurações para

especificar configurações referentes a classes de armazenamento, ACLs, tags de objeto, metadados, criptografia do lado do servidor e somas de verificação adicionais.

8. Selecione Move (Mover) no canto inferior direito. O Amazon S3 move seus objetos para o destino.

Como usar o AWS CLI

Você também pode usar a AWS Command Line Interface (AWS CLI) para mover um objeto do S3. Para obter mais informações, consulte mv na Referência de comandos da AWS CLI.

Para obter informações sobre o AWS CLI, consulte O que é AWS Command Line Interface? no Guia do usuário do AWS Command Line Interface.

Para renomear um objeto

Use o procedimento a seguir para renomear um objeto.

> **Note**
>
> - Você pode renomear um objeto se ele tiver menos de 5 GB. Para renomear objetos com menos de 5 GB, você deve usar a AWS CLIou SDKs da AWS para copiar o objeto com um novo nome e, em seguida, excluir o objeto original.
> - Para obter uma lista das permissões adicionais necessárias para copiar objetos, consulte the section called “Permissões obrigatórias para operações de API do S3”. Para ver exemplos das políticas que concedem essas permissões, consulte the section called “Exemplos de políticas baseadas em identidade”.
> - A renomeação de um objeto cria uma cópia do objeto com uma nova data de última modificação, depois adiciona um marcador de exclusão ao objeto original.
> - As configurações de bucket para criptografia padrão são aplicadas automaticamente a qualquer objeto especificado que não esteja criptografado.
> - Não é possível usar o console do Amazon S3 para renomear objetos com chaves de criptografia fornecidas pelo cliente (SSE-C). Para renomear objetos criptografados com SSE-C, use a AWS CLI, os AWS SDKs ou a API REST do Amazon S3 para copiar esses objetos com novos nomes.

- Se esse bucket usar a configuração aplicada pelo proprietário do bucket para a funcionalidade Propriedade de Objeto do S3, as listas de controle de acesso (ACLs) a objetos não serão copiadas.

Para renomear um objeto

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação, escolha Buckets e selecione a guia Buckets de uso geral. Navegue até a pasta ou o bucket do Amazon S3 que contém o objeto que você deseja copiar.
3. Marque a caixa de seleção referente ao objeto que você quer renomear.
4. No menu Ações, selecione Renomear objeto.
5. Na caixa Nome do novo objeto, insira o novo nome do objeto.
6. Em Configurações adicionais de cópia, escolha se você quer Copiar configurações de origem, Não especificar configurações ou Especificar configurações. Copiar configurações de origem é a opção padrão. Se você quiser copiar o objeto somente sem os atributos das configurações de origem, escolha Não especificar configurações. Escolha Especificar configurações para especificar configurações referentes a classes de armazenamento, ACLs, tags de objeto, metadados, criptografia do lado do servidor e somas de verificação adicionais.
7. Escolha Salvar alterações. O Amazon S3 renomeia o objeto.

Baixar objetos

Esta seção explica como baixar objetos de um bucket do Amazon S3. Com o Amazon S3, é possível armazenar objetos em um ou mais buckets e cada objeto pode ter até 5 TB de tamanho. Qualquer objeto do Amazon S3 que não esteja arquivado pode ser acessado em tempo real. Os objetos arquivados, no entanto, devem ser restaurados antes de serem baixados. Para obter informações sobre como baixar objetos arquivados, consulte the section called “Baixar objetos arquivados”.

É possível baixar um único objeto usando o console do Amazon S3, a AWS Command Line Interface (AWS CLI), AWS SDKs ou a API REST do Amazon S3. Para baixar um objeto do S3 sem escrever nenhum código ou executar nenhum comando, use o console do S3. Para obter mais informações, consulte the section called “Fazer download de um objeto”.

Para baixar vários objetos, use o AWS CloudShell, a AWS CLI ou os AWS SDKs. Para obter mais informações, consulte the section called “Baixar vários objetos”.

Se precisar baixar parte de um objeto, use parâmetros extras com a AWS CLI ou a API REST para especificar somente os bytes que você deseja baixar. Para obter mais informações, consulte the section called “Baixar parte de um objeto”.

Se você precisar baixar um objeto que não seja seu, peça ao proprietário do objeto para gerar um URL pré-assinado que permita baixá-lo. Para obter mais informações, consulte the section called “Baixar um objeto de outra Conta da AWS”.

Quando você baixa objetos fora da rede da AWS, aplicam-se taxas de transferência de dados. A transferência de dados dentro da rede da AWS é gratuita dentro da mesma Região da AWS, mas haverá cobrança por qualquer solicitação `GET`. Para obter mais informações sobre custos de transferência de dados e cobranças de recuperação de dados, consulte Preços do Amazon S3.

Tópicos

- Fazer download de um objeto
- Baixar vários objetos
- Baixar parte de um objeto
- Baixar um objeto de outra Conta da AWS
- Baixar objetos arquivados
- Baixar objetos com base em metadados
- Solução de problemas de download de objetos

Fazer download de um objeto

É possível baixar um objeto usando o console do Amazon S3, a AWS CLI, AWS SDKs ou a API REST.

Usar o console do S3

Esta seção explica como usar o console do Amazon S3 para fazer baixar um objeto de um bucket do S3.

> **Note**
>
> - Só é possível baixar um objeto por vez.

- Se você usar o console do Amazon S3 para baixar um objeto cujo nome da chave termine com um ponto (`.`), o ponto será removido do nome da chave do objeto baixado. Para reter o ponto no final do nome do objeto baixado, você deve usar a AWS Command Line Interface (AWS CLI), AWS SDKs ou a API REST do Amazon S3.

Fazer download de um objeto de um bucket do S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets de uso geral ou Buckets de diretórios.
3. Na lista de buckets, escolha o nome do bucket do qual você deseja fazer download de um objeto.
4. Você pode baixar um objeto de um bucket do S3 de uma das seguintes formas:
   - Marque a caixa de seleção ao lado do objeto e escolha Fazer download. Se você quiser baixar o objeto em uma pasta específica, no menu Ações, escolha Fazer download como.
   - Se você quiser baixar uma versão específica do objeto, ative Mostrar versões (ao lado da caixa de pesquisa). Marque a caixa de seleção ao lado da versão do objeto que você deseja e escolha Fazer Download. Se você quiser baixar o objeto em uma pasta específica, no menu Ações, escolha Fazer download como.

Como usar o AWS CLI

O exemplo de `get-object` a seguir mostra como você pode usar a AWS CLI para baixar um objeto do Amazon S3. Esse comando obtém o objeto *`folder/my_image`* do bucket *`amzn-s3-demo-bucket1`*. Você deve incluir um `outfile`, que é um nome de arquivo para o objeto baixado, como *`my_downloaded_image.jpg`*.

```
aws s3api get-object --bucket amzn-s3-demo-bucket1 --key folder/
my_image my_downloaded_image.jpg
```

Para obter mais informações e exemplos, consulte get-object na Referência de comandos da AWS CLI.

Uso dos SDKs da AWS

Consulte exemplos de como baixar um objeto com os SDKs da AWS em Code examples na Referência de API do Amazon S3.

Consulte informações gerais sobre como usar diferentes SDKs da AWS em Developing with Amazon S3 using the AWS SDKs na Referência de API do Amazon S3.

Uso da API REST

É possível usar a API REST para recuperar objetos do Amazon S3. Para obter mais informações, consulte GetObject na Referência da API do Amazon Simple Storage Service.

Baixar vários objetos

Você pode baixar vários objetos usando o AWS CloudShell, a AWS CLI ou os AWS SDKs.

Usar AWS CloudShell no AWS Management Console

O AWS CloudShell é um shell pré-autenticado baseado em navegador que você pode iniciar diretamente do AWS Management Console.

Para obter mais informações sobre o AWS CloudShell, consulte O que é o CloudShell? no Guia do usuário do AWS CloudShell.

> **Important**
>
> Com o AWS CloudShell, o diretório inicial tem armazenamento de até 1 GB por Região da AWS. Portanto, você não pode sincronizar buckets com objetos cujo total ultrapasse esse valor. Para consultar mais limitações, acesse Cotas e restrições de serviço no Guia do usuário do AWS CloudShell.

Para baixar objetos usando o AWS CloudShell

1. Faça login no AWS Management Console e abra o console do CloudShell em https://console.aws.amazon.com/cloudshell/.
2. Os comandos a seguir são executados para sincronizar objetos no bucket com o CloudShell. O comando a seguir sincroniza objetos do bucket chamado *amzn-s3-demo-bucket1* e cria uma

pasta chamada *temp* no CloudShell. O CloudShell sincroniza os objetos com essa pasta. Para usar esse comando, substitua *user input placeholders* por suas informações.

```
aws s3 sync s3://amzn-s3-demo-bucket1 ./temp
```

> **Note**
>
> O comando `sync` não é compatível com buckets de diretório.
> Para realizar a correspondência de padrões e excluir ou incluir objetos específicos, você pode usar os parâmetros `--exclude "value"` e `--include "value"` com o comando `sync`.

3. Execute o comando a seguir para compactar objetos na pasta chamada *temp* para um arquivo chamado *temp.zip*.

   ```
   zip temp.zip -r temp/
   ```

4. Escolha Ações e Baixar arquivo.
5. Insira um nome para o arquivo **temp.zip** e escolha Baixar.
6. (Opcional) Exclua o arquivo *temp.zip* e os objetos que estão sincronizados com a pasta *temp* no CloudShell. Com o AWS CloudShell, você tem armazenamento persistente de até 1 GB para cada Região da AWS.

   Você pode usar os exemplos de comandos a seguir para excluir o arquivo `.zip` e a pasta. Para usar esse exemplo de comando, substitua os *user input placeholders* por suas próprias informações.

   ```
   rm temp.zip && rm -rf temp/
   ```

Como usar o AWS CLI

Os exemplos a seguir mostram como você pode usar a AWS CLI para baixar todos os arquivos ou objetos no diretório ou prefixo especificado. Esse comando copia todos os objetos do bucket *amzn-s3-demo-bucket1* para o diretório atual. Para usar esse exemplo de comando, use o nome do seu bucket no lugar de *amzn-s3-demo-bucket1*.

```
aws s3 cp s3://amzn-s3-demo-bucket1 . --recursive
```

O comando a seguir baixa todos os objetos com o prefixo *logs* no bucket *amzn-s3-demo-bucket1* para o diretório atual. Ele também usa os parâmetros `--exclude` e `--include` para copiar somente objetos com o sufixo *.log*. Para usar esse exemplo de comando, substitua os *user input placeholders* por suas próprias informações.

```
aws s3 cp s3://amzn-s3-demo-bucket1/logs/ . --recursive --exclude "*" --include "*.log"
```

Para obter mais informações e exemplos, consulte cp na Referência de comandos da AWS CLI.

Uso dos SDKs da AWS

Consulte exemplos de como baixar todos os objetos em um bucket do Amazon S3 com os SDKs da AWS em Code examples na Referência de API do Amazon S3.

Consulte informações gerais sobre como usar diferentes SDKs da AWS em Developing with Amazon S3 using the AWS SDKs na Referência de API do Amazon S3.

Baixar parte de um objeto

É possível baixar parte de um objeto usando a AWS CLI ou a API REST. Para fazer isso, use parâmetros adicionais a fim de especificar qual parte de um objeto você deseja baixar.

Como usar o AWS CLI

O exemplo de comando a seguir executa uma solicitação `GET` para um intervalo de bytes no objeto chamado *folder/my_data* no bucket denominado *amzn-s3-demo-bucket1*. Na solicitação, o intervalo de bytes deve ter `bytes=` como prefixo. O objeto parcial é baixado para o arquivo de saída chamado *my_data_range*. Para usar esse exemplo de comando, substitua os *user input placeholders* por suas próprias informações.

```
aws s3api get-object --bucket amzn-s3-demo-bucket1 --key folder/my_data --range
 bytes=0-500 my_data_range
```

Para obter mais informações e exemplos, consulte get-object na Referência de comandos da AWS CLI.

Para obter mais informações sobre o cabeçalho HTTP `Range`, consulte RFC 9110 no site do RFC Editor.

> **Note**
>
> O Amazon S3 não comporta a recuperação de vários intervalos de dados em uma única solicitação `GET`.

Uso da API REST

Você pode usar os parâmetros `partNumber` e `Range` na API REST para recuperar partes de objetos do Amazon S3. Para obter mais informações, consulte GetObject na Referência da API do Amazon Simple Storage Service.

Baixar um objeto de outra Conta da AWS

É possível usar um URL pré-assinado para conceder acesso por tempo limitado aos objetos sem atualizar a política de bucket.

O URL pré-assinado pode ser inserido em um navegador ou usado por um programa para baixar um objeto. As credenciais usadas pelo URL são as do usuário da AWS que gerou o URL. Depois que o URL for criado, qualquer pessoa com o URL pré-assinado poderá baixar o objeto correspondente até que o URL expire.

Usar um URL pré-assinado no console do S3

É possível usar o console do Amazon S3 para gerar um URL pré-assinado para compartilhar um objeto em um bucket de uso geral seguindo estas etapas. Ao usar o console, o tempo máximo de validade de um URL pré-assinado é de 12 horas a partir do momento da criação.

Para gerar um URL pré-assinado usando o console do Amazon S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets de uso geral.
3. Na lista de buckets, selecione o nome do bucket que contém os objetos para os quais você deseja obter um URL pré-assinado.
4. Na lista Objects (Objetos), selecione o objeto para o qual deseja criar um URL pré-assinado.
5. No menu Ações de objeto, escolha Compartilhar com um URL pré-assinado.
6. Especifique por quanto tempo deseja que o URL pré-assinado seja válido.
7. Escolha Create presigned URL (Criar URL pré-assinado).

8. Quando uma mensagem de confirmação é exibida, o URL é copiado automaticamente para a área de transferência. Você verá um botão para copiar o URL pré-assinado se precisar copiá-lo novamente.
9. Para baixar o objeto, cole o URL em qualquer navegador para que o objeto tente fazer download.

Para obter mais informações sobre URLs pré-assinados e outros métodos para criá-los, consulte Baixar e fazer upload de objetos com URLs pré-assinados.

Baixar objetos arquivados

Para reduzir os custos de armazenamento de objetos acessados com pouca frequência, você pode arquivar esses objetos. Quando você arquiva um objeto, ele é movido para um armazenamento de baixo custo, o que significa que não é possível acessá-lo em tempo real. Para baixar um objeto arquivado, você deve restaurá-lo primeiro.

Os objetos arquivados podem ser restaurados em minutos ou horas, dependendo da classe de armazenamento. Você pode restaurar um objeto arquivado usando o console do Amazon S3, Operações em Lote do S3, a API REST do Amazon S3, os AWS SDKs e a AWS Command Line Interface (AWS CLI).

Para instruções, consulte Restaurar um objeto arquivado. Depois de restaurar o objeto arquivado, você poderá baixá-lo.

Baixar objetos com base em metadados

É possível adicionar condições prévias para baixar um objeto com base nos respectivos metadados usando uma solicitação de leitura condicional. Você pode exibir um objeto com base na tag da entidade (ETag) ou na data da última modificação. Isso pode limitar uma operação do S3 a objetos atualizados desde uma data especificada ou exibir somente uma versão específica de um objeto.

É possível usar gravações condicionais para solicitações GetObject ou HeadObject.

Para ter mais informações sobre solicitações condicionais, consulte Adicionar condições prévias às operações do S3 com solicitações condicionais.

Solução de problemas de download de objetos

Permissões insuficientes ou políticas incorretas de bucket ou de usuário do AWS Identity and Access Management (IAM) podem causar erros ao tentar baixar objetos do Amazon S3. Esses problemas

geralmente podem provocar erros de acesso negado (403 proibido), nos quais o Amazon S3 não consegue permitir o acesso a um recurso.

Para ver as causas comuns de erros de acesso negado (403 proibido), consulte Solucionar erros de acesso negado (403 Forbidden) no Amazon S3.

Se você estiver recebendo um erro 404 NoSuchKey ao tentar acessar um objeto, consulte Como posso solucionar o erro 404 “NoSuchKey” do Amazon S3? no Centro de Conhecimento do AWS re:Post.

Verificar a integridade do objeto no Amazon S3

O Amazon S3 usa valores de soma de verificação para verificar a integridade dos dados que você carrega ou baixa. Além disso, você pode solicitar que outro valor de soma de verificação seja calculado para qualquer objeto armazenado no Amazon S3. Você pode escolher um algoritmo de soma de verificação para operações de upload, cópia simples cópia em lote dos dados.

Quando você faz upload dos dados, o Amazon S3 usa o algoritmo que você escolheu para calcular uma soma de verificação do lado do servidor e a valida com o valor fornecido antes de armazenar o objeto e a soma de verificação como parte dos metadados do objeto. Essa validação funciona de maneira consistente em todos os modos de criptografia, tamanhos de objetos e classes de armazenamento para uploads de parte única e fracionados. No entanto, quando você faz uma cópia simples ou em lote dos dados, o Amazon S3 calcula a soma de verificação no objeto de origem e a move para o objeto de destino.

> **Note**
>
> Ao realizar um upload de parte única ou fracionado, você também pode incluir uma soma de verificação pré-calculada como parte da solicitação e usar o tipo de soma de verificação de objeto inteiro. Para usar valores pré-calculados com vários objetos, use a AWS CLI ou os AWS SDKs.

Usar algoritmos de soma de verificação compatíveis

Com o Amazon S3, você pode escolher um algoritmo de soma de verificação para validar os dados durante os uploads. O algoritmo de soma de verificação especificado é armazenado com o objeto e

pode ser usado para validar a integridade dos dados durante os downloads. Você pode selecionar um dos seguintes algoritmos de soma de verificação Secure Hash Algorithms (SHA) ou Cyclic Redundancy Check (CRC) para calcular o valor da soma de verificação:

- CRC-64/NVME (`CRC64NVME`)
- CRC-32 (`CRC32`)
- CRC-32C (`CRC32C`)
- SHA-1 (`SHA1`)
- SHA-256 (`SHA256`)

Além disso, você pode fornecer uma soma de verificação com cada solicitação usando o cabeçalho Content-MD5.

Ao fazer upload de um objeto, especifique o algoritmo que deseja usar:

- Ao usar o AWS Management Console, escolha o algoritmo de soma de verificação que deseja usar. Você também pode especificar o valor da soma de verificação do objeto. Quando o Amazon S3 recebe o objeto, ele calcula a soma de verificação usando o algoritmo especificado. Se os dois valores de soma de verificação não corresponderem, o Amazon S3 gerará um erro.
- Ao usar um SDK, esteja ciente do seguinte:
  - Defina o parâmetro `ChecksumAlgorithm` como o algoritmo que você deseja que o Amazon S3 use. Se você já tem uma soma de verificação pré-calculada, envie o valor da soma de verificação para o AWS SDK, que incluirá o valor na solicitação. Se você não enviar um valor de soma de verificação ou não especificar um algoritmo de soma de verificação, o SDK calculará automaticamente um valor de soma de verificação para você e o incluirá na solicitação a fim de fornecer proteções de integridade. Se o valor da soma de verificação individual não corresponder ao valor definido do algoritmo de soma de verificação, o Amazon S3 rejeitará a solicitação com um erro `BadDigest`.
  - Se você estiver usando um AWS SDK atualizado, o SDK escolherá um algoritmo de soma de verificação para você. No entanto, você pode substituir esse algoritmo de soma de verificação.
  - Se você não especificar um algoritmo de soma de verificação e o SDK também não calcular uma soma de verificação para você, o S3 escolherá automaticamente o algoritmo de soma de verificação CRC-64/NVME (`CRC64NVME`).
- Ao utilizar a API REST, não use o parâmetro `x-amz-sdk-checksum-algorithm`. Em vez disso, use um dos cabeçalhos específicos do algoritmo (por exemplo, `x-amz-checksum-crc32`).

Para aplicar qualquer um desses valores de soma de verificação a objetos que já foram carregados no Amazon S3, você pode copiar o objeto e especificar se deseja usar o algoritmo de soma de verificação existente ou um novo. Se você não especificar um algoritmo, o S3 usará o algoritmo existente. Se o objeto de origem não tiver um algoritmo de soma de verificação ou valor de soma de verificação especificado, o Amazon S3 usará o algoritmo CRC-64/NVME para calcular o valor da soma de verificação do objeto de destino. Também é possível especificar um algoritmo de soma de verificação ao copiar objetos usando a funcionalidade Operações em Lote do S3.

> **Important**
>
> Se você usar um upload fracionado com somas de verificação para somas de verificação compostas (ou no nível da parte), os números de partes do upload fracionado deverão ser consecutivos e começar com 1. Se você tentar concluir uma solicitação de upload fracionado com números de parte não consecutivos, o Amazon S3 gerará um erro `HTTP 500 Internal Server`.

Tipos de soma de verificação de objeto inteiro e composta

No Amazon S3, há dois tipos de somas de verificação compatíveis:

- Somas de verificação de objeto inteiro: uma soma de verificação de objeto inteiro é calculada com base em todo o conteúdo de um upload fracionado, abrangendo todos os dados desde o primeiro byte da primeira parte até o último byte da última parte.

  > **Note**
  >
  > Todas as solicitações PUT exigem um tipo de soma de verificação de objeto inteiro.

- Somas de verificação compostas: uma soma de verificação composta é calculada com base nas somas de verificação individuais de cada parte em um upload fracionado. Em vez de calcular uma soma de verificação com base em todo o conteúdo dos dados, essa abordagem agrega as somas de verificação ao nível da parte (da primeira à última parte) para produzir uma única soma de verificação combinada para o objeto inteiro.

> **Note**
>
> Quando um objeto é carregado como um upload fracionado, a tag de entidade (ETag) do objeto não é um resumo MD5 do objeto inteiro. Em vez disso, o Amazon S3 calcula o resumo MD5 de cada parte à medida que são carregadas. Os resumos MD5 são usados para determinar a ETag do objeto final. O Amazon S3 concatena os bytes para os resumos MD5 e, depois, calcula o resumo MD5 desses valores concatenados. Durante a etapa final de criação da ETag, o Amazon S3 adiciona um traço com o número total de partes ao final.

O Amazon S3 oferece suporte aos seguintes tipos de algoritmo de soma de verificação de objeto inteiro e composta:

- CRC-64/NVME (`CRC64NVME`): compatível somente com o tipo de algoritmo de objeto inteiro.
- CRC-32 (`CRC32`): compatível com os tipos de algoritmo de objeto inteiro e composto.
- CRC-32C (`CRC32C`): compatível com os tipos de algoritmo de objeto inteiro e composto.
- SHA-1 (`SHA1`): compatível com os tipos de algoritmo de objeto inteiro e composto.
- SHA-256 (`SHA256`): compatível com os tipos de algoritmo de objeto inteiro e composto.

> **Note**
>
> Se você estiver usando um algoritmo de soma de verificação `SHA-1` ou `SHA-256` para um carregamento fracionado, deverá usar o tipo de algoritmo composto. Se você estiver usando um algoritmo de soma de verificação `SHA-1` ou `SHA-256` para o upload de uma única parte, somente o tipo de algoritmo de objeto inteiro é aceito.

Uploads de parte única

As somas de verificação de objetos que são carregados em uma única parte (usando `PutObject`) são tratadas como somas de verificação de objeto inteiro. Ao fazer upload de um objeto no console do Amazon S3, você pode escolher o algoritmo de soma de verificação que deseja que o S3 use e também (opcionalmente) fornecer um valor pré-calculado. O Amazon S3 valida essa soma de verificação antes de armazenar o objeto e o valor de soma de verificação dele. Você pode verificar a

integridade dos dados de um objeto ao solicitar o valor da soma de verificação durante os downloads de objetos.

Carregamentos fracionados

Ao fazer upload do objeto em várias partes usando a API `MultipartUpload`, você pode especificar o algoritmo de soma de verificação que deseja que o Amazon S3 use e o tipo de soma de verificação (objeto inteiro ou composta).

A tabela a seguir indica qual tipo de algoritmo de soma de verificação é compatível com cada algoritmo de soma de verificação em um upload fracionado:

Algoritmo da soma de verificação	Objeto inteiro	Composto
CRC-64/NVME (`CRC64NVME`)	Sim	Não
CRC-32 (`CRC32`)	Sim	Sim
CRC-32C (`CRC32C`)	Sim	Sim
SHA-1 (`SHA1`)	Não	Sim
SHA-256 (`SHA256`)	Não	Sim

Usar somas de verificação de objetos inteiros para upload fracionado

Ao criar ou realizar um upload fracionado, você pode usar somas de verificação de objeto inteiro para validação no upload. Isso significa que é possível fornecer o algoritmo de soma de verificação para a API `MultipartUpload`, simplificando as ferramentas de validação de integridade, pois você não precisa mais rastrear os limites das partes dos objetos carregados. Você pode fornecer a soma de verificação do objeto inteiro na solicitação `CompleteMultipartUpload` com o tamanho do objeto.

Ao fornecer uma soma de verificação de objeto inteiro durante um upload fracionado, o AWS SDK envia a soma de verificação para o Amazon S3, e o S3 valida a integridade do objeto do lado do servidor, comparando-a com o valor recebido. Depois, o Amazon S3 armazena o objeto se os valores corresponderem. Se os dois valores não corresponderem, o S3 reprovará a solicitação com

um erro `BadDigest`. A soma de verificação do objeto também é armazenada nos metadados do objeto que você usará posteriormente para validar a integridade dos dados do objeto.

Para somas de verificação de objeto inteiro, você pode usar os algoritmos de soma de verificação CRC-64/NVME (`CRC64NVME`), CRC-32 (`CRC32`) ou CRC-32C (`CRC32C`) no S3. As somas de verificação de objeto inteiro em uploads fracionados só estão disponíveis para somas de verificação baseadas em CRC porque podem ser linearizadas em uma soma de verificação de objeto inteiro. Essa linearização permite que o Amazon S3 paralelize as solicitações para melhorar a performance. Em particular, o S3 pode calcular a soma de verificação do objeto inteiro com base nas somas de verificação ao nível da parte. Esse tipo de validação não está disponível para outros algoritmos, como SHA e MD5. Como o S3 tem proteções de integridade padrão, se os objetos forem carregados sem uma soma de verificação, o S3 anexará automaticamente o algoritmo de soma de verificação CRC-64/NVME (`CRC64NVME`) de objeto inteiro recomendado ao objeto.

> **Note**
>
> Para inicializar o upload fracionado, você pode especificar o algoritmo de soma de verificação e o tipo de soma de verificação de objeto inteiro. Depois de especificar o algoritmo de soma de verificação e o tipo de soma de verificação de objeto inteiro, você pode fornecer o valor da soma de verificação de objeto inteiro para o upload fracionado.

Usar somas de verificação ao nível da parte para upload fracionado

Quando os objetos são carregados no Amazon S3, eles podem ser carregados como um único objeto ou em partes por meio do processo de upload fracionado. Você pode escolher um tipo de Checksum para o upload fracionado. Para somas de verificação ao nível da parte (ou somas de verificação compostas) em uploads fracionados, o Amazon S3 calcula a soma de verificação de cada parte usando o algoritmo de soma de verificação especificado. Você pode usar `UploadPart` para fornecer os valores de soma de verificação de cada parte. Se o objeto que você tentar carregar no console do Amazon S3 estiver configurado para usar o algoritmo de soma de verificação CRC-64/NVME (`CRC64NVME`) e exceder 16 MB, ele será automaticamente designado como uma soma de verificação de objeto inteiro.

Depois, o Amazon S3 usa os valores de soma de verificação ao nível da parte armazenados para confirmar se cada parte foi carregada corretamente. Quando a soma de verificação de cada parte (para o objeto inteiro) é fornecida, o S3 usa os valores de soma de verificação armazenados de cada parte para calcular a soma de verificação do objeto inteiro internamente, comparando esse valor com

o valor de soma de verificação fornecido. Isso minimiza os custos de computação, pois o S3 pode calcular uma soma de verificação de objeto inteiro usando a soma de verificação das partes. Para ter mais informações sobre os uploads fracionados, consulte Carregar e copiar objetos usando upload fracionado no Amazon S3 e Usar somas de verificação de objetos inteiros para upload fracionado.

Quando o objeto tiver sido completamente carregado, você poderá usar a soma de verificação final calculada para verificar a integridade dos dados do objeto.

Ao fazer upload de uma parte do upload fracionado, esteja ciente do seguinte:

- Para recuperar informações sobre o objeto, incluindo o número de partes que compõem o objeto inteiro, você pode usar a operação `GetObjectAttributes`. Com somas de verificação adicionais, também é possível recuperar informações de cada parte, incluindo o valor da soma de verificação da parte.
- Para uploads concluídos, é possível obter a soma de verificação de uma parte individual usando as operações `GetObject` ou `HeadObject` e especificando um número de partes ou intervalo de bytes que se alinha a uma única parte. Se você quiser recuperar os valores da soma de verificação para partes individuais de carregamentos fracionados ainda em andamento, poderá usar `ListParts`.
- Devido à forma como o Amazon S3 calcula a soma de verificação para objetos fracionados, o valor da soma de verificação do objeto poderá ser alterado se você copiá-lo. Se estiver usando um SDK ou a API REST e chamar `CopyObject`, o Amazon S3 copiará qualquer objeto até as limitações de tamanho da operação de API `CopyObject`. O Amazon S3 faz essa cópia como uma única ação, independentemente de o objeto ter sido carregado em uma única solicitação ou como parte de um carregamento fracionado. Com um comando copy, a soma de verificação do objeto é uma soma de verificação direta do objeto completo. Se o objeto tiver sido originalmente carregado usando um upload fracionado, o valor da soma de verificação será alterado mesmo que os dados não mudem.
- Os objetos que ultrapassam as limitações de tamanho da operação de API `CopyObject` devem usar comandos de cópia de upload fracionado.
- Quando você executar algumas operações usando o AWS Management Console, o Amazon S3 usará o carregamento fracionado se o objeto tiver mais de 16 MB.

Operações de soma de verificação

Depois de fazer upload de objetos, você pode obter o valor da soma de verificação e compará-lo com um valor de soma de verificação pré-calculado ou armazenado anteriormente do mesmo tipo de

algoritmo. Os exemplos a seguir mostram quais operações de soma de verificação ou métodos você pode usar para verificar a integridade dos dados.

Usar o console do S3

Para saber mais sobre como usar o console e especificar algoritmos de soma de verificação a serem usados ao carregar objetos, consulte Fazer upload de objetos e Tutorial: verificar a integridade dos dados no Amazon S3 com somas de verificação adicionais.

Uso dos SDKs da AWS

O exemplo a seguir mostra como usar os AWS SDKs para fazer upload de um arquivo grande com upload fracionado, baixar um arquivo grande e validar um arquivo de upload fracionado usando SHA-256 para validação de arquivos.

Java

Example Exemplo: carregar, baixar e verificar um arquivo grande com SHA-256

Consulte instruções sobre como criar e testar uma amostra funcional em Getting Started no Guia do desenvolvedor do AWS SDK para Java.

```
import software.amazon.awssdk.auth.credentials.AwsCredentials;
import software.amazon.awssdk.auth.credentials.AwsCredentialsProvider;
import software.amazon.awssdk.core.ResponseInputStream;
import software.amazon.awssdk.core.sync.RequestBody;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3.S3Client;
import software.amazon.awssdk.services.s3.model.AbortMultipartUploadRequest;
import software.amazon.awssdk.services.s3.model.ChecksumAlgorithm;
import software.amazon.awssdk.services.s3.model.ChecksumMode;
import software.amazon.awssdk.services.s3.model.CompleteMultipartUploadRequest;
import software.amazon.awssdk.services.s3.model.CompleteMultipartUploadResponse;
import software.amazon.awssdk.services.s3.model.CompletedMultipartUpload;
import software.amazon.awssdk.services.s3.model.CompletedPart;
import software.amazon.awssdk.services.s3.model.CreateMultipartUploadRequest;
import software.amazon.awssdk.services.s3.model.CreateMultipartUploadResponse;
import software.amazon.awssdk.services.s3.model.GetObjectAttributesRequest;
import software.amazon.awssdk.services.s3.model.GetObjectAttributesResponse;
import software.amazon.awssdk.services.s3.model.GetObjectRequest;
import software.amazon.awssdk.services.s3.model.GetObjectResponse;
import software.amazon.awssdk.services.s3.model.GetObjectTaggingRequest;
import software.amazon.awssdk.services.s3.model.ObjectAttributes;
```

```
    import software.amazon.awssdk.services.s3.model.PutObjectTaggingRequest;
    import software.amazon.awssdk.services.s3.model.Tag;
    import software.amazon.awssdk.services.s3.model.Tagging;
    import software.amazon.awssdk.services.s3.model.UploadPartRequest;
    import software.amazon.awssdk.services.s3.model.UploadPartResponse;

    import java.io.File;
    import java.io.FileInputStream;
    import java.io.FileOutputStream;
    import java.io.IOException;
    import java.io.InputStream;
    import java.io.OutputStream;
    import java.nio.ByteBuffer;
    import java.security.MessageDigest;
    import java.security.NoSuchAlgorithmException;
    import java.util.ArrayList;
    import java.util.Base64;
    import java.util.List;

    public class LargeObjectValidation {
        private static String FILE_NAME = "sample.file";
        private static String BUCKET = "sample-bucket";
        //Optional, if you want a method of storing the full multipart object
 checksum in S3.
        private static String CHECKSUM_TAG_KEYNAME = "fullObjectChecksum";
        //If you have existing full-object checksums that you need to validate
 against, you can do the full object validation on a sequential upload.
        private static String SHA256_FILE_BYTES = "htCM5g7ZNdoSw8bN/
mkgiAhXt5MFoVowVg+LE9aIQmI=";
        //Example Chunk Size - this must be greater than or equal to 5MB.
        private static int CHUNK_SIZE = 5 * 1024 * 1024;

        public static void main(String[] args) {
            S3Client s3Client = S3Client.builder()
                    .region(Region.US_EAST_1)
                    .credentialsProvider(new AwsCredentialsProvider() {
                        @Override
                        public AwsCredentials resolveCredentials() {
                            return new AwsCredentials() {
                                @Override
                                public String accessKeyId() {
                                    return Constants.ACCESS_KEY;
                                }
```

```
                                @Override
                                public String secretAccessKey() {
                                    return Constants.SECRET;
                                }
                            };
                        }
                    })
                    .build();
            uploadLargeFileBracketedByChecksum(s3Client);
            downloadLargeFileBracketedByChecksum(s3Client);
            validateExistingFileAgainstS3Checksum(s3Client);
        }

        public static void uploadLargeFileBracketedByChecksum(S3Client s3Client) {
            System.out.println("Starting uploading file validation");
            File file = new File(FILE_NAME);
            try (InputStream in = new FileInputStream(file)) {
                MessageDigest sha256 = MessageDigest.getInstance("SHA-256");
                CreateMultipartUploadRequest createMultipartUploadRequest =
CreateMultipartUploadRequest.builder()
                        .bucket(BUCKET)
                        .key(FILE_NAME)
                        .checksumAlgorithm(ChecksumAlgorithm.SHA256)
                        .build();
                CreateMultipartUploadResponse createdUpload =
s3Client.createMultipartUpload(createMultipartUploadRequest);
                List<CompletedPart> completedParts = new ArrayList<CompletedPart>();
                int partNumber = 1;
                byte[] buffer = new byte[CHUNK_SIZE];
                int read = in.read(buffer);
                while (read != -1) {
                    UploadPartRequest uploadPartRequest =
UploadPartRequest.builder()

.partNumber(partNumber).uploadId(createdUpload.uploadId()).key(FILE_NAME).bucket(BUCKET).ch
                    UploadPartResponse uploadedPart =
s3Client.uploadPart(uploadPartRequest,
RequestBody.fromByteBuffer(ByteBuffer.wrap(buffer, 0, read)));
                    CompletedPart part =
CompletedPart.builder().partNumber(partNumber).checksumSHA256(uploadedPart.checksumSHA256()
                    completedParts.add(part);
                    sha256.update(buffer, 0, read);
                    read = in.read(buffer);
                    partNumber++;
```

```
                }
                String fullObjectChecksum =
Base64.getEncoder().encodeToString(sha256.digest());
                if (!fullObjectChecksum.equals(SHA256_FILE_BYTES)) {
                    //Because the SHA256 is uploaded after the part is uploaded; the
upload is bracketed and the full object can be fully validated.

s3Client.abortMultipartUpload(AbortMultipartUploadRequest.builder().bucket(BUCKET).key(FILE
                    throw new IOException("Byte mismatch between stored checksum and
upload, do not proceed with upload and cleanup");
                }
                CompletedMultipartUpload completedMultipartUpload =
CompletedMultipartUpload.builder().parts(completedParts).build();
                CompleteMultipartUploadResponse completedUploadResponse =
s3Client.completeMultipartUpload(

CompleteMultipartUploadRequest.builder().bucket(BUCKET).key(FILE_NAME).uploadId(createdUplo
                Tag checksumTag =
Tag.builder().key(CHECKSUM_TAG_KEYNAME).value(fullObjectChecksum).build();
                //Optionally, if you need the full object checksum stored with the
file; you could add it as a tag after completion.

s3Client.putObjectTagging(PutObjectTaggingRequest.builder().bucket(BUCKET).key(FILE_NAME).t
            } catch (IOException | NoSuchAlgorithmException e) {
                e.printStackTrace();
            }
            GetObjectAttributesResponse
                    objectAttributes =
s3Client.getObjectAttributes(GetObjectAttributesRequest.builder().bucket(BUCKET).key(FILE_N
                    .objectAttributes(ObjectAttributes.OBJECT_PARTS,
ObjectAttributes.CHECKSUM).build());
            System.out.println(objectAttributes.objectParts().parts());
            System.out.println(objectAttributes.checksum().checksumSHA256());
        }

        public static void downloadLargeFileBracketedByChecksum(S3Client s3Client) {
            System.out.println("Starting downloading file validation");
            File file = new File("DOWNLOADED_" + FILE_NAME);
            try (OutputStream out = new FileOutputStream(file)) {
                GetObjectAttributesResponse
                        objectAttributes =
s3Client.getObjectAttributes(GetObjectAttributesRequest.builder().bucket(BUCKET).key(FILE_N
                        .objectAttributes(ObjectAttributes.OBJECT_PARTS,
ObjectAttributes.CHECKSUM).build());
```

```
                //Optionally if you need the full object checksum, you can grab a
 tag you added on the upload
                List<Tag> objectTags =
 s3Client.getObjectTagging(GetObjectTaggingRequest.builder().bucket(BUCKET).key(FILE_NAME).b
                String fullObjectChecksum = null;
                for (Tag objectTag : objectTags) {
                    if (objectTag.key().equals(CHECKSUM_TAG_KEYNAME)) {
                        fullObjectChecksum = objectTag.value();
                        break;
                    }
                }
                MessageDigest sha256FullObject =
 MessageDigest.getInstance("SHA-256");
                MessageDigest sha256ChecksumOfChecksums =
 MessageDigest.getInstance("SHA-256");

                //If you retrieve the object in parts, and set the ChecksumMode to
 enabled, the SDK will automatically validate the part checksum
                for (int partNumber = 1; partNumber <=
 objectAttributes.objectParts().totalPartsCount(); partNumber++) {
                    MessageDigest sha256Part = MessageDigest.getInstance("SHA-256");
                    ResponseInputStream<GetObjectResponse> response =
 s3Client.getObject(GetObjectRequest.builder().bucket(BUCKET).key(FILE_NAME).partNumber(part
                    GetObjectResponse getObjectResponse = response.response();
                    byte[] buffer = new byte[CHUNK_SIZE];
                    int read = response.read(buffer);
                    while (read != -1) {
                        out.write(buffer, 0, read);
                        sha256FullObject.update(buffer, 0, read);
                        sha256Part.update(buffer, 0, read);
                        read = response.read(buffer);
                    }
                    byte[] sha256PartBytes = sha256Part.digest();
                    sha256ChecksumOfChecksums.update(sha256PartBytes);
                    //Optionally, you can do an additional manual validation again
 the part checksum if needed in addition to the SDK check
                    String base64PartChecksum =
 Base64.getEncoder().encodeToString(sha256PartBytes);
                    String base64PartChecksumFromObjectAttributes =
 objectAttributes.objectParts().parts().get(partNumber - 1).checksumSHA256();
                    if (!
base64PartChecksum.equals(getObjectResponse.checksumSHA256()) || !
base64PartChecksum.equals(base64PartChecksumFromObjectAttributes)) {
```

```
                        throw new IOException("Part checksum didn't match for the
 part");
                    }
                    System.out.println(partNumber + " " + base64PartChecksum);
                }
                //Before finalizing, do the final checksum validation.
                String base64FullObject =
 Base64.getEncoder().encodeToString(sha256FullObject.digest());
                String base64ChecksumOfChecksums =
 Base64.getEncoder().encodeToString(sha256ChecksumOfChecksums.digest());
                if (fullObjectChecksum != null && !
fullObjectChecksum.equals(base64FullObject)) {
                    throw new IOException("Failed checksum validation for full
 object");
                }
                System.out.println(fullObjectChecksum);
                String base64ChecksumOfChecksumFromAttributes =
 objectAttributes.checksum().checksumSHA256();
                if (base64ChecksumOfChecksumFromAttributes != null && !
base64ChecksumOfChecksums.equals(base64ChecksumOfChecksumFromAttributes)) {
                    throw new IOException("Failed checksum validation for full
 object checksum of checksums");
                }
                System.out.println(base64ChecksumOfChecksumFromAttributes);
                out.flush();
            } catch (IOException | NoSuchAlgorithmException e) {
                //Cleanup bad file
                file.delete();
                e.printStackTrace();
            }
        }

        public static void validateExistingFileAgainstS3Checksum(S3Client s3Client)
 {
            System.out.println("Starting existing file validation");
            File file = new File("DOWNLOADED_" + FILE_NAME);
            GetObjectAttributesResponse
                    objectAttributes =
 s3Client.getObjectAttributes(GetObjectAttributesRequest.builder().bucket(BUCKET).key(FILE_N
                    .objectAttributes(ObjectAttributes.OBJECT_PARTS,
 ObjectAttributes.CHECKSUM).build());
            try (InputStream in = new FileInputStream(file)) {
                MessageDigest sha256ChecksumOfChecksums =
 MessageDigest.getInstance("SHA-256");
```

```
                MessageDigest sha256Part = MessageDigest.getInstance("SHA-256");
                byte[] buffer = new byte[CHUNK_SIZE];
                int currentPart = 0;
                int partBreak =
 objectAttributes.objectParts().parts().get(currentPart).size();
                int totalRead = 0;
                int read = in.read(buffer);
                while (read != -1) {
                    totalRead += read;
                    if (totalRead >= partBreak) {
                        int difference = totalRead - partBreak;
                        byte[] partChecksum;
                        if (totalRead != partBreak) {
                            sha256Part.update(buffer, 0, read - difference);
                            partChecksum = sha256Part.digest();
                            sha256ChecksumOfChecksums.update(partChecksum);
                            sha256Part.reset();
                            sha256Part.update(buffer, read - difference,
 difference);
                        } else {
                            sha256Part.update(buffer, 0, read);
                            partChecksum = sha256Part.digest();
                            sha256ChecksumOfChecksums.update(partChecksum);
                            sha256Part.reset();
                        }
                        String base64PartChecksum =
 Base64.getEncoder().encodeToString(partChecksum);
                        if (!
base64PartChecksum.equals(objectAttributes.objectParts().parts().get(currentPart).checksumSH
 {
                            throw new IOException("Part checksum didn't match S3");
                        }
                        currentPart++;
                        System.out.println(currentPart + " " + base64PartChecksum);
                        if (currentPart <
 objectAttributes.objectParts().totalPartsCount()) {
                            partBreak +=
 objectAttributes.objectParts().parts().get(currentPart - 1).size();
                        }
                    } else {
                        sha256Part.update(buffer, 0, read);
                    }
                    read = in.read(buffer);
                }
```

```
                if (currentPart != objectAttributes.objectParts().totalPartsCount())
 {
                    currentPart++;
                    byte[] partChecksum = sha256Part.digest();
                    sha256ChecksumOfChecksums.update(partChecksum);
                    String base64PartChecksum =
 Base64.getEncoder().encodeToString(partChecksum);
                    System.out.println(currentPart + " " + base64PartChecksum);
                }

                String base64CalculatedChecksumOfChecksums =
 Base64.getEncoder().encodeToString(sha256ChecksumOfChecksums.digest());
                System.out.println(base64CalculatedChecksumOfChecksums);
                System.out.println(objectAttributes.checksum().checksumSHA256());
                if (!
base64CalculatedChecksumOfChecksums.equals(objectAttributes.checksum().checksumSHA256()))
 {
                    throw new IOException("Full object checksum of checksums don't
 match S3");
                }

            } catch (IOException | NoSuchAlgorithmException e) {
                e.printStackTrace();
            }
        }
    }
```

Uso da API REST

Você pode enviar solicitações REST para carregar um objeto com um valor de soma de verificação para verificar a integridade dos dados com PutObject. Você também pode recuperar o valor da soma de verificação para objetos usando GetObject ou HeadObject.

Como usar o AWS CLI

Você pode enviar uma solicitação PUT para carregar um objeto de até 5 GB em uma única operação. Para obter mais informações, consulte `PutObject` na Referência de comando da AWS CLI. Você também pode usar `get-object` e `head-object` para recuperar a soma de verificação de um objeto já carregado a fim de verificar a integridade dos dados.

Para obter informações, consulte Amazon S3 CLI FAQ no Guia do usuário da AWS Command Line Interface.

Usar Content-MD5 ao carregar objetos

Outra maneira de verificar a integridade do objeto após o carregamento é fornecer um resumo MD5 do objeto quando você o carrega. Se você calcular o resumo MD5 para seu objeto, poderá fornecê-lo com o comando PUT usando o cabeçalho `Content-MD5`.

Após o carregamento do objeto, o Amazon S3 calcula o resumo MD5 do objeto e o compara com o valor que você forneceu. A solicitação só será bem-sucedida se os dois resumos corresponderem.

Não é necessário fornecer um resumo MD5, mas você pode usá-lo para verificar a integridade do objeto como parte do processo de carregamento.

Usar Content-MD5 e a ETag para verificar objetos carregados

A etiqueta de entidade (ETag) de um objeto representa uma versão específica dele. Lembre-se de que a ETag reflete apenas as alterações no conteúdo de um objeto, não as alterações nos metadados dele. Se apenas os metadados de um objeto forem alterados, a ETag permanecerá a mesma.

Dependendo do objeto, a ETag do objeto pode ser um resumo MD5 dos dados do objeto:

- Se um objeto for criado pela operação `PutObject`, `PostObject` ou `CopyObject`, ou por meio do AWS Management Console, e ele também for em texto simples ou criptografado no lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3), ele terá uma ETag que é um resumo MD5 dos respectivos dados.
- Se um objeto for criado pela operação `PutObject`, `PostObject` ou `CopyObject`, ou por meio do AWS Management Console, e for criptografado no lado do servidor com chaves fornecidas pelo cliente (SSE-C) ou com criptografia no lado do servidor com chaves AWS Key Management Service(AWS KMS) (SSE-KMS), ele terá uma ETag que não é um resumo MD5 dos respectivos dados.
- Se um objeto for criado pelo processo de carregamento fracionado ou pela operação `UploadPartCopy`, a respectiva ETag não será um resumo MD5, independentemente do método de criptografia. Se um objeto for maior que 16 MB, o AWS Management Console o carregará ou copiará como carregamento fracionado e, por isso, a ETag não será um resumo MD5.

Para objetos em que a ETag é o resumo `Content-MD5` do objeto, você pode comparar o valor da ETag do objeto com um resumo `Content-MD5` calculado ou armazenado anteriormente.

Usar somas de verificação à direita

Ao fazer upload de objetos no Amazon S3, você pode fornecer uma soma de verificação pré-calculada para o objeto ou usar um AWS SDK para criar automaticamente somas de verificação finais para uploads fragmentados em seu nome. Se você usar uma soma de verificação final, o Amazon S3 gerará automaticamente a soma de verificação usando o algoritmo especificado para validar a integridade do objeto nos uploads fragmentados, quando você fizer upload de um objeto.

Para criar uma soma de verificação à direita ao usar um AWS SDK, preencha o parâmetro `ChecksumAlgorithm` com seu algoritmo preferido. O SDK usa esse algoritmo para calcular a soma de verificação do objeto (ou das partes do objeto) e a anexa automaticamente ao final da solicitação de upload fragmentado. Esse comportamento economiza tempo porque o Amazon S3 executa a verificação e o carregamento de seus dados em uma única passagem.

> **Important**
>
> Se estiver usando o S3 Object Lambda, todas as solicitações ao S3 Object Lambda serão assinadas usando `s3-object-lambda` em vez de `s3`. Esse comportamento afeta a assinatura dos valores de soma de verificação à direita. Para obter mais informações sobre o S3 Object Lambda, consulte Transformar objetos com o S3 Object Lambda.

Cabeçalhos de soma de verificação final

Para fazer uma solicitação de codificação de conteúdo fragmentado, o Amazon S3 exige que os clientes incluam vários cabeçalhos para analisar corretamente a solicitação. Os clientes devem incluir os seguintes cabeçalhos:

- **`x-amz-decoded-content-length`**: esse cabeçalho indica o tamanho em texto simples dos dados reais que estão sendo carregados no Amazon S3 com a solicitação.
- **`x-amz-content-sha256`**: esse cabeçalho indica o tipo de upload fragmentado incluído na solicitação. Para uploads fragmentados com somas de verificação finais, o valor do cabeçalho é `STREAMING-UNSIGNED-PAYLOAD-TRAILER` para solicitações que não usam assinatura de carga útil e `STREAMING-AWS4-HMAC-SHA256-PAYLOAD-TRAILER` para solicitações que usam assinatura de carga útil SigV4. (Para ter mais informações sobre a implementação de cargas úteis assinadas, consulte Signature calculations for the authorization header: Transferring a payload in multiple chunks.)

- **`x-amz-trailer`**: esse cabeçalho indica o nome do cabeçalho final na solicitação. Se existirem somas de verificação finais (em que os AWS SDKs anexam somas de verificação aos corpos de solicitações codificadas), o valor do cabeçalho `x-amz-trailer` inclui o prefixo `x-amz-checksum-` e termina com o nome do algoritmo. No momento, os seguintes valores de `x-amz-trailer` são compatíveis:
  - `x-amz-checksum-crc32`
  - `x-amz-checksum-crc32c`
  - `x-amz-checksum-crc64nvme`
  - `x-amz-checksum-sha1`
  - `x-amz-checksum-sha256`

> **Note**
>
> Você também pode incluir o cabeçalho `Content-Encoding`, com o valor fragmentado, na solicitação. Embora esse cabeçalho não seja obrigatório, incluí-lo pode minimizar os problemas de proxy HTTP ao transmitir dados codificados. Se outro cabeçalho `Content-Encoding` (como gzip) existir na solicitação, o cabeçalho `Content-Encoding` incluirá o valor fragmentado em uma lista de codificações separadas por vírgulas. Por exemplo, .`Content-Encoding: aws-chunked, gzip`

Partes fragmentadas

Quando você faz upload de um objeto para o Amazon S3 usando codificação fragmentada, a solicitação de upload inclui os seguintes tipos de fragmentos (formatados na ordem listada):

- Fragmentos de corpo de objeto: pode haver um, vários ou nenhum fragmento de corpo associado a uma solicitação de upload fragmentado.
- Fragmentos de conclusão: pode haver um, vários ou nenhum fragmento de corpo associado a uma solicitação de upload fragmentado.
- Fragmentos finais: a soma de verificação final é listada após o fragmento de conclusão. Só é permitido um fragmento final.

> **Note**
>
> Cada upload fragmentado deve terminar com um CRLF final (como `\r\n`) para indicar o fim da solicitação.

Para conferir exemplos de formatação fragmentada, consulte Exemplos: uploads fragmentados com somas de verificação finais.

Fragmentos de corpo de objeto

Os fragmentos de corpo de objeto são os fragmentos que contêm os dados reais do objeto que estão sendo carregados no S3. Esses fragmentos têm restrições consistentes de tamanho e formato.

Tamanho do fragmento de corpo de objeto

Esses fragmentos devem conter pelo menos 8.192 bytes (ou 8 KiB) de dados do objeto, exceto o fragmento final do corpo, que pode ser menor. Não há um tamanho máximo explícito para os fragmentos, mas todos serão menores do que o tamanho máximo de upload de 5 GB. Os tamanhos dos fragmentos podem variar de um para o outro com base na implementação do servidor cliente.

Formato do fragmento de corpo de objeto

Os fragmentos de corpo de objeto começam com a codificação hexadecimal do número de bytes no fragmento de corpo de objeto, seguidos por um CRLF (Carriage Return Line Feed), os bytes do objeto desse fragmento e outro CRLF.

Por exemplo:

```
hex-encoding-of-object-bytes-in-chunk\r\n
chunk-object-bytes\r\n
```

No entanto, quando o fragmento é assinado, o fragmento de corpo de objeto segue um formato diferente, em que a assinatura é anexada ao tamanho do fragmento com um delimitador de ponto e vírgula. Por exemplo:

```
hex-encoding-of-object-bytes-in-chunk;chunk-signature\r\n
 chunk-object-bytes\r\n
```

Para ter mais informações sobre a assinatura de fragmentos, consulte Signature calculations for the Authorization Header: Transferring a payload in multiple chunks (AWS Signature Version 4). Para ter

mais informações sobre a formatação de fragmentos, consulte Chunked transfer encoding no site do RFC Editor.

Fragmentos de conclusão

É necessário que os fragmentos de conclusão sejam o último fragmento de corpo de objeto de cada upload fragmentado. O formato de um fragmento de conclusão é semelhante ao de um fragmento de corpo, mas sempre contém zero byte de dados do objeto. (O valor de zero byte de dados do objeto indica que todos os dados foram carregados.) Os uploads fragmentados devem incluir um fragmento de conclusão como último fragmento de corpo de objeto, seguindo um formato como este:

```
0\r\n
```

No entanto, se a solicitação de codificação de conteúdo usar assinatura de carga útil, o formato será o seguinte:

```
0;chunk-signature\r\n
```

Fragmentos finalizadores

Os fragmentos finalizadores contêm a soma de verificação calculada para todas as solicitações de upload do S3. Os fragmentos finalizadores incluem dois campos: um campo de nome de cabeçalho e um campo de valor de cabeçalho. O campo de nome de cabeçalho de uma solicitação de upload deve corresponder ao valor enviado no cabeçalho da solicitação `x-amz-trailer`. Por exemplo, se uma solicitação contiver `x-amz-trailer: x-amz-checksum-crc32` e o fragmento finalizador tiver o nome de cabeçalho `x-amz-checksum-sha1`, a solicitação falhará. O campo de valor no fragmento finalizador inclui uma codificação base64 do valor de soma de verificação big-endian desse objeto. (A ordenação big-endian armazena o byte de dados mais significativo no endereço de memória mais baixo e o byte menos significativo no maior endereço de memória.) O algoritmo usado para calcular essa soma de verificação é o mesmo que o sufixo do nome de cabeçalho (por exemplo, `crc32`).

Formato do fragmento finalizador

Os fragmentos finalizadores usam o seguinte formato para solicitações de carga útil não assinadas:

```
x-amz-checksum-lowercase-checksum-algorithm-name:base64-checksum-value\n\r\n\r\n
```

Para solicitações com cargas úteis assinadas com SigV4, o fragmento finalizador inclui uma assinatura finalizadora após o fragmento.

```
trailer-checksum\n\r\n
trailer-signature\r\n
```

Você também pode adicionar o CRLF diretamente ao final do valor de soma de verificação base64. Por exemplo:

```
x-amz-checksum-lowercase-checksum-algorithm-name:base64-checksum-value\r\n\r\n
```

Exemplos: uploads fragmentados com somas de verificação finais

O Amazon S3 oferece suporte a uploads fragmentados que usam codificação de conteúdo `aws-chunked` para solicitações `PutObject` e `UploadPart` com somas de verificação finais.

Example 1: solicitação **`PutObject`** fragmentada não assinada com uma soma de verificação final CRC-32

Veja a seguir um exemplo de uma solicitação `PutObject` fragmentada com uma soma de verificação final CRC-32. Nesse exemplo, o cliente faz upload de um objeto de 17 KB em três fragmentos não assinados e acrescenta um fragmento de soma de verificação final CRC-32 usando o cabeçalho `x-amz-checksum-crc32`.

```
PUT /Key+ HTTP/1.1
Host: amzn-s3-demo-bucket
Content-Encoding: aws-chunked
x-amz-decoded-content-length: 17408
x-amz-content-sha256: STREAMING-UNSIGNED-PAYLOAD-TRAILER
x-amz-trailer: x-amz-checksum-crc32

2000\r\n                                    // Object body chunk 1 (8192 bytes)
object-bytes\r\n
2000\r\n                                    // Object body chunk 2 (8192 bytes)
object-bytes\r\n
400\r\n                                     // Object body chunk 3 (1024 bytes)
object-bytes\r\n
0\r\n                                       // Completion chunk
x-amz-checksum-crc32:YABb/g==\n\r\n\r\n     // Trailer chunk (note optional \n
 character)
\r\n                                          // CRLF
```

Veja aqui um exemplo de resposta:

```
HTTP/1.1 200
ETag: ETag
x-amz-checksum-crc32: YABb/g==
```

> **Note**
>
> O uso da quebra de linha \n no final do valor da soma de verificação pode variar entre os clientes.

Example 2: solicitação **`PutObject`** fragmentada assinada com SigV4 com uma soma de verificação final CRC-32 (**`CRC32`**)

Veja a seguir um exemplo de uma solicitação `PutObject` fragmentada com uma soma de verificação final CRC-32. Essa solicitação usa a assinatura de carga útil SigV4. Nesse exemplo, o cliente faz upload de um objeto de 17 KB em três fragmentos assinados. Além dos fragmentos `object body`, o `completion chunk` e o `trailer chunk` também são assinados.

```
PUT /Key+ HTTP/1.1
Host: amzn-s3-demo-bucket.s3.amazonaws.com
Content-Encoding: aws-chunked
x-amz-decoded-content-length: 17408
x-amz-content-sha256: STREAMING-AWS4-HMAC-SHA256-PAYLOAD-TRAILER
x-amz-trailer: x-amz-checksum-crc32

authorization-code                              // SigV4 headers authorization

2000;chunk-signature=signature-value...\r\n   // Object body chunk 1 (8192 bytes)
object-bytes\r\n
2000;chunk-signature\r\n                        // Object body chunk 2 (8192 bytes)
object-bytes\r\n
400;chunk-signature\r\n                         // Object body chunk 3 (1024 bytes)
object-bytes\r\n
0;chunk-signature\r\n                           // Completion chunk
x-amz-checksum-crc32:YABb/g==\n\r\n             // Trailer chunk (note optional \n
 character)
trailer-signature\r\n
\r\n                                            // CRLF
```

Veja aqui um exemplo de resposta:

```
HTTP/1.1 200
ETag: ETag
x-amz-checksum-crc32: YABb/g==
```

Excluir objetos do Amazon S3

Você pode excluir um ou mais objetos diretamente do Amazon S3 usando o console do Amazon S3, os AWS SDKs, a AWS Command Line Interface (AWS CLI) ou a API REST. Se estiver coletando arquivos de log, por exemplo, é uma boa ideia excluí-los quando eles não forem mais necessários. É possível configurar uma regra do Ciclo de Vida do S3 para excluir automaticamente determinados objetos, como arquivos de log.

Para excluir um objeto, você pode usar uma das seguintes operações de API:

- Excluir um único objeto: o Amazon S3 fornece a operação de API `DELETE` (`DeleteObject`) que pode ser usada para excluir um objeto em uma única solicitação HTTP.
- Excluir vários objetos: o Amazon S3 fornece a operação de API para exclusão de vários objetos (`DeleteObjects`) que pode ser usada para excluir até 1.000 objetos em uma única solicitação HTTP.

Ao excluir objetos de um bucket sem o versionamento habilitado, você fornece apenas o nome da chave de objeto. No entanto, ao excluir objetos de um bucket com o versionamento habilitado, você pode fornecer o ID da versão do objeto para excluir uma versão específica dele.

Práticas recomendadas a serem consideradas antes de excluir um objeto

Antes de excluir um objeto, considere as seguintes práticas recomendadas:

- Habilite o versionamento do bucket. O Versionamento do S3 adiciona proteção contra solicitações `DeleteObject` simples para evitar exclusões acidentais. Para buckets com versionamento, se você excluir a versão atual de um objeto ou quando uma solicitação de exclusão não especificar um ID de versão específico, o Amazon S3 não excluirá permanentemente o objeto. Em vez disso, o S3 adiciona um marcador de exclusão, emitindo uma exclusão temporária do objeto. O marcador de exclusão então se torna a versão atual (ou a mais recente) do objeto com um novo ID de versão. Consulte mais informações em Deleting object versions from a versioning-enabled bucket.
- Se você quiser excluir um grande número de objetos ou excluir objetos de forma programática com base na respectiva data de criação, defina uma configuração do Ciclo de Vida do S3

no bucket. Para monitorar essas exclusões, recomendamos que você use uma notificação de evento do Ciclo de Vida do S3. Quando você configura as notificações do Ciclo de Vida do S3, o tipo de evento `s3:LifecycleExpiration:Delete` notifica você quando um objeto em um bucket é excluído. Ele também notifica quando uma versão de objeto é excluída permanentemente por uma configuração do S3 Lifecycle. O tipo de evento `s3:LifecycleExpiration:DeleteMarkerCreated` notifica você quando o Ciclo de Vida do S3 cria um marcador de exclusão. Um marcador de exclusão é criado quando uma versão atual de um objeto em um bucket com versionamento é excluída.

- Antes de fazer qualquer atualização na configuração do Ciclo de Vida do S3, confirme se ele concluiu as ações em todos os objetos pretendidos. Consulte mais informações na seção Atualizar, desabilitar ou excluir regras de ciclo de vida em Definir uma configuração de ciclo de vida em um bucket.

  > **Note**
  >
  > As regras do Ciclo de Vida do S3 devem ser aplicadas ao subconjunto correto de objetos para evitar exclusões indesejadas. Você pode filtrar objetos por prefixos, tags de objeto ou tamanhos de objeto ao criar as regras de ciclo de vida.

- Considere impedir que os usuários removam ou excluam objetos do bucket. Para restringir os usuários, você precisará negar explicitamente as permissões para as seguintes ações nas políticas de bucket do Amazon S3:
  - `s3:DeleteObject`, `s3:DeleteObjectVersion` (para controlar quem pode excluir objetos usando solicitações de API)
  - `s3:PutLifecycleConfiguration` (para controlar quem pode adicionar as regras de expiração do Ciclo de Vida do S3)
- Considere usar o recurso Replicação do S3 para criar várias cópias de seus dados e replicá-los em vários locais ao mesmo tempo. Você pode escolher quantos buckets de destino forem necessários. Além disso, se um objeto for excluído acidentalmente, você ainda terá uma cópia dos dados.

Excluir objetos de um bucket com versionamento habilitado

Se o bucket tiver o versionamento habilitado, várias versões do mesmo objeto poderão existir no bucket. Ao trabalhar com buckets com versionamento habilitado, as operações de API `Delete` permitem as seguintes opções:

- Especificar uma solicitação de exclusão não versionada: especifique somente a chave do objeto, e não o ID de versão. Nesse caso, o Amazon S3 cria um marcador de exclusão sobre a versão atual do objeto e retorna o ID de versão na resposta. Isso faz com que o objeto desapareça do bucket. Para obter informações sobre versionamento de objetos e sobre o conceito de marcador de exclusão, consulte Reter várias versões de objetos com o Versionamento do S3.
- Especificar uma solicitação de exclusão com versionamento: especifique a chave e o ID da versão. Nesse caso, os seguintes resultados são possíveis:
  - Se o ID de versão for mapeado para uma versão de objeto específica, o Amazon S3 excluirá versão específica do objeto.
  - Se o ID de versão for mapeado para o marcador de exclusão de um objeto, o Amazon S3 excluirá o marcador de exclusão. Quando o marcador de exclusão é excluído, o objeto reaparece no bucket.

Excluir objetos de um bucket com versionamento suspenso

Se o bucket estiver com versionamento suspenso, as operações de API `Delete` se comportarão da mesma forma para buckets com versionamento habilitado (exceto quando a versão atual tiver um ID de versão nulo). Para obter mais informações, consulte Excluir objetos de buckets com versionamento suspenso.

Excluir objetos de um bucket sem versionamento

Se o bucket não tiver versionamento, será possível especificar a chave do objeto nas operações de API `Delete`, e o Amazon S3 excluirá permanentemente o objeto. Para evitar a exclusão permanente de um objeto, habilite o versionamento do bucket.

Excluir objetos de um bucket com MFA habilitada

Ao excluir objetos de um bucket habilitado para autenticação multifator (MFA, Multi-Factor Authentication), observe:

- Se você fornecer um token de MFA inválido, a solicitação falhará sempre.
- Se você tiver um bucket habilitado para MFA e fizer uma solicitação de exclusão em versões (fornecendo uma chave de objeto e um ID de versão), a solicitação falhará se você não fornecer um token de MFA válido. Além disso, ao usar a operação de API `Delete` de vários objetos em um bucket com MFA habilitada, se alguma exclusão for uma solicitação de exclusão com

versionamento (se você especificar uma chave de objeto e um ID de versão), a solicitação inteira falhará se o token de MFA não for fornecido.

No entanto, nos seguintes casos a solicitação é bem-sucedida:

- Se você tiver um bucket habilitado para MFA, fizer uma solicitação de exclusão não versionada (sem excluir um objeto versionado) e não fornecer um token de MFA, a exclusão será concluída.
- Se você tiver uma solicitação de exclusão de vários objetos que especifica somente objetos não versionados a serem excluídos de um bucket habilitado para MFA e não fornecer um token de MFA, as exclusões serão feitas com êxito.

Para obter informações sobre a exclusão de MFA, consulte Configurando a exclusão de MFA.

Tópicos

- Excluir um único objeto
- Excluir vários objetos

Excluir um único objeto

Você pode usar o console do Amazon S3 ou a API DELETE para excluir um único objeto existente de um bucket do S3. Para obter mais informações sobre como excluir objetos no Amazon S3, consulte Excluir objetos do Amazon S3.

Como todos os objetos em seu bucket do S3 incorrem em custos de armazenamento, você deve excluir os objetos de que não precisa mais. Por exemplo, se estiver coletando arquivos de log, é uma boa ideia excluí-los quando não forem mais necessários. Você pode definir uma regra de ciclo de vida para excluir automaticamente objetos como arquivos de log. Para obter mais informações, consulte the section called “Definir a configuração do ciclo de vida”.

Para obter informações sobre os recursos e a definição de preço do Amazon S3, consulte a definição de preço do Amazon S3.

Uso do console do S3

Siga as etapas a seguir para usar o console do Amazon S3 a fim de excluir um único objeto de um bucket.

> **Warning**
>
> Quando você excluir permanentemente um objeto ou uma versão especificada do objeto no console do Amazon S3, a exclusão não poderá ser desfeita.

Como excluir um objeto com versionamento habilitado ou suspenso

> **Note**
>
> Se o ID da versão de um objeto em um bucket com versionamento suspenso estiver marcado como NULL, o S3 excluirá permanentemente o objeto, pois não existirão versões anteriores. No entanto, se um ID de versão válido estiver listado para o objeto em um bucket com versionamento suspenso, o S3 criará um marcador de exclusão para o objeto excluído, mantendo as versões anteriores do objeto.

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets de uso geral ou Buckets de diretórios.
3. Na lista de buckets, escolha o nome do bucket do qual deseja excluir um objeto.
4. Selecione o objeto e escolha Excluir.
5. Para confirmar a exclusão da lista de objetos em Objetos especificados, insira **`delete`** na caixa de texto Excluir objetos?.

Como excluir permanente uma versão específica do objeto em um bucket habilitado para versionamento

> **Warning**
>
> Quando você excluir permanentemente uma versão específica do objeto no Amazon S3, a exclusão não poderá ser desfeita.

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.

2. Na lista Bucket name (Nome do bucket), escolha o nome do bucket do qual você deseja excluir um objeto.
3. Selecione o objeto que deseja excluir.
4. Escolha a opção Mostrar versões.
5. Selecione a versão do objeto e escolha Excluir.
6. Para confirmar a exclusão permanente das versões específicas do objeto em Objetos especificados, insira Excluir permanentemente na caixa de texto Excluir objetos?. O Amazon S3 excluirá permanentemente a versão específica do objeto.

Como excluir permanentemente um objeto de um bucket do Amazon S3 que não tenha o versionamento habilitado

> **Warning**
>
> Quando você excluir permanentemente um objeto no Amazon S3, a exclusão não poderá ser desfeita. Além disso, as exclusões são permanentes para todos os buckets que não tenham o versionamento habilitado.

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets de uso geral.
3. Na lista de buckets, escolha o nome do bucket do qual deseja excluir um objeto.
4. Selecione o objeto e escolha Excluir.
5. Para confirmar a exclusão permanente do objeto listado em Objetos especificados, insira Excluir permanentemente na caixa de texto Excluir objetos?.

> **Note**
>
> Se você enfrentar problemas ao excluir um objeto, consulte Quero excluir permanentemente objetos com versionamento.

Usar a AWS CLI

Para excluir um objeto por solicitação, use a API `DELETE`. Para obter mais informações, consulte DELETE Object. Para obter mais informações sobre como usar a CLI para excluir um objeto, consulte delete-object.

Uso dos REST API

Você pode usar os AWS SDKs para excluir um objeto. Contudo, se o seu aplicativo exigir, você pode enviar solicitações REST diretamente. Para obter mais informações, consulte DELETE Object na Referência de APIs do Amazon Simple Storage Service.

Uso da SDKs AWS

Os exemplos a seguir mostram como você pode usar os AWS SDKs para excluir um objeto de um bucket. Para obter mais informações, acesse DELETE Object na Referência de APIs do Amazon Simple Storage Service.

Se tiver habilitado o versionamento do S3 no bucket, você terá as seguintes opções:

- Excluir uma versão específica do objeto ao especificar um ID de versão.
- Excluir um objeto sem especificar um ID de versão, caso em que o Amazon S3 adicionará um marcador de exclusão para o objeto.

Para obter mais informações sobre o S3 Versioning, consulte Reter várias versões de objetos com o Versionamento do S3.

Para obter mais exemplos e exemplos em outras linguagens, consulte Use `DeleteObject` with an AWS SDK or CLI na Referência de API do Amazon S3.

Java

Example Exemplo 1: Excluir um objeto (bucket sem versionamento)

O exemplo a seguir pressupõe que o bucket não esteja habilitado para versionamento e o objeto não tenha IDs de versão. Na solicitação de exclusão, especifique somente a chave do objeto e não um ID de versão.

Consulte instruções sobre como criar e testar uma amostra funcional em Getting Started no Guia do desenvolvedor do AWS SDK para Java.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.DeleteObjectRequest;

import java.io.IOException;

public class DeleteObjectNonVersionedBucket {

    public static void main(String[] args) throws IOException {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "*** Bucket name ***";
        String keyName = "*** Key name ****";

        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(clientRegion)
                    .build();

            s3Client.deleteObject(new DeleteObjectRequest(bucketName, keyName));
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Example Exemplo 2: excluir um objeto (bucket com versionamento)

O exemplo a seguir exclui um objeto de um bucket com versionamento. O exemplo exclui uma versão específica do objeto ao especificar o nome da chave e o ID de versão do objeto.

O exemplo faz o seguinte:

1. Adiciona um objeto de exemplo ao bucket. O Amazon S3 retorna o ID de versão do objeto recém-adicionado. O exemplo usa esse ID de versão na solicitação de exclusão.
2. Exclui a versão do objeto ao especificar o nome da chave e um ID de versão do objeto. Se não houver nenhuma outra versão do objeto, o Amazon S3 excluirá o objeto totalmente. Caso contrário, o Amazon S3 excluirá somente a versão especificada.

> **Note**
>
> Você pode obter os IDs de versão de um objeto enviando uma solicitação `ListVersions`.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.BucketVersioningConfiguration;
import com.amazonaws.services.s3.model.DeleteVersionRequest;
import com.amazonaws.services.s3.model.PutObjectResult;

import java.io.IOException;

public class DeleteObjectVersionEnabledBucket {

    public static void main(String[] args) throws IOException {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "*** Bucket name ***";
        String keyName = "*** Key name ****";

        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(clientRegion)
                    .build();

            // Check to ensure that the bucket is versioning-enabled.
            String bucketVersionStatus =
 s3Client.getBucketVersioningConfiguration(bucketName).getStatus();
```

```
            if (!bucketVersionStatus.equals(BucketVersioningConfiguration.ENABLED))
{
                System.out.printf("Bucket %s is not versioning-enabled.",
bucketName);
            } else {
                // Add an object.
                PutObjectResult putResult = s3Client.putObject(bucketName, keyName,
                        "Sample content for deletion example.");
                System.out.printf("Object %s added to bucket %s\n", keyName,
bucketName);

                // Delete the version of the object that we just created.
                System.out.println("Deleting versioned object " + keyName);
                s3Client.deleteVersion(new DeleteVersionRequest(bucketName, keyName,
putResult.getVersionId()));
                System.out.printf("Object %s, version %s deleted\n", keyName,
putResult.getVersionId());
            }
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

.NET

Os exemplos a seguir mostram como excluir um objeto de buckets com e sem versionamento. Para obter mais informações sobre o S3 Versioning, consulte Reter várias versões de objetos com o Versionamento do S3.

Example Excluir um objeto de um bucket sem versionamento

O exemplo do C# a seguir exclui um objeto de um bucket sem versionamento. O exemplo pressupõe que os objetos não têm IDs de versão, portanto, você não especifica IDs de versão. Especifique somente a chave do objeto.

Para obter informações sobre como configurar e executar exemplos de código, consulte Conceitos básicos do AWS SDK for .NET no Guia do desenvolvedor do AWS SDK for .NET.

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class DeleteObjectNonVersionedBucketTest
    {
        private const string bucketName = "*** bucket name ***";
        private const string keyName = "*** object key ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 client;

        public static void Main()
        {
            client = new AmazonS3Client(bucketRegion);
            DeleteObjectNonVersionedBucketAsync().Wait();
        }
        private static async Task DeleteObjectNonVersionedBucketAsync()
        {
            try
            {
                var deleteObjectRequest = new DeleteObjectRequest
                {
                    BucketName = bucketName,
                    Key = keyName
                };

                Console.WriteLine("Deleting an object");
                await client.DeleteObjectAsync(deleteObjectRequest);
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered on server. Message:'{0}' when
 deleting an object", e.Message);
            }
```

```
            catch (Exception e)
            {
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
 deleting an object", e.Message);
            }
        }
    }
}
```

Example Excluir um objeto de um bucket com versionamento

O exemplo do C# a seguir exclui um objeto de um bucket com versionamento. Ele exclui uma versão específica do objeto ao especificar o nome da chave e o ID de versão do objeto.

O código realiza as seguintes tarefas:

1. Permite o versionamento do S3 no bucket que você especificar (se o versionamento do S3 já estiver habilitado, isso não terá efeito).
2. Adiciona um objeto de exemplo ao bucket. Em resposta, o Amazon S3 retorna o ID de versão do objeto recém-adicionado. O exemplo usa esse ID de versão na solicitação de exclusão.
3. Exclui o objeto de exemplo ao especificar o nome da chave e um ID de versão do objeto.

> **Note**
>
> Você também pode obter o ID de versão de um objeto enviando uma solicitação `ListVersions`.
>
> ```
> var listResponse = client.ListVersions(new ListVersionsRequest { BucketName
>  = bucketName, Prefix = keyName });
> ```

Para obter informações sobre como configurar e executar exemplos de código, consulte Conceitos básicos do AWS SDK for .NET no Guia do desenvolvedor do AWS SDK for .NET.

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Threading.Tasks;
```

```
namespace Amazon.DocSamples.S3
{
    class DeleteObjectVersion
    {
        private const string bucketName = "*** versioning-enabled bucket name ***";
        private const string keyName = "*** Object Key Name ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 client;

        public static void Main()
        {
            client = new AmazonS3Client(bucketRegion);
            CreateAndDeleteObjectVersionAsync().Wait();
        }

        private static async Task CreateAndDeleteObjectVersionAsync()
        {
            try
            {
                // Add a sample object.
                string versionID = await PutAnObject(keyName);

                // Delete the object by specifying an object key and a version ID.
                DeleteObjectRequest request = new DeleteObjectRequest
                {
                    BucketName = bucketName,
                    Key = keyName,
                    VersionId = versionID
                };
                Console.WriteLine("Deleting an object");
                await client.DeleteObjectAsync(request);
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered on server. Message:'{0}' when
 deleting an object", e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
 deleting an object", e.Message);
            }
```

```
        }

        static async Task<string> PutAnObject(string objectKey)
        {
            PutObjectRequest request = new PutObjectRequest
            {
                BucketName = bucketName,
                Key = objectKey,
                ContentBody = "This is the content body!"
            };
            PutObjectResponse response = await client.PutObjectAsync(request);
            return response.VersionId;
        }
    }
}
```

PHP

Este exemplo mostra como usar classes da versão 3 do AWS SDK para PHP para excluir um objeto de um bucket sem versionamento. Para obter informações sobre como excluir um objeto de um bucket com versões, consulte Uso dos REST API.

Para obter mais informações sobre a API do AWS SDK for Ruby, acesse AWS SDK for Ruby Version 2.

O exemplo de PHP a seguir exclui um objeto de um bucket. Como esse exemplo mostra como excluir objetos de bucket sem versionamento, ele oferece apenas o nome do bucket e a chave do objeto (não um ID de versão) na solicitação de exclusão.

```
<?php

require 'vendor/autoload.php';

use Aws\S3\S3Client;
use Aws\S3\Exception\S3Exception;

$bucket = '*** Your Bucket Name ***';
$keyname = '*** Your Object Key ***';

$s3 = new S3Client([
    'version' => 'latest',
    'region'  => 'us-east-1'
]);
```

```
// 1. Delete the object from the bucket.
try
{
    echo 'Attempting to delete ' . $keyname . '...' . PHP_EOL;

    $result = $s3->deleteObject([
        'Bucket' => $bucket,
        'Key'    => $keyname
    ]);

    if ($result['DeleteMarker'])
    {
        echo $keyname . ' was deleted or does not exist.' . PHP_EOL;
    } else {
        exit('Error: ' . $keyname . ' was not deleted.' . PHP_EOL);
    }
}
catch (S3Exception $e) {
    exit('Error: ' . $e->getAwsErrorMessage() . PHP_EOL);
}

// 2. Check to see if the object was deleted.
try
{
    echo 'Checking to see if ' . $keyname . ' still exists...' . PHP_EOL;

    $result = $s3->getObject([
        'Bucket' => $bucket,
        'Key'    => $keyname
    ]);

    echo 'Error: ' . $keyname . ' still exists.';
}
catch (S3Exception $e) {
    exit($e->getAwsErrorMessage());
}
```

Javascript

```
import { DeleteObjectCommand } from "@aws-sdk/client-s3";
import { s3Client } from "./libs/s3Client.js" // Helper function that creates Amazon
 S3 service client module.
```

```
export const bucketParams = { Bucket: "BUCKET_NAME", Key: "KEY" };

export const run = async () => {
  try {
    const data = await s3Client.send(new DeleteObjectCommand(bucketParams));
    console.log("Success. Object deleted.", data);
    return data; // For unit tests.
  } catch (err) {
    console.log("Error", err);
  }
};
run();
```

Excluir vários objetos

Como todos os objetos em seu bucket do S3 incorrem em custos de armazenamento, você deve excluir os objetos de que não precisa mais. Por exemplo, se estiver coletando arquivos de log, é uma boa ideia excluí-los quando não forem mais necessários. Você pode definir uma regra de ciclo de vida para excluir automaticamente objetos como arquivos de log. Para obter mais informações, consulte the section called “Definir a configuração do ciclo de vida”.

Para obter informações sobre os recursos e a definição de preço do Amazon S3, consulte a definição de preço do Amazon S3.

É possível usar o console do Amazon S3, AWS SDKs ou a API REST para excluir simultaneamente vários objetos de um bucket do S3.

Usar o console do S3

Siga etapas a seguir para usar o console do Amazon S3 a fim de excluir vários objetos de um bucket.

⚠ Warning

- A exclusão de um objeto especificado não pode ser desfeita.
- Essa ação exclui todos os objetos especificados. Ao excluir pastas, aguarde a conclusão da ação de exclusão antes de adicionar objetos novos à pasta. Caso contrário, os objetos novos também podem ser excluídos.
- Ao excluir objetos de um bucket sem o versionamento habilitado, inclusive buckets de diretório, o Amazon S3 exclui permanentemente os objetos.

- Ao excluir objetos em um bucket com o versionamento de buckets habilitado ou suspenso, o Amazon S3 cria marcadores de exclusão. Para obter mais informações, consulte Trabalhar com marcadores de exclusão.

Como excluir objetos que têm versionamento habilitado ou suspenso

> **Note**
>
> Se os IDs da versão do objeto em um bucket com versionamento suspenso estiverem marcados como NULL, o S3 excluirá permanentemente os objetos, já que não há versões anteriores. No entanto, se um ID de versão válido estiver listado para os objetos em um bucket com versionamento suspenso, o S3 criará marcadores de exclusão para os objetos excluídos, mantendo as versões anteriores dos objetos.

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets de uso geral.
3. Na lista de buckets, escolha o nome do bucket do qual você deseja excluir objetos.
4. Selecione os objetos e escolha Excluir.
5. Para confirmar a exclusão da lista de objetos em Objetos especificados, insira **`delete`** na caixa de texto Excluir objetos?.

Como excluir permanente versões específicas de objetos em um bucket habilitado para versionamento

> **Warning**
>
> Quando você excluir permanentemente versões específicas de objetos no Amazon S3, a exclusão não poderá ser desfeita.

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets de uso geral.

3. Na lista de buckets, escolha o nome do bucket do qual você deseja excluir objetos.
4. Selecione os objetos do que deseja excluir.
5. Escolha a opção Mostrar versões.
6. Selecione as versões de objetos e escolha Excluir.
7. Para confirmar a exclusão permanente das versões específicas do objeto em Objetos especificados, insira Excluir permanentemente na caixa de texto Excluir objetos?. O Amazon S3 exclui permanentemente as versões específicas de objetos.

Como excluir permanentemente os objetos em um bucket do Amazon S3 que não tenham o versionamento habilitado

> **Warning**
>
> Quando você excluir permanentemente um objeto no Amazon S3, a exclusão não poderá ser desfeita. Além disso, as exclusões são permanentes para todos os buckets que não tenham o versionamento habilitado, inclusive buckets de diretório.

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets de uso geral ou Buckets de diretórios.
3. Na lista de buckets, escolha o nome do bucket do qual você deseja excluir objetos.
4. Selecione os objetos e escolha Excluir.
5. Para confirmar a exclusão permanente dos objetos listados em Objetos especificados, insira excluir permanentemente na caixa de texto Excluir objetos?.

> **Note**
>
> Se você enfrentar problemas ao excluir os objetos, consulte Quero excluir permanentemente objetos com versionamento.

Uso da SDKs AWS

Consulte exemplos de como excluir vários objetos com os SDKs da AWS em Code examples na Referência de API do Amazon S3.

Consulte informações gerais sobre como usar diferentes SDKs da AWS em Developing with Amazon S3 using the AWS SDKs na Referência de API do Amazon S3.

Uso da API REST

Você pode usar os AWS SDKs para excluir vários objetos usando a API Multi-Object Delete. Contudo, se o seu aplicativo exigir, você pode enviar solicitações REST diretamente.

Para obter mais informações, consulte Excluir vários objetos na Referência da API do Amazon Simple Storage Service.

Organizar, listar e trabalhar com seus objetos

No Amazon S3, você pode usar prefixos para organizar seu armazenamento. Um prefixo é um agrupamento lógico dos objetos em um bucket. O valor do prefixo é semelhante a um nome de diretório que permite que você armazene dados semelhantes em um bucket no mesmo diretório. Quando você faz upload de objetos de maneira programática, é possível usar prefixos para organizar seus dados.

No console do Amazon S3, os prefixos são chamados de pastas. Você pode exibir todos os objetos e pastas no console do S3 navegando até um bucket. Você também pode exibir informações sobre cada objeto incluindo propriedades do objeto.

Para obter mais informações sobre como listar e organizar seus dados no Amazon S3, consulte os tópicos a seguir.

Tópicos

- Organizar objetos usando prefixos
- Listar chaves de objeto programaticamente
- Organizar objetos no console do Amazon S3 usando pastas
- Exibir propriedades do objeto no console do Amazon S3
- Categorizar seu armazenamento usando tags

Organizar objetos usando prefixos

Você pode usar prefixos para organizar os dados armazenados nos buckets do Amazon S3. Um prefixo é uma string no início do nome da chave do objeto. Um prefixo pode ter qualquer comprimento, sujeito ao comprimento máximo do nome da chave do objeto (1.024 bytes). Você pode pensar nos prefixos como uma forma de organizar seus dados de forma semelhante aos diretórios. No entanto, os prefixos não são diretórios.

Pesquisar por prefixo limita os resultados a somente essas chaves que começam com o prefixo especificado. O delimitador faz com que uma operação de lista acumule todas as chaves que compartilham um prefixo comum em um único resultado da lista de resumo.

A finalidade dos parâmetros de prefixo e delimitador é ajudá-lo a organizar e navegar, hierarquicamente, por suas chaves. Para fazer isso, escolha primeiro um delimitador para seu bucket, tal como barra (/), que você não prevê que apareça em nomes de chave. Você pode usar outro caractere como um delimitador. Não há nada de especial no caractere barra (/), mas esse um delimitador de prefixo muito comum. Em seguida, crie seus nomes de chave concatenando todos os níveis de contenção de hierarquia, separando cada nível com o delimitador.

Por exemplo, se você estava armazenando informações sobre cidades, pode, naturalmente, organizá-las por continente, país, província ou estado. Como esses nomes geralmente não usam pontuação, você pode usar a barra (/) como delimitador. Os seguintes exemplos usam uma barra (/) como delimitador.

- Europa/França/Nova Aquitânia/Bordeaux
- América do Norte/Canadá/Quebec/Montreal
- América do Norte /EUA/Washington/Bellevue
- América do Norte /EUA/Washington/Seattle

Se você armazenou dados de cada cidade do mundo desta forma, ficaria estranho gerenciar um namespace plano de chave. Usando `Prefix` e `Delimiter` com a operação de lista, você pode usar a hierarquia que criou para listar os dados. Por exemplo, para listar todos os estados nos EUA, defina `Delimiter='/'` e `Prefix='North America/USA/'`. Para listar todas as províncias no Canadá para as quais você tem dados, defina `Delimiter='/'` e `Prefix='North America/Canada/'`.

Para obter mais informações sobre delimitadores, prefixos e pastas aninhadas, consulte Diferença entre prefixos e pastas aninhadas.

Listar objetos usando prefixos e delimitadores

Se emitir uma solicitação de lista com um delimitador, você poderá pesquisar a hierarquia apenas em um nível, pulando e resumindo as chaves aninhadas (possivelmente milhões) em níveis mais profundos. Por exemplo, suponha que você tenha um bucket (*amzn-s3-demo-bucket*) com as seguintes chaves:

`sample.jpg`

`photos/2006/January/sample.jpg`

`photos/2006/February/sample2.jpg`

`photos/2006/February/sample3.jpg`

`photos/2006/February/sample4.jpg`

O bucket de exemplo tem somente `sample.jpg` o objeto no nível raiz. Para listar somente os objetos no nível raiz no bucket, você envia uma solicitação GET no bucket com o caractere delimitador barra (`/`). Em resposta, o Simple Storage Service (Amazon S3) retorna a chave do objeto `sample.jpg` porque não contém o caractere delimitador `/`. Todas as outras chaves contêm o caractere delimitador. O Simple Storage Service (Amazon S3) agrupa essas chaves e retorna um único elemento `CommonPrefixes` com valor de prefixo `photos/`, que é uma substring que vai do início dessas chaves até a primeira ocorrência do delimitador especificado.

Example

```
<ListBucketResult xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Name>amzn-s3-demo-bucket</Name>
  <Prefix></Prefix>
  <Marker></Marker>
  <MaxKeys>1000</MaxKeys>
  <Delimiter>/</Delimiter>
  <IsTruncated>false</IsTruncated>
  <Contents>
    <Key>sample.jpg</Key>
    <LastModified>2011-07-24T19:39:30.000Z</LastModified>
    <ETag>&quot;d1a7fb5eab1c16cb4f7cf341cf188c3d&quot;</ETag>
    <Size>6</Size>
    <Owner>
      <ID>75cc57f09aa0c8caeab4f8c24e99d10f8e7faeebf76c078efc7c6caea54ba06a</ID>
      <DisplayName>displayname</DisplayName>
    </Owner>
```

```
    <StorageClass>STANDARD</StorageClass>
  </Contents>
  <CommonPrefixes>
    <Prefix>photos/</Prefix>
  </CommonPrefixes>
</ListBucketResult>
```

Para obter mais informações sobre como listar chaves de objeto programaticamente, consulte Listar chaves de objeto programaticamente.

Listar chaves de objeto programaticamente

No Amazon S3, as chaves podem ser listadas por prefixo. Você pode escolher um prefixo comum para os nomes das chaves relacionadas e marcar essas chaves com um caractere especial que delimite a hierarquia. Em seguida, você pode usar a operação de lista para selecionar e procurar chaves hierarquicamente. Isso é semelhante à forma como arquivos são armazenados em diretórios em um sistema de arquivos.

O Amazon S3 expõe uma operação de lista que permite a enumeração das chaves contidas em um bucket. As chaves são selecionadas para a listagem pelo bucket e pelo prefixo. Por exemplo, considere um bucket chamado “`dictionary`” que contém uma chave para cada palavra inglesa. Você pode fazer uma chamada para listar todas as chaves no bucket iniciadas com a letra “q”. Os resultados da lista são obtidos sempre em ordem binária UTF-8.

As operações de lista SOAP e REST retornam um documento XML que contém nomes de chaves correspondentes e informações sobre o objeto identificado em cada chave.

> **Note**
>
> As APIs SOAP não estão disponíveis para novos clientes e chegam ao fim da vida útil (EOL) em 31 de agosto de 2025. Recomendamos usar a API REST ou os AWS SDKs.

Grupos de chaves que compartilham um prefixo terminado por um delimitador especial podem ser rolados para acima pelo prefixo comum para fins de listagem. Isso permite que aplicativos organizem e naveguem por suas chaves hierarquicamente, de maneira muito similar a como você organizaria seus arquivos em diretórios em um sistema de arquivos.

Por exemplo, para estender o bucket de dicionário para conter mais do que apenas palavras inglesas, você poderia formar chaves prefixando cada palavra com seu idioma e um delimitador,

tal como "`French/logical`". Usando esse esquema de nomeação e o recurso hierárquico de listagem, você poderia recuperar uma lista somente de palavras francesas. Você também poderia pesquisar a parte superior da lista de idiomas sem ter que iterar com todas as chaves de iteração lexicográficas. Para obter mais informações sobre esse aspecto de listagem, consulte Organizar objetos usando prefixos.

API REST

Se a sua aplicação exigir, você pode enviar solicitações REST diretamente. Você pode enviar uma solicitação GET para retornar alguns ou todos os objetos em um bucket ou pode usar critérios de seleção para obter um subconjunto de objetos em um bucket. Para obter mais informações, consulte GET Bucket (listar objetos) versão 2 na Referência da API do Amazon Simple Storage Service.

Implementação eficiente de lista

A performance da lista não é substancialmente afetada pelo número total de chaves no bucket. Também não é afetada pela presença ou ausência dos argumentos `prefix`, `marker`, `maxkeys` ou `delimiter`.

Iterar em resultados de várias páginas

Como os buckets podem conter um número praticamente ilimitado de chaves, os resultados completos de uma consulta de lista podem ser muito extensos. Para gerenciar grandes conjuntos de resultados, a API do Amazon S3 é compatível com a paginação para separá-los em várias respostas. Cada resposta de chaves de lista retorna uma página com até 1.000 chaves com um indicador apontando se a resposta está truncada. Você envia uma série de solicitações de chaves de lista até receber todas elas. AWS As bibliotecas wrapper do SDK fornecem a mesma paginação.

Exemplos

Ao listar todos os objetos no bucket, observe que você deve ter a permissão `s3:ListBucket`.

CLI

list-objects

O seguinte exemplo usa o comando `list-objects` para exibir os nomes de todos os objetos presentes no bucket especificado:

```
aws s3api list-objects --bucket text-content --query 'Contents[].{Key: Key, Size:
 Size}'
```

O exemplo usa o argumento `--query` para filtrar a saída de `list-objects` até encontrar o valor e o tamanho da chave de cada objeto

Para obter mais informações sobre objetos, consulte Trabalhar com objetos no Amazon S3.

- Para obter detalhes da API, consulte ListObjects na Referência de comandos da AWS CLI.

ls

O exemplo a seguir lista todos os objetos e prefixos em um bucket usando o comando `ls`.

Para usar esse exemplo de comando, substitua *amzn-s3-demo-bucket* pelo nome do seu bucket.

```
$ aws s3 ls s3://amzn-s3-demo-bucket
```

- Consulte mais informações sobre o comando de algo nível `ls` em List buckets and objects no Guia do usuário do AWS Command Line Interface.

PowerShell

Ferramentas para PowerShell V4

Exemplo 1: este comando recupera as informações sobre todos os itens no bucket “test-files”.

```
Get-S3Object -BucketName amzn-s3-demo-bucket
```

Exemplo 2: este comando recupera as informações sobre o item “sample.txt” do bucket “test-files”.

```
Get-S3Object -BucketName amzn-s3-demo-bucket -Key sample.txt
```

Exemplo 3: este comando recupera as informações sobre todos os itens com prefixo “sample” do bucket “test-files”.

```
Get-S3Object -BucketName amzn-s3-demo-bucket -KeyPrefix sample
```

- Para ver detalhes da API, consulte ListObjects na Ferramentas da AWS para PowerShell Cmdlet Reference (V4).

Ferramentas para PowerShell V5

Exemplo 1: este comando recupera as informações sobre todos os itens no bucket “test-files”.

```
Get-S3Object -BucketName amzn-s3-demo-bucket
```

Exemplo 2: este comando recupera as informações sobre o item “sample.txt” do bucket “test-files”.

```
Get-S3Object -BucketName amzn-s3-demo-bucket -Key sample.txt
```

Exemplo 3: este comando recupera as informações sobre todos os itens com prefixo “sample” do bucket “test-files”.

```
Get-S3Object -BucketName amzn-s3-demo-bucket -KeyPrefix sample
```

- Para ver detalhes da API, consulte ListObjects na Ferramentas da AWS para PowerShell Cmdlet Reference (V5).

Organizar objetos no console do Amazon S3 usando pastas

Nos buckets de uso geral do Amazon S3, os objetos são os recursos primários e são armazenados em buckets. Os buckets de uso geral do Amazon S3 têm uma estrutura plana em vez de uma hierarquia como você normalmente veria em um sistema de arquivos. No entanto, para fins de simplicidade organizacional, o console do Amazon S3 oferece suporte ao conceito de pastas como meio de agrupar objetos. O console faz isso usando um prefixo de nome compartilhado para os objetos agrupados. Em outras palavras, os objetos agrupados têm nomes que começam com uma string comum. Essa string comum, ou prefixo compartilhado, é o nome da pasta. Os nomes de objeto também são chamados de nomes de chave.

Por exemplo, é possível usar o console para criar uma pasta chamada `photos` em um bucket de uso geral e armazenar um objeto chamado `myphoto.jpg` nela. Em seguida, o objeto é armazenado como o nome da chave `photos/myphoto.jpg`, em que `photos/` é o prefixo.

Estes são mais dois exemplos:

- Se você tiver três objetos no bucket de uso geral (`logs/date1.txt`, `logs/date2.txt` e `logs/date3.txt`), o console mostrará uma pasta chamada `logs`. Se você abrir a pasta no console, verá três objetos: `date1.txt`, `date2.txt` e `date3.txt`.

- Se você tiver um objeto chamado `photos/2017/example.jpg`, o console mostrará uma pasta chamada `photos` que contém a pasta `2017`. A pasta `2017` contém o objeto `example.jpg`.

Você pode ter pastas dentro de pastas, mas não buckets dentro de buckets. Você pode carregar e copiar objetos diretamente em uma pasta. As pastas podem ser criadas, excluídas e tornadas públicas, mas não podem ser renomeadas. Os objetos podem ser copiados de uma pasta para outra.

> **Important**
>
> Quando você cria uma pasta no console do Amazon S3, o S3 cria um objeto de zero byte. Essa chave de objeto é definida como o nome da pasta que você forneceu, com um caractere de barra (/) no final. Por exemplo, no console do Amazon S3, se você criar uma pasta chamada `photos` no bucket, o console do Amazon S3 criará um objeto de zero byte com a chave `photos/`. O console cria esse objeto para ser compatível com a ideia de pastas.
>
> Além disso, qualquer objeto existente que tenha sido nomeado com um caractere de barra (/) no final aparecerá como uma pasta no console do Amazon S3. Por exemplo, um objeto com o nome de chave `examplekeyname/` aparece como uma pasta no console do Amazon S3 e não como um objeto. Caso contrário, ele se comporta como qualquer outro objeto e pode ser visualizado e manipulado por meio da AWS Command Line Interface (AWS CLI), de AWS SDKs ou da API REST. Também não é possível fazer upload de um objeto que tenha um nome de chave com um caractere de barra (/) no final usando o console do Amazon S3. No entanto, é possível fazer upload de objetos nomeados com uma barra (/) no final usando a AWS Command Line Interface (AWS CLI), os AWS SDKs ou a API REST.
>
> Além disso, o console do Amazon S3 não exibe o conteúdo e os metadados dos objetos de pasta da mesma forma que exibe para outros objetos. Quando você usa o console para copiar um objeto nomeado com uma barra (/) no final, uma pasta é criada no local de destino, mas os dados e os metadados do objeto não são copiados. Além disso, uma barra (/) nos nomes de chave de objeto pode exigir tratamento especial. Para obter mais informações, consulte Nomear objetos do Amazon S3.

Para criar pastas em buckets de diretório, faça upload de uma pasta. Para obter mais informações, consulte Fazer upload de objetos em um bucket de diretório.

Tópicos

- Criar uma pasta

- Tornar as pastas públicas
- Calcular o tamanho da pasta
- Excluir pastas

Criar uma pasta

Esta seção descreve como usar o console do Amazon S3 para criar uma pasta.

> **Important**
>
> Se a política de bucket não permitir o carregamento de objetos para esse bucket sem tags, metadados ou beneficiados da lista de controle de acesso (ACL), você não poderá criar uma pasta usando o procedimento a seguir. Em vez disso, carregue uma pasta vazia e especifique as configurações a seguir na configuração de carregamento.

Para criar uma pasta

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets de uso geral.
3. Na lista de buckets, escolha o nome do bucket no qual você deseja criar uma pasta.
4. Na guia Objetos, escolha Criar pasta.
5. Insira um nome para a pasta (por exemplo, **`favorite-pics`**).

   > **Note**
   >
   > Os nomes de pasta estão sujeitos a certas limitações e diretrizes e são considerados parte do nome da chave de um objeto, que é limitado a 1.024 bytes. Para obter mais informações, consulte the section called “Nomear objetos”.

6. (Opcional) Se a política do bucket exigir que os objetos sejam criptografados com uma chave de criptografia específica, em Criptografia do lado do servidor, você deverá escolher Especificar chave de criptografia e especificar a mesma chave de criptografia ao criar uma pasta. Caso contrário, a criação da pasta falhará.
7. Selecione Criar pasta.

Tornar as pastas públicas

Recomendamos bloquear todo o acesso público às pastas e aos buckets do Amazon S3, a menos que você exija especificamente uma pasta ou um bucket públicos. Ao tornar uma pasta pública, qualquer pessoa na Internet pode visualizar todos os objetos agrupados nessa pasta.

No console do Amazon S3, você pode tornar uma pasta pública. Também é possível tornar uma pasta pública criando uma política de bucket que limita o acesso aos dados por prefixo. Para obter mais informações, consulte Gerenciamento de identidade e acesso para o Amazon S3.

> **Warning**
>
> Após tornar uma pasta pública no console do Amazon S3, não será possível torná-la privada novamente. Em vez disso, é necessário definir permissões em cada objeto individual na pasta pública para que o objeto não tenha acesso público. Para obter mais informações, consulte Configurar ACLs.

Tópicos

- Calcular o tamanho da pasta
- Excluir pastas

Calcular o tamanho da pasta

Esta seção descreve como usar o console do Amazon S3 para calcular o tamanho de uma pasta.

Como calcular o tamanho de uma pasta

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets de uso geral.
3. Na lista Buckets de uso geral, escolha o nome do bucket no qual a pasta está armazenada.
4. Na lista Objetos, marque a caixa de seleção ao lado do nome da pasta.
5. Escolha Actions (Ações), depois escolha Calculate total size (Calcular tamanho total).

> **Note**
>
> Ao sair da página, as informações da pasta (incluindo o tamanho total) não estarão mais disponíveis. É necessário calcular o tamanho total novamente se quiser vê-lo outra vez.

> **Important**
>
> Quando você usa a ação Calculate total size (Calcular tamanho total) em objetos ou pastas especificados em seu bucket, o Amazon S3 calcula o número total de objetos e o tamanho total do armazenamento. No entanto, carregamentos fracionados incompletos ou em andamento e versões anteriores ou desatualizadas não são calculados no número total de objetos ou no tamanho total. Essa ação calcula somente o número total de objetos e o tamanho total da versão atual ou mais recente de cada objeto armazenado no bucket. Por exemplo, se houver duas versões de um objeto em seu bucket, a calculadora de armazenamento no Amazon S3 as contará como apenas um objeto. Como resultado, o número total de objetos que é calculado no console do Amazon S3 pode ser diferente da métrica Quantidade de objetos mostrada na funcionalidade Lente de Armazenamento do S3 e do número informado pela métrica `NumberOfObjects` do Amazon CloudWatch. Da mesma forma, o tamanho total do armazenamento também pode ser diferente da métrica Total Storage (Armazenamento total) mostrada no S3 Storage Lens e da métrica `BucketSizeBytes` mostrada no CloudWatch.

Excluir pastas

Esta seção explica como usar o console do Amazon S3 para excluir pastas de um bucket do S3.

Para obter informações sobre os recursos e a definição de preço do Amazon S3, consulte Amazon S3.

Para excluir pastas de um bucket do S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets de uso geral.
3. Na lista Buckets de uso geral, escolha o nome do bucket do qual você deseja excluir pastas.

4. Na lista Objetos, marque a caixa de seleção ao lado das pastas e dos objetos que deseja excluir.
5. Escolha Excluir.
6. Na página Excluir objetos, verifique se os nomes das pastas e dos objetos selecionados para exclusão estão listados em Objetos especificados.
7. Na caixa Delete objects (Excluir objetos), insira **`delete`** e escolha Delete objects (Excluir objetos).

> ⚠ Warning
>
> Essa ação exclui todos os objetos especificados. Ao excluir pastas, aguarde a conclusão da ação de exclusão antes de adicionar objetos novos à pasta. Caso contrário, os objetos novos também podem ser excluídos.

Exibir propriedades do objeto no console do Amazon S3

Você pode usar o console do Amazon S3 para exibir as propriedades de um objeto, como a classe de armazenamento, as configurações de criptografia, as etiquetas e os metadados.

Para visualizar as propriedades de um objeto

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets de uso geral ou Buckets de diretórios.
3. Na lista de buckets, escolha o nome do bucket que contém o objeto.
4. Na lista Objects (Objetos), escolha o nome do objeto do qual você deseja visualizar as propriedades.

   A Object overview (Visão geral do objeto) de seu objeto é aberta. Você pode rolar para baixo para exibir as propriedades do objeto.
5. Na página Visão geral do objeto, você pode visualizar ou configurar as propriedades a seguir para o objeto.

> **Note**
>
> - Se você alterar as propriedades Storage Class (Classe de armazenamento), Encryption (Criptografia) ou Metadata (Metadados), um novo objeto será criado para substituir o antigo. Se o versionamento do S3 estiver habilitado, uma nova versão do objeto será criada e o objeto existente se tornará uma versão mais antiga. A função que altera a propriedade também se torna o proprietário do novo objeto ou (versão do objeto).
> - Para alterar as propriedades Classe de armazenamento, Criptografia ou Metadados de um objeto que tem etiquetas definidas pelo usuário, você precisa ter a permissão `s3:GetObjectTagging`. Para alterar essas propriedades de um objeto que não tem etiquetas definidas pelo usuário, mas que tem mais de 16 MB, você também precisa ter a permissão `s3:GetObjectTagging`.
>
>   Se a política do bucket de destino negar a ação `s3:GetObjectTagging`, essas propriedades do objeto serão atualizadas, mas as etiquetas definidas pelo usuário serão removidas do objeto e você receberá um erro.

a. Storage class (Classe de armazenamento) – cada objeto no Amazon S3 tem uma classe de armazenamento associada a ela. A classe de armazenamento que você decide usar depende da frequência com que acessa o objeto. A classe de armazenamento padrão de objetos do S3 em buckets de uso geral é STANDARD. A classe de armazenamento padrão de objetos do S3 em buckets de diretório é S3 Express One Zone. Escolha qual classe de armazenamento usar ao fazer upload de um objeto. Para obter mais informações sobre classes de armazenamento, consulte Compreender e gerenciar classes de armazenamento do Amazon S3.

   Para alterar a classe de armazenamento depois de fazer upload de um objeto em um bucket de uso geral, escolha Classe de armazenamento. Escolha a classe de armazenamento desejada e Save (Salvar).

> **Note**
>
> Não é possível alterar a classe de armazenamento de objetos em um bucket de diretório.

b. Server-side encryption settings (Configurações de criptografia no lado do servidor): você pode usar a criptografia no lado do servidor para criptografar seus objetos do S3. Para ter mais informações, consulte Especificando criptografia no lado do servidor com o AWS KMS (SSE-KMS) ou Especificar a criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3).

c. Metadata (Metadados) – cada objeto no Amazon S3 tem um conjunto de pares de nome-valor que representa seus metadados. Para obter informações sobre como adicionar metadados a um objeto do S3, consulte Editar metadados de objeto no console do Amazon S3.

d. Tags: você categoriza o armazenamento adicionando tags a um objeto do S3 em um bucket de uso geral. Para obter mais informações, consulte Categorizar seu armazenamento usando tags.

e. Retenção jurídica e retenção do bloqueio de objetos: você pode impedir que um objeto em um bucket de uso geral seja excluído. Para obter mais informações, consulte Bloquear objetos com o Bloqueio de Objetos.

Categorizar seu armazenamento usando tags

Use a marcação de objetos para classificar o armazenamento. Cada tag é um par de chave-valor.

Você pode adicionar tags a objetos novos ao fazer upload deles ou pode adicioná-las aos objetos existentes.

- Você pode associar até 10 tags a um objeto. As tags associadas a um objeto devem ter chaves de tag exclusivas.
- Um chave de tag pode ter até 128 caracteres Unicode e os valores de tag podem ter até 256 caracteres Unicode. As tags de objeto do Amazon S3 são representadas internamente em UTF-16. Observe que, em UTF-16, os caracteres utilizam posições de um ou de dois caracteres.
- As chaves e os valores diferenciam letras maiúsculas de minúsculas.

- Consulte mais informações sobre restrições de tags em User-defined tag restrictions no Guia do usuário do Gerenciamento de Faturamento e Custos da AWS. Consulte as restrições básicas de tag em Restrições de tags no Guia do usuário do Amazon EC2.

Exemplos

Considere os seguintes exemplos de marcação:

Example Informação de PHI

Suponha que um objeto contenha dados de informações de saúde protegidas (PHI). Você pode marcar o objeto usando o par de chave/valor a seguir.

```
PHI=True
```

ou

```
Classification=PHI
```

Example Arquivos do projeto

Suponha que você armazene arquivos de projeto em seu bucket do S3. Você pode marcar esses objetos com uma chave denominada `Project` e um valor, como mostrado a seguir.

```
Project=Blue
```

Example Várias tags

Você pode adicionar várias tags a um objeto, como mostrado a seguir.

```
Project=x
Classification=confidential
```

Prefixos e tags de nome de chave

Os prefixos de nome da chave do objeto também permitem categorizar o armazenamento. No entanto, a categorização baseada em prefixo é unidimensional. Considere os seguintes nomes de chave de objeto:

```
photos/photo1.jpg
project/projectx/document.pdf
project/projecty/document2.pdf
```

Esses nomes de chave têm os prefixos `photos/`, `project/projectx/` e `project/projecty/`. Esses prefixos habilitam a classificação de uma dimensão. Isto é, tudo que tiver um prefixo pertencerá a uma categoria. Por exemplo, o prefixo `project/projectx` identifica todos os documentos relacionados ao projeto x.

Com a marcação, você agora tem outra dimensão. Se você quiser que photo1 esteja na categoria projeto x, poderá marcar o objeto conforme necessário.

Benefícios adicionais

Além de classificação de dados, a marcação oferece benefícios como os seguintes:

- As tags de objeto permitem ter controle de acesso de permissões. Por exemplo, você pode conceder a um usuário permissões a objetos somente leitura com etiquetas específicas.
- As tags de objeto permitem o gerenciamento de ciclo de vida do objeto em que você pode especificar um filtro com base em tag, além de um prefixo de nome da chave, em uma regra de ciclo de vida.
- Ao usar a análise do Amazon S3, você pode configurar filtros para agrupar objetos para análise por tags de objeto, prefixo de nome da chave ou ambos, prefixo e tags.
- Você também pode personalizar métricas do Amazon CloudWatch para exibir informações por filtros de tag específicos. As seguintes seções fornecem detalhes.

> **Important**
>
> É aceitável usar tags para identificar objetos que contêm dados confidenciais, como informações de identificação pessoal (PII) ou informações de saúde protegidas (PHI). No entanto, as próprias tags não devem conter nenhuma informação confidencial.

Adição de conjuntos de tags de objeto a vários objetos do Amazon S3 com uma única solicitação

Para adicionar conjuntos de tags de objeto a mais de um objeto do Amazon S3 com uma única solicitação, você pode usar operações em lote do S3. Você fornece às operações em lote do S3 uma

lista de objetos nos quais operar. O S3 Batch Operations chama a respectiva operação de API para executar a operação especificada. Um único trabalho de operações em lote pode realizar a operação especificada em bilhões de objetos contendo exabytes de dados.

O recurso S3 Batch Operations rastreia o progresso, envia notificações e armazena um relatório de conclusão detalhado de todas as ações, fornecendo uma experiência totalmente gerenciada, auditável e sem servidor. É possível usar as operações em lote do S3 por meio do console do Amazon S3, da AWS CLI, de AWS SDKs ou da API REST. Para obter mais informações, consulte the section called “Conceitos básicos do Batch Operations”.

Para obter mais informações sobre tags de objeto, consulte Gerenciar tags de objeto.

Operações de API relacionadas à marcação de objetos

O Amazon S3 oferece suporte às seguintes operações de API que são especificamente para marcação de objetos:

Operações de API do objeto

- Atribuição de tags de objeto PUT: Substitui tags em um objeto. Especifique tags no corpo de solicitação. Há dois cenários distintos de gerenciamento de tags de objeto usando essa API.
  - O objeto não tem tags – Usando essa API, você pode adicionar um conjunto de tags a um objeto (o objeto não tem nenhuma tag anterior).
  - O objeto tem um conjunto de tags existentes – Para modificar o conjunto de tags existente, você deve primeiro recuperar o conjunto de tags existente, modificá-lo no lado do cliente e usar essa API para substituir o conjunto de tags.

    > **Note**
    >
    > Se você enviar essa solicitação com o conjunto de tags vazio, o Amazon S3 excluirá o conjunto de tags existente no objeto. Se você usar esse método, será cobrado por uma solicitação de nível 1 (PUT). Para obter mais informações, consulte Definição de preço do Amazon S3.
    >
    > A solicitação de Atribuição de tags de objeto DELETE é preferível, pois atinge o mesmo resultado sem incorrer em cobranças.
- Atribuição de tags de objeto GET: retorna o conjunto de tags associado a um objeto. O Amazon S3 retorna tags de objetos no corpo da resposta.
- Atribuição de tags de objeto DELETE: exclui o conjunto de tags associado a um objeto.

Outras operações de API que oferecem suporte à atribuição de tags

- Objeto PUT e Iniciar multipart upload: você pode especificar tags ao criar objetos. Especifique tags usando o cabeçalho de solicitação `x-amz-tagging`.
- Objeto GET: em vez de retornar o conjunto de tags, o Amazon S3 retorna a contagem de tags de objeto no cabeçalho `x-amz-tag-count` (somente se o solicitante tiver permissões para ler tags) porque o tamanho de resposta do cabeçalho está limitado a 8 KB. Caso queira ver as tags, faça outra solicitação para a operação de API Atribuição de tags de objeto GET.
- Objeto POST: você pode especificar tags na solicitação POST.

  Contanto que as tags na solicitação não ultrapassem o limite de tamanho de cabeçalho de solicitações HTTP de 8 KB, você pode usar a `PUT Object` API para criar objetos com tags. Se as tags especificadas ultrapassarem o limite de tamanho do cabeçalho, você poderá usar esse método POST para incluir as tags no corpo.

  Objeto PUT - Copiar: você pode especificar a `x-amz-tagging-directive` na solicitação para instruir o Amazon S3 a copiar (comportamento padrão) as tags ou substituir as tags por um novo conjunto de tags fornecido na solicitação.

Observe o seguinte:

- A atribuição de tags de objetos do S3 é muito consistente. Para obter mais informações, consulte Modelo de consistência de dados do Amazon S3.

Configurações adicionais

Esta seção explica como a marcação de objetos está relacionada a outras configurações.

Marcação de objetos e gerenciamento do ciclo de vida

Na configuração de ciclo de vida de bucket, você pode especificar um filtro para selecionar um subconjunto de objetos ao qual a regra se aplica. Você pode especificar um filtro com base em prefixos de nome de chave, em tags de objeto ou em ambos.

Suponha que você armazene fotos (brutas e no formato concluído) no bucket do Amazon S3. Você pode marcar esses objetos como mostrado a seguir.

```
phototype=raw
```

```
or
phototype=finished
```

Você pode considerar o arquivamento das fotos brutas no S3 Glacier pouco tempo depois de serem criadas. Você pode configurar uma regra de ciclo de vida com um filtro que identifica o subconjunto de objetos com o prefixo de nome de chave (`photos/`) que têm uma tag específica (`phototype=raw`).

Para obter mais informações, consulte Gerenciar o ciclo de vida dos objetos.

Marcação e replicação de objetos

Se você tiver configurado a replicação no bucket, o Amazon S3 replicará as tags, contanto que você conceda permissão ao Amazon S3 para ler as tags. Para obter mais informações, consulte Visão geral da configuração da replicação em tempo real.

Notificações de evento de marcação de objetos

É possível configurar uma notificação de evento do Amazon S3 para receber um aviso quando uma etiqueta de objeto for adicionada ou excluída de um objeto. O tipo de evento `s3:ObjectTagging:Put` notifica você quando ocorre PUT de uma etiqueta em um objeto ou quando uma etiqueta existente é atualizada. O tipo de evento `s3:ObjectTagging:Delete` notifica você quando uma etiqueta é removida de um objeto. Para obter mais informações, consulte Habilitar notificações de eventos.

Para obter mais informações sobre a marcação de objetos, consulte os seguintes tópicos:

Tópicos

- Marcação e políticas de controle de acesso
- Gerenciar tags de objeto

Marcação e políticas de controle de acesso

Você também pode usar políticas de permissões (políticas de bucket e de usuário) para gerenciar permissões relacionadas à atribuição de tags de objetos. Para ver ações de política, consulte os seguintes tópicos:

- Operações com objetos
- Operações de buckets

As tags de objeto permitem ter controle de acesso para gerenciar permissões. Você pode conceder permissões condicionais com base em tags de objeto. O Amazon S3 oferece suporte às seguintes chaves de condição que podem ser usadas para conceder permissões condicionais com base em tags de objeto:

- `s3:ExistingObjectTag/<tag-key>` – Use esta chave de condição para verificar se uma tag de objeto existente tem a chave e o valor de tag específicos.

  > **Note**
  >
  > Para conceder permissões para as operações `PUT Object` e `DELETE Object`, não é permitido usar essa chave de condição. Isto é, você não pode criar uma política para conceder ou negar permissões de usuário para excluir ou substituir um objeto existente com base nas tags existentes.

- `s3:RequestObjectTagKeys` – Use esta chave de condição para restringir as chaves de tag que deseja permitir em objetos. Isso é útil para adicionar tags a objetos usando as solicitações PutObjectTagging e PutObject e de POST objeto.
- `s3:RequestObjectTag/<tag-key>` – Use esta chave de condição para restringir as chaves e os valores de tag que deseja permitir em objetos. Isso é útil para adicionar tags a objetos usando as solicitações PutObjectTagging e PutObject e de bucket POST.

Para obter uma lista completa de chaves de condição específicas de serviço do Amazon S3, consulte Exemplos de políticas de bucket usando chaves de condição. As seguintes políticas de permissões ilustram como a marcação de objetos permite gerenciar permissões de acesso.

Example 1: Permitir que um usuário leia somente os objetos que têm a chave e o valor de uma etiqueta específica

A política de permissões a seguir limita a capacidade de leitura dos usuários para que leiam somente objetos que tenham a chave e o valor da tag `environment: production`. Essa política usa a chave de condição `s3:ExistingObjectTag` para especificar a chave e o valor da etiqueta.

```
{
  "Version": "2012-10-17",
  "Statement": [
  {
    "Principal": {
      "AWS": [
```

```
        "arn:aws:iam::111122223333:role/JohnDoe"
      ]
    },
    "Effect": "Allow",
    "Action": ["s3:GetObject", "s3:GetObjectVersion"],
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
    "Condition": {
      "StringEquals":
        {"s3:ExistingObjectTag/environment": "production"}
    }
  }
  ]
}
```

Example 2: Restringir quais chaves de etiqueta de objeto os usuários podem adicionar

A política de permissões a seguir concede ao usuário permissões para executar a ação `s3:PutObjectTagging`, que permite que o usuário adicione tags a um objeto existente. A condição usa a chave de condição `s3:RequestObjectTagKeys` para especificar as chaves de etiqueta permitidas, como `Owner` ou `CreationDate`. Para obter mais informações, consulte Criar uma condição que testa vários valores de chave no Guia do usuário do IAM.

A política garante que cada chave de etiqueta especificada na solicitação seja uma chave de etiqueta autorizada. O qualificador `ForAnyValue` na condição garante que pelo menos uma das chaves especificadas esteja presente na solicitação.

```
{
   "Version": "2012-10-17",
  "Statement": [
    {"Principal":{"AWS":[
            "arn:aws:iam::111122223333:role/JohnDoe"
        ]
      },
 "Effect": "Allow",
      "Action": [
        "s3:PutObjectTagging"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
      ],
      "Condition": {"ForAnyValue:StringEquals": {"s3:RequestObjectTagKeys": [
            "Owner",
```

```
            "CreationDate"
          ]
        }
      }
    }
  ]
}
```

Example 3: Exigir a chave e o valor de uma etiqueta específica ao permitir que os usuários adicionem etiquetas de objeto

O exemplo de política a seguir concede ao usuário permissão para executar a ação `s3:PutObjectTagging`, que permite que o usuário adicione etiquetas a um objeto existente. A condição requer que o usuário inclua uma chave de etiqueta específica (como *`Project`*) com o valor definido como *`X`*.

```
{
   "Version": "2012-10-17",
  "Statement": [
    {"Principal":{"AWS":[
       "arn:aws:iam::111122223333:user/JohnDoe"
        ]
      },
      "Effect": "Allow",
      "Action": [
        "s3:PutObjectTagging"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
      ],
      "Condition": {"StringEquals": {"s3:RequestObjectTag/Project": "X"
        }
      }
    }
  ]
}
```

Gerenciar tags de objeto

Esta seção explica como você pode gerenciar tags de objeto usando os AWS SDKs for Java e .NET ou o console do Amazon S3.

A marcação de objetos é uma forma de categorizar o armazenamento nos buckets de uso geral. Cada tag é um par de valores chave que segue as regras a seguir:

- Você pode associar até 10 tags a um objeto. As tags associadas a um objeto devem ter chaves de tag exclusivas.
- Um chave de tag pode ter até 128 caracteres Unicode e os valores de tag podem ter até 256 caracteres Unicode. As tags de objeto do Amazon S3 são representadas internamente em UTF-16. Observe que, em UTF-16, os caracteres utilizam posições de um ou de dois caracteres.
- As chaves e os valores diferenciam letras maiúsculas de minúsculas.

Para obter mais informações sobre tags de objeto, consulte Categorizar seu armazenamento usando tags. Para obter mais informações sobre restrições de tags, consulte Restrições de tags definidas pelo usuário no Manual do usuário do Gerenciamento de Faturamento e Custos da AWS.

Uso do console do S3

Para adicionar tags a um objeto

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets de uso geral.
3. Na lista de buckets, escolha o nome do bucket que contém o objeto.
4. Marque a caixa de seleção à esquerda dos nomes dos objetos que você quer alterar.
5. No menu Actions (Ações), escolha Edit (Editar).
6. Revise os objetos listados e escolha Add tags (Adicionar tags).
7. Cada tag de objeto é um par de chave-valor. Insira uma Key (Chave) e um Value (Valor). Para adicionar outra tag, escolha Add Tag (Adicionar tag).

   Você pode digitar até 10 tags para um objeto.
8. Selecione Save changes.

   O Amazon S3 adiciona as tags aos objetos especificados.

Para obter mais informações, consulte também Exibir propriedades do objeto no console do Amazon S3 e Fazer upload de objetos neste guia.

Uso da SDKs AWS

Java

O exemplo a seguir mostra como usar o AWS SDK para Java para definir tags para um objeto novo e recuperar ou substituir tags para um objeto existente. Para obter mais informações sobre marcação de objetos, consulte Categorizar seu armazenamento usando tags. Consulte instruções sobre como criar e testar uma amostra funcional em Getting Started no Guia do desenvolvedor do AWS SDK para Java.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.*;

import java.io.File;
import java.util.ArrayList;
import java.util.List;

public class ManagingObjectTags {

    public static void main(String[] args) {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "*** Bucket name ***";
        String keyName = "*** Object key ***";
        String filePath = "*** File path ***";

        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(clientRegion)
                    .build();

            // Create an object, add two new tags, and upload the object to Amazon
 S3.
            PutObjectRequest putRequest = new PutObjectRequest(bucketName, keyName,
 new File(filePath));
            List<Tag> tags = new ArrayList<Tag>();
            tags.add(new Tag("Tag 1", "This is tag 1"));
```

```
            tags.add(new Tag("Tag 2", "This is tag 2"));
            putRequest.setTagging(new ObjectTagging(tags));
            PutObjectResult putResult = s3Client.putObject(putRequest);

            // Retrieve the object's tags.
            GetObjectTaggingRequest getTaggingRequest = new
 GetObjectTaggingRequest(bucketName, keyName);
            GetObjectTaggingResult getTagsResult =
 s3Client.getObjectTagging(getTaggingRequest);

            // Replace the object's tags with two new tags.
            List<Tag> newTags = new ArrayList<Tag>();
            newTags.add(new Tag("Tag 3", "This is tag 3"));
            newTags.add(new Tag("Tag 4", "This is tag 4"));
            s3Client.setObjectTagging(new SetObjectTaggingRequest(bucketName,
 keyName, new ObjectTagging(newTags)));
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

.NET

O exemplo a seguir mostra como usar o AWS SDK para .NET para definir as tags para um objeto novo e recuperar ou substituir as tags para um objeto existente. Para obter mais informações sobre marcação de objetos, consulte Categorizar seu armazenamento usando tags.

Para obter informações sobre como configurar e executar exemplos de código, consulte Conceitos básicos do AWS SDK for .NET no Guia do desenvolvedor do AWS SDK for .NET.

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Collections.Generic;
```

```
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    public class ObjectTagsTest
    {
        private const string bucketName = "*** bucket name ***";
        private const string keyName = "*** key name for the new object ***";
        private const string filePath = @"*** file path ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 client;

        public static void Main()
        {
            client = new AmazonS3Client(bucketRegion);
            PutObjectWithTagsTestAsync().Wait();
        }

        static async Task PutObjectWithTagsTestAsync()
        {
            try
            {
                // 1. Put an object with tags.
                var putRequest = new PutObjectRequest
                {
                    BucketName = bucketName,
                    Key = keyName,
                    FilePath = filePath,
                    TagSet = new List<Tag>{
                        new Tag { Key = "Keyx1", Value = "Value1"},
                        new Tag { Key = "Keyx2", Value = "Value2" }
                    }
                };

                PutObjectResponse response = await
 client.PutObjectAsync(putRequest);
                // 2. Retrieve the object's tags.
                GetObjectTaggingRequest getTagsRequest = new GetObjectTaggingRequest
                {
                    BucketName = bucketName,
                    Key = keyName
                };
```

```
                GetObjectTaggingResponse objectTags = await
client.GetObjectTaggingAsync(getTagsRequest);
                for (int i = 0; i < objectTags.Tagging.Count; i++)
                    Console.WriteLine("Key: {0}, Value: {1}",
objectTags.Tagging[i].Key, objectTags.Tagging[i].Value);


                // 3. Replace the tagset.

                Tagging newTagSet = new Tagging();
                newTagSet.TagSet = new List<Tag>{
                    new Tag { Key = "Key3", Value = "Value3"},
                    new Tag { Key = "Key4", Value = "Value4" }
                };


                PutObjectTaggingRequest putObjTagsRequest = new
PutObjectTaggingRequest()
                {
                    BucketName = bucketName,
                    Key = keyName,
                    Tagging = newTagSet
                };
                PutObjectTaggingResponse response2 = await
client.PutObjectTaggingAsync(putObjTagsRequest);

                // 4. Retrieve the object's tags.
                GetObjectTaggingRequest getTagsRequest2 = new
GetObjectTaggingRequest();
                getTagsRequest2.BucketName = bucketName;
                getTagsRequest2.Key = keyName;
                GetObjectTaggingResponse objectTags2 = await
client.GetObjectTaggingAsync(getTagsRequest2);
                for (int i = 0; i < objectTags2.Tagging.Count; i++)
                    Console.WriteLine("Key: {0}, Value: {1}",
objectTags2.Tagging[i].Key, objectTags2.Tagging[i].Value);

            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine(
                        "Error encountered ***. Message:'{0}' when writing an
object"
```

```
                        , e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine(
                    "Encountered an error. Message:'{0}' when writing an object"
                    , e.Message);
            }
        }
    }
}
```

Baixar e fazer upload de objetos com URLs pré-assinados

É possível usar URLs pré-assinados para conceder acesso por tempo limitado a objetos no Amazon S3 sem atualizar a política de bucket. Um URL pré-assinado pode ser inserido em um navegador ou usado por um programa para baixar um objeto. As credenciais usadas pelo URL pré-assinado são as do usuário da AWS que gerou o URL.

Também é possível usar URLs pré-assinados para permitir que alguém carregue um objeto específico para o bucket do Amazon S3. Isso permite um carregamento sem exigir que outra parte tenha credenciais ou permissões de segurança da AWS. Se um objeto com a mesma chave já existe no bucket como especificado no URL pré-assinado, o Amazon S3 substitui o objeto existente pelo objeto carregado.

É possível usar o pre-signed URL várias vezes, até a data e a hora de expiração.

Ao criar um URL pré-assinado, você deve fornecer suas credenciais de segurança e especificar o seguinte:

- Um bucket do Amazon S3
- Uma chave de objeto (se o download desse objeto for no bucket do Amazon S3, se estiver carregando, esse é o nome do arquivo a ser carregado)
- Um método HTTP (`GET` para baixar objetos, `PUT` fazer upload, `HEAD` para ler metadados de objetos etc.)
- Um intervalo de tempo de validade

No momento, os URLs pré-assinados do Amazon S3 não comportam o uso dos algoritmos de soma de verificação de integridade de dados (CRC32, CRC32C, SHA-1, SHA-256) a seguir quando você carrega objetos. Para verificar a integridade do objeto após o carregamento, forneça um resumo MD5 do objeto ao carregá-lo com um URL pré-assinado. Para ter mais informações sobre integridade de objeto, consulte Verificar a integridade do objeto no Amazon S3.

Tópicos

- Quem pode criar um URL pré-assinado
- Tempo de validade para URLs pré-assinados
- Limitar recursos de pre-signed URLs
- Compartilhar objetos com URLs pré-assinados
- Carregar objetos com URLs pré-assinados

Quem pode criar um URL pré-assinado

Qualquer um com credenciais de segurança válidas pode criar um pre-signed URL. Mas para que alguém acesse com êxito um objeto, o URL pré-assinado deve ter sido criado por alguém que tenha permissão para executar a operação na qual o URL pré-assinado é baseado.

Veja a seguir os tipos de credencial que podem ser usados para criar um URL pré-assinado:

- Perfil de instância do IAM: válido por até 6 horas.
- AWS Security Token Service: válido até no máximo 36 horas quando assinado com credenciais de segurança de longo prazo ou com a duração da credencial temporária, o que terminar primeiro.
- Usuário do IAM: válido por até 7 dias quando você estiver usando o AWS Signature Version 4.

  Para criar um URL pré-assinado que seja válido por até sete dias, primeiro delegue credenciais de usuário do IAM (a chave de acesso e a chave secreta) ao método usado para criar o URL pré-assinado.

> **Note**
>
> Se você criou um URL pré-assinado usando uma credencial temporária, o URL expirará quando a credencial expirar. Em geral, um URL pré-assinado expira quando a credencial que você usou para criá-lo é revogada, excluída ou desativada. Isso se aplica mesmo que o URL tenha sido criado com um prazo de validade posterior. Para receber informações

sobre a permanência de credenciais de segurança temporárias, consulte Comparação das operações de API do AWS STS no Guia do usuário do IAM.

Tempo de validade para URLs pré-assinados

Um URL pré-assinado permanece válido pelo período de tempo especificado quando o URL é gerado. Se você criar um URL pré-assinado com o console do Amazon S3, o tempo de validade pode ser definido entre 1 minuto e 12 horas. Se você usar a AWS CLI ou AWS SDKs, o tempo de validade poderá ser definido como até sete dias.

Se você criou um URL pré-assinado usando um token temporário, o URL expirará quando o token expirar. Em geral, um URL pré-assinado expira quando a credencial que você usou para criá-lo é revogada, excluída ou desativada. Isso se aplica mesmo que o URL tenha sido criado com um prazo de validade posterior. Para obter mais informações sobre como as credenciais que você usa afetam o tempo de validade, consulte Quem pode criar um URL pré-assinado.

O Amazon S3 confere a data e hora de validade de um URL assinado no momento da solicitação HTTP. Por exemplo, se um cliente começar a baixar um arquivo grande imediatamente antes do tempo de expiração, o download continuará mesmo que o tempo de expiração acabe durante o download. No entanto, se a conexão cair e o cliente tentar reiniciar o download posteriormente ao término do tempo de expiração, o download vai falhar.

Limitar recursos de pre-signed URLs

Os recursos de um URL pré-assinado são limitados pelas permissões do usuário que o criou. Em essência, os URLs pré-assinados são tokens ao portador que concedem acesso ao portador. Dessa forma, recomendamos que você os proteja adequadamente. Veja a seguir alguns métodos que podem ser usados para restringir o uso de URLs pré-assinados.

AWS Signature Version 4 (SigV4)

Para aplicar um comportamento específico quando solicitações de URL pré-assinado forem autenticadas usando AWS Signature Version 4 (SigV4), você pode usar chaves de condição nas políticas de bucket e políticas de ponto de acesso. Por exemplo, a política de bucket a seguir usará a condição `s3:signatureAge` para negar qualquer solicitação de URL pré-assinado do Amazon S3 em objetos no bucket *`amzn-s3-demo-bucket`* se a assinatura tiver mais de 10 minutos de idade. Para usar esse exemplo, substitua os *`user input placeholders`* por suas próprias informações.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "Deny a presigned URL request if the signature is more than 10 min
 old",
         "Effect": "Deny",
         "Principal": {"AWS":"*"},
         "Action": "s3:*",
         "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
         "Condition": {
            "NumericGreaterThan": {
               "s3:signatureAge": 600000
            }
         }
      }
   ]
}
```

Para obter mais informações sobre as chaves de política relacionadas ao AWS Signature versão 4, consulte Autenticação do AWS Signature versão 4 na Referência de API do Amazon Simple Storage Service.

Restrição de caminho de rede

Se quiser restringir o uso de URLs pré-assinados e todo o acesso do Amazon S3 a caminhos de rede específicos, você poderá escrever políticas do AWS Identity and Access Management (IAM). Essas políticas podem ser definidas na entidade principal do IAM que faz a chamada, no bucket do Amazon S3 ou em ambos.

Uma restrição de caminho de rede na entidade principal do IAM exige que o usuário dessas credenciais faça solicitações pela rede especificada. Uma restrição no bucket ou no ponto de acesso exige que todas as solicitações encaminhadas para esse recurso tenham origem na rede especificada. Essas restrições também são aplicadas fora do cenário de URL pré-assinado.

A condição global do IAM que você usa depende do tipo de endpoint. Se estiver usando o endpoint público para o Amazon S3, use `aws:SourceIp`. Se você estiver usando um endpoint de nuvem privada virtual (VPC) para o Amazon S3, use `aws:SourceVpc` ou `aws:SourceVpce`.

A declaração de política do IAM a seguir requer que a entidade principal só acesse a AWS do intervalo de rede especificado. Com essa declaração de política, exige-se que qualquer acesso

tenha origem nesse intervalo. Isso inclui o caso de alguém que esteja usando um URL pré-assinado para o Amazon S3. Para usar esse exemplo, substitua os *user input placeholders* por suas próprias informações.

```
{
    "Sid": "NetworkRestrictionForIAMPrincipal",
    "Effect": "Deny",
    "Action": "*",
    "Resource": "*",
    "Condition": {
        "NotIpAddressIfExists": {"aws:SourceIp": "IP-address-range"},
        "BoolIfExists": {"aws:ViaAWSService": "false"}
    }
}
```

Compartilhar objetos com URLs pré-assinados

Por padrão, todos os objetos do Amazon S3 são privados, somente o proprietário dos objetos tem permissão para acessá-los. No entanto, o proprietário dos objetos pode compartilhá-los com outras pessoas criando um URL pré-assinado. Um URL pré-assinado usa credenciais de segurança para conceder permissão por tempo limitado para baixar objetos. O URL pode ser inserido em um navegador ou usado por um programa para baixar o objeto. As credenciais usadas pelo URL pré-assinado são as do usuário da AWS que gerou o URL.

Para obter informações gerais sobre URLs pré-assinados, consulte Baixar e fazer upload de objetos com URLs pré-assinados.

É possível criar um URL pré-assinado para compartilhar um objeto sem escrever nenhum código usando o console do Amazon S3, o AWS Explorer for Visual Studio (Windows) ou AWS Toolkit for Visual Studio Code. Também é possível gerar um URL pré-assinado programaticamente usando a AWS Command Line Interface (AWS CLI) ou AWS SDKs.

Usar o console do S3

É possível usar o console do Amazon S3 para gerar um URL pré-assinado para compartilhar um objeto seguindo estas etapas. Ao usar o console, o tempo máximo de validade de um URL pré-assinado é de 12 horas a partir do momento da criação.

Para gerar um URL pré-assinado usando o console do Amazon S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets de uso geral.
3. Na lista Buckets de uso geral, escolha o nome do bucket de uso geral que contém o objeto para o qual você deseja obter um URL pré-assinado.
4. Na lista Objects (Objetos), selecione o objeto para o qual deseja criar um URL pré-assinado.
5. No menu Ações de objeto, escolha Compartilhar com um URL pré-assinado.
6. Especifique por quanto tempo deseja que o URL pré-assinado seja válido.
7. Escolha Create presigned URL (Criar URL pré-assinado).
8. Quando uma confirmação é exibida, o URL é copiado automaticamente para a área de transferência. Você verá um botão para copiar o URL pré-assinado se precisar copiá-lo novamente.

Como usar o AWS CLI

O exemplo do comando da AWS CLI a seguir gera um URL pré-assinado para compartilhar um objeto de um bucket do Amazon S3. Ao usar a AWS CLI, o tempo máximo de validade de um URL pré-assinado é de sete dias a partir do momento da criação. Para usar esse exemplo, substitua os *`user input placeholders`* por suas próprias informações.

```
aws s3 presign s3://amzn-s3-demo-bucket/mydoc.txt --expires-in 604800
```

> **Note**
>
> Para todas as Regiões da AWS lançadas após 20 de março de 2019, você precisa especificar o `endpoint-url` e a `Região da AWS` com a solicitação. Para obter uma lista de todos os endpoints e as regiões do Amazon S3, consulte Regiões e endpoints na Referência geral da AWS.

```
aws s3 presign s3://amzn-s3-demo-bucket/mydoc.txt --expires-in 604800 --region af-south-1 --endpoint-url https://s3.af-south-1.amazonaws.com
```

Para obter mais informações, consulte presign na Referência de comandos da AWS CLI.

Uso dos SDKs da AWS

Também é possível gerar um URL pré-assinado programaticamente usando SDKs da AWS.

Python

O script do Python a seguir gera um URL GET pré-assinado para compartilhar um objeto.

1. Copie o conteúdo do script e salve-o como arquivo "*get-only-url.py*". Para usar os exemplos a seguir, substitua os *espaços reservados para entrada do usuário* por suas próprias informações (como o nome de seu arquivo).

```
import argparse
import boto3
from botocore.exceptions import ClientError

def generate_presigned_url(s3_client, client_method, method_parameters,
 expires_in):
    """
    Generate a presigned Amazon S3 URL that can be used to perform an action.

    :param s3_client: A Boto3 Amazon S3 client.
    :param client_method: The name of the client method that the URL performs.
    :param method_parameters: The parameters of the specified client method.
    :param expires_in: The number of seconds the presigned URL is valid for.
    :return: The presigned URL.
    """
    try:
        url = s3_client.generate_presigned_url(
            ClientMethod=client_method,
            Params=method_parameters,
            ExpiresIn=expires_in
        )
    except ClientError:
        print(f"Couldn't get a presigned URL for client method
 '{client_method}'.")
        raise
    return url

def main():
    parser = argparse.ArgumentParser()
```

```
    parser.add_argument("bucket", help="The name of the bucket.")
    parser.add_argument(
        "key", help="The key (path and filename) in the S3 bucket.",
    )
    args = parser.parse_args()

    # By default, this will use credentials from ~/.aws/credentials
    s3_client = boto3.client("s3")

    # The presigned URL is specified to expire in 1000 seconds
    url = generate_presigned_url(
        s3_client,
        "get_object",
        {"Bucket": args.bucket, "Key": args.key},
        1000
    )
    print(f"Generated GET presigned URL: {url}")

if __name__ == "__main__":
    main()
```

2. Para gerar um URL GET pré-assinado para compartilhar um arquivo, execute o script a seguir com o nome do bucket e o caminho do objeto desejado.

   O comando a seguir usa exemplo de valores. Substitua os *espaços reservados para entrada do usuário* por suas próprias informações.

   ```
   python get-only-url.py amzn-s3-demo-bucket <object-path>
   ```

   O script exibirá um URL GET pré-assinado:

   ```
   Generated GET presigned URL: https://amzn-s3-demo-
   bucket.s3.amazonaws.com/object.txt?
   AWSAccessKeyId=AKIAIOSFODNN7EXAMPLE&Signature=vjbyNxybdZaMmLa
   %2ByT372YEAiv4%3D&Expires=1741978496
   ```

3. Agora você pode baixar o arquivo usando o URL pré-assinado gerado com curl:

   ```
   curl -X GET "generated-presigned-url" -o "path/to/save/file"
   ```

Para obter exemplos de uso de SDKs da AWS para gerar um URL pré-assinado e compartilhar um objeto, consulte Create a presigned URL for Amazon S3 by using an AWS SDK.

> **Note**
>
> Para todas as Regiões da AWS lançadas após 20 de março de 2019, você precisa especificar o `endpoint-url` e a `Região da AWS` com a solicitação. Para obter uma lista de todos os endpoints e as regiões do Amazon S3, consulte Regiões e endpoints na Referência geral da AWS.

> **Note**
>
> Ao usar AWS SDKs, o atributo de marcação deve ser um cabeçalho e não um parâmetro de consulta. Todos os outros atributos podem ser transmitidos como um parâmetro para o URL pré-assinado.

Usar o AWS Toolkit for Visual Studio (Windows)

> **Note**
>
> No momento, o AWS Toolkit for Visual Studio não é compatível com o Visual Studio para Mac.

1. Instale o AWS Toolkit for Visual Studio usando as instruções a seguir, Installing and setting up the Toolkit for Visual Studio no Guia do usuário do AWS Toolkit for Visual Studio.
2. Conecte-se à AWS usando as etapas a seguir, Conectar-se ao AWS no Guia do usuário do AWS Toolkit for Visual Studio.
3. No painel do lado esquerdo chamado AWS Explorer, clique duas vezes no bucket que contém seu objeto.
4. Clique com o botão direito do mouse no objeto para o qual você deseja gerar um URL pré-assinado e selecione Criar URL pré-assinado….
5. Na janela pop-up, defina a data e hora de validade para o URL pré-assinado.
6. A Chave de objeto deve ser preenchida previamente com base no objeto selecionado.

7. Escolha GET para especificar que esse URL pré-assinado será usado para baixar um objeto.
8. Escolha o botão Generate (Gerar).
9. Para copiar o URL para a área de transferência, escolha Copy (Copiar).
10. Para usar o URL pré-assinado gerado, cole o URL em qualquer navegador.

Usar o AWS Toolkit for Visual Studio Code

Se estiver usando o Visual Studio Code, você poderá gerar um URL pré-assinado para compartilhar um objeto sem escrever nenhum código usando o AWS Toolkit for Visual Studio Code. Para obter informações gerais, consulte AWS Toolkit for Visual Studio Code no Guia do usuário do AWS Toolkit for Visual Studio Code.

Para obter instruções sobre como instalar o AWS Toolkit for Visual Studio Code, consulte Instalar o AWS Toolkit for Visual Studio Code no Guia do usuário do AWS Toolkit for Visual Studio Code.

1. Conecte-se à AWS usando as etapas a seguir, Conectar-se ao AWS Toolkit for Visual Studio Code no Guia do usuário do AWS Toolkit for Visual Studio Code.
2. Selecione o logotipo da AWS no painel esquerdo do Visual Studio Code.
3. Em EXPLORER, selecione S3.
4. Escolha um bucket e um arquivo e abra o menu de contexto (clique com o botão direito do mouse).
5. Escolha Gerar URL pré-assinado e defina o tempo de validade (em minutos).
6. Pressione Enter e o URL pré-assinado será copiado para a área de transferência.

Carregar objetos com URLs pré-assinados

Você pode usar URLs pré-assinados para permitir que alguém carregue um objeto no seu bucket do Amazon S3. O uso de um URL pré-assinado permitirá um carregamento sem exigir que outra pessoa tenha credenciais ou permissões de segurança da AWS. Um URL pré-assinado é limitado pelas permissões do usuário que o criou. Isto é, se você receber um URL pré-assinado para carregar um objeto, só poderá fazer isso se o criador do URL pré-assinado tiver as permissões necessárias para carregar esse objeto.

Quando alguém usa o URL para carregar um objeto, o Amazon S3 cria o objeto no bucket especificado. Se um objeto com a mesma chave especificada no pre-signed URL já existir no bucket,

o Amazon S3 substituirá o objeto existente pelo objeto obtido por upload. Após o carregamento, o proprietário do bucket será o proprietário do objeto.

Para obter informações gerais sobre URLs pré-assinados, consulte Baixar e fazer upload de objetos com URLs pré-assinados.

É possível criar um URL pré-assinado para carregar um objeto sem escrever nenhum código usando o AWS Explorer for Visual Studio. Também é possível gerar um URL pré-assinado programaticamente usando AWS SDKs.

> **Note**
>
> No momento, o AWS Toolkit for Visual Studio não é compatível com o Visual Studio para Mac.

Usar o AWS Toolkit for Visual Studio (Windows)

1. Instale o AWS Toolkit for Visual Studio usando as instruções a seguir, Installing and setting up the Toolkit for Visual Studio no Guia do usuário do AWS Toolkit for Visual Studio.
2. Conecte-se à AWS usando as etapas a seguir, Conectar-se ao AWS no Guia do usuário do AWS Toolkit for Visual Studio.
3. No painel do lado esquerdo chamado AWS Explorer, clique com o botão direito do mouse no bucket para o qual você deseja que um objeto seja carregado.
4. Escolha Criar URL pré-assinado….
5. Na janela pop-up, defina a data e hora de validade para o URL pré-assinado.
6. Em Chave de objeto, defina o nome do arquivo a ser carregado. O arquivo que você está carregando deve corresponder exatamente a esse nome. Se já existir um objeto com a mesma chave de objeto no bucket, o Amazon S3 substituirá o objeto existente pelo objeto recém-carregado.
7. Escolha PUT para especificar que esse URL pré-assinado será usado para carregar um objeto.
8. Escolha o botão Generate (Gerar).
9. Para copiar o URL para a área de transferência, escolha Copy (Copiar).
10. Para usar esse URL, você pode enviar uma solicitação PUT com o comando `curl`. Inclua o caminho completo para o arquivo e o próprio URL pré-assinado.

```
curl -X PUT -T "/path/to/file" "presigned URL"
```

Usar SDKs da AWS para gerar um URL pré-assinado **PUT** e fazer upload de um arquivo

É possível gerar um URL pré-assinado que possa realizar uma ação do S3 por tempo limitado.

> **Note**
>
> Se você usar a AWS CLI ou SDKs da AWS, o tempo de validade dos URLs pré-assinados poderá ser definido como até sete dias. Para obter mais informações, consulte Tempo de validade para URLs pré-assinados.

Python

O script do Python a seguir gera um URL PUT pré-assinado para fazer upload de um objeto em um bucket de uso geral do S3.

1. Copie o conteúdo do script e salve-o como arquivo "*put-only-url.py*". Para usar os exemplos a seguir, substitua os *espaços reservados para entrada do usuário* por suas próprias informações (como o nome de seu arquivo).

```
import argparse
import boto3
from botocore.exceptions import ClientError

def generate_presigned_url(s3_client, client_method, method_parameters,
 expires_in):
    """
    Generate a presigned Amazon S3 URL that can be used to perform an action.

    :param s3_client: A Boto3 Amazon S3 client.
    :param client_method: The name of the client method that the URL performs.
    :param method_parameters: The parameters of the specified client method.
    :param expires_in: The number of seconds the presigned URL is valid for.
    :return: The presigned URL.
    """
    try:
        url = s3_client.generate_presigned_url(
```

```
            ClientMethod=client_method,
            Params=method_parameters,
            ExpiresIn=expires_in
        )
    except ClientError:
        print(f"Couldn't get a presigned URL for client method
 '{client_method}'.")
        raise
    return url

def main():
    parser = argparse.ArgumentParser()
    parser.add_argument("bucket", help="The name of the bucket.")
    parser.add_argument(
        "key", help="The key (path and filename) in the S3 bucket.",
    )
    args = parser.parse_args()

    # By default, this will use credentials from ~/.aws/credentials
    s3_client = boto3.client("s3")

    # The presigned URL is specified to expire in 1000 seconds
    url = generate_presigned_url(
        s3_client,
        "put_object",
        {"Bucket": args.bucket, "Key": args.key},
        1000
    )
    print(f"Generated PUT presigned URL: {url}")

if __name__ == "__main__":
    main()
```

2. Para gerar uma URL PUT pré-assinado para fazer upload de um arquivo, execute o script a seguir com o nome do bucket e o caminho do objeto desejado.

   O comando a seguir usa exemplo de valores. Substitua os *espaços reservados para entrada do usuário* por suas próprias informações.

   ```
   python put-only-url.py amzn-s3-demo-bucket <object-path>
   ```

   O script exibirá um URL PUT pré-assinado:

```
Generated PUT presigned URL: https://amzn-s3-demo-
bucket.s3.amazonaws.com/object.txt?
AWSAccessKeyId=AKIAIOSFODNN7EXAMPLE&Signature=vjbyNxybdZaMmLa
%2ByT372YEAiv4%3D&Expires=1741978496
```

3. Agora você pode fazer upload do arquivo usando o URL pré-assinado gerado com curl:

```
curl -X PUT -T "path/to/your/local/file" "generated-presigned-url"
```

Para obter mais exemplos de como usar SDKs da AWS para gerar um URL pré-assinado para fazer upload de um objeto, consulte Create a presigned URL for Amazon S3 by using an AWS SDK.

Transformar objetos com o S3 Object Lambda

Com o Amazon S3 Object Lambda, você pode adicionar seu próprio código às solicitações `GET`, `LIST` e `HEAD` do Amazon S3 para modificar e processar dados, conforme eles são retornados para uma aplicação. Você pode usar o código personalizado para modificar os dados retornados por solicitações `GET` do S3 para filtrar linhas, redimensionar imagens e marcas d'água dinamicamente, editar dados confidenciais e muito mais. Você também pode usar o S3 Object Lambda para modificar a saída das solicitações `LIST` do S3 para criar uma visualização personalizada de todos os objetos em um bucket e as solicitações `HEAD` do S3 para modificar os metadados do objeto, como nome e tamanho do objeto. Você pode usar o S3 Object Lambda como origem para sua distribuição do Amazon CloudFront a fim de personalizar dados para usuários finais, como redimensionar imagens automaticamente, transcodificar formatos mais antigos (como de JPEG para WebP) ou remover metadados. Para obter mais informações, consulte a publicação do blog da AWS Usar o Amazon S3 Object Lambda com o Amazon CloudFront. Alimentado pelas funções do AWS Lambda, seu código é executado em uma infraestrutura totalmente gerenciada pela AWS. O uso do S3 Object Lambda reduz a necessidade de criar e armazenar cópias derivadas de seus dados ou de executar proxies, tudo sem a necessidade de alterar suas aplicações.

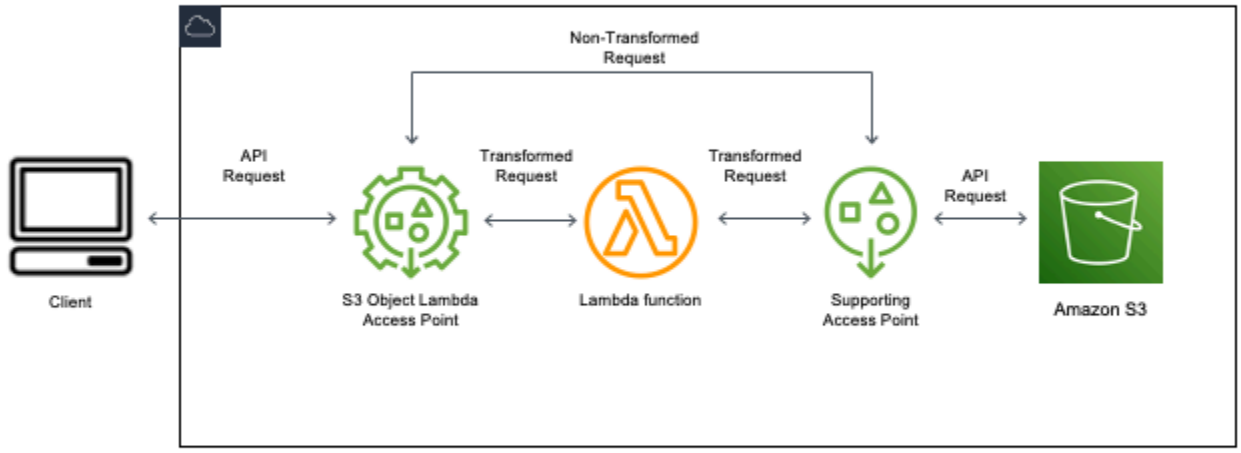
Como o S3 Object Lambda funciona

O S3 Object Lambda usa funções do AWS Lambda para processar automaticamente a saída de solicitações `GET`, `LIST` e `HEAD` padrão do S3. O AWS Lambda é um serviço de computação sem servidor que executa código definido pelo cliente sem exigir o gerenciamento de recursos

de computação subjacentes. Você pode criar e executar suas próprias funções do Lambda personalizadas, adaptando a transformação de dados para seus casos de uso específicos.

Depois de configurar uma função do Lambda, anexe-a a um endpoint de serviço do S3 Object Lambda, conhecido como ponto de acesso do Object Lambda. O ponto de acesso do Object Lambda usa um ponto de acesso padrão do S3, conhecido como ponto de acesso de suporte, para acessar os dados.

Quando você envia uma solicitação para seu ponto de acesso do Object Lambda, o Amazon S3 chama automaticamente a função do Lambda. Qualquer dado recuperado usando uma solicitação `GET`, `LIST` ou `HEAD` do S3 por meio do ponto de acesso do Object Lambda retorna um resultado transformado de volta à aplicação. Todas as outras solicitações são processadas como normais, conforme ilustrado no diagrama a seguir.



Os tópicos nesta seção descrevem como trabalhar com o S3 Object Lambda.

Tópicos

- Criar pontos de acesso do Object Lambda
- Usar pontos de acesso do Amazon S3 Object Lambda
- Considerações sobre segurança para pontos de acesso do S3 Object Lambda

- Escrever funções do Lambda para pontos de acesso do S3 Object Lambda
- Usar funções do Lambda criadas pela AWS
- Práticas recomendadas e diretrizes para o S3 Object Lambda
- Tutoriais do S3 Object Lambda
- Depurar e solucionar problemas do S3 Object Lambda

Criar pontos de acesso do Object Lambda

Um ponto de acesso do Object Lambda está associado exatamente a um único ponto de acesso padrão, que você especifica durante a criação. Para criar um ponto de acesso do Object Lambda, você precisa dos seguintes recursos:

- Um ponto de acesso do S3 padrão. Quando você trabalha com pontos de acesso do Object Lambda, esse ponto de acesso padrão é conhecido como ponto de acesso de suporte e está anexado a um bucket do S3 ou a um volume do Amazon FSx para OpenZFS. Para obter informações sobre a criação de pontos de acesso padrão, consulte the section called “Criar um ponto de acesso”.
- Uma função do AWS Lambda. Você pode criar sua própria função do Lambda ou usar uma função pré-criada. Para obter mais informações sobre como criar funções do Lambda, consulte the section called “Escrever funções do Lambda”. Para obter mais informações sobre funções pré-construídas, consulte Usar funções do Lambda criadas pela AWS.
- (Opcional) Uma política do AWS Identity and Access Management (IAM). Os pontos de acesso do Amazon S3 são compatíveis com políticas de recursos do IAM que você pode usar para controlar o uso do ponto de acesso por recurso, usuário ou outras condições. Para obter mais informações sobre como criar essas políticas, consulte the section called “Configurar políticas do IAM”.

As seções a seguir descrevem como criar um ponto de acesso do Object Lambda usando:

- A AWS Management Console
- A AWS Command Line Interface (AWS CLI)
- Um modelo do AWS CloudFormation
- A AWS Cloud Development Kit (AWS CDK)

Para obter informações sobre como criar um ponto de acesso do Object Lambda usando a API REST, consulte `CreateAccessPointForObjectLambda` na Referência de API do Amazon Simple Storage Service.

Criar um ponto de acesso do Object Lambda

Use um dos procedimentos a seguir para criar o ponto de acesso do Object Lambda.

Usar o console do S3

Para criar um ponto de acesso do Object Lambda usando o console

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Na barra de navegação, escolha o nome da Região da AWS exibida no momento. Em seguida, escolha a região para a qual você deseja mudar.
3. No painel de navegação à esquerda, escolha Object Lambda access points (Pontos de acesso do Object Lambda).
4. Na página Object Lambda Access Points (Pontos de acesso do Object Lambda), escolha Create Object Lambda Access Point (Criar ponto de acesso do Object Lambda).
5. Em Object Lambda Access Point name (Nome do ponto de acesso do Object Lambda), insira o nome que deseja usar para o ponto de acesso.

   Tal como acontece com pontos de acesso padrão, existem regras para nomeação de pontos de acesso do Object Lambda. Para obter mais informações, consulte Regras de nomenclatura para pontos de acesso.
6. Para Supporting Access Point (Ponto de acesso de suporte), insira ou navegue até o ponto de acesso padrão que você deseja usar. O ponto de acesso deve estar na mesma Região da AWS que os objetos que você deseja transformar. Para obter informações sobre a criação de pontos de acesso padrão, consulte the section called “Criar um ponto de acesso”.
7. Em Configuração de transformação, você pode adicionar uma função que transforma os dados para o ponto de acesso do Object Lambda. Execute um destes procedimentos:

   - Se você já tem uma função do AWS Lambda em sua conta, pode escolhê-la em Invoke Lambda function (Invocar função do Lambda). Aqui você pode inserir o nome do recurso da Amazon (ARN) de uma função do Lambda em sua Conta da AWS ou escolher uma função do Lambda no menu suspenso.

- Se você quiser usar uma função integrada à AWS, escolha o nome da função em Função criada pela AWS e selecione Criar função do Lambda. Isso levará você ao console do Lambda, onde poderá implantar uma função integrada à sua Conta da AWS. Para obter mais informações sobre funções integradas, consulte Usar funções do Lambda criadas pela AWS.

Em S3 APIs (APIs do S3), escolha uma ou mais operações de API para invocar. Para cada API selecionada, você deve especificar uma função do Lambda para invocar.

8. (Opcional) Em Payload (Carga útil), adicione o texto JSON que você quer fornecer para a função do Lambda como entrada. Você pode configurar cargas com parâmetros diferentes para pontos de acesso do Object Lambda diferentes que invocam a mesma função do Lambda, estendendo, assim, a flexibilidade da função do Lambda.

> **Important**
>
> Ao usar os pontos de acesso do Object Lambda, verifique se a carga útil não contém informações sigilosas.

9. (Opcional) Em Range and part number (Intervalo e número de peça), você deve habilitar essa opção a fim processar solicitações `GET` e `HEAD` com cabeçalhos de intervalo e número de peça. Habilitar essa opção confirma que sua função do Lambda é capaz de reconhecer e processar essas solicitações. Para obter mais informações sobre cabeçalhos de intervalo e números de peça, consulte Trabalhar com cabeçalhos Range e partNumber.
10. (Opcional) Em Métricas de solicitação, escolha Ativar ou Desativar para adicionar o monitoramento do Amazon S3 ao ponto de acesso do Object Lambda. As métricas de solicitação são cobradas na taxa padrão do Amazon CloudWatch.
11. (Opcional) Em Object Lambda Access Point policy (Política de ponto de acesso do Object Lambda), defina uma política de recursos. As políticas de recursos concedem permissões para o ponto de acesso do Object Lambda especificado e podem controlar o uso do ponto de acesso por recurso, usuário ou outras condições. Para obter mais informações sobre as políticas de recursos de ponto de acesso do Object Lambda, consulte Configurar políticas do IAM para pontos de acesso do Object Lambda.
12. Em Block Public Access settings for this Object Lambda Access Point (Configurações de bloqueio de acesso público para este ponto de acesso do Object Lambda), selecione as configurações de bloqueio de acesso público que você deseja aplicar. Todas as configurações de bloqueio de acesso público são habilitadas por padrão para novos pontos de acesso do Object Lambda, e recomendamos que você deixe as configurações padrão habilitadas.

Atualmente, o Amazon S3 não oferece suporte à alteração das configurações de bloqueio de acesso público a pontos de acesso do Object Lambda após a criação de pontos de acesso do Object Lambda.

Para obter mais informações sobre como usar o bloqueio de acesso público do Amazon S3, consulte Gerenciar o acesso público a pontos de acesso para buckets de uso geral.

13. Escolha Create Object Lambda Access Point (Criar ponto de acesso do Object Lambda).

Como usar o AWS CLI

Para criar um ponto de acesso do Object Lambda usando um modelo do AWS CloudFormation

> **Note**
>
> Para usar os comandos a seguir, substitua *user input placeholders* por suas próprias informações.

1. Baixe o pacote de implantação da função `s3objectlambda_deployment_package.zip` do AWS Lambda em S3 Object Lambda default configuration (Configuração padrão do S3 Object Lambda).
2. Execute o comando `put-object` a seguir para fazer upload do pacote em um bucket do Amazon S3.

```
aws s3api put-object --bucket Amazon S3 bucket name --key
 s3objectlambda_deployment_package.zip --body release/
s3objectlambda_deployment_package.zip
```

3. Baixe o modelo `s3objectlambda_defaultconfig.yaml` do AWS CloudFormation em S3 Object Lambda default configuration (Configuração padrão do S3 Object Lambda).
4. Execute o comando `deploy` a seguir para implantar o modelo em sua Conta da AWS.

```
aws cloudformation deploy --template-file s3objectlambda_defaultconfig.yaml \
 --stack-name AWS CloudFormation stack name \
 --parameter-overrides ObjectLambdaAccessPointName=Object Lambda Access Point name
 \
  SupportingAccessPointName=Amazon S3 access point S3BucketName=Amazon S3 bucket \
  LambdaFunctionS3BucketName=Amazon S3 bucket containing your Lambda package \
```

```
 LambdaFunctionS3Key=Lambda object key LambdaFunctionS3ObjectVersion=Lambda object
version \
 LambdaFunctionRuntime=Lambda function runtime --capabilities capability_IAM
```

Você pode configurar esse modelo do AWS CloudFormation para invocar o Lambda para as operações de API `GET`, `HEAD` e `LIST`. Para obter mais informações sobre como modificar a configuração padrão do modelo, consulte the section called “Automatizar a configuração do S3 Object Lambda com AWS CloudFormation”.

Para criar um ponto de acesso do Object Lambda usando a AWS CLI

> **Note**
>
> Para usar os comandos a seguir, substitua *`user input placeholders`* por suas próprias informações.

O exemplo a seguir cria um ponto de acesso do Object Lambda chamado *`my-object-lambda-ap`* para o bucket *`amzn-s3-demo-bucket1`* na conta *`111122223333`*. Esse exemplo pressupõe que um ponto de acesso padrão denominado *`example-ap`* já tenha sido criado. Para obter informações sobre como criar um ponto de acesso padrão, consulte the section called “Criar um ponto de acesso”.

Este exemplo usa a função pré-criada `decompress` da AWS. Para obter mais informações sobre funções pré-construídas, consulte the section called “Usar funções criadas pela AWS”.

1. Crie um bucket. Neste exemplo, usaremos *`amzn-s3-demo-bucket1`*. Para obter mais informações sobre a criação de buckets, consulte the section called “Criar um bucket de uso geral”.
2. Crie um ponto de acesso padrão e anexe-o ao seu bucket. Neste exemplo, usaremos *`example-ap`*. Para obter informações sobre a criação de pontos de acesso padrão, consulte the section called “Criar um ponto de acesso”.
3. Execute um destes procedimentos:

   - Crie na conta uma função do Lambda que você deseja usar para transformar o objeto do Simple Storage Service (Amazon S3). Para obter mais informações sobre como criar funções do Lambda, consulte the section called “Escrever funções do Lambda”. Para usar sua função

personalizada com a AWS CLI, consulte Como usar o Lambda com a AWS CLI no Guia do desenvolvedor do AWS Lambda.

- Use uma função do Lambda pré-criada pela AWS. Para obter mais informações sobre funções pré-construídas, consulte Usar funções do Lambda criadas pela AWS.

4. Crie um arquivo de configuração JSON chamado `my-olap-configuration.json`. Nessa configuração, forneça o ponto de acesso de suporte e o nome do recurso da Amazon (ARN) para a função do Lambda que você criou nas etapas anteriores ou o ARN da função pré-criada que você está usando.

   Example

```
{
    "SupportingAccessPoint" : "arn:aws:s3:us-
east-1:111122223333:accesspoint/example-ap",
    "TransformationConfigurations": [{
        "Actions" : ["GetObject", "HeadObject", "ListObjects", "ListObjectsV2"],
        "ContentTransformation" : {
            "AwsLambda": {
                "FunctionPayload" : "{\"compressionType\":\"gzip\"}",
                "FunctionArn" : "arn:aws:lambda:us-east-1:111122223333:function/
compress"
            }
        }
    }]
}
```

5. Execute o comando `create-access-point-for-object-lambda` para criar o ponto de acesso do Object Lambda.

```
aws s3control create-access-point-for-object-lambda --account-id 111122223333 --
name my-object-lambda-ap --configuration file://my-olap-configuration.json
```

6. (Opcional) Crie um arquivo de política JSON chamado `my-olap-policy.json`.

   Adicionar uma política de recursos de ponto de acesso do Object Lambda pode controlar o uso do ponto de acesso por recurso, usuário ou outras condições. Essa política de recursos concede a permissão `GetObject` para a conta *444455556666* ao ponto de acesso do Object Lambda especificado.

Example

```
{
    "Version": "2008-10-17",
    "Statement": [
        {
            "Sid": "Grant account 444455556666 GetObject access",
            "Effect": "Allow",
            "Action": "s3-object-lambda:GetObject",
            "Principal": {
                "AWS": "arn:aws:iam::444455556666:root"
            },
            "Resource": "your-object-lambda-access-point-arn"
        }
    ]
}
```

7. (Opcional) Execute o comando `put-access-point-policy-for-object-lambda` para definir sua política de recursos.

```
aws s3control put-access-point-policy-for-object-lambda --account-id 111122223333
 --name my-object-lambda-ap --policy file://my-olap-policy.json
```

8. (Opcional) Especifique uma carga útil.

   Uma carga útil é um JSON opcional que você pode fornecer à sua função do AWS Lambda como entrada. Você pode configurar cargas com parâmetros diferentes para pontos de acesso do Object Lambda diferentes que invocam a mesma função do Lambda, estendendo, assim, a flexibilidade da função do Lambda.

   A configuração do ponto de acesso do Object Lambda a seguir mostra uma carga útil com dois parâmetros.

```
{
 "SupportingAccessPoint": "AccessPointArn",
 "CloudWatchMetricsEnabled": false,
 "TransformationConfigurations": [{
  "Actions": ["GetObject", "HeadObject", "ListObjects", "ListObjectsV2"],
  "ContentTransformation": {
   "AwsLambda": {
```

```
    "FunctionArn": "FunctionArn",
    "FunctionPayload": "{\"res-x\": \"100\",\"res-y\": \"100\"}"
   }
  }
 }]
}
```

A configuração de ponto de acesso do Object Lambda a seguir mostra uma carga útil com um único parâmetro e com `GetObject-Range`, `GetObject-PartNumber`, `HeadObject-Range` e `HeadObject-PartNumber` ativados.

```
{
    "SupportingAccessPoint":"AccessPointArn",
    "CloudWatchMetricsEnabled": false,
    "AllowedFeatures": ["GetObject-Range", "GetObject-PartNumber", "HeadObject-
Range", "HeadObject-PartNumber"],
    "TransformationConfigurations": [{
        "Action": ["GetObject", "HeadObject", "ListObjects", "ListObjectsV2"],
        "ContentTransformation": {
            "AwsLambda": {
                "FunctionArn":"FunctionArn",
                "FunctionPayload": "{\"compression-amount\": \"5\"}"
            }
        }
    }]
}
```

Important

Ao usar os pontos de acesso do Object Lambda, verifique se a carga útil não contém informações sigilosas.

Usar o console e o template do AWS CloudFormation

É possível criar um ponto de acesso do Object Lambda usando a configuração padrão fornecida pelo Amazon S3. Você pode baixar um modelo do AWS CloudFormation e o código-fonte da função do Lambda do repositório do GitHub e implantar esses recursos para configurar um ponto de acesso funcional do Object Lambda.

Para obter informações sobre como modificar a configuração padrão do template do AWS CloudFormation, consulte the section called “Automatizar a configuração do S3 Object Lambda com AWS CloudFormation”.

Para obter informações sobre como configurar pontos de acesso do Object Lambda usando o AWS CloudFormation sem o modelo, consulte `AWS::S3ObjectLambda::AccessPoint` no Guia do usuário do AWS CloudFormation.

Para carregar o pacote de implantação da função Lambda

1. Baixe o pacote de implantação da função `s3objectlambda_deployment_package.zip` do AWS Lambda em S3 Object Lambda default configuration (Configuração padrão do S3 Object Lambda).
2. Faça upload do pacote em um bucket do Amazon S3.

Para criar um ponto de acesso do Object Lambda usando o console do AWS CloudFormation

1. Baixe o modelo `s3objectlambda_defaultconfig.yaml` do AWS CloudFormation em S3 Object Lambda default configuration (Configuração padrão do S3 Object Lambda).
2. Faça login no Console de Gerenciamento da AWS e abra o console do AWS CloudFormation em https://console.aws.amazon.com/cloudformation.
3. Execute um destes procedimentos:
   - Se você nunca usou o AWS CloudFormation, na página inicial do AWS CloudFormation, escolha Create stack (Criar pilha).
   - Se você já usou o AWS CloudFormation, no painel de navegação à esquerda, selecione Stacks (Pilhas). Selecione Create stack (Criar pilha), depois escolha With new resources (standard) (Com novos recursos (padrão)).
4. Em Prerequisite - Prepare template (Pré-requisito - Preparar template), escolha Template is ready (O template está pronto).
5. Em Specify template (Especificar modelo), escolha Upload a template file (Fazer upload de um arquivo de modelo) e faça upload de `s3objectlambda_defaultconfig.yaml`.
6. Escolha Próximo.
7. Na página Specify stack details (Especificar detalhes da pilha), insira um nome para a pilha.
8. Na seção Parameters (Parâmetros), especifique os parâmetros que são definidos no modelo da pilha:

a. Em CreateNewSupportingAccessPoint, siga um destes procedimentos:

   - Se você já tem um ponto de acesso de suporte para o bucket do S3 em que fez upload do modelo, escolha false (falso).
   - Se quiser criar um ponto de acesso para esse bucket, selecione true (verdadeiro).

b. Para EnableCloudWatchMonitoring, escolha true (verdadeiro) ou false (falso), dependendo se deseja habilitar as métricas e os alarmes de solicitação do Amazon CloudWatch.

c. (Opcional) Em LambdaFunctionPayload, adicione o texto JSON que você quer fornecer para a função do Lambda como entrada. Você pode configurar cargas com parâmetros diferentes para pontos de acesso do Object Lambda diferentes que invocam a mesma função do Lambda, estendendo, assim, a flexibilidade da função do Lambda.

   > **Important**
   >
   > Ao usar os pontos de acesso do Object Lambda, verifique se a carga útil não contém informações sigilosas.

d. Em LambdaFunctionRuntime, insira seu tempo de execução preferido para a função do Lambda. As opções disponíveis são `nodejs14.x`, `python3.9` e `java11`.

e. Em LambdaFunctionS3BucketName, insira o nome do bucket do Amazon S3 para o qual você fez upload do pacote de implantação.

f. Em LambdaFunctionS3Key, insira o nome da chave de objeto do Amazon S3 para o qual você fez upload do pacote de implantação.

g. Em LambdaFunctionS3Key, insira a versão do objeto do Amazon S3 no qual você fez upload do pacote de implantação.

h. Em ObjectLambdaAccessPointName, insira um nome para o ponto de acesso do Object Lambda.

i. Em S3BucketName, insira o nome do bucket do Amazon S3 que será associado ao ponto de acesso do Object Lambda.

j. Em SupportingAccessPointName, insira o nome de seu ponto de acesso de suporte.

   > **Note**
   >
   > Trata-se de um ponto de acesso associado ao bucket do Amazon S3 que você escolheu na etapa anterior. Caso não tenha nenhum ponto de acesso associado ao

bucket do Amazon S3, você poderá configurar o modelo para criar um selecionando true (verdadeiro) em CreateNewSupportingAccessPoint.

9. Escolha Avançar.
10. Na página Configurar opções de pilha, selecione Avançar.

    Para obter mais informações sobre as configurações opcionais nesta página, consulte Configurar opções de pilha do AWS CloudFormation no Guia do usuário do AWS CloudFormation.
11. Na página Review (Revisão), escolha Create stack (Criar pilha).

Como usar o AWS Cloud Development Kit (AWS CDK)

Para obter mais informações sobre como configurar pontos de acesso do Object Lambda usando o AWS CDK, consulte Biblioteca de estruturas do `AWS::S3ObjectLambda` na Referência de API do AWS Cloud Development Kit (AWS CDK).

Automatizar a configuração do S3 Object Lambda com um modelo do CloudFormation

Você pode usar um modelo do AWS CloudFormation para criar rapidamente um ponto de acesso do Amazon S3 Object Lambda. O modelo do CloudFormation cria automaticamente recursos relevantes, configura perfis do AWS Identity and Access Management (IAM) e configura uma função do AWS Lambda que lida automaticamente com solicitações por meio do ponto de acesso do Object Lambda. Com o modelo do CloudFormation, é possível implementar práticas recomendadas, melhorar seu procedimento de segurança e reduzir erros causados por processos manuais.

Esse repositório GitHub contém o modelo do CloudFormation e o código-fonte da função do Lambda. Para obter instruções sobre como usar o modelo, consulte the section called “Criar pontos de acesso do Object Lambda”.

A função do Lambda fornecida no modelo não executa nenhuma transformação. Em vez disso, ele retorna seus objetos como estão da fonte de dados subjacente. Você pode clonar a função e adicionar seu próprio código de transformação para modificar e processar dados à medida que eles são retornados a uma aplicação. Para obter mais informações sobre como modificar a função, consulte the section called “Modificar a função Lambda” e the section called “Escrever funções do Lambda”.

Modificar o template

Criar um ponto de acesso de suporte

O S3 Object Lambda usa dois pontos de acesso: um ponto de acesso do Object Lambda e um ponto de acesso padrão do S3, chamado de ponto de acesso de suporte. Quando você faz uma solicitação a um ponto de acesso do Object Lambda, o S3 chama o Lambda em seu nome ou delega a solicitação ao ponto de acesso de suporte, de acordo com a configuração do S3 Object Lambda. É possível criar um ponto de acesso de suporte transmitindo o seguinte parâmetro como parte do comando `aws cloudformation deploy` ao implantar o modelo.

```
CreateNewSupportingAccessPoint=true
```

Configurar uma carga útil de função

Você pode configurar uma carga útil para fornecer dados complementares à função Lambda transmitindo o seguinte parâmetro como parte do comando `aws cloudformation deploy` ao implantar o template.

```
LambdaFunctionPayload="format=json"
```

Habilitar o monitoramento do Amazon CloudWatch

Você pode habilitar o monitoramento do CloudWatch transmitindo o seguinte parâmetro como parte do comando `aws cloudformation deploy` ao implantar o template.

```
EnableCloudWatchMonitoring=true
```

Esse parâmetro habilita o ponto de acesso do Object Lambda para métricas de solicitação do Amazon S3 e cria dois alarmes do CloudWatch para monitorar erros no lado do cliente e no lado do servidor.

> **Note**
>
> O uso do Amazon CloudWatch incorrerá em custos adicionais. Para obter mais informações sobre métricas de solicitação do Amazon S3, consulte Monitorar e registrar de pontos de acesso.
> Para obter detalhes sobre os preços, consulte Definição de preço do CloudWatch.

Configurar a simultaneidade provisionada

Para reduzir a latência, é possível configurar a simultaneidade provisionada para a função do Lambda com base no ponto de acesso do Object Lambda editando o modelo para incluir as seguintes linhas em `Resources`.

```
LambdaFunctionVersion:
      Type: AWS::Lambda::Version
      Properties:
        FunctionName: !Ref LambdaFunction
        ProvisionedConcurrencyConfig:
            ProvisionedConcurrentExecutions: Integer
```

> **Note**
>
> Haverá cobranças adicionais pela simultaneidade de provisionamento. Para obter mais informações sobre simultaneidade provisionada, consulte Gerenciar a simultaneidade provisionada do Lambda no Guia do desenvolvedor do AWS Lambda.
> Para obter detalhes de preço, consulte Definição de preço do AWS Lambda.

Modificar a função Lambda

Alterar os valores do cabeçalho de uma solicitação **`GetObject`**

Por padrão, a função do Lambda encaminha todos os cabeçalhos, exceto `Content-Length` e `ETag`, da solicitação de URL pré-assinado ao cliente do `GetObject`. Com base em seu código de transformação na função Lambda, é possível escolher enviar novos valores de cabeçalho ao cliente do `GetObject`.

Você pode atualizar sua função do Lambda para enviar novos valores de cabeçalho, transmitindo-os na operação de API `WriteGetObjectResponse`.

Por exemplo, se a função Lambda traduzir texto em objetos do Amazon S3 para um idioma diferente, você poderá transmitir um novo valor no cabeçalho `Content-Language`. Faça isso modificando a função `writeResponse`, conforme mostrado abaixo:

```
async function writeResponse (s3Client: S3, requestContext: GetObjectContext,
 transformedObject: Buffer,
```

```
  headers: Headers): Promise<PromiseResult<{}, AWSError>> {
  const { algorithm, digest } = getChecksum(transformedObject);

  return s3Client.writeGetObjectResponse({
    RequestRoute: requestContext.outputRoute,
    RequestToken: requestContext.outputToken,
    Body: transformedObject,
    Metadata: {
      'body-checksum-algorithm': algorithm,
      'body-checksum-digest': digest
    },
    ...headers,
    ContentLanguage: 'my-new-language'
  }).promise();
}
```

Para obter uma lista completa dos cabeçalhos compatíveis, consulte `WriteGetObjectResponse` na Referência da API do Amazon Simple Storage Service.

Retornar cabeçalhos de metadados

Você pode atualizar sua função do Lambda para enviar novos valores de cabeçalho, transmitindo-os na solicitação de operação de API `WriteGetObjectResponse`.

```
async function writeResponse (s3Client: S3, requestContext: GetObjectContext,
 transformedObject: Buffer,
  headers: Headers): Promise<PromiseResult<{}, AWSError>> {
  const { algorithm, digest } = getChecksum(transformedObject);

  return s3Client.writeGetObjectResponse({
    RequestRoute: requestContext.outputRoute,
    RequestToken: requestContext.outputToken,
    Body: transformedObject,
    Metadata: {
      'body-checksum-algorithm': algorithm,
      'body-checksum-digest': digest,
      'my-new-header': 'my-new-value'
    },
    ...headers
  }).promise();
}
```

Retornar um novo código de status

É possível retornar um código de status personalizado ao cliente do `GetObject` transmitindo-o na solicitação de operação de API `WriteGetObjectResponse`.

```
async function writeResponse (s3Client: S3, requestContext: GetObjectContext,
 transformedObject: Buffer,
  headers: Headers): Promise<PromiseResult<{}, AWSError>> {
  const { algorithm, digest } = getChecksum(transformedObject);

  return s3Client.writeGetObjectResponse({
    RequestRoute: requestContext.outputRoute,
    RequestToken: requestContext.outputToken,
    Body: transformedObject,
    Metadata: {
      'body-checksum-algorithm': algorithm,
      'body-checksum-digest': digest
    },
    ...headers,
    StatusCode: Integer
  }).promise();
}
```

Para obter uma lista completa dos códigos de status compatíveis, consulte `WriteGetObjectResponse` na Referência da API do Amazon Simple Storage Service.

Aplicar os parâmetros **`Range`** e **`partNumber`** no objeto de origem

Por padrão, o ponto de acesso do Object Lambda criado pelo modelo do CloudFormation pode lidar com os parâmetros `Range` e `partNumber`. A função Lambda aplica o intervalo ou o número da parte solicitado ao objeto transformado. Para isso, a função precisa baixar o objeto inteiro e executar a transformação. Em alguns casos, os intervalos de objetos transformados podem mapear exatamente para seus intervalos de objetos de origem. Isso significa que solicitar o intervalo de bytes A–B no objeto de origem e executar a transformação poderá produzir o mesmo resultado que solicitar o objeto inteiro, executar a transformação e retornar o intervalo de bytes A–B no objeto transformado.

Nesses casos, é possível alterar a implementação da função Lambda para aplicar o intervalo ou o número da parte diretamente no objeto de origem. Essa abordagem reduz a latência geral da função e a memória necessárias. Para obter mais informações, consulte the section called “Trabalhar com cabeçalhos Range e partNumber”.

Desabilitar o tratamento de **`Range`** e **`partNumber`**

Por padrão, o ponto de acesso do Object Lambda criado pelo modelo do CloudFormation pode lidar com os parâmetros `Range` e `partNumber`. Se você não precisar desse comportamento, poderá desabilitá-lo removendo as seguintes linhas do modelo:

```
AllowedFeatures:
  - GetObject-Range
  - GetObject-PartNumber
  - HeadObject-Range
  - HeadObject-PartNumber
```

Transformar objetos grandes

Por padrão, a função Lambda processa todo o objeto na memória antes que ele possa começar a transmitir a resposta ao S3 Object Lambda. É possível modificar a função para transmitir a resposta à medida que ela executa a transformação. Isso ajuda a reduzir a latência de transformação e o tamanho da memória da função do Lambda. Para obter um exemplo de implementação, consulte o Exemplo de conteúdo compactado de transmissão.

Usar pontos de acesso do Amazon S3 Object Lambda

Fazer solicitações via Pontos de Acesso do Amazon S3 Object Lambda funciona da mesma forma que fazer solicitações por meio de outros pontos de acesso. Para obter mais informações sobre como fazer solicitações via ponto de acesso, consulte Usar o recurso Pontos de Acesso Amazon S3 para buckets de uso geral. Você pode fazer solicitações via pontos de acesso do Object Lambda usando o console do Amazon S3, a AWS Command Line Interface (AWS CLI), AWS SDKs ou API REST do Amazon S3.

> **Important**
>
> Os nomes do recursos da Amazon (ARNs) para pontos de acesso do Object Lambda usam um nome de serviço de `s3-object-lambda`. Assim, os ARNs dos pontos de acesso do Object Lambda começam com `arn:aws::s3-object-lambda`, em vez do prefixo `arn:aws::s3` usado com outros pontos de acesso.

Como encontrar o ARN do ponto de acesso do Object Lambda

Para usar um ponto de acesso do Object Lambda com a AWS CLI ou AWS SDKs, é necessário saber o nome do recurso da Amazon (ARN) do ponto de acesso do Object Lambda. Os exemplos

a seguir mostram como encontrar o ARN para um ponto de acesso do Object Lambda usando o console ou a AWS CLI do Amazon S3.

Usar o console do S3

Para encontrar o ARN do seu ponto de acesso do Object Lambda usando o console

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Object Lambda access points (Pontos de acesso do Object Lambda).
3. Selecione o botão de opção próximo ao ponto de acesso do Object Lambda cujo ARN você deseja copiar.
4. Escolha Copy ARN (Copiar ARN).

Como usar o AWS CLI

Para encontrar o ARN do ponto de acesso do Object Lambda usando a AWS CLI

1. Para recuperar uma lista dos pontos de acesso do Object Lambda associados à Conta da AWS, execute o comando a seguir. Antes de executar o comando, substitua o ID da conta *111122223333* pelo ID da sua Conta da AWS.

```
aws s3control list-access-points-for-object-lambda --account-id 111122223333
```

2. Revise a saída do comando para localizar o ARN do ponto de acesso do Object Lambda que deseja usar. A saída do comando anterior será semelhante à saída do exemplo a seguir.

```
{
    "ObjectLambdaAccessPointList": [
        {
            "Name": "my-object-lambda-ap",
            "ObjectLambdaAccessPointArn": "arn:aws:s3-object-lambda:us-
east-1:111122223333:accesspoint/my-object-lambda-ap"
        },
        ...
    ]
}
```

Como usar um alias no estilo do bucket para o ponto de acesso do Object Lambda do bucket do S3

Quando você cria um ponto de acesso do Object Lambda, o Amazon S3 gera automaticamente um alias exclusivo para seu ponto de acesso do Object Lambda. É possível usar esse alias em vez de um nome de bucket do Amazon S3 ou o nome do recurso da Amazon (ARN) do ponto de acesso do Object Lambda em uma solicitação para operações de plano de dados do ponto de acesso. Para obter uma lista dessas operações, consulte Compatibilidade dos pontos de acesso.

Um nome de alias do ponto de acesso do Object Lambda é criado dentro do mesmo namespace de um bucket do Amazon S3. Esse nome de alias é gerado automaticamente, e não é possível alterá-lo. Para um ponto de acesso do Object Lambda existente, um alias é automaticamente atribuído para uso. Um nome de alias de ponto de acesso do Object Lambda atende a todos os requisitos de um nome de bucket válido do Amazon S3 e consiste nas seguintes partes:

`Object Lambda Access Point name prefix``-metadata--ol-s3`

> **Note**
>
> O sufixo `--ol-s3` é reservado para nomes de alias de ponto de acesso e não pode ser usado para nomes de bucket ou de ponto de acesso do Object Lambda. Para obter mais informações sobre as regras para nomes de bucket do Amazon S3, consulte Regras de nomenclatura de buckets de uso geral.

Os exemplos a seguir mostram o ARN e o alias de ponto de acesso do Object Lambda para um ponto de acesso do Object Lambda chamado *`my-object-lambda-access-point`*:

- ARN: `arn:aws:s3-object-lambda:`*`region`*`:`*`account-id`*`:accesspoint/`*`my-object-lambda-access-point`*
- Alias de ponto de acesso do Object Lambda: *`my-object-lambda-acc-1a4n8yjrb3kda96f67zwrwiiuse1a`*`--ol-s3`

Ao usar um ponto de acesso do Object Lambda, você pode usar o nome do alias do ponto de acesso do Object Lambda sem exigir grandes alterações no código.

Quando você exclui um ponto de acesso do Object Lambda, o nome do alias do ponto de acesso do Object Lambda se torna inativo e não provisionado.

Como encontrar o alias do ponto de acesso do Object Lambda

Usar o console do S3

Para encontrar o alias do ponto de acesso do Object Lambda usando o console

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Object Lambda access points (Pontos de acesso do Object Lambda).
3. Para o ponto de acesso do Object Lambda que você deseja usar, copie o valor do alias do ponto de acesso do Object Lambda.

Como usar o AWS CLI

Quando você cria um ponto de acesso do Object Lambda, o Amazon S3 gera automaticamente um nome de alias de ponto de acesso do Object Lambda, conforme mostrado no exemplo de comando a seguir. Para executar esse comando, substitua os *`user input placeholders`* por suas próprias informações. Para obter informações sobre como criar um ponto de acesso do Object Lambda usando a AWS CLI, consulte Para criar um ponto de acesso do Object Lambda usando a AWS CLI.

```
aws s3control create-access-point-for-object-lambda --account-id 111122223333 --
name my-object-lambda-access-point --configuration file://my-olap-configuration.json
{
    "ObjectLambdaAccessPointArn": "arn:aws:s3:region:111122223333:accesspoint/my-
access-point",
    "Alias": {
        "Value": "my-object-lambda-acc-1a4n8yjrb3kda96f67zwrwiiuse1a--ol-s3",
        "Status": "READY"
    }
}
```

O nome do alias do ponto de acesso do Object Lambda gerado tem dois campos:

- O campo `Value` é o valor do alias do ponto de acesso do Object Lambda.
- O campo `Status` é o status do alias do ponto de acesso do Object Lambda. Se o status for `PROVISIONING`, o Amazon S3 estará provisionando o alias do ponto de acesso do Object Lambda, e o alias ainda não estará pronto para uso. Se o status for `READY`, o alias do ponto de acesso do Object Lambda terá sido provisionado com êxito e estará pronto para uso.

Para obter mais informações sobre o tipo de dados `ObjectLambdaAccessPointAlias` na API REST, consulte CreateAccessPointForObjectLambda e ObjectLambdaAccessPointAlias na Referência da API do Amazon Simple Storage Service.

Como usar o alias do ponto de acesso do Object Lambda

É possível usar um alias de ponto de acesso do Object Lambda em vez de um nome de bucket do Amazon S3 para as operações listadas em Compatibilidade dos pontos de acesso.

O exemplo da AWS CLI a seguir para o comando `get-bucket-location` usa o alias do ponto de acesso do bucket para retornar a Região da AWS em que o bucket está. Para executar esse comando, substitua os *`user input placeholders`* por suas próprias informações.

```
aws s3api get-bucket-location --bucket my-object-lambda-
acc-w7i37nq6xuzgax3jw3oqtifiusw2a--ol-s3

{
    "LocationConstraint": "us-west-2"
}
```

Se o alias do ponto de acesso do Object Lambda em uma solicitação não for válido, o código de erro `InvalidAccessPointAliasError` será retornado. Para obter mais informações sobre `InvalidAccessPointAliasError`, consulte Lista de códigos de erro na Referência de API do Amazon Simple Storage Service.

As limitações de um alias de um ponto de acesso do Object Lambda são as mesmas de um alias de ponto de acesso. Para obter mais informações sobre os limites de um alias do ponto de acesso, consulte Limitações dos alias de ponto de acesso.

Considerações sobre segurança para pontos de acesso do S3 Object Lambda

Com o Amazon S3 Object Lambda, você pode realizar transformações personalizadas em dados à medida que deixa o S3 usando a escala e a flexibilidade do AWS Lambda como uma plataforma de computação. O S3 e o Lambda permanecem seguros por padrão, mas, para manter a segurança, é necessária uma consideração especial do autor da função do Lambda. O S3 Object Lambda exige que todo o acesso seja feito por entidades autenticadas (sem acesso anônimo) e por HTTPS.

Para mitigar os riscos de segurança, recomendamos o seguinte:

- Defina o escopo do perfil de execução do Lambda com o menor conjunto de permissões possível.
- Sempre que possível, verifique se a função do Lambda acessa o Amazon S3 por meio do URL pré-assinado fornecido.

Configurar políticas do IAM

Os pontos de acesso do S3 são compatíveis com as políticas de recursos do AWS Identity and Access Management (IAM) que permitem controlar o uso do ponto de acesso por recurso, usuário ou por outras condições. Para obter mais informações, consulte Configurar políticas do IAM para pontos de acesso do Object Lambda.

Comportamento de criptografia

Como os pontos de acesso do Object Lambda usam o Amazon S3 e o AWS Lambda, há diferenças no comportamento de criptografia. Para obter mais informações sobre o comportamento de criptografia padrão do S3, consulte Definir o comportamento padrão da criptografia para os buckets do Amazon S3.

- Quando você usa a criptografia do lado do servidor do S3 com pontos de acesso do Object Lambda, o objeto é descriptografado antes de ser enviado para o Lambda. Depois que o objeto é enviado para o Lambda, ele é processado sem criptografia (no caso de uma solicitação `GET` ou `HEAD`).
- Para evitar que a chave de criptografia seja registrada em log, o S3 rejeitará solicitações `GET` e `HEAD` para objetos criptografados usando criptografia no servidor com chaves fornecidas pelo cliente (SSE-C). No entanto, a função do Lambda ainda pode recuperar esses objetos desde que tenha acesso à chave fornecida pelo cliente.
- Ao usar a criptografia do lado do cliente do S3 com pontos de acesso do Object Lambda, verifique se o Lambda tem acesso à chave de criptografia para descriptografar e criptografar novamente o objeto.

Segurança dos pontos de acesso

O S3 Object Lambda usa dois pontos de acesso: um ponto de acesso do Object Lambda e um ponto de acesso padrão do S3, chamado de ponto de acesso de suporte. Quando você faz uma solicitação a um ponto de acesso do Object Lambda, o S3 chama o Lambda em seu nome ou delega a solicitação ao ponto de acesso de suporte, de acordo com a configuração do S3 Object Lambda. Quando o Lambda é chamado para uma solicitação, o S3 gera um URL pré-assinado para seu

objeto em seu nome por meio do ponto de acesso de suporte. Sua função do Lambda receberá esse URL como entrada quando a função for chamada.

É possível definir sua função do Lambda para usar esse URL pré-assinado ao recuperar o objeto original, em vez de chamar o S3 diretamente. Usando esse modelo, você pode aplicar melhores limites de segurança a seus objetos. É possível limitar o acesso direto a objetos por meio de buckets do S3 ou de pontos de acesso do S3 a um conjunto limitado de funções ou usuários do IAM. Essa abordagem também protege suas funções do Lambda de estarem sujeitas ao problema Confused Deputy, no qual uma função mal configurada com permissões diferentes das permissões de seu chamador poderia permitir ou negar acesso a objetos quando não deveria.

Acesso público do ponto de acesso do Object Lambda

O S3 Object Lambda não permite acesso anônimo ou público, pois o Amazon S3 precisa autorizar sua identidade para concluir qualquer solicitação do S3 Object Lambda. Ao chamar solicitações por um ponto de acesso do Object Lambda, é necessário ter a permissão `lambda:InvokeFunction` para a função do Lambda configurada. Da mesma forma, ao chamar outras operações de API por um ponto de acesso do Object Lambda, você precisa ter as permissões `s3:*` necessárias.

Sem essas permissões, as solicitações para chamar o Lambda ou delegar ao S3 apresentarão falha com erros HTTP 403 (Proibido). Todo o acesso deve ser feito por entidades autenticadas. Se precisar de acesso público, use o Lambda@Edge como uma possível alternativa. Para obter mais informações, consulte Personalizar o conteúdo na borda com o Lambda@Edge no Guia do desenvolvedor do Amazon CloudFront.

Endereços IP de ponto de acesso do Object Lambda

As sub-redes de `describe-managed-prefix-lists` são compatíveis com endpoints de nuvem privada virtual (VPC) do gateway e são relacionadas à tabela de roteamento de endpoints da VPC. Como o ponto de acesso do Object Lambda não é compatível com a VPC do gateway, seus intervalos de IP estão ausentes. Os intervalos ausentes pertencem ao Amazon S3, mas não são compatíveis com endpoints da VPC de gateway. Para obter mais informações sobre `describe-managed-prefix-lists`, consulte DescribeManagedPrefixLists na Referência da API do Amazon EC2 e Intervalos de endereços IP da AWS na Referência geral da AWS.

Configurar políticas do IAM para pontos de acesso do Object Lambda

Os pontos de acesso do Amazon S3 são compatíveis com as políticas de recursos do AWS Identity and Access Management (IAM) que você pode usar para controlar o uso do ponto de acesso por

recurso, usuário ou outras condições. Você pode controlar o acesso por meio de uma política de recursos opcional no ponto de acesso do Object Lambda ou uma política de recursos no ponto de acesso de suporte. Para obter um exemplo detalhado, consulte Tutorial: Como transformar dados para sua aplicação com o S3 Object Lambda e Tutorial: Detectar e editar dados PII com o S3 Object Lambda e o Amazon Comprehend.

Os quatro recursos a seguir devem ter permissões concedidas para trabalhar com pontos de acesso do Object Lambda:

- A identidade do IAM, como um usuário ou um perfil. Para obter mais informações sobre as identidades do IAM e as práticas recomendadas, consulte Identidades do IAM (usuários, grupos de usuários e perfis) no Guia do usuário do IAM.
- O ponto de acesso padrão conectado a uma fonte de dados subjacente, como um bucket do S3 ou um volume do Amazon FSx para OpenZFS. Quando você trabalha com pontos de acesso do Object Lambda, esse ponto de acesso padrão é conhecido como ponto de acesso de suporte.
- O ponto de acesso do Object Lambda.
- A função do AWS Lambda.

> **Important**
>
> Antes de salvar a política, solucione os avisos de segurança, os erros, os avisos gerais e as sugestões de AWS Identity and Access Management Access Analyzer. O IAM Access Analyzer executa verificações de política para validar sua política em relação à gramática das políticas e às práticas recomendadas do IAM. Essas verificações geram descobertas e fornecem recomendações práticas que ajudam a criar políticas que sejam funcionais e estejam em conformidade com as práticas recomendadas de segurança.
> Para saber mais sobre a validação de políticas usando o IAM Access Analyzer, consulte Validação de políticas do IAM Access Analyzer no Guia do usuário do IAM. Para visualizar uma lista de avisos, erros e sugestões retornados pelo IAM Access Analyzer, consulte Referência de verificação de políticas do IAM Access Analyzer.

Os seguintes exemplos de política assumem que você tem os seguintes recursos:

- Um bucket do Amazon S3 com o seguinte nome do recurso da Amazon (ARN):

  `arn:aws:s3:::amzn-s3-demo-bucket1`

- Um ponto de acesso do Amazon S3 Standard nesse bucket com o seguinte ARN:

  `arn:aws:s3:us-east-1:111122223333:accesspoint/my-access-point`

- Um ponto de acesso do Object Lambda com o seguinte ARN:

  `arn:aws:s3-object-lambda:us-east-1:111122223333:accesspoint/my-object-lambda-ap`

- Uma função do AWS Lambda com o seguinte ARN:

  `arn:aws:lambda:us-east-1:111122223333:function:MyObjectLambdaFunction`

> **Note**
>
> Se estiver usando uma função do Lambda em sua conta, você deverá incluir a versão da função na declaração da política. No seguinte exemplo de ARN, a versão é indicada por *1*: `arn:aws:lambda:us-east-1:111122223333:function:MyObjectLambdaFunction:1`
> O Lambda não permite adicionar políticas do IAM à versão $LATEST. Para obter mais informações sobre as versões de funções do Lambda, consulte Versões de funções do Lambda no Guia do desenvolvedor do AWS Lambda.

Example : Política de buckets que delega controle de acesso a pontos de acesso

O exemplo de política de buckets do S3 a seguir delega o controle de acesso para um bucket aos pontos de acesso padrão do bucket. Essa política permite total acesso a todos os pontos de acesso pertencentes à conta do proprietário do bucket. Assim, todo o acesso a esse bucket é controlado pelas políticas anexadas aos seus pontos de acesso. Os usuários só podem ler no bucket por meio de um ponto de acesso, o que significa que as operações só podem ser invocadas por meio dos pontos de acesso. Para obter mais informações, consulte Delegar controle de acesso a pontos de acesso.

```
{
    "Version": "2012-10-17",
    "Statement" : [
    {
        "Effect": "Allow",
        "Principal" : { "AWS":"account-ARN"},
```

```
        "Action" : "*",
        "Resource" : [
            "arn:aws:s3:::amzn-s3-demo-bucket1",
            "arn:aws:s3:::amzn-s3-demo-bucket1/*"
        ],
        "Condition": {
            "StringEquals" : { "s3:DataAccessPointAccount" : "Bucket owner's account
 ID" }
        }
    }]
}
```

Example : política do IAM que concede ao usuário as permissões necessárias para usar um ponto de acesso do Object Lambda

A seguinte política do IAM concede a um usuário permissões para a função do Lambda, o ponto de acesso padrão e o ponto de acesso do Object Lambda.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowLambdaInvocation",
      "Action": [
        "lambda:InvokeFunction"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:lambda:us-
east-1:111122223333:function:MyObjectLambdaFunction:1",
      "Condition": {
        "ForAnyValue:StringEquals": {
          "aws:CalledVia": [
            "s3-object-lambda.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "AllowStandardAccessPointAccess",
      "Action": [
        "s3:Get*",
        "s3:List*"
      ],
```

```
      "Effect": "Allow",
      "Resource": "arn:aws:s3:us-east-1:111122223333:accesspoint/my-access-point/*",
      "Condition": {
        "ForAnyValue:StringEquals": {
          "aws:CalledVia": [
            "s3-object-lambda.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "AllowObjectLambdaAccess",
      "Action": [
        "s3-object-lambda:Get*",
        "s3-object-lambda:List*"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3-object-lambda:us-east-1:111122223333:accesspoint/my-
object-lambda-ap"
    }
  ]
}
```

Habilitar permissões para funções de execução do Lambda

Quando são feitas solicitações `GET` a um ponto de acesso do Object Lambda, a função do Lambda precisa de permissão para enviar dados ao ponto de acesso do S3 Object Lambda. Isso é fornecido habilitando a permissão `s3-object-lambda:WriteGetObjectResponse` na função de execução da sua função do Lambda. Crie uma nova função de execução ou atualize uma existente.

> **Note**
>
> Sua função precisa da permissão `s3-object-lambda:WriteGetObjectResponse` somente se você estiver fazendo uma solicitação `GET`.

Como criar uma função de execução no console do IAM

1. Abra o console do IAM, em https://console.aws.amazon.com/iam/.
2. No painel de navegação à esquerda, escolha Funções.
3. Selecione Create role (Criar função).

4. Em Common use cases (Casos de uso comuns), selecione Lambda.
5. Escolha Próximo.
6. Na página Add permissions (Adicionar permissões), pesquise a política `AmazonS3ObjectLambdaExecutionRolePolicy`gerenciada pela AWS e marque a caixa de seleção ao lado do nome da política.

   Essa política deve conter a ação `s3-object-lambda:WriteGetObjectResponse`.
7. Escolha Próximo.
8. Na página Name, review, and create (Nomear, revisar e criar), para Role name (Nome da função), insira **`s3-object-lambda-role`**.
9. (Opcional) Adicione uma descrição e etiquetas para esse perfil.
10. Selecione Criar perfil.
11. Aplique a **`s3-object-lambda-role`** recém-criada como a função de execução de sua função Lambda. Isso pode ser feito durante ou após a criação da função do Lambda no console do Lambda.

Para obter informações sobre funções de execução, consulte Função de execução do Lambda no Guia do desenvolvedor do AWS Lambda.

Usar chaves de contexto com pontos de acesso do Object Lambda

O S3 Object Lambda avaliará chaves de contexto, como `s3-object-lambda:TlsVersion` ou `s3-object-lambda:AuthType`, relacionadas à conexão ou assinatura da solicitação. Todas as outras chaves de contexto, como `s3:prefix`, são avaliadas pelo Simple Storage Service (Amazon S3).

Suporte ao CORS de ponto de acesso do Object Lambda

Ao receber uma solicitação de um navegador ou quando a solicitação inclui um cabeçalho `Origin`, o S3 Object Lambda sempre adiciona um campo de cabeçalho `"AllowedOrigins":"*"`.

Para obter mais informações, consulte Usar o compartilhamento de recursos de origem cruzada (CORS).

Escrever funções do Lambda para pontos de acesso do S3 Object Lambda

Essa seção apresenta detalhes de como escrever funções do AWS Lambda para usar com pontos de acesso do Amazon S3 Object Lambda.

Para saber mais sobre procedimentos completos para algumas tarefas do S3 Object Lambda, consulte o seguinte:

- Tutorial: Como transformar dados para sua aplicação com o S3 Object Lambda
- Tutorial: Detectar e editar dados PII com o S3 Object Lambda e o Amazon Comprehend
- Tutorial: Using S3 Object Lambda to dynamically watermark images as they are retrieved (Tutorial: Como usar o S3 Object Lambda para colocar marca d'água em imagens de maneira dinâmica à medida que são recuperadas)

Tópicos

- Trabalhar com solicitações GetObject no Lambda
- Trabalhar com solicitações HeadObject no Lambda
- Trabalhar com solicitações ListObjects no Lambda
- Trabalhar com solicitações ListObjectsV2 no Lambda
- Formato e uso de contexto de evento
- Trabalhar com cabeçalhos Range e partNumber

Trabalhar com solicitações `GetObject` no Lambda

Esta seção pressupõe que seu ponto de acesso do Object Lambda está configurado para chamar a função do Lambda para `GetObject`. O S3 Object Lambda inclui a operação de API do Amazon S3, `WriteGetObjectResponse`, que permite que a função do Lambda apresente dados personalizados e cabeçalhos de resposta para o chamador de `GetObject`.

`WriteGetObjectResponse` oferece controle extensivo sobre código de status, cabeçalhos de resposta e corpo de resposta, com base nas suas necessidades de processamento. Você pode usar `WriteGetObjectResponse` para responder com todo o objeto transformado, partes do objeto transformado ou outras respostas com base no contexto da sua aplicação. A seção a seguir mostra exemplos exclusivos do uso da operação da API `WriteGetObjectResponse`.

- Exemplo 1: Responder com código de status HTTP 403 (Proibido)
- Exemplo 2:responda com uma imagem transformada
- Exemplo 3: Transmitir conteúdo compactado

Exemplo 1: Responder com código de status HTTP 403 (Proibido)

Você pode usar `WriteGetObjectResponse` para responder com o código de status HTTP 403 (Proibido) com base no conteúdo do objeto.

Java

```
package com.amazon.s3.objectlambda;

import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.events.S3ObjectLambdaEvent;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3Client;
import com.amazonaws.services.s3.model.WriteGetObjectResponseRequest;

import java.io.ByteArrayInputStream;
import java.net.URI;
import java.net.http.HttpClient;
import java.net.http.HttpRequest;
import java.net.http.HttpResponse;

public class Example1 {

    public void handleRequest(S3ObjectLambdaEvent event, Context context) throws
 Exception {
        AmazonS3 s3Client = AmazonS3Client.builder().build();

        // Check to see if the request contains all of the necessary information.
        // If it does not, send a 4XX response and a custom error code and message.
        // Otherwise, retrieve the object from S3 and stream it
        // to the client unchanged.
        var tokenIsNotPresent = !
event.getUserRequest().getHeaders().containsKey("requiredToken");
        if (tokenIsNotPresent) {
            s3Client.writeGetObjectResponse(new WriteGetObjectResponseRequest()
                    .withRequestRoute(event.outputRoute())
                    .withRequestToken(event.outputToken())
                    .withStatusCode(403)
                    .withContentLength(0L).withInputStream(new
 ByteArrayInputStream(new byte[0]))
                    .withErrorCode("MissingRequiredToken")
                    .withErrorMessage("The required token was not present in the
 request."));
            return;
        }
```

```
        // Prepare the presigned URL for use and make the request to S3.
        HttpClient httpClient = HttpClient.newBuilder().build();
        var presignedResponse = httpClient.send(
                HttpRequest.newBuilder(new URI(event.inputS3Url())).GET().build(),
                HttpResponse.BodyHandlers.ofInputStream());

        // Stream the original bytes back to the caller.
        s3Client.writeGetObjectResponse(new WriteGetObjectResponseRequest()
                .withRequestRoute(event.outputRoute())
                .withRequestToken(event.outputToken())
                .withInputStream(presignedResponse.body()));
    }
}
```

Python

```
import boto3
import requests

def handler(event, context):
    s3 = boto3.client('s3')

    """
    Retrieve the operation context object from the event. This object indicates
 where the WriteGetObjectResponse request
    should be delivered and contains a presigned URL in 'inputS3Url' where we can
 download the requested object from.
    The 'userRequest' object has information related to the user who made this
 'GetObject' request to
    S3 Object Lambda.
    """
    get_context = event["getObjectContext"]
    user_request_headers = event["userRequest"]["headers"]

    route = get_context["outputRoute"]
    token = get_context["outputToken"]
    s3_url = get_context["inputS3Url"]

    # Check for the presence of a 'CustomHeader' header and deny or allow based on
 that header.
    is_token_present = "SuperSecretToken" in user_request_headers
```

```
    if is_token_present:
        # If the user presented our custom 'SuperSecretToken' header, we send the
 requested object back to the user.
        response = requests.get(s3_url)
        s3.write_get_object_response(RequestRoute=route, RequestToken=token,
 Body=response.content)
    else:
        # If the token is not present, we send an error back to the user.
        s3.write_get_object_response(RequestRoute=route, RequestToken=token,
 StatusCode=403,
        ErrorCode="NoSuperSecretTokenFound", ErrorMessage="The request was not
 secret enough.")

    # Gracefully exit the Lambda function.
    return { 'status_code': 200 }
```

Node.js

```
const { S3 } = require('aws-sdk');
const axios = require('axios').default;

exports.handler = async (event) => {
    const s3 = new S3();

    // Retrieve the operation context object from the event. This object indicates
 where the WriteGetObjectResponse request
    // should be delivered and contains a presigned URL in 'inputS3Url' where we can
 download the requested object from.
    // The 'userRequest' object has information related to the user who made this
 'GetObject' request to S3 Object Lambda.
    const { userRequest, getObjectContext } = event;
    const { outputRoute, outputToken, inputS3Url } = getObjectContext;

    // Check for the presence of a 'CustomHeader' header and deny or allow based on
 that header.
    const isTokenPresent = Object
        .keys(userRequest.headers)
        .includes("SuperSecretToken");

    if (!isTokenPresent) {
        // If the token is not present, we send an error back to the user. The
 'await' in front of the request
```

```
        // indicates that we want to wait for this request to finish sending before
 moving on.
        await s3.writeGetObjectResponse({
            RequestRoute: outputRoute,
            RequestToken: outputToken,
            StatusCode: 403,
            ErrorCode: "NoSuperSecretTokenFound",
            ErrorMessage: "The request was not secret enough.",
        }).promise();
    } else {
        // If the user presented our custom 'SuperSecretToken' header, we send the
 requested object back to the user.
        // Again, note the presence of 'await'.
        const presignedResponse = await axios.get(inputS3Url);
        await s3.writeGetObjectResponse({
            RequestRoute: outputRoute,
            RequestToken: outputToken,
            Body: presignedResponse.data,
        }).promise();
    }

    // Gracefully exit the Lambda function.
    return { statusCode: 200 };
}
```

Exemplo 2:responda com uma imagem transformada

Ao executar uma transformação de imagem, talvez você ache que precisa de todos os bytes do objeto de origem antes de começar a processá-los. Nesse caso, a solicitação `WriteGetObjectResponse` retorna todo o objeto para a aplicação solicitante em uma chamada.

Java

```
package com.amazon.s3.objectlambda;

import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.events.S3ObjectLambdaEvent;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3Client;
import com.amazonaws.services.s3.model.WriteGetObjectResponseRequest;

import javax.imageio.ImageIO;
```

```
import java.awt.image.BufferedImage;
import java.awt.Image;
import java.io.ByteArrayInputStream;
import java.io.ByteArrayOutputStream;
import java.net.URI;
import java.net.http.HttpClient;
import java.net.http.HttpRequest;
import java.net.http.HttpResponse;

public class Example2 {

    private static final int HEIGHT = 250;
    private static final int WIDTH = 250;

    public void handleRequest(S3ObjectLambdaEvent event, Context context) throws
 Exception {
        AmazonS3 s3Client = AmazonS3Client.builder().build();
        HttpClient httpClient = HttpClient.newBuilder().build();

        // Prepare the presigned URL for use and make the request to S3.
        var presignedResponse = httpClient.send(
                HttpRequest.newBuilder(new URI(event.inputS3Url())).GET().build(),
                HttpResponse.BodyHandlers.ofInputStream());

        // The entire image is loaded into memory here so that we can resize it.
        // Once the resizing is completed, we write the bytes into the body
        // of the WriteGetObjectResponse request.
        var originalImage = ImageIO.read(presignedResponse.body());
        var resizingImage = originalImage.getScaledInstance(WIDTH, HEIGHT,
 Image.SCALE_DEFAULT);
        var resizedImage = new BufferedImage(WIDTH, HEIGHT,
 BufferedImage.TYPE_INT_RGB);
        resizedImage.createGraphics().drawImage(resizingImage, 0, 0, WIDTH, HEIGHT,
 null);

        var baos = new ByteArrayOutputStream();
        ImageIO.write(resizedImage, "png", baos);

        // Stream the bytes back to the caller.
        s3Client.writeGetObjectResponse(new WriteGetObjectResponseRequest()
                .withRequestRoute(event.outputRoute())
                .withRequestToken(event.outputToken())
                .withInputStream(new ByteArrayInputStream(baos.toByteArray())));
    }
```

```
}
```

Python

```
import boto3
import requests
import io
from PIL import Image

def handler(event, context):
    """
    Retrieve the operation context object from the event. This object indicates
 where the WriteGetObjectResponse request
    should be delivered and has a presigned URL in 'inputS3Url' where we can
 download the requested object from.
    The 'userRequest' object has information related to the user who made this
 'GetObject' request to
    S3 Object Lambda.
    """
    get_context = event["getObjectContext"]
    route = get_context["outputRoute"]
    token = get_context["outputToken"]
    s3_url = get_context["inputS3Url"]

    """
    In this case, we're resizing .png images that are stored in S3 and are
 accessible through the presigned URL
    'inputS3Url'.
    """
    image_request = requests.get(s3_url)
    image = Image.open(io.BytesIO(image_request.content))
    image.thumbnail((256,256), Image.ANTIALIAS)

    transformed = io.BytesIO()
    image.save(transformed, "png")

    # Send the resized image back to the client.
    s3 = boto3.client('s3')
    s3.write_get_object_response(Body=transformed.getvalue(), RequestRoute=route,
 RequestToken=token)

    # Gracefully exit the Lambda function.
```

```
    return { 'status_code': 200 }
```

Node.js

```
const { S3 } = require('aws-sdk');
const axios = require('axios').default;
const sharp = require('sharp');

exports.handler = async (event) => {
    const s3 = new S3();

    // Retrieve the operation context object from the event. This object indicates
 where the WriteGetObjectResponse request
    // should be delivered and has a presigned URL in 'inputS3Url' where we can
 download the requested object from.
    const { getObjectContext } = event;
    const { outputRoute, outputToken, inputS3Url } = getObjectContext;

    // In this case, we're resizing .png images that are stored in S3 and are
 accessible through the presigned URL
    // 'inputS3Url'.
    const { data } = await axios.get(inputS3Url, { responseType: 'arraybuffer' });

    // Resize the image.
    const resized = await sharp(data)
        .resize({ width: 256, height: 256 })
        .toBuffer();

    // Send the resized image back to the client.
    await s3.writeGetObjectResponse({
        RequestRoute: outputRoute,
        RequestToken: outputToken,
        Body: resized,
    }).promise();

    // Gracefully exit the Lambda function.
    return { statusCode: 200 };
}
```

Exemplo 3: Transmitir conteúdo compactado

Quando objetos são comprimidos, os dados compactados são produzidos de forma incremental. Consequentemente, você pode usar sua solicitação `WriteGetObjectResponse` para retornar os dados compactados assim que eles estiverem prontos. Como mostrado neste exemplo, não é necessário saber o tamanho da transformação concluída.

Java

```
package com.amazon.s3.objectlambda;

import com.amazonaws.services.lambda.runtime.events.S3ObjectLambdaEvent;
import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3Client;
import com.amazonaws.services.s3.model.WriteGetObjectResponseRequest;

import java.net.URI;
import java.net.http.HttpClient;
import java.net.http.HttpRequest;
import java.net.http.HttpResponse;

public class Example3 {

    public void handleRequest(S3ObjectLambdaEvent event, Context context) throws
 Exception {
        AmazonS3 s3Client = AmazonS3Client.builder().build();
        HttpClient httpClient = HttpClient.newBuilder().build();

        // Request the original object from S3.
        var presignedResponse = httpClient.send(
                HttpRequest.newBuilder(new URI(event.inputS3Url())).GET().build(),
                HttpResponse.BodyHandlers.ofInputStream());

        // Consume the incoming response body from the presigned request,
        // apply our transformation on that data, and emit the transformed bytes
        // into the body of the WriteGetObjectResponse request as soon as they're
 ready.
        // This example compresses the data from S3, but any processing pertinent
        // to your application can be performed here.
        var bodyStream = new GZIPCompressingInputStream(presignedResponse.body());

        // Stream the bytes back to the caller.
        s3Client.writeGetObjectResponse(new WriteGetObjectResponseRequest()
```

```
                .withRequestRoute(event.outputRoute())
                .withRequestToken(event.outputToken())
                .withInputStream(bodyStream));
    }

}
```

Python

```
import boto3
import requests
import zlib
from botocore.config import Config


"""
A helper class to work with content iterators. Takes an interator and compresses the
 bytes that come from it. It
implements 'read' and '__iter__' so that the SDK can stream the response.
"""
class Compress:
    def __init__(self, content_iter):
        self.content = content_iter
        self.compressed_obj = zlib.compressobj()

    def read(self, _size):
        for data in self.__iter__()
            return data

    def __iter__(self):
        while True:
            data = next(self.content)
            chunk = self.compressed_obj.compress(data)
            if not chunk:
                break

            yield chunk

        yield self.compressed_obj.flush()


def handler(event, context):
    """
```

```
   Setting the 'payload_signing_enabled' property to False allows us to send a
streamed response back to the client.
   in this scenario, a streamed response means that the bytes are not buffered into
memory as we're compressing them,
   but instead are sent straight to the user.
   """
   my_config = Config(
       region_name='eu-west-1',
       signature_version='s3v4',
       s3={
           "payload_signing_enabled": False
       }
   )
   s3 = boto3.client('s3', config=my_config)

   """
   Retrieve the operation context object from the event. This object indicates
where the WriteGetObjectResponse request
   should be delivered and has a presigned URL in 'inputS3Url' where we can
download the requested object from.
   The 'userRequest' object has information related to the user who made this
'GetObject' request to S3 Object Lambda.
   """
   get_context = event["getObjectContext"]
   route = get_context["outputRoute"]
   token = get_context["outputToken"]
   s3_url = get_context["inputS3Url"]

   # Compress the 'get' request stream.
   with requests.get(s3_url, stream=True) as r:
       compressed = Compress(r.iter_content())

       # Send the stream back to the client.
       s3.write_get_object_response(Body=compressed, RequestRoute=route,
RequestToken=token, ContentType="text/plain",
                                    ContentEncoding="gzip")

   # Gracefully exit the Lambda function.
   return {'status_code': 200}
```

Node.js

```
const { S3 } = require('aws-sdk');
```

```
const axios = require('axios').default;
const zlib = require('zlib');

exports.handler = async (event) => {
    const s3 = new S3();

    // Retrieve the operation context object from the event. This object indicates
 where the WriteGetObjectResponse request
    // should be delivered and has a presigned URL in 'inputS3Url' where we can
 download the requested object from.
    const { getObjectContext } = event;
    const { outputRoute, outputToken, inputS3Url } = getObjectContext;

    // Download the object from S3 and process it as a stream, because it might be a
 huge object and we don't want to
    // buffer it in memory. Note the use of 'await' because we want to wait for
 'writeGetObjectResponse' to finish
    // before we can exit the Lambda function.
    await axios({
        method: 'GET',
        url: inputS3Url,
        responseType: 'stream',
    }).then(
        // Gzip the stream.
        response => response.data.pipe(zlib.createGzip())
    ).then(
        // Finally send the gzip-ed stream back to the client.
        stream => s3.writeGetObjectResponse({
            RequestRoute: outputRoute,
            RequestToken: outputToken,
            Body: stream,
            ContentType: "text/plain",
            ContentEncoding: "gzip",
        }).promise()
    );

    // Gracefully exit the Lambda function.
    return { statusCode: 200 };
}
```

> **Note**
>
> Embora o S3 Object Lambda permita enviar uma resposta completa ao autor da chamada por meio da solicitação `WriteGetObjectResponse`, a quantidade real de tempo disponível pode ser menor. Por exemplo, o tempo limite da função do Lambda pode ser inferior a 60 segundos. Em outros casos, o autor da chamada pode ter tempos limites mais rigorosos.

Para que o autor da chamada original receba uma resposta diferente de código de status HTTP 500 (Erro interno do servidor), a chamada `WriteGetObjectResponse` deve ser concluída. Se a função do Lambda retornar, excepcionalmente ou de outra forma, antes que a operação da API `WriteGetObjectResponse` seja chamada, o autor da chamada original receberá uma resposta 500 (Erro interno do servidor). Exceções lançadas durante o tempo necessário para concluir a resposta resultam em respostas truncadas ao autor da chamada. Se a função do Lambda recebe uma resposta com código de status HTTP 200 (OK) da chamada da API `WriteGetObjectResponse`, o autor da chamada original enviou a solicitação completa. A resposta da função do Lambda, independentemente de uma exceção ser lançada ou não, é ignorada pelo S3 Object Lambda.

Ao chamar a operação de API `WriteGetObjectResponse`, o Amazon S3 exige a rota e o token de solicitação do contexto do evento. Para obter mais informações, consulte Formato e uso de contexto de evento.

Os parâmetros de token de roteamento e solicitação são necessários para conectar a resposta `WriteGetObjectResult` com o autor da chamada original. Ainda que sempre seja apropriado repetir respostas 500 (Erro interno do servidor), como o token de solicitação é um token de uso único, as tentativas subsequentes de usá-lo podem resultar em respostas com código de status HTTP 400 (Solicitação inválida). Embora a chamada para `WriteGetObjectResponse` com tokens de roteamento e solicitação não precise ser feita a partir da função do Lambda invocada, ela deve ser feita por uma identidade na mesma conta. A chamada também deverá ser concluída antes que a função do Lambda termine a execução.

Trabalhar com solicitações **`HeadObject`** no Lambda

Esta seção pressupõe que seu ponto de acesso do Object Lambda está configurado para chamar a função do Lambda para `HeadObject`. O Lambda receberá uma carga útil JSON que contém uma chave chamada `headObjectContext`. Dentro do contexto, há uma única propriedade chamada `inputS3Url`, que é um URL pré-assinado para o ponto de acesso de suporte para `HeadObject`.

O URL pré-assinado incluirá as seguintes propriedades se elas forem especificadas:

- `versionId` (nos parâmetros de consulta)
- `requestPayer` (no cabeçalho de `x-amz-request-payer`)
- `expectedBucketOwner` (no cabeçalho de `x-amz-expected-bucket-owner`)

Outras propriedades não serão pré-assinadas e, portanto, não serão incluídas. As opções não assinadas enviadas como cabeçalhos podem ser adicionadas manualmente à solicitação ao chamar o URL pré-assinado encontrado nos cabeçalhos de `userRequest`. As opções de criptografia do lado do servidor não são compatíveis com `HeadObject`.

Para ver os parâmetros de URI da sintaxe da solicitação, consulte `HeadObject` na Amazon Simple Storage Service API Reference (Referência da API do Amazon Simple Storage Service).

O exemplo a seguir mostra uma carga útil JSON de entrada do Lambda para `HeadObject`.

```
{
  "xAmzRequestId": "requestId",
  "**headObjectContext**": {
    "**inputS3Url**": "https://my-s3-ap-111122223333.s3-accesspoint.us-
east-1.amazonaws.com/example?X-Amz-Security-Token=<snip>"
  },
  "configuration": {
        "accessPointArn": "arn:aws:s3-object-lambda:us-
east-1:111122223333:accesspoint/example-object-lambda-ap",
        "supportingAccessPointArn": "arn:aws:s3:us-
east-1:111122223333:accesspoint/example-ap",
        "payload": "{}"
  },
  "userRequest": {
        "url": "https://object-lambda-111122223333.s3-object-lambda.us-
east-1.amazonaws.com/example",
        "headers": {
            "Host": "object-lambda-111122223333.s3-object-lambda.us-
east-1.amazonaws.com",
            "Accept-Encoding": "identity",
            "X-Amz-Content-SHA256": "e3b0c44298fc1example"
        }
   },
   "userIdentity": {
        "type": "AssumedRole",
```

```
        "principalId": "principalId",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/example",
        "accountId": "111122223333",
        "accessKeyId": "accessKeyId",
        "sessionContext": {
             "attributes": {
             "mfaAuthenticated": "false",
             "creationDate": "Wed Mar 10 23:41:52 UTC 2021"
        },
        "sessionIssuer": {
             "type": "Role",
             "principalId": "principalId",
             "arn": "arn:aws:iam::111122223333:role/Admin",
             "accountId": "111122223333",
             "userName": "Admin"
             }
        }
    },
  "protocolVersion": "1.00"
}
```

Sua função do Lambda deve retornar um objeto JSON que contém os cabeçalhos e os valores que serão retornados para a chamada de `HeadObject`.

O exemplo a seguir mostra a estrutura do JSON de resposta do Lambda para `HeadObject`.

```
{
    "statusCode": <number>; // Required
    "errorCode": <string>;
    "errorMessage": <string>;
    "headers": {
        "Accept-Ranges": <string>,
        "x-amz-archive-status": <string>,
        "x-amz-server-side-encryption-bucket-key-enabled": <boolean>,
        "Cache-Control": <string>,
        "Content-Disposition": <string>,
        "Content-Encoding": <string>,
        "Content-Language": <string>,
        "Content-Length": <number>, // Required
        "Content-Type": <string>,
        "x-amz-delete-marker": <boolean>,
        "ETag": <string>,
        "Expires": <string>,
```

```
        "x-amz-expiration": <string>,
        "Last-Modified": <string>,
        "x-amz-missing-meta": <number>,
        "x-amz-object-lock-mode": <string>,
        "x-amz-object-lock-legal-hold": <string>,
        "x-amz-object-lock-retain-until-date": <string>,
        "x-amz-mp-parts-count": <number>,
        "x-amz-replication-status": <string>,
        "x-amz-request-charged": <string>,
        "x-amz-restore": <string>,
        "x-amz-server-side-encryption": <string>,
        "x-amz-server-side-encryption-customer-algorithm": <string>,
        "x-amz-server-side-encryption-aws-kms-key-id": <string>,
        "x-amz-server-side-encryption-customer-key-MD5": <string>,
        "x-amz-storage-class": <string>,
        "x-amz-tagging-count": <number>,
        "x-amz-version-id": <string>,
        <x-amz-meta-headers>: <string>, // user-defined metadata
        "x-amz-meta-meta1": <string>, // example of the user-defined metadata header,
 it will need the x-amz-meta prefix
        "x-amz-meta-meta2": <string>
        ...
    };
}
```

O exemplo a seguir mostra como usar o URL pré-assinado para preencher sua resposta modificando os valores do cabeçalho conforme necessário antes de retornar o JSON.

Python

```
import requests

def lambda_handler(event, context):
    print(event)

    # Extract the presigned URL from the input.
    s3_url = event["headObjectContext"]["inputS3Url"]

    # Get the head of the object from S3.
    response = requests.head(s3_url)

    # Return the error to S3 Object Lambda (if applicable).
    if (response.status_code >= 400):
```

```
        return {
            "statusCode": response.status_code,
            "errorCode": "RequestFailure",
            "errorMessage": "Request to S3 failed"
    }

    # Store the headers in a dictionary.
    response_headers = dict(response.headers)

    # This obscures Content-Type in a transformation, it is optional to add
    response_headers["Content-Type"] = ""

    # Return the headers to S3 Object Lambda.
    return {
        "statusCode": response.status_code,
        "headers": response_headers
        }
```

Trabalhar com solicitações **`ListObjects`** no Lambda

Esta seção pressupõe que seu ponto de acesso do Object Lambda está configurado para chamar a função do Lambda para `ListObjects`. O Lambda receberá a carga JSON com um novo objeto chamado `listObjectsContext`. `listObjectsContext` contém uma única propriedade, `inputS3Url`, que é um URL pré-assinado para o ponto de acesso de suporte para `ListObjects`.

Ao contrário de `GetObject` e `HeadObject`, o URL pré-assinado incluirá as seguintes propriedades se elas forem especificadas:

- Todos os parâmetros de consulta
- `requestPayer` (no cabeçalho de `x-amz-request-payer`)
- `expectedBucketOwner` (no cabeçalho de `x-amz-expected-bucket-owner`)

Para ver os parâmetros de URI da sintaxe da solicitação, consulte `ListObjects` na Referência da API do Amazon Simple Storage Service.

> **Important**
>
> Recomendamos que você use a versão mais recente, ListObjectsV2, ao desenvolver aplicações. Para compatibilidade com versões anteriores, o Amazon S3 continua a oferecer suporte a `ListObjects`.

O exemplo a seguir mostra a carga útil JSON de entrada do Lambda para `ListObjects`.

```
{
    "xAmzRequestId": "requestId",
     "**listObjectsContext**": {
     "**inputS3Url**": "https://my-s3-ap-111122223333.s3-accesspoint.us-
east-1.amazonaws.com/?X-Amz-Security-Token=<snip>",
     },
    "configuration": {
        "accessPointArn": "arn:aws:s3-object-lambda:us-
east-1:111122223333:accesspoint/example-object-lambda-ap",
        "supportingAccessPointArn": "arn:aws:s3:us-
east-1:111122223333:accesspoint/example-ap",
        "payload": "{}"
    },
    "userRequest": {
        "url": "https://object-lambda-111122223333.s3-object-lambda.us-
east-1.amazonaws.com/example",
        "headers": {
            "Host": "object-lambda-111122223333.s3-object-lambda.us-
east-1.amazonaws.com",
            "Accept-Encoding": "identity",
            "X-Amz-Content-SHA256": "e3b0c44298fc1example"
        }
    },
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "principalId",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/example",
        "accountId": "111122223333",
        "accessKeyId": "accessKeyId",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "Wed Mar 10 23:41:52 UTC 2021"
```

```
            },
            "sessionIssuer": {
                "type": "Role",
                "principalId": "principalId",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            }
        }
    },
  "protocolVersion": "1.00"
}
```

Sua função do Lambda deve retornar um objeto JSON que contém o código de status, o resultado XML da lista ou as informações de erro que serão retornadas do S3 Object Lambda.

O S3 Object Lambda não processa nem valida `listResultXml`. Em vez disso, o encaminha para o chamador de `ListObjects`. Para `listBucketResult`, o S3 Object Lambda espera que certas propriedades sejam de um tipo específico e lançará exceções se não puder analisá-las. `listResultXml` e `listBucketResult` não podem ser fornecidas ao mesmo tempo.

O exemplo a seguir demonstra como usar o URL pré-assinado para chamar o Amazon S3 e usar o resultado para preencher uma resposta, incluindo a verificação de erros.

Python

```
import requests
import xmltodict

def lambda_handler(event, context):
    # Extract the presigned URL from the input.
    s3_url = event["listObjectsContext"]["inputS3Url"]


    # Get the head of the object from Amazon S3.
    response = requests.get(s3_url)

    # Return the error to S3 Object Lambda (if applicable).
    if (response.status_code >= 400):
        error = xmltodict.parse(response.content)
        return {
            "statusCode": response.status_code,
            "errorCode": error["Error"]["Code"],
```

```
            "errorMessage": error["Error"]["Message"]
        }

    # Store the XML result in a dict.
    response_dict = xmltodict.parse(response.content)

    # This obscures StorageClass in a transformation, it is optional to add
    for item in response_dict['ListBucketResult']['Contents']:
        item['StorageClass'] = ""

    # Convert back to XML.
    listResultXml = xmltodict.unparse(response_dict)

    # Create response with listResultXml.
    response_with_list_result_xml = {
        'statusCode': 200,
        'listResultXml': listResultXml
    }

    # Create response with listBucketResult.
    response_dict['ListBucketResult'] =
 sanitize_response_dict(response_dict['ListBucketResult'])
    response_with_list_bucket_result = {
        'statusCode': 200,
        'listBucketResult': response_dict['ListBucketResult']
    }

    # Return the list to S3 Object Lambda.
    # Can return response_with_list_result_xml or response_with_list_bucket_result
    return response_with_list_result_xml

# Converting the response_dict's key to correct casing
def sanitize_response_dict(response_dict: dict):
    new_response_dict = dict()
    for key, value in response_dict.items():
        new_key = key[0].lower() + key[1:] if key != "ID" else 'id'
        if type(value) == list:
            newlist = []
            for element in value:
                if type(element) == type(dict()):
                    element = sanitize_response_dict(element)
                newlist.append(element)
            value = newlist
        elif type(value) == dict:
```

```
            value = sanitize_response_dict(value)
        new_response_dict[new_key] = value
    return new_response_dict
```

O exemplo a seguir mostra a estrutura do JSON de resposta do Lambda para `ListObjects`.

```
{
  "statusCode": <number>; // Required
  "errorCode": <string>;
  "errorMessage": <string>;
  "listResultXml": <string>; // This can also be Error XML string in case S3 returned
 error response when calling the pre-signed URL

  "listBucketResult": {  // listBucketResult can be provided instead of listResultXml,
 however they can not both be provided in the JSON response
       "name": <string>,  // Required for 'listBucketResult'
       "prefix": <string>,
       "marker": <string>,
       "nextMarker": <string>,
       "maxKeys": <int>,   // Required for 'listBucketResult'
       "delimiter": <string>,
       "encodingType": <string>
       "isTruncated": <boolean>,  // Required for 'listBucketResult'
       "contents": [  {
           "key": <string>,  // Required for 'content'
           "lastModified": <string>,
           "eTag": <string>,
           "checksumAlgorithm": <string>,   // CRC32,  CRC32C,  SHA1,  SHA256
           "size": <int>,   // Required for 'content'
           "owner": {
               "displayName": <string>,  // Required for 'owner'
               "id": <string>,  // Required for 'owner'
           },
           "storageClass": <string>
           },
       ...
       ],
       "commonPrefixes": [  {
           "prefix": <string>   // Required for 'commonPrefix'
       },
       ...
       ],
```

```
    }
}
```

Trabalhar com solicitações **`ListObjectsV2`** no Lambda

Esta seção pressupõe que seu ponto de acesso do Object Lambda está configurado para chamar a função do Lambda para `ListObjectsV2`. O Lambda receberá a carga JSON com um novo objeto chamado `listObjectsV2Context`. `listObjectsV2Context` contém uma única propriedade, `inputS3Url`, que é um URL pré-assinado para o ponto de acesso de suporte para `ListObjectsV2`.

Ao contrário de `GetObject` e `HeadObject`, o URL pré-assinado incluirá as seguintes propriedades se elas forem especificadas:

- Todos os parâmetros de consulta
- `requestPayer` (no cabeçalho de `x-amz-request-payer`)
- `expectedBucketOwner` (no cabeçalho de `x-amz-expected-bucket-owner`)

Para ver os parâmetros de URI da sintaxe da solicitação, consulte `ListObjectsV2` na Referência da API do Amazon Simple Storage Service.

O exemplo a seguir mostra a carga útil JSON de entrada do Lambda para `ListObjectsV2`.

```
{
    "xAmzRequestId": "requestId",
     "**listObjectsV2Context**": {
     "**inputS3Url**": "https://my-s3-ap-111122223333.s3-accesspoint.us-
east-1.amazonaws.com/?list-type=2&X-Amz-Security-Token=<snip>",
     },
    "configuration": {
        "accessPointArn": "arn:aws:s3-object-lambda:us-
east-1:111122223333:accesspoint/example-object-lambda-ap",
        "supportingAccessPointArn": "arn:aws:s3:us-
east-1:111122223333:accesspoint/example-ap",
        "payload": "{}"
    },
    "userRequest": {
        "url": "https://object-lambda-111122223333.s3-object-lambda.us-
east-1.amazonaws.com/example",
        "headers": {
```

```
            "Host": "object-lambda-111122223333.s3-object-lambda.us-
east-1.amazonaws.com",
            "Accept-Encoding": "identity",
            "X-Amz-Content-SHA256": "e3b0c44298fc1example"
        }
    },
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "principalId",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/example",
        "accountId": "111122223333",
        "accessKeyId": "accessKeyId",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "Wed Mar 10 23:41:52 UTC 2021"
            },
            "sessionIssuer": {
                "type": "Role",
                "principalId": "principalId",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            }
        }
    },
  "protocolVersion": "1.00"
}
```

Sua função do Lambda deve retornar um objeto JSON que contém o código de status, o resultado XML da lista ou as informações de erro que serão retornadas do S3 Object Lambda.

O S3 Object Lambda não processa nem valida `listResultXml`. Em vez disso, o encaminha para o chamador de `ListObjectsV2`. Para `listBucketResult`, o S3 Object Lambda espera que certas propriedades sejam de um tipo específico e lançará exceções se não puder analisá-las. `listResultXml` e `listBucketResult` não podem ser fornecidas ao mesmo tempo.

O exemplo a seguir demonstra como usar o URL pré-assinado para chamar o Amazon S3 e usar o resultado para preencher uma resposta, incluindo a verificação de erros.

Python

```
import requests
```

```
import xmltodict

def lambda_handler(event, context):
    # Extract the presigned URL from the input.
    s3_url = event["listObjectsV2Context"]["inputS3Url"]


    # Get the head of the object from Amazon S3.
    response = requests.get(s3_url)

    # Return the error to S3 Object Lambda (if applicable).
    if (response.status_code >= 400):
        error = xmltodict.parse(response.content)
        return {
            "statusCode": response.status_code,
            "errorCode": error["Error"]["Code"],
            "errorMessage": error["Error"]["Message"]
        }

    # Store the XML result in a dict.
    response_dict = xmltodict.parse(response.content)

    # This obscures StorageClass in a transformation, it is optional to add
    for item in response_dict['ListBucketResult']['Contents']:
        item['StorageClass'] = ""

    # Convert back to XML.
    listResultXml = xmltodict.unparse(response_dict)

    # Create response with listResultXml.
    response_with_list_result_xml = {
        'statusCode': 200,
        'listResultXml': listResultXml
    }

    # Create response with listBucketResult.
    response_dict['ListBucketResult'] =
 sanitize_response_dict(response_dict['ListBucketResult'])
    response_with_list_bucket_result = {
        'statusCode': 200,
        'listBucketResult': response_dict['ListBucketResult']
    }

    # Return the list to S3 Object Lambda.
```

```
    # Can return response_with_list_result_xml or response_with_list_bucket_result
    return response_with_list_result_xml

# Converting the response_dict's key to correct casing
def sanitize_response_dict(response_dict: dict):
    new_response_dict = dict()
    for key, value in response_dict.items():
        new_key = key[0].lower() + key[1:] if key != "ID" else 'id'
        if type(value) == list:
            newlist = []
            for element in value:
                if type(element) == type(dict()):
                    element = sanitize_response_dict(element)
                newlist.append(element)
            value = newlist
        elif type(value) == dict:
            value = sanitize_response_dict(value)
        new_response_dict[new_key] = value
    return new_response_dict
```

O exemplo a seguir mostra a estrutura do JSON de resposta do Lambda para `ListObjectsV2`.

```
{
    "statusCode": <number>; // Required
    "errorCode": <string>;
    "errorMessage": <string>;
    "listResultXml": <string>; // This can also be Error XML string in case S3 returned
 error response when calling the pre-signed URL

    "listBucketResult": {  // listBucketResult can be provided instead of
 listResultXml, however they can not both be provided in the JSON response
        "name": <string>, // Required for 'listBucketResult'
        "prefix": <string>,
        "startAfter": <string>,
        "continuationToken": <string>,
        "nextContinuationToken": <string>,
        "keyCount": <int>, // Required for 'listBucketResult'
        "maxKeys": <int>, // Required for 'listBucketResult'
        "delimiter": <string>,
        "encodingType": <string>
        "isTruncated": <boolean>, // Required for 'listBucketResult'
        "contents": [ {
```

```
            "key": <string>, // Required for 'content'
            "lastModified": <string>,
            "eTag": <string>,
            "checksumAlgorithm": <string>, // CRC32, CRC32C, SHA1, SHA256
            "size": <int>, // Required for 'content'
            "owner": {
                "displayName": <string>, // Required for 'owner'
                "id": <string>, // Required for 'owner'
            },
            "storageClass": <string>
            },
            ...
        ],
        "commonPrefixes": [ {
            "prefix": <string> // Required for 'commonPrefix'
            },
        ...
        ],
    }
}
```

Formato e uso de contexto de evento

O Amazon S3 Object Lambda fornece contexto sobre a solicitação que está sendo feita no evento passado para a função AWS Lambda. Veja a seguir um exemplo de solicitação. As descrições dos campos são incluídas após o exemplo.

```
{
    "xAmzRequestId": "requestId",
    "getObjectContext": {
        "inputS3Url": "https://my-s3-ap-111122223333.s3-accesspoint.us-
east-1.amazonaws.com/example?X-Amz-Security-Token=<snip>",
        "outputRoute": "io-use1-001",
        "outputToken": "OutputToken"
    },
    "configuration": {
        "accessPointArn": "arn:aws:s3-object-lambda:us-
east-1:111122223333:accesspoint/example-object-lambda-ap",
        "supportingAccessPointArn": "arn:aws:s3:us-
east-1:111122223333:accesspoint/example-ap",
        "payload": "{}"
    },
    "userRequest": {
```

```
        "url": "https://object-lambda-111122223333.s3-object-lambda.us-
east-1.amazonaws.com/example",
        "headers": {
            "Host": "object-lambda-111122223333.s3-object-lambda.us-
east-1.amazonaws.com",
            "Accept-Encoding": "identity",
            "X-Amz-Content-SHA256": "e3b0c44298fc1example"
        }
    },
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "principalId",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/example",
        "accountId": "111122223333",
        "accessKeyId": "accessKeyId",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "Wed Mar 10 23:41:52 UTC 2021"
            },
            "sessionIssuer": {
                "type": "Role",
                "principalId": "principalId",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            }
        }
    },
    "protocolVersion": "1.00"
}
```

Os seguintes arquivos estão incluídos na solicitação:

- `xAmzRequestId`: o ID da solicitação do Amazon S3 para essa solicitação. Recomendamos que você registre em log esse valor para ajudar na depuração.
- `getObjectContext`: os detalhes de entrada e saída para conexões com o Amazon S3 e o S3 Object Lambda.
  - `inputS3Url`: um URL pré-designado que pode ser usado para buscar o objeto original do Amazon S3. O URL é assinado usando a identidade do autor da chamada original, e as permissões desse usuário serão aplicadas quando o URL for usado. Se houver cabeçalhos

assinados no URL, a função do Lambda deverá incluí-los na chamada para o Amazon S3, exceto para o cabeçalho `Host`.

- `outputRoute`: um token de roteamento que é adicionado ao URL do S3 Object Lambda quando a função do Lambda chama `WriteGetObjectResponse`.
- `outputToken`: um token opaco usado pelo S3 Object Lambda para corresponder a chamada de `WriteGetObjectResponse` com o autor da chamada original.

- `configuration`: informações de configuração sobre o ponto de acesso do Object Lambda.
  - `accessPointArn`: o nome do recurso da Amazon (ARN) do ponto de acesso do Object Lambda que recebeu essa solicitação.
  - `supportingAccessPointArn`: o ARN do ponto de acesso de suporte especificado na configuração do ponto de acesso do Object Lambda.
  - `payload`: dados personalizados que são aplicados à configuração do ponto de acesso do Object Lambda. O S3 Object Lambda trata esses dados como uma string opaca, portanto, ela pode precisar ser decodificada antes do uso.
- `userRequest`: informações sobre a chamada original para o S3 Object Lambda.
  - `url`: o URL decodificado da solicitação, conforme recebido pelo S3 Object Lambda, excluindo qualquer parâmetro de consulta relacionado à autorização.
  - `headers`: um mapa de string para strings contendo os cabeçalhos HTTP e seus valores da chamada original, excluindo qualquer cabeçalho relacionado à autorização. Se o mesmo cabeçalho aparecer várias vezes, os valores de cada instância do mesmo cabeçalho serão combinados em uma lista delimitada por vírgulas. O caso dos cabeçalhos originais é retido neste mapa.
- `userIdentity`: detalhes sobre a identidade que fez a chamada para o S3 Object Lambda. Para obter mais informações, consulte Registro eventos de dados em logs para trilhas no Guia do usuário do AWS CloudTrail.
  - `type`: o tipo da identidade.
  - `accountId`: a Conta da AWS à qual a identidade pertence.
  - `userName`: o nome amigável da identidade que fez a chamada.
  - `principalId`: o identificador exclusivo da identidade que fez a chamada.
  - `arn`: o ARN da entidade principal que fez a chamada. A última seção do ARN contém o usuário ou função que fez a chamada.
  - `sessionContext`: se a solicitação foi feita com credenciais de segurança temporárias, esse elemento fornece informações sobre a sessão que foi criada para essas credenciais.

  - `invokedBy`: o nome do serviço da AWS service (Serviço da AWS) que fez a solicitação, como o Amazon EC2 Auto Scaling ou AWS Elastic Beanstalk.
  - `sessionIssuer`: se a solicitação foi feita com credenciais de segurança temporárias, esse elemento fornece informações sobre como as credenciais foram obtidas.
- `protocolVersion`: o ID da versão do contexto fornecido. O formato desse campo é `{Major Version}.{Minor Version}`. Os números de versão menores são sempre números de dois dígitos. Qualquer remoção ou alteração na semântica de um campo exigirá o aumento da versão principal e adesão ativa. O Amazon S3 pode adicionar novos campos a qualquer momento, no qual você pode experimentar um aumento da versão secundária. Devido à natureza das implementações de software, é possível que você veja várias versões secundárias em uso ao mesmo tempo.

Trabalhar com cabeçalhos Range e partNumber

Ao trabalhar com objetos grandes no Amazon S3 Object Lambda, você pode usar o cabeçalho HTTP `Range` para baixar um intervalo de bytes especificado de um objeto. É possível usar conexões simultâneas ao Amazon S3 para buscar diferentes escalas de bytes no mesmo objeto. Você também pode usar o parâmetro `partNumber` (inteiro entre 1 e 10.000) que executa uma solicitação em um intervalo para a parte especificada do objeto.

Como há várias maneiras pelas quais você pode querer lidar com uma solicitação que inclua os parâmetros `Range` ou `partNumber`, o S3 Object Lambda não aplica esses parâmetros ao objeto transformado. Em vez disso, sua função do AWS Lambda deve implementar essa funcionalidade conforme necessário para a aplicação.

Para usar os parâmetros `Range` e `partNumber` com o S3 Object Lambda, faça o seguinte:

- Ative esses parâmetros na configuração do ponto de acesso do Object Lambda.
- Escreva uma função do Lambda capaz de lidar com solicitações que incluam esses parâmetros.

As etapas a seguir descrevem como fazer isso.

Etapa 1: configurar o ponto de acesso do Object Lambda

Por padrão, os pontos de acesso do Object Lambda respondem com um erro de código de status HTTP 501 (não implementado) a qualquer solicitação `GetObject` ou `HeadObject` que contém um parâmetro `Range` ou `partNumber` nos cabeçalhos ou nos parâmetros de consulta.

Para permitir que um ponto de acesso do Object Lambda aceite essas solicitações, é necessário incluir `GetObject-Range`, `GetObject-PartNumber`, `HeadObject-Range` ou `HeadObject-PartNumber` na seção `AllowedFeatures` da configuração do ponto de acesso do Object Lambda. Para obter mais informações sobre como atualizar a configuração do ponto de acesso do Object Lambda, consulte Criar pontos de acesso do Object Lambda.

Etapa 2: Implementar o tratamento de **`Range`** ou **`partNumber`** na função do Lambda

Quando o ponto de acesso do Object Lambda invoca a função do Lambda com uma solicitação `GetObject` ou `HeadObject` em um intervalo, o parâmetro `Range` ou `partNumber` é incluído no contexto do evento. A localização do parâmetro no contexto do evento depende de qual parâmetro foi usado e de como ele foi incluído na solicitação original para o ponto de acesso do Object Lambda, conforme explicado na tabela a seguir.

Parameter	Localização do contexto do evento
`Range` (cabeçalho)	`userRequest.headers.Range`
`Range` (parâmetro de consulta)	`userRequest.url` (parâmetro de consulta `Range`)
`partNumber`	`userRequest.url` (parâmetro de consulta `partNumber`)

> **Important**
>
> O URL pré-assinado fornecido para o ponto de acesso do Object Lambda não contém o parâmetro `Range` ou `partNumber` da solicitação original. Veja as opções a seguir sobre como lidar com esses parâmetros na função do AWS Lambda.

Depois de extrair o valor `Range` ou `partNumber`, você poderá adotar uma das seguintes abordagens com base nas necessidades da aplicação:

A. Mapear o **`Range`** ou **`partNumber`** solicitado para o objeto transformado (recomendado).

O jeito mais confiável de lidar com solicitações `Range` e `partNumber` é fazer o seguinte:

- Recupere o objeto completo do Amazon S3.
- Transforme o objeto.

- Aplique os parâmetros `Range` ou `partNumber` solicitados ao objeto transformado.

Para fazer isso, use o URL pré-assinado fornecido para buscar todo o objeto do Amazon S3 e, em seguida, processe o objeto conforme necessário. Para obter um exemplo de função do Lambda que processa o parâmetro `Range` dessa forma, consulte este exemplo no repositório de exemplos da AWS no GitHub.

B. Associe o **`Range`** solicitado ao URL pré-assinado.

Em alguns casos, a função do Lambda pode associar o `Range` solicitado diretamente ao URL pré-assinado para recuperar apenas parte do objeto do Amazon S3. Essa abordagem será apropriada somente se sua transformação atender a ambos os seguintes critérios:

1. Sua função de transformação pode ser aplicada a intervalos de objetos parciais.
2. Aplicar o parâmetro `Range` antes ou depois da função de transformação ocasiona a transformação do mesmo objeto.

Por exemplo, uma função de transformação que converte todos os caracteres em um objeto codificado em ASCII em maiúsculas atende a ambos os critérios anteriores. A transformação pode ser aplicada a parte de um objeto, e aplicar o parâmetro `Range` ou antes da transformação produz o mesmo resultado que a aplicação do parâmetro após a transformação.

Por outro lado, uma função que inverte os caracteres em um objeto codificado em ASCII não atende a esses critérios. Essa função atende ao critério 1, pois pode ser aplicada a intervalos de objetos parciais. No entanto, ela não atende ao critério 2, porque aplicar o parâmetro `Range` antes da transformação produz resultados diferentes do que a aplicação do parâmetro após a transformação.

Pense em uma solicitação para aplicar a função aos três primeiros caracteres de um objeto com o conteúdo `abcdefg`. Aplicar o parâmetro `Range` antes da transformação recupera somente `abc` e, em seguida, reverte os dados, retornando `cba`. Mas se o parâmetro for aplicado após a transformação, a função recuperará todo o objeto, o reverterá e, em seguida, aplicará o parâmetro `Range`, retornando `gfe`. Como esses resultados são diferentes, essa função não deve aplicar o parâmetro `Range` ao recuperar o objeto do Amazon S3. Em vez disso, ela deve recuperar todo o objeto, executar a transformação e, somente então, aplicar o parâmetro `Range`.

> **Warning**
>
> Em muitos casos, aplicar o parâmetro `Range` ao URL pré-assinado resultará em um comportamento inesperado da função do Lambda ou do cliente solicitante. A menos

que você tenha certeza de que seu aplicativo funcionará corretamente ao recuperar apenas um objeto parcial do Amazon S3, recomendamos recuperar e transformar objetos completos, conforme descrito anteriormente na abordagem A.

Se a aplicação atender aos critérios descritos anteriormente na abordagem B, você poderá simplificar a função do AWS Lambda buscando apenas o intervalo de objetos solicitado e executando a transformação nesse intervalo.

O exemplo de código Java a seguir demonstra como fazer o seguinte:

- Recuperar o cabeçalho `Range` da solicitação `GetObject`.
- Adicionar o cabeçalho `Range` ao URL pré-assinado que o Lambda pode usar para recuperar o intervalo solicitado do Amazon S3.

```
private HttpRequest.Builder applyRangeHeader(ObjectLambdaEvent event,
 HttpRequest.Builder presignedRequest) {
    var header = event.getUserRequest().getHeaders().entrySet().stream()
            .filter(e -> e.getKey().toLowerCase(Locale.ROOT).equals("range"))
            .findFirst();

    // Add check in the query string itself.
    header.ifPresent(entry -> presignedRequest.header(entry.getKey(),
 entry.getValue()));
    return presignedRequest;
}
```

Usar funções do Lambda criadas pela AWS

A AWS fornece algumas funções pré-criadas do AWS Lambda que você pode usar com o Amazon S3 Object Lambda para detectar e remover informações de identificação pessoal (PII) e descompactar objetos do S3. Essas funções do Lambda estão disponíveis no AWS Serverless Application Repository. Essas funções do Lambda estão disponíveis no AWS Management Console quando você cria um ponto de acesso do Object Lambda.

Para obter mais informações sobre como implantar aplicações de tecnologia sem servidor pelo AWS Serverless Application Repository, consulte Implantação de aplicações no Guia do desenvolvedor do AWS Serverless Application Repository.

> **Note**
>
> Os exemplos a seguir só podem ser usados com solicitações `GetObject`.

Exemplo 1: Controle de acesso de PII

Essa função do Lambda usa o Amazon Comprehend, um serviço de processamento de linguagem natural (PLN) que usa machine learning para encontrar insights e relações no texto. Essa função detecta automaticamente informações de identificação pessoal (PII), como nomes, endereços, datas, números de cartão de crédito e números de previdência social de documentos em seu bucket do Amazon S3. Se você tiver documentos no bucket que incluam PII, poderá configurar a função de controle de acesso de PII para detectar esses tipos de entidade de PII e restringir o acesso a usuários não autorizados.

Para começar, implante a função do Lambda a seguir em sua conta e adicione o nome do recurso da Amazon (ARN) da função na configuração do ponto de acesso do Object Lambda.

Veja o seguinte exemplo de ARN para essa função:

```
arn:aws:serverlessrepo:us-east-1:111122223333:applications/
ComprehendPiiAccessControlS3ObjectLambda
```

Você pode adicionar ou exibir essa função no AWS Management Console usando o seguinte link do AWS Serverless Application Repository: ComprehendPiiAccessControlS3ObjectLambda.

Para visualizar essa função no GitHub, consulte Amazon Comprehend S3 Object Lambda.

Exemplo 2: Edição de PII

Essa função do Lambda usa o Amazon Comprehend, um serviço de processamento de linguagem natural (PLN) que usa machine learning para encontrar insights e relações no texto. Essa função remove automaticamente informações de identificação pessoal (PII), como nomes, endereços, datas, números de cartão de crédito e números de previdência social, de documentos em seu bucket do Amazon S3.

Se você tiver documentos em seu bucket que incluam informações como números de cartão de crédito ou informações de contas bancárias, poderá configurar a função do S3 Object Lambda de edição de PII para detectar PII e, em seguida, retornar uma cópia desses documentos nas quais os tipos de entidade de PII estejam editados.

Para começar, implante a função do Lambda a seguir em sua conta e adicione o ARN da função na configuração do ponto de acesso do Object Lambda.

Veja a seguir um exemplo de ARN para essa função:

```
arn:aws:serverlessrepo:us-east-1:111122223333::applications/
ComprehendPiiRedactionS3ObjectLambda
```

Você pode adicionar ou exibir essa função no AWS Management Console usando o seguinte link do AWS Serverless Application Repository: ComprehendPiiRedactionS3ObjectLambda.

Para visualizar essa função no GitHub, consulte Amazon Comprehend S3 Object Lambda.

Para saber mais sobre procedimentos completos para algumas tarefas do S3 Object Lambda em edição de PII, consulte Tutorial: Detectar e editar dados PII com o S3 Object Lambda e o Amazon Comprehend.

Exemplo 3: descompressão

A função `S3ObjectLambdaDecompression` do Lambda pode descompactar objetos armazenados no Amazon S3 em um dos seis formatos de arquivo compactados: `bzip2`, `gzip`, `snappy`, `zlib`, `zstandard` e `ZIP`.

Para começar, implante a função do Lambda a seguir em sua conta e adicione o ARN da função na configuração do ponto de acesso do Object Lambda.

Veja a seguir um exemplo de ARN para essa função:

```
arn:aws:serverlessrepo:us-east-1:111122223333::applications/S3ObjectLambdaDecompression
```

Você pode adicionar ou exibir essa função no AWS Management Console usando o seguinte link do AWS Serverless Application Repository: S3ObjectLambdaDecompression.

Para visualizar essa função no GitHub, consulte S3 Object Lambda Decompression.

Práticas recomendadas e diretrizes para o S3 Object Lambda

Ao usar o S3 Object Lambda, siga essas práticas recomendadas e diretrizes para otimizar operações e performance.

Tópicos

- Trabalhar com o S3 Object Lambda
- Serviços da AWS usados em conexão com o S3 Object Lambda
- Cabeçalhos Range e partNumber
- Transformar expiry-date
- Como trabalhar com a AWS CLI e AWS SDKs

Trabalhar com o S3 Object Lambda

O S3 Object Lambda é compatível apenas com o processamento de solicitações `GET`, `LIST` e `HEAD`. Qualquer outra solicitação não invocará AWS Lambda; em vez disso, retornará respostas de API padrão e não transformadas. Você pode criar no máximo 1.000 pontos de acesso do Object Lambda por Conta da AWS por região. A função do AWS Lambda que você usa deve estar nas mesmas Conta da AWS e região que o ponto de acesso do Object Lambda.

O S3 Object Lambda permite transmitir uma resposta completa ao autor da chamada em até 60 segundos. Sua função também está sujeita a cotas padrão do AWS Lambda. Para obter mais informações, consulte Cotas do Lambda no Guia do desenvolvedor do AWS Lambda.

Quando o S3 Object Lambda invoca a função do Lambda especificada, você é responsável por garantir que todos os dados substituídos ou excluídos do Amazon S3 pela função ou aplicação do Lambda especificada sejam intencionais e corretos.

Você só pode usar o S3 Object Lambda para realizar operações em objetos. Você não pode usá-lo para realizar outras operações do Amazon S3, como modificar ou excluir buckets. Para obter uma lista completa das operações do S3 que oferecem suporte a pontos de acesso, consulte Compatibilidade de pontos de acesso com operações do S3.

Além dessa lista, os pontos de acesso do Object Lambda não são compatíveis com as operações de API `POST Object`, `CopyObject` (como origem) e `SelectObjectContent`.

Serviços da AWS usados em conexão com o S3 Object Lambda

O S3 Object Lambda conecta Amazon S3, o AWS Lambda e, opcionalmente, outros Serviços da AWS de sua escolha para fornecer objetos relevantes para as aplicações solicitadas. Todos os Serviços da AWS usados com o S3 Object Lambda são regidos por seus respectivos Acordos de Serviço (SLAs). Por exemplo, no caso de qualquer AWS service (Serviço da AWS) não cumprir seu compromisso de serviço, você será elegível para receber um crédito de serviço conforme documentado no SLA do serviço.

Cabeçalhos `Range` e `partNumber`

Ao trabalhar com objetos grandes, você pode usar o cabeçalho HTTP `Range` para baixar um intervalo de bytes especificado de um objeto. Quando você usa o cabeçalho `Range`, sua solicitação busca somente a parte especificada do objeto. Você também pode usar o cabeçalho `partNumber` para realizar uma solicitação em um intervalo para a parte especificada do objeto.

Para obter mais informações, consulte Trabalhar com cabeçalhos Range e partNumber.

Transformar `expiry-date`

Você pode abrir ou baixar objetos transformados do ponto de acesso do Object Lambda no AWS Management Console. Esses objetos devem ser válidos (não expirados). Se sua função do Lambda transformar `expiry-date` dos objetos, você poderá ver objetos expirados que não poderão ser abertos nem baixados. Esse comportamento se aplica somente a objetos restaurados do S3 Glacier Flexible Retrieval e do S3 Glacier Deep Archive.

Como trabalhar com a AWS CLI e AWS SDKs

Os subcomandos do S3 (`cp`, `mv` e `sync`) da AWS Command Line Interface (AWS CLI) e o uso da classe AWS SDK para Java `TransferManager` não são compatíveis com o S3 Object Lambda.

Tutoriais do S3 Object Lambda

Os tutoriais a seguir apresentam procedimentos completos para algumas tarefas do S3 Object Lambda.

Com o S3 Object Lambda você pode adicionar seu próprio código para processar dados recuperados do S3 antes de retorná-los para uma aplicação. Cada um dos tutoriais a seguir modificará os dados à medida que forem recuperados do Amazon S3, sem alterar o objeto existente ou manter várias cópias dos dados. O primeiro tutorial explicará como adicionar uma função do AWS Lambda a uma solicitação GET do S3 para modificar um objeto recuperado do S3. O segundo tutorial demonstra como usar uma função do Lambda predefinida com o Amazon Comprehend para proteger informações de identificação pessoal (PII) recuperadas do S3 antes de retorná-las a uma aplicação. O terceiro tutorial usa o S3 Object Lambda para adicionar uma marca d'água a uma imagem à medida que ela é recuperada do Amazon S3.

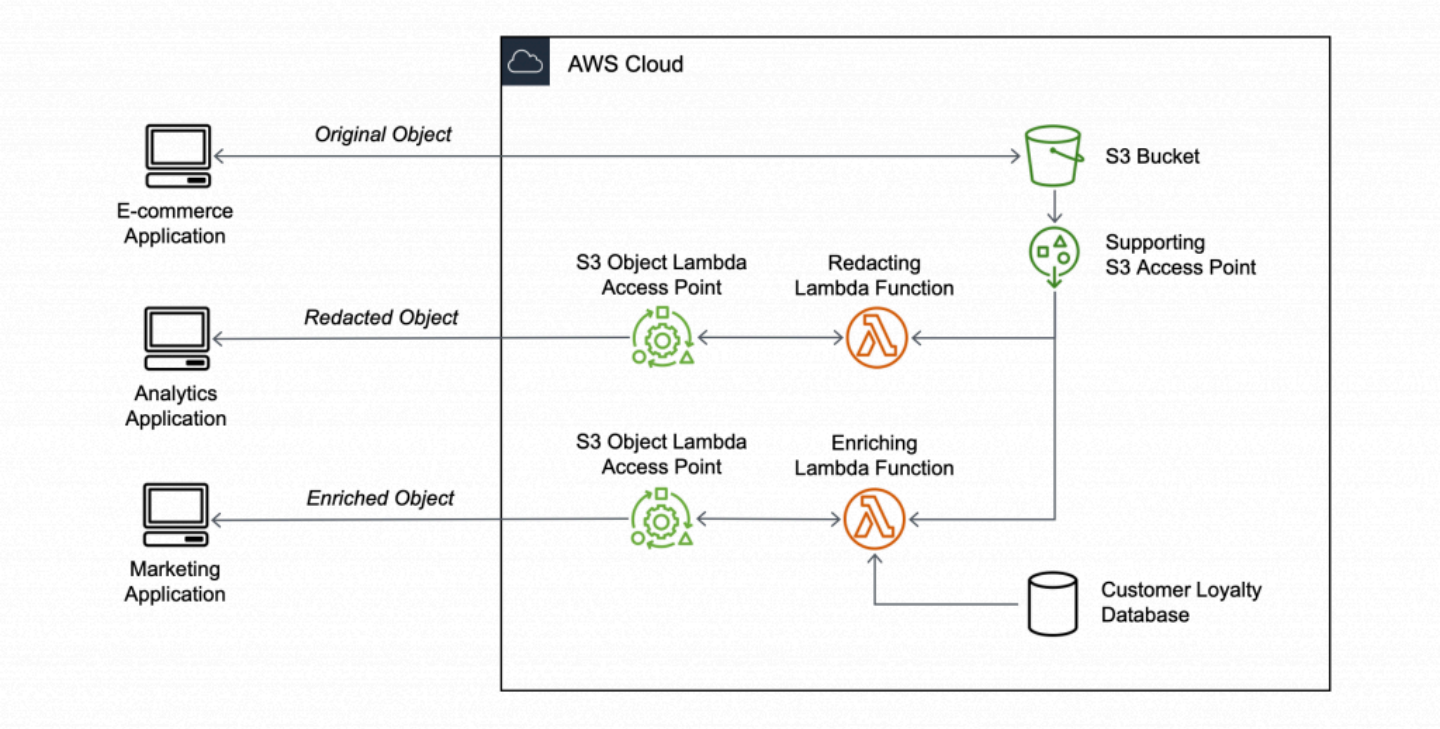
- Tutorial: Como transformar dados para sua aplicação com o S3 Object Lambda
- Tutorial: Detectar e editar dados PII com o S3 Object Lambda e o Amazon Comprehend

- Tutorial: Using S3 Object Lambda to dynamically watermark images as they are retrieved (Tutorial: Como usar o S3 Object Lambda para colocar marca d'água em imagens de maneira dinâmica à medida que são recuperadas)

Tutorial: Como transformar dados para sua aplicação com o S3 Object Lambda

Quando você armazena dados no Amazon S3, você pode compartilhá-los facilmente para usar várias aplicações. No entanto, cada aplicação pode ter requisitos de formato de dados exclusivos e pode precisar de modificação ou processamento de seus dados para um caso de uso específico. Por exemplo, um conjunto de dados criado por uma aplicação de comércio eletrônico pode incluir informações de identificação pessoal (PII). Quando os mesmos dados são processados para análise, essas PII não são necessárias e devem ser editadas. No entanto, se o mesmo conjunto de dados for usado para uma campanha de marketing, talvez seja necessário enriquecer os dados com detalhes adicionais, como informações do banco de dados de fidelidade do cliente.

Com o S3 Object Lambda você pode adicionar seu próprio código para processar dados recuperados do S3 antes de retorná-los para uma aplicação. É possível, especificamente, configurar uma função do AWS Lambda e anexá-la a um ponto de acesso do S3 Object Lambda. Quando uma aplicação envia solicitações GET padrão do S3 por meio do ponto de acesso do S3 Object Lambda, a função do Lambda especificada é invocada para processar quaisquer dados recuperados da fonte de dados subjacente por meio do ponto de acesso de suporte do S3. Depois, o ponto de acesso do S3 Object Lambda retorna o resultado transformado de volta à aplicação. Você pode criar e executar suas próprias funções Lambda personalizadas, adaptando a transformação de dados do S3 Object Lambda ao seu caso de uso específico, tudo sem a necessidade de alterações em suas aplicações.



Objetivo

Neste tutorial, você aprende como adicionar código personalizado a solicitações GET padrão do S3 para modificar o objeto solicitado recuperado do S3 para que o objeto atenda às necessidades do cliente ou aplicação solicitante. Especificamente, você aprende a transformar todo o texto no objeto original armazenado no bucket do S3 em maiúsculas por meio do S3 Object Lambda.

> **Note**
>
> Este tutorial usa código Python para transformar os dados. Para ter exemplos de uso de outros AWS SDKs, consulte Como transformar dados para sua aplicação com o S3 Object Lambda na Biblioteca de códigos de exemplo de AWS SDK.

Tópicos

- Pré-requisitos
- Etapa 1: criar um bucket do S3
- Etapa 2: fazer upload do arquivo para seu bucket do S3
- Etapa 3: criar um ponto de acesso do S3
- Etapa 4: Criar uma função Lambda

- Etapa 5: configurar uma política do IAM para a função de execução da função Lambda
- Etapa 6: criar um ponto de acesso do S3 Object Lambda
- Etapa 7: exibir os dados transformados
- Etapa 8: limpar
- Próximas etapas

Pré-requisitos

Antes de começar este tutorial, você deve ter uma Conta da AWS na qual possa fazer login como um usuário do AWS Identity and Access Management (IAM) com permissões corretas. Você também deve instalar a versão 3.8 ou posterior do Python.

Subetapas

- Criar um usuário do IAM com permissões em sua Conta da AWS (console)
- Instale o Python 3.8 ou posterior em sua máquina local

Criar um usuário do IAM com permissões em sua Conta da AWS (console)

Você pode criar um usuário do IAM para o tutorial. Para concluir este tutorial, o usuário do IAM deve anexar as seguintes políticas do IAM para acessar recursos da AWS e executar ações específicas. Para obter mais informações sobre como criar um usuário do IAM, consulte Criar usuários do IAM (console) no Guia do usuário do IAM.

Seu usuário do IAM requer as seguintes políticas:

- AmazonS3FullAccess: concede permissões a todas as ações do Amazon S3, incluindo permissões para criar e usar um ponto de acesso do Object Lambda.
- AWSLambda_FullAccess: concede permissões a todas as ações do Lambda.
- IAMFullAccess: concede permissões a todas as ações do IAM.
- IAMAccessAnalyzerReadOnlyAccess: concede permissões para ler todas as informações de acesso fornecidas pelo IAM Access Analyzer.
- CloudWatchLogsFullAccess: concede acesso total ao CloudWatch Logs.

> **Note**
>
> Para simplificar, este tutorial cria e usa um usuário do IAM. Depois de concluir este tutorial, lembre-se de Excluir o usuário do IAM. Para uso em produção, recomendamos que você siga as Práticas recomendadas de segurança no IAM no Guia do usuário do IAM. Uma das práticas recomendadas exige que os usuários humanos usem a federação com um provedor de identidades para acessar a AWS usando credenciais temporárias. Outra prática recomendada é exigir que as workloads usem credenciais temporárias com perfis do IAM para acessar a AWS. Para saber como usar o AWS IAM Identity Center para criar usuários com credenciais temporárias, consulte Getting started (Conceitos básicos) no Guia do usuário do AWS IAM Identity Center.
> Este tutorial também usa políticas de acesso total gerenciadas pela AWS. Para uso em produção, recomendamos que você conceda apenas as permissões mínimas necessárias para seu caso de uso, de acordo com as práticas recomendadas de segurança.

Instale o Python 3.8 ou posterior em sua máquina local

Use o procedimento a seguir para instalar o Python 3.8 ou posterior em sua máquina local. Para obter instruções de instalação, consulte a página Downloading Python (Como baixar Python) no Guia do iniciante do Python.

1. Abra seu terminal local ou shell e execute o seguinte comando para determinar se o Python já está instalado e, em caso afirmativo, qual versão está instalada.

   ```
   python --version
   ```

2. Se não tiver o Python 3.8 nem posterior, faça download do instalador oficial do Python 3.8 ou posterior que é adequado para sua máquina local.
3. Execute o instalador clicando duas vezes no arquivo baixado e siga as etapas para concluir a instalação.

   Para os Usuários do Windows, escolha Adicionar Python 3.X ao PATH no assistente de instalação antes de escolher Instalar agora.
4. Reinicie o terminal fechando-o e reabrindo-o.
5. Execute o seguinte comando para verificar se o Python 3.8 ou posterior está instalado corretamente.

Para os usuários do macOS, execute este comando:

```
python3 --version
```

Para usuários do Windows, execute este comando:

```
python --version
```

6. Execute o comando a seguir para verificar se o gerenciador de pacotes pip3 está instalado. Se você vir um número de versão pip e python 3.8 ou posterior na resposta do comando, isso significa que o gerenciador de pacotes pip3 está instalado com sucesso.

```
pip --version
```

Etapa 1: criar um bucket do S3

Crie um bucket para armazenar os dados originais que você planeja transformar.

> **Note**
>
> Os pontos de acesso podem ser conectados a outra fonte de dados, como um volume do Amazon FSx para OpenZFS, mas este tutorial usa um ponto de acesso de suporte conectado a um bucket do S3.

Para criar um bucket

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets.
3. Selecione Create bucket (Criar bucket).

   A página Create bucket (Criar bucket) é aberta.
4. Para Bucket name (Nome do bucket), insira um nome para o seu bucket (por exemplo, **`tutorial-bucket`**).

Para obter mais informações sobre como nomear buckets no Amazon S3, consulte Regras de nomenclatura de buckets de uso geral.

5. Em Region (Região), escolha a Região da AWS onde deseja que o bucket resida.

   Para obter mais informações sobre a região do bucket, consulte Visão geral dos buckets de uso geral.

6. Para Block Public Access settings for this bucket (Configurações de acesso de bloqueio público para este bucket), mantenha as configurações padrão (Block allpublic access (Bloquear todo acesso público) está habilitado).

   Recomendamos que você mantenha todas as configurações de acesso de bloqueio público ativadas, a menos que precise desativar uma ou mais delas para seu caso de uso. Para obter mais informações sobre como bloquear o acesso público, consulte Bloquear o acesso público ao armazenamento do Amazon S3.

7. Mantenha as configurações restantes definidas conforme os padrões.

   (Opcional) Se quiser definir configurações de bucket adicionais para o caso de uso específico, consulte Criar um bucket de uso geral.

8. Escolha Criar bucket.

Etapa 2: fazer upload do arquivo para seu bucket do S3

Carregue um arquivo de texto para o bucket do S3. Este arquivo de texto contém os dados originais que você transformará em maiúsculas posteriormente neste tutorial.

Por exemplo, você pode carregar um `tutorial.txt` que contém o seguinte texto:

```
Amazon S3 Object Lambda Tutorial:
You can add your own code to process data retrieved from S3 before
returning it to an application.
```

Fazer upload de um arquivo para um bucket

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets.

3. Na lista de Buckets, escolha o nome do bucket que você criou na Etapa 1 (por exemplo, **`tutorial-bucket`**) para carregar seu arquivo.
4. Na guia Objects (Objetos) do bucket, escolha Upload (Fazer upload).
5. Na página Upload (Carregar), em Files and folders (Arquivos e pastas), escolha Add files (Adicionar arquivos).
6. Escolha um arquivo para carregar e, em seguida, escolha Open (Abrir). Por exemplo, você pode carregar o exemplo de arquivo `tutorial.txt`mencionado anteriormente.
7. Escolha Upload (Carregar).

Etapa 3: criar um ponto de acesso do S3

Para usar um ponto de acesso do S3 Object Lambda para acessar e transformar os dados originais, você deve criar um ponto de acesso do S3 e associá-lo ao bucket do S3 criado na Etapa 1. O ponto de acesso deve estar na mesma Região da AWS que os objetos que você deseja transformar.

Mais adiante neste tutorial, você usará esse ponto de acesso como um ponto de acesso de suporte para o ponto de acesso do Object Lambda.

Para criar um ponto de acesso

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação, escolha Access Points (Pontos de acesso).
3. Na página Access Points (Pontos de acesso), escolha Create access point (Criar ponto de acesso).
4. No campo Access point name (Nome do ponto de acesso), insira o nome (por exemplo, **`tutorial-access-point`**) para o ponto de acesso.

   Para obter mais informações sobre nomenclatura de pontos de acesso, consulte Regras de nomenclatura para pontos de acesso.
5. No campo Fonte de dados insira o nome do bucket criado na Etapa 1 (por exemplo, **`tutorial-bucket`**). O S3 anexa o ponto de acesso a este bucket.

   (Opcional) Você pode escolher Browse S3 (Procurar S3) para navegar e pesquisar buckets na sua conta. Se você escolher Browse S3 (Procurar S3), selecione o bucket desejado e escolha Choose path (Escolher caminho) para preencher o campo Bucket name (Nome do bucket) com o nome do bucket.

6. Para Network origin (Origem de rede), escolha Internet.

   Para obter mais informações sobre origens de rede para pontos de acesso, consulte Criar pontos de acesso restritos a uma nuvem privada virtual.

7. Por padrão, todas as configurações de bloqueio de acesso público são habilitadas para seu ponto de acesso. Recomendamos manter a opção Block all public access (Bloquear todo o acesso público) ativada.

   Para obter mais informações, consulte Gerenciar o acesso público a pontos de acesso para buckets de uso geral.

8. Para todas as outras configurações de ponto de acesso, mantenha as configurações padrão.

   (Opcional) Você pode modificar as configurações do ponto de acesso para dar suporte ao caso de uso. Para este tutorial, recomendamos manter as configurações padrão.

   (Opcional) Se você precisar gerenciar o acesso ao seu ponto de acesso, você pode especificar uma política de ponto de acesso. Para obter mais informações, consulte Exemplos de política para pontos de acesso.

9. Selecione Create access point (Criar ponto de acesso).

Etapa 4: Criar uma função Lambda

Para transformar dados originais, crie uma função do Lambda para usar com o ponto de acesso do S3 Object Lambda.

Subetapas

- Gravar código de função Lambda e criar um pacote de implantação com um ambiente virtual
- Crie uma função Lambda com uma função de execução (console)
- Implante seu código de função Lambda com arquivos .zip e configure a função Lambda (console)

Gravar código de função Lambda e criar um pacote de implantação com um ambiente virtual

1. Na sua máquina local, crie uma pasta com o nome da pasta `object-lambda` para que o ambiente virtual use posteriormente neste tutorial.
2. Na pasta `object-lambda`, crie um arquivo com uma função Lambda que altere todo o texto no objeto original para maiúsculas. Por exemplo, você pode usar a seguinte função gravada em Python. Salve esta função em um arquivo chamado `transform.py`.

```
import boto3
import requests
from botocore.config import Config

# This function capitalizes all text in the original object
def lambda_handler(event, context):
    object_context = event["getObjectContext"]
    # Get the presigned URL to fetch the requested original object
    # from S3
    s3_url = object_context["inputS3Url"]
    # Extract the route and request token from the input context
    request_route = object_context["outputRoute"]
    request_token = object_context["outputToken"]

    # Get the original S3 object using the presigned URL
    response = requests.get(s3_url)
    original_object = response.content.decode("utf-8")

    # Transform all text in the original object to uppercase
    # You can replace it with your custom code based on your use case
    transformed_object = original_object.upper()

    # Write object back to S3 Object Lambda
    s3 = boto3.client('s3', config=Config(signature_version='s3v4'))
    # The WriteGetObjectResponse API sends the transformed data
    # back to S3 Object Lambda and then to the user
    s3.write_get_object_response(
        Body=transformed_object,
        RequestRoute=request_route,
        RequestToken=request_token)

    # Exit the Lambda function: return the status code
    return {'status_code': 200}
```

Note

O exemplo anterior da função Lambda carrega todo o objeto solicitado na memória antes de transformá-lo e retorná-lo para o cliente. Como alternativa, você pode transmitir o objeto do S3 para evitar o carregamento do objeto inteiro na memória. Essa abordagem pode ser útil ao trabalhar com objetos grandes. Para obter mais informações sobre

streaming de respostas com pontos de acesso do Object Lambda, consulte os exemplos de streaming em Trabalhar com solicitações `GetObject` no Lambda.

Quando você está gravando uma função do Lambda para uso com um ponto de acesso do S3 Object Lambda, a função é baseada no contexto de evento de entrada que o S3 Object Lambda fornece à função do Lambda. O contexto do evento fornece informações sobre a solicitação que está sendo feita no evento passado do S3 Object Lambda para o Lambda. Ele contém os parâmetros que você usa para criar a função Lambda.

Os campos usados para criar a função Lambda anterior são os seguintes:

O campo `getObjectContext` significa os detalhes de entrada e saída para conexões com o Amazon S3 e S3 Object Lambda. Ele tem os seguintes campos:

- `inputS3Url`: um URL pré-assinado que a função Lambda pode usar para baixar o objeto original do ponto de acesso de suporte. Usando um URL pré-assinado, a função Lambda não precisa ter permissões de leitura do Amazon S3 para recuperar o objeto original e só pode acessar o objeto processado por cada chamada.
- `outputRoute`: um token de roteamento que é adicionado ao URL do Object Lambda do S3 quando a função Lambda chama `WriteGetObjectResponse` para enviar de volta o objeto transformado.
- `outputToken`: um token usado pelo S3 Object Lambda para corresponder à chamada `WriteGetObjectResponse` com o chamador original ao enviar de volta o objeto transformado.

Para obter mais informações sobre todos os campos no contexto de evento, consulte Formato e uso de contexto de evento e Escrever funções do Lambda para pontos de acesso do S3 Object Lambda.

3. No terminal local, insira o seguinte comando para instalar o comando do pacote `virtualenv`:

```
python -m pip install virtualenv
```

4. No terminal local, abra o `object-lambda` que você criou anteriormente e insira o seguinte comando para criar e inicializar um ambiente virtual chamado `venv`.

```
python -m virtualenv venv
```

5. Para ativar o ambiente virtual, insira o seguinte comando para executar o arquivo `activate` da pasta do ambiente:

   Para os usuários do macOS, execute este comando:

   ```
   source venv/bin/activate
   ```

   Para usuários do Windows, execute este comando:

   ```
   .\venv\Scripts\activate
   ```

   Agora, seu prompt de comando é alterado para mostrar (venv), indicando que o ambiente virtual está ativo.

6. Para instalar as bibliotecas necessárias, execute os seguintes comandos linha por linha no ambiente virtual do `venv`.

   Esses comandos instalam versões atualizadas das dependências de sua função Lambda `lambda_handler`. Essas dependências são o AWSSDK for Python (Boto3) e o módulo de solicitações.

   ```
   pip3 install boto3
   ```

   ```
   pip3 install requests
   ```

7. Para desativar o ambiente virtual, execute o seguinte comando:

   ```
   deactivate
   ```

8. Para criar um pacote de implantação com as bibliotecas instaladas como um arquivo `.zip` chamado `lambda.zip` na raiz do diretório , execute os comandos a seguir, linha por linha, em seu terminal local.

   > **Tip**
   >
   > Os comandos a seguir talvez precisem ser ajustados para funcionar em seu ambiente específico. Por exemplo, uma biblioteca pode aparecer em `site-packages`ou em `dist-packages` e a primeira pasta pode ser `lib` ou `lib64`. Além disso, a pasta

`python` pode ser nomeada com uma versão Python diferente. Use o comando `pip show` para localizar um pacote específico.

Para usuários do macOS, execute estes comandos:

```
cd venv/lib/python3.8/site-packages
```

```
zip -r ../../../../lambda.zip .
```

Para usuários do Windows, execute estes comandos:

```
cd .\venv\Lib\site-packages\
```

```
powershell Compress-Archive * ../../../lambda.zip
```

O último comando salva o pacote de implantação na raiz do diretório do `object-lambda`.

9. Adicione o arquivo de código de função `transform.py` à raiz do pacote de implantação.

Para usuários do macOS, execute estes comandos:

```
cd ../../../../
```

```
zip -g lambda.zip transform.py
```

Para usuários do Windows, execute estes comandos:

```
cd ..\..\..\
```

```
powershell Compress-Archive -update transform.py lambda.zip
```

Depois de concluir esta etapa, você deverá ter seguinte estrutura de diretórios:

```
lambda.zip$
  # transform.py
  # __pycache__
```

```
| boto3/
# certifi/
# pip/
# requests/
...
```

Crie uma função Lambda com uma função de execução (console)

1. Faça login no AWS Management Console e abra o console do AWS Lambda em https://console.aws.amazon.com/lambda/.
2. No painel de navegação à esquerda, escolha Functions (Funções).
3. Escolha Create function (Criar função).
4. Escolha Author from scratch (Criar do zero).
5. Em Basic information (Informações básicas), faça o seguinte:
   a. Em Function name (Nome da função), insira **`tutorial-object-lambda-function`**.
   b. Para Runtime (Tempo de execução), escolha Python 3.8 ou uma versão posterior.
6. Expandir a seção Alterar função de execução padrão. Em Execution role (Função de execução), selecione Create a new role with basic Lambda permissions (Criar uma função com permissões básicas do Lambda).

   Na Etapa 5, posteriormente neste tutorial, você anexa o AmazonS3ObjectLambdaExecutionRolePolicy a essa função de execução do Lambda.
7. Mantenha as configurações restantes definidas conforme os padrões.
8. Escolha Create function (Criar função).

Implante seu código de função Lambda com arquivos .zip e configure a função Lambda (console)

1. No console do AWS Lambda em https://console.aws.amazon.com/lambda/, escolha Functions (Funções) no painel de navegação à esquerda.
2. Escolha a função do Lambda que você criou anteriormente (por exemplo, **`tutorial-object-lambda-function`**).
3. Na página de detalhes da função Lambda, selecione a guia Code (Código). Na seção Code Source (Origem do código), escolha Upload from (Carregar de) e depois arquivo .zip.
4. Selecione Upload (Carregar) para selecionar seu arquivo `.zip` local.

5. Selecione o arquivo `lambda.zip` que você criou anteriormente e, em seguida, selecione Open (Abrir).
6. Escolha Salvar.
7. Na seção Runtime settings (Configurações do tempo de execução), escolha Edit (Editar).
8. Na página Edit runtime settings (Editar configurações do tempo de execução), confirme se Runtime (Tempo de execução) foi definido como Python 3.8 ou uma versão posterior.
9. Para informar ao tempo de execução do Lambda qual método de handler em seu código de função Lambda chamar, insira **`transform.lambda_handler`** para Handler.

   Ao configurar uma função em Python, o valor da configuração do handler é o nome do arquivo e o nome do módulo do handler exportado, separados por um ponto. Por exemplo, `transform.lambda_handler` chama o método `lambda_handler` definido no arquivo `transform.py`.
10. Escolha Salvar.
11. (Opcional) Na página de detalhes da função Lambda, escolha a guia Configuration (Configuração). No painel de navegação à esquerda, selecione General configuration (Configuração geral) e, depois, escolha Edit (Editar). No campo Timeout (Tempo limite), insira **`1`** min **`0`** segundos. Mantenha as configurações restantes definidas, conforme os padrões e escolha Save (Salvar).

    Timeout (Tempo limite) é a quantidade de tempo durante a qual o Lambda permite que uma função seja executada entes de interrompê-la. O padrão é 3 segundos. A duração máxima para uma função Lambda usada pelo S3 Object Lambda é de 60 segundos. O preço é baseado na quantidade de memória configurada e na quantidade de tempo em que o código é executado.

Etapa 5: configurar uma política do IAM para a função de execução da função Lambda

Para habilitar sua função Lambda para fornecer dados personalizados e cabeçalhos de resposta para o chamador de `GetObject`, a função de execução da função Lambda precisa ter permissões do IAM para chamar a API `WriteGetObjectResponse`.

Para anexar uma política do IAM à atribuição da função Lambda

1. No console do AWS Lambda em https://console.aws.amazon.com/lambda/, escolha Functions (Funções) no painel de navegação à esquerda.

2. Escolha a função que você criou na Etapa 4 (por exemplo, **`tutorial-object-lambda-function`**).
3. Na página de detalhes da função Lambda, selecione a guia Configuration (Configuração) e, depois, escolha Permission (Permissões) no painel de navegação à esquerda.
4. Em Execution role (Função de execução), escolha o link do Role name (Nome da função). O console do IAM é aberto.
5. Na página Summary (Resumo) do console do IAM para o perfil de execução da função do Lambda, escolha a guia Permissions (Permissões). Depois, no menu Add Permissions (Adicionar permissões), escolha Attach policies (Anexar políticas).
6. Na página Attach Permissions (Anexar permissões), insira **`AmazonS3ObjectLambdaExecutionRolePolicy`** na caixa de pesquisa para filtrar a lista de políticas. Marque a caixa de seleção ao lado do nome da política AmazonS3ObjectLambdaExecutionRolePolicy.
7. Escolha Anexar políticas.

Etapa 6: criar um ponto de acesso do S3 Object Lambda

Um ponto de acesso do S3 Object Lambda fornece a flexibilidade de chamar uma função do Lambda diretamente de uma solicitação GET do S3 para que a função possa processar dados recuperados de um ponto de acesso do S3. Ao criar e configurar um ponto de acesso do S3 Object Lambda, você deve especificar a função do Lambda para chamar e fornecer o contexto do evento no formato JSON como parâmetros personalizados para o Lambda usar.

Para criar um ponto de acesso do S3 Object Lambda

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Object Lambda access points (Pontos de acesso do Object Lambda).
3. Na página Object Lambda Access Points (Pontos de acesso do Object Lambda), escolha Create Object Lambda Access Point (Criar ponto de acesso do Object Lambda).
4. Para Nome do Ponto de acesso Lambda do objeto, informe o nome que você deseja usar para o ponto de acesso Lambda do objeto (por exemplo, **`tutorial-object-lambda-accesspoint`**).

5. Para Supporting Access Point (Ponto de acesso de suporte), informe ou procure o ponto de acesso padrão criado na Etapa 3 (por exemplo, **`tutorial-access-point`**) e, em seguida, escolha Choose supporting Access Point (Escolher ponto de acesso de suporte).
6. Para recuperar objetos do bucket do S3 para que a função do Lambda processe, selecione GetObject em S3 APIs (APIs do S3).
7. Para Invoke Lambda function (Chamar função Lambda), você pode escolher qualquer uma das duas opções a seguir para este tutorial.
   - Selecione Choose from functions in your account (Escolher das funções de sua conta) e escolha a função Lambda que você criou na Etapa 4 (por exemplo, **`tutorial-object-lambda-function`**) da lista suspensa Lambda function (Função Lambda).
   - Escolha Enter ARN (Inserir ARN) e depois informe o Nome do recurso da Amazon (ARN) da função Lambda que você criou na Etapa 4.
8. Para Lambda function version (Versão da função Lambda), escolha $LATEST (a versão mais recente da função Lambda que você criou na Etapa 4).
9. (Opcional) Se precisar da função Lambda para reconhecer e processar solicitações GET com cabeçalhos de intervalo e número de peça, selecione Lambda function supports requests using range (A função Lambda suporta solicitações usando intervalo) e Lambda function supports requests using part numbers (A função Lambda suporta solicitações usando números de parte). Caso contrário, desmarque essas duas caixas de seleção.

   Para obter mais informações sobre como usar números de intervalo ou de parte com o S3 Object Lambda, consulte Trabalhar com cabeçalhos Range e partNumber.
10. (Opcional) Em Payload - optional (Carga útil - opcional), adicione um texto JSON para fornecer informações adicionais à sua função Lambda.

    Uma carga útil é um texto JSON opcional que você pode fornecer à sua função do Lambda como entrada para todas as chamadas provenientes de um ponto de acesso do S3 Object Lambda específico. Para personalizar os comportamentos de vários pontos de acesso Lambda do objeto que chamam a mesma função do Lambda, você pode configurar cargas úteis com diferentes parâmetros, estendendo, assim, a flexibilidade da função do Lambda.

    Para obter mais informações sobre carga útil, consulte Formato e uso de contexto de evento.
11. (Opcional) Para Métricas de solicitação – opcional, escolha Desativar ou Ativar para adicionar o monitoramento do Amazon S3 ao ponto de acesso Lambda do objeto. As métricas de solicitação são cobradas na taxa padrão do Amazon CloudWatch. Para obter mais informações, consulte Preço do CloudWatch.

12. Em Object Lambda Access Point policy - optional (Política do ponto de acesso do Object Lambda - opcional), mantenha a configuração padrão.

    (Opcional) Você pode definir uma política de recursos. Essa política de recursos concede permissão da API `GetObject` para usar o ponto de acesso do Object Lambda especificado.
13. Mantenha as configurações restantes definidas conforme os padrões e escolha Create Object Lambda Access Point (Criar ponto de acesso do Object Lambda).

Etapa 7: exibir os dados transformados

Agora, o S3 Object Lambda está pronto para transformar seus dados para seu caso de uso. Neste tutorial, o S3 Object Lambda transforma todo o texto em seu objeto em maiúsculas.

Subetapas

- Exibir os dados transformados no ponto de acesso do S3 Object Lambda
- Execute um script Python para imprimir os dados originais e transformados

Exibir os dados transformados no ponto de acesso do S3 Object Lambda

Quando você solicita para recuperar um arquivo por meio do ponto de acesso do S3 Object Lambda, você faz uma chamada de API `GetObject` para o S3 Object Lambda. O S3 Object Lambda chama a função Lambda para transformar seus dados e, em seguida, retorna os dados transformados como a resposta à chamada de API de `GetObject` do S3 padrão.

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Object Lambda access points (Pontos de acesso do Object Lambda).
3. Na página Pontos de acesso do Object Lambda, escolha o ponto de acesso do S3 Object Lambda que você criou na Etapa 6 (por exemplo, **`tutorial-object-lambda-accesspoint`**).
4. Na guia Objetos do ponto de acesso do S3 Object Lambda, selecione o arquivo que tem o mesmo nome (por exemplo, `tutorial.txt`) daquele que você carregou no bucket do S3 na Etapa 2.

   Esse arquivo deve conter todos os dados transformados.
5. Para exibir os dados transformados, escolha Open (Abrir) ou Download (Baixar).

Execute um script Python para imprimir os dados originais e transformados

Você pode usar o S3 Object Lambda com suas aplicações existentes. Para fazer isso, atualize a configuração da aplicação para usar o novo ARN do ponto de acesso do S3 Object Lambda criado na Etapa 6 para recuperar dados do S3.

O exemplo de script Python a seguir imprime os dados originais do bucket do S3 e os dados transformados do ponto de acesso do S3 Object Lambda.

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Object Lambda access points (Pontos de acesso do Object Lambda).
3. Na página Pontos de acesso Lambda de objeto, selecione o botão de opção à esquerda do ponto de acesso do S3 Object Lambda que você criou na Etapa 6 (por exemplo, **`tutorial-object-lambda-accesspoint`**).
4. Escolha Copy ARN (Copiar ARN).
5. Salve o ARN para uso mais tarde.
6. Grave um script Python na máquina local para imprimir os dados originais (por exemplo, `tutorial.txt`) do bucket do S3 e os dados transformados (por exemplo, `tutorial.txt`) do ponto de acesso do S3 Object Lambda). Você pode usar o seguinte script de exemplo:

```
import boto3
from botocore.config import Config

s3 = boto3.client('s3', config=Config(signature_version='s3v4'))

def getObject(bucket, key):
    objectBody = s3.get_object(Bucket = bucket, Key = key)
    print(objectBody["Body"].read().decode("utf-8"))
    print("\n")

print('Original object from the S3 bucket:')
# Replace the two input parameters of getObject() below with
# the S3 bucket name that you created in Step 1 and
# the name of the file that you uploaded to the S3 bucket in Step 2
getObject("tutorial-bucket",
          "tutorial.txt")

print('Object transformed by S3 Object Lambda:')
```

```
# Replace the two input parameters of getObject() below with
# the ARN of your S3 Object Lambda Access Point that you saved earlier and
# the name of the file with the transformed data (which in this case is
# the same as the name of the file that you uploaded to the S3 bucket
# in Step 2)
getObject("arn:aws:s3-object-lambda:us-west-2:111122223333:accesspoint/tutorial-
object-lambda-accesspoint",
          "tutorial.txt")
```

7. Salve seu script Python com um nome personalizado (por exemplo, `tutorial_print.py`) na pasta (por exemplo, `object-lambda`) que você criou na Etapa 4 na sua máquina local.
8. No terminal local, execute o seguinte comando da raiz do diretório (por exemplo, `object-lambda`) que você criou na Etapa 4.

```
python3 tutorial_print.py
```

Você deve ver os dados originais e os dados transformados (todo o texto em maiúsculas) através do terminal. Por exemplo, você deve ver algo parecido com o texto a seguir.

```
Original object from the S3 bucket:
Amazon S3 Object Lambda Tutorial:
You can add your own code to process data retrieved from S3 before
returning it to an application.

Object transformed by S3 Object Lambda:
AMAZON S3 OBJECT LAMBDA TUTORIAL:
YOU CAN ADD YOUR OWN CODE TO PROCESS DATA RETRIEVED FROM S3 BEFORE
RETURNING IT TO AN APPLICATION.
```

Etapa 8: limpar

Se você transformou seus dados por meio do S3 Object Lambda apenas como um exercício de aprendizado, exclua os recursos da AWS que você alocou para que não haja mais encargos.

Subetapas

- Excluir o ponto de acesso do Object Lambda
- Exclua o ponto de acesso do S3
- Exclua a função de execução de sua função Lambda
- Excluir a função Lambda

- Excluir o grupo de logs do CloudWatch
- Exclua o arquivo original no bucket de origem do S3
- Exclua o bucket de origem do S3
- Excluir o usuário do IAM

Excluir o ponto de acesso do Object Lambda

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Object Lambda access points (Pontos de acesso do Object Lambda).
3. Na página Pontos de acesso Lambda de objeto, selecione o botão de opção à esquerda do ponto de acesso do S3 Object Lambda que você criou na Etapa 6 (por exemplo, **`tutorial-object-lambda-accesspoint`**).
4. Escolha Excluir.
5. Confirme se deseja excluir o ponto de acesso do Lambda, inserindo o nome no campo de texto exibido e escolha Excluir.

Exclua o ponto de acesso do S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação, escolha Access Points (Pontos de acesso).
3. Navegue até o ponto de acesso que você criou na Etapa 3 (por exemplo, **`tutorial-access-point`**) e escolha o botão de opção ao lado do nome do ponto de acesso.
4. Escolha Excluir.
5. Confirme se deseja excluir o ponto de acesso inserindo o nome no campo de texto exibido e escolha Delete (Excluir).

Exclua a função de execução de sua função Lambda

1. Faça login no AWS Management Console e abra o console do AWS Lambda em https://console.aws.amazon.com/lambda/.
2. No painel de navegação à esquerda, escolha Functions (Funções).

3. Escolha a função que você criou na Etapa 4 (por exemplo, **`tutorial-object-lambda-function`**).
4. Na página de detalhes da função Lambda, selecione a guia Configuration (Configuração) e, depois, escolha Permission (Permissões) no painel de navegação à esquerda.
5. Em Execution role (Função de execução), escolha o link do Role name (Nome da função). O console do IAM é aberto.
6. Na página Summary (Resumo) do console do IAM da função de execução da função Lambda, selecione Delete role (Excluir função).
7. Na caixa de diálogo Delete role (Excluir função), selecione Yes, delete (Sim, excluir).

Excluir a função Lambda

1. No console do AWS Lambda em https://console.aws.amazon.com/lambda/, escolha Functions (Funções) no painel de navegação à esquerda.
2. Marque a caixa de seleção à esquerda do nome da função que você criou na Etapa 4 (por exemplo, **`tutorial-object-lambda-function`**).
3. Escolha Ações e, em seguida, escolha Excluir.
4. Na caixa de diálogo Delete function (Excluir função), escolha Delete (Excluir).

Excluir o grupo de logs do CloudWatch

1. Abra o console do CloudWatch em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação esquerdo, escolha Log groups (Grupos de log).
3. Localize o grupo de logs cujo nome termina com a função Lambda que você criou na Etapa 4 (por exemplo, **`tutorial-object-lambda-function`**).
4. Marque a caixa de seleção à esquerda do nome do grupo de logs.
5. Escolha Actions (Ações) e Delete log group(s) (Excluir grupo(s) de log).
6. Na caixa de diálogo Delete log group(s) (Excluir grupo(s) de logs), escolha Delete (Excluir).

Exclua o arquivo original no bucket de origem do S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets.

3. Na lista Bucket name (Nome do bucket), escolha o nome do bucket para o qual você carregou o arquivo original na Etapa 2 (por exemplo, **`tutorial-bucket`**).
4. Marque a caixa de seleção à esquerda do nome do objeto que você deseja excluir (por exemplo, `tutorial.txt`).
5. Escolha Excluir.
6. Na página Delete objects (Excluir objetos) na seção Permanently delete objects? (Excluir objetos permanentemente?), confirme se deseja excluir este objeto informando **`permanently delete`** na caixa de texto.
7. Escolha Delete objects (Excluir objetos).

Exclua o bucket de origem do S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets.
3. Na lista de Buckets, escolha o botão de opção ao lado do nome do bucket que você criou na Etapa 1 (por exemplo, **`tutorial-bucket`**).
4. Escolha Excluir.
5. Na página Delete bucket (Excluir bucket), confirme se deseja excluir o bucket inserindo o nome do bucket no campo de texto e escolha Delete bucket (Excluir bucket).

Excluir o usuário do IAM

1. Faça login no AWS Management Console e abra o console do IAM, em https://console.aws.amazon.com/iam/.
2. No painel de navegação esquerdo, escolha Users (Usuários) e marque a caixa de seleção ao lado do nome do usuário que você deseja excluir.
3. Na parte superior da página, escolha Delete (Excluir).
4. Na caixa de diálogo Delete ***`user name`***? (Excluir nome de usuário?), insira o nome de usuário no campo de entrada de texto para confirmar a exclusão do usuário. Escolha Excluir.

Próximas etapas

Após concluir este tutorial, você pode personalizar a função Lambda para o caso de uso para modificar os dados retornados por solicitações S3 GET padrão.

Veja a seguir uma lista de casos de uso comuns para o S3 Object Lambda:

- Mascaramento de dados confidenciais para segurança e conformidade.

  Para obter mais informações, consulte Tutorial: Detectar e editar dados PII com o S3 Object Lambda e o Amazon Comprehend.
- Filtragem de determinadas linhas de dados para fornecer informações específicas.
- Aumento de dados com informações de outros serviços ou bancos de dados.
- Conversão entre formatos de dados, como conversão de XML em JSON para compatibilidade de aplicações.
- Compactação ou descompactação de arquivos enquanto eles estão sendo baixados.
- Redimensionamento e marcação d'água de imagens.

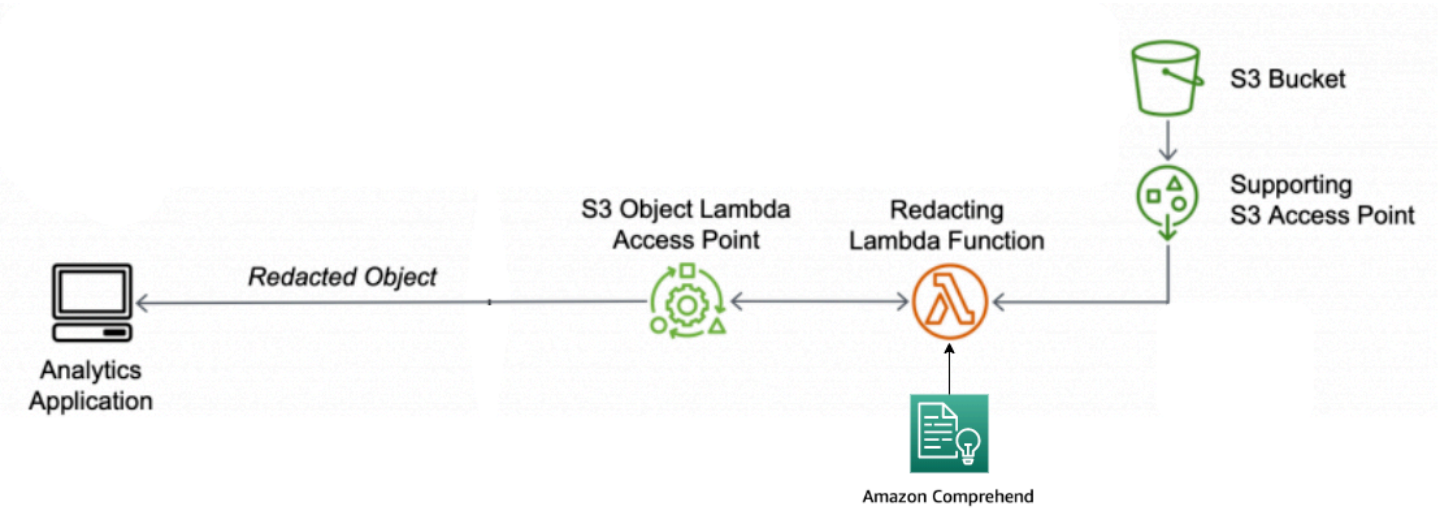
  Para obter mais informações, consulte Tutorial: Using S3 Object Lambda to dynamically watermark images as they are retrieved (Tutorial: Como usar o S3 Object Lambda para colocar marca d'água em imagens de maneira dinâmica à medida que são recuperadas).
- Implementação de regras de autorização personalizadas para acessar dados.

Para obter mais informações sobre o S3 Object Lambda, consulte Transformar objetos com o S3 Object Lambda.

Tutorial: Detectar e editar dados PII com o S3 Object Lambda e o Amazon Comprehend

Quando você estiver usando o Amazon S3 para conjuntos de dados compartilhados para várias aplicações e os usuários acessarem, é importante restringir informações privilegiadas, como informações de identificação pessoal (PII) apenas para entidades autorizadas. Por exemplo, quando uma aplicação de marketing usa alguns dados contendo PII, ela pode precisar primeiro mascarar dados PII para atender aos requisitos de privacidade de dados. Além disso, quando um aplicação de análise usa um conjunto de dados de inventário de ordem de produção, talvez seja necessário primeiro editar as informações do cartão de crédito do cliente para evitar perdas não intencionais de dados.

Com o S3 Object Lambda e uma função do AWS Lambda pré-construída, habilitada pelo Amazon Comprehend, você pode proteger dados de PII recuperados do S3 antes de retorná-los para uma aplicação. Especificamente, é possível usar a função do Lambda pré-criada como função de edição e anexá-la a um ponto de acesso do S3 Object Lambda. Quando uma aplicação (por exemplo, uma aplicação de analytics) envia solicitações GET padrão do S3, essas solicitações feitas por meio do ponto de acesso do S3 Object Lambda invocam a função do Lambda de edição predefinida para detectar e editar dados de PII recuperados de uma fonte de dados subjacente por meio de um ponto de acesso de suporte do S3. Depois, o ponto de acesso do S3 Object Lambda retorna o resultado editado de volta à aplicação.



No processo, a função do Lambda pré-criada usa o Amazon Comprehend, um serviço de processamento de linguagem natural (PNL) para registrar variações em como as PII são representadas, independentemente de como as PII existem no texto (por exemplo, numericamente ou uma combinação de palavras e números). O Amazon Comprehend pode até usar o contexto no texto para entender se um número de quatro dígitos é um PIN, os últimos quatro números de um número de Seguridade Social (SSN) ou um ano. O Amazon Comprehend processa qualquer arquivo de texto no formato UTF-8 e pode proteger as PII em escala sem afetar a precisão. Para obter mais informações, consulte O que é Amazon Comprehend? no Guia do desenvolvedor do Amazon Comprehend.

Objetivo

Neste tutorial, você aprenderá a usar o S3 Object Lambda com a função Lambda pré-criada`ComprehendPiiRedactionS3ObjectLambda`. Essa função usa o Amazon Comprehend para detectar entidades de PII. Em seguida, ele edita essas entidades substituindo-as por asteriscos. Ao editar as PII, você oculta dados sigilosos, o que pode ajudar com segurança e conformidade.

Você também aprende a usar e configurar uma função AWS Lambda pré-criada no AWS Serverless Application Repository para trabalhar em conjunto com o S3 Object Lambda para facilitar a implantação.

Tópicos

- Pré-requisitos: criar um usuário do IAM com permissões
- Etapa 1: criar um bucket do S3
- Etapa 2: fazer upload do arquivo para seu bucket do S3
- Etapa 3: criar um ponto de acesso do S3
- Etapa 4: configurar e implantar uma função Lambda pré-construída
- Etapa 5: criar um ponto de acesso do S3 Object Lambda
- Etapa 6: usar o ponto de acesso do S3 Object Lambda para recuperar o arquivo editado
- Etapa 7: limpar
- Próximas etapas

Pré-requisitos: criar um usuário do IAM com permissões

Antes de iniciar este tutorial, você deve ter uma conta da AWS na qual possa fazer login como um usuário do AWS Identity and Access Management (usuário do IAM) com permissões corretas.

Você pode criar um usuário do IAM para o tutorial. Para concluir este tutorial, o usuário do IAM deve anexar as seguintes políticas do IAM para acessar recursos da AWS e executar ações específicas.

> **Note**
>
> Para simplificar, este tutorial cria e usa um usuário do IAM. Depois de concluir este tutorial, lembre-se de Excluir o usuário do IAM. Para uso em produção, recomendamos que você siga as Práticas recomendadas de segurança no IAM no Guia do usuário do IAM. Uma das práticas recomendadas exige que os usuários humanos usem a federação com um provedor de identidades para acessar a AWS usando credenciais temporárias. Outra prática recomendada é exigir que as workloads usem credenciais temporárias com perfis do IAM para acessar a AWS. Para saber como usar o AWS IAM Identity Center para criar usuários com credenciais temporárias, consulte Getting started (Conceitos básicos) no Guia do usuário do AWS IAM Identity Center.

> Este tutorial usa políticas de acesso total. Para uso em produção, recomendamos que você conceda apenas as permissões mínimas necessárias para seu caso de uso, de acordo com as práticas recomendadas de segurança.

Seu usuário do IAM requer as seguintes políticas gerenciadas pela AWS:

- AmazonS3FullAccess: concede permissões a todas as ações do Amazon S3, incluindo permissões para criar e usar um ponto de acesso do Object Lambda.
- AWSLambda_FullAccess: concede permissões a todas as ações do Lambda.
- AWSCloudFormationFullAccess: concede permissões a todas as ações do AWS CloudFormation.
- IAMFullAccess: concede permissões a todas as ações do IAM.
- IAMAccessAnalyzerReadOnlyAccess: concede permissões para ler todas as informações de acesso fornecidas pelo IAM Access Analyzer.

Você pode anexar diretamente essas políticas existentes ao criar um usuário do IAM. Para obter mais informações sobre como criar um usuário do IAM, consulte Criar usuários do IAM (console) no Guia do usuário do IAM.

Além disso, seu usuário do IAM requer uma política gerenciada pelo cliente. Para conceder permissões de usuário do IAM a todos os recursos e ações do AWS Serverless Application Repository, você deve criar uma política do IAM e anexá-la ao usuário do IAM.

Para criar e anexar uma política do IAM para um usuário do IAM

1. Faça login no AWS Management Console e abra o console do IAM, em https://console.aws.amazon.com/iam/.
2. No painel de navegação à esquerda, escolha Políticas.
3. Escolha Create policy (Criar política).
4. Na guia Visual editor (Editor visual) de Service (Serviço), selecione Choose a service (Escolher um serviço). Em seguida, escolha Serverless Application Repository (Repositório de aplicações sem servidor).
5. Para Actions (Ações), em Manual actions (Ações manuais), selecione All Serverless Application Repository actions (serverlessrepo:*) (Todas as ações do Serverless Application Repository (serverlessrepo: *)) para este tutorial.

Como uma prática recomendada de segurança, você deve conceder permissões somente para as ações e os recursos dos quais um usuário precisa, com base no seu caso de uso. Para obter mais informações, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.

6. Para Resources (Recursos), escolha All resources (Todos os recursos) para este tutorial.

   Como prática recomendada, você deve definir permissões somente para recursos específicos em contas específicas. Como alternativa, você pode conceder menos privilégios usando chaves de condição. Para obter mais informações, consulte Grant least privilege (Conceder privilégio mínimo) no Guia do usuário do IAM.

7. Escolha Próximo: etiquetas.
8. Selecione Next: Review (Próximo: revisar).
9. Na página Review policy (Revisar política), insira um Name (Nome) (por exemplo, **`tutorial-serverless-application-repository`**) e uma Description (Descrição) (opcional) para a política que você está criando. Revise o resumo da política para assegurar-se de ter concedido as permissões que pretendia e, em seguida, escolha Create policy (Criar política) para salvar sua nova política.
10. No painel de navegação à esquerda, escolha Usuários. Em seguida, escolha o usuário do IAM para este tutorial.
11. Na página Summary (Resumo) do usuário escolhido, escolha a guia Permissions (Permissões) e escolha Add permissions (Adicionar permissões).
12. Em Grant permissions (Conceder permissões), escolha Attach existing policies directly (Anexar políticas existentes diretamente).
13. Marque a caixa de seleção ao lado da política que você acabou de criar (por exemplo, **`tutorial-serverless-application-repository`**) e, depois, escolha Next: Review (Próximo: Revisar).
14. Em Permissions summary (Resumo de permissões), revise o resumo para se certificar de que anexou a política que pretendia. Em seguida, selecione Add permissions (Adicionar permissões).

Etapa 1: criar um bucket do S3

Crie um bucket para armazenar os dados originais que você planeja transformar.

> **Note**
>
> Os pontos de acesso podem ser conectados a outra fonte de dados, como um volume do Amazon FSx para OpenZFS, mas este tutorial usa um ponto de acesso de suporte conectado a um bucket do S3.

Para criar um bucket

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets.
3. Selecione Create bucket (Criar bucket).

   A página Create bucket (Criar bucket) é aberta.
4. Para Bucket name (Nome do bucket), insira um nome para o seu bucket (por exemplo, **`tutorial-bucket`**).

   Para obter mais informações sobre como nomear buckets no Amazon S3, consulte Regras de nomenclatura de buckets de uso geral.
5. Em Region (Região), escolha a Região da AWS onde deseja que o bucket resida.

   Para obter mais informações sobre a região do bucket, consulte Visão geral dos buckets de uso geral.
6. Para Block Public Access settings for this bucket (Configurações de acesso de bloqueio público para este bucket), mantenha as configurações padrão (Block allpublic access (Bloquear todo acesso público) está habilitado).

   Recomendamos que você mantenha todas as configurações de acesso de bloqueio público ativadas, a menos que precise desativar uma ou mais delas para seu caso de uso. Para obter mais informações sobre como bloquear o acesso público, consulte Bloquear o acesso público ao armazenamento do Amazon S3.
7. Mantenha as configurações restantes definidas conforme os padrões.

   (Opcional) Se quiser definir configurações de bucket adicionais para o caso de uso específico, consulte Criar um bucket de uso geral.
8. Escolha Criar bucket.

Etapa 2: fazer upload do arquivo para seu bucket do S3

Carregue um arquivo de texto contendo dados de PII conhecidos de vários tipos, como nomes, informações bancárias, números de telefone e SSNs, para o bucket do S3 como os dados originais dos quais você editará as PII posteriormente neste tutorial.

Por exemplo, você pode carregar seguindo o arquivo `tutorial.txt`. Este é um exemplo de arquivo de entrada do Amazon Comprehend.

```
Hello Zhang Wei, I am John. Your AnyCompany Financial Services,
LLC credit card account 1111-0000-1111-0008 has a minimum payment
of $24.53 that is due by July 31st. Based on your autopay settings,
we will withdraw your payment on the due date from your
bank account number XXXXXX1111 with the routing number XXXXX0000.

Your latest statement was mailed to 100 Main Street, Any City,
WA 98121.
After your payment is received, you will receive a confirmation
text message at 206-555-0100.
If you have questions about your bill, AnyCompany Customer Service
is available by phone at 206-555-0199 or
email at support@anycompany.com.
```

Fazer upload de um arquivo para um bucket

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets.
3. Na lista de Buckets, escolha o nome do bucket que você criou na Etapa 1 (por exemplo, **`tutorial-bucket`**) para carregar seu arquivo.
4. Na guia Objects (Objetos) do bucket, escolha Upload (Fazer upload).
5. Na página Upload (Carregar), em Files and folders (Arquivos e pastas), escolha Add files (Adicionar arquivos).
6. Escolha um arquivo para carregar e, em seguida, escolha Open (Abrir). Por exemplo, você pode carregar o exemplo de arquivo `tutorial.txt`mencionado anteriormente.
7. Escolha Upload (Carregar).

Etapa 3: criar um ponto de acesso do S3

Para usar um ponto de acesso do S3 Object Lambda para acessar e transformar os dados originais, você deve criar um ponto de acesso do S3 e associá-lo ao bucket do S3 criado na Etapa 1. O ponto de acesso deve estar na mesma Região da AWS que os objetos que você deseja transformar.

Mais adiante neste tutorial, você usará esse ponto de acesso como um ponto de acesso de suporte para o ponto de acesso do Object Lambda.

Para criar um ponto de acesso

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação, escolha Access Points (Pontos de acesso).
3. Na página Access Points (Pontos de acesso), escolha Create access point (Criar ponto de acesso).
4. No campo Access point name (Nome do ponto de acesso), insira o nome (por exemplo, **`tutorial-pii-access-point`**) para o ponto de acesso.

   Para obter mais informações sobre nomenclatura de pontos de acesso, consulte Regras de nomenclatura para pontos de acesso.
5. No campo Fonte de dados insira o nome do bucket criado na Etapa 1 (por exemplo, **`tutorial-bucket`**). O S3 anexa o ponto de acesso a este bucket.

   (Opcional) Você pode escolher Browse S3 (Procurar S3) para navegar e pesquisar buckets na sua conta. Se você escolher Browse S3 (Procurar S3), selecione o bucket desejado e escolha Choose path (Escolher caminho) para preencher o campo Bucket name (Nome do bucket) com o nome do bucket.
6. Para Network origin (Origem de rede), escolha Internet.

   Para obter mais informações sobre origens de rede para pontos de acesso, consulte Criar pontos de acesso restritos a uma nuvem privada virtual.
7. Por padrão, todas as configurações de bloqueio de acesso público são habilitadas para seu ponto de acesso. Recomendamos manter a opção Block all public access (Bloquear todo o acesso público) ativada. Para obter mais informações, consulte Gerenciar o acesso público a pontos de acesso para buckets de uso geral.
8. Para todas as outras configurações de ponto de acesso, mantenha as configurações padrão.

(Opcional) Você pode modificar as configurações do ponto de acesso para dar suporte ao caso de uso. Para este tutorial, recomendamos manter as configurações padrão.

(Opcional) Se você precisar gerenciar o acesso ao seu ponto de acesso, você pode especificar uma política de ponto de acesso. Para obter mais informações, consulte Exemplos de política para pontos de acesso.

9. Selecione Create access point (Criar ponto de acesso).

Etapa 4: configurar e implantar uma função Lambda pré-construída

Para editar dados de PII, configure e implante a função `ComprehendPiiRedactionS3ObjectLambda` do AWS Lambda pré-criada para uso com o ponto de acesso do S3 Object Lambda.

Para configurar e implantar a função Lambda

1. Faça login no AWS Management Console e visualize a função `ComprehendPiiRedactionS3ObjectLambda` no AWS Serverless Application Repository.
2. Para Application settings (Configurações da aplicação), em Application name (Nome da aplicação), mantenha o valor padrão (`ComprehendPiiRedactionS3ObjectLambda`) para este tutorial.

   (Opcional) Você pode inserir o nome que deseja dar a esta aplicação. Talvez você queira fazer isso se pretende configurar várias funções Lambda para diferentes necessidades de acesso para o mesmo conjunto de dados compartilhado.
3. Para MaskCharacter, mantenha o valor padrão (*****). O caractere de máscara substitui cada caractere na entidade PII editada.
4. Para MaskMode, mantenha o valor padrão (MASK). O valor MaskMode especifica se a entidade de PII é editada com o caractere `MASK` ou com o valor `PII_ENTITY_TYPE`.
5. Para editar os tipos de dados especificados, paraPiiEntityTypes, mantenha o valor padrão ALL. O valor PiiEntityTypes especifica os tipos de entidade de PII a serem considerados para edição.

   Para obter mais informações sobre a lista de tipos de entidade PII compatíveis, consulte Detectar informações de identificação pessoal (PII) no Guia do desenvolvedor do Amazon Comprehend.
6. Mantenha as configurações restantes definidas conforme os padrões.

(Opcional) Se quiser definir configurações adicionais para o caso de uso específico, consulte a seção Readme file (Arquivo Leiame) no lado esquerdo da página.

7. Marque a caixa de seleção próxima a I acknowledge that this app creates custom IAM roles (Reconheço que esta aplicação cria funções personalizadas do IAM).
8. Escolha Implantar.
9. Na página da nova aplicação, em Resources (Recursos), escolha o Logical ID (ID lógico) da função Lambda que você implantou para revisar a função na página da função Lambda.

Etapa 5: criar um ponto de acesso do S3 Object Lambda

Um ponto de acesso do S3 Object Lambda fornece a flexibilidade de invocar uma função do Lambda diretamente de uma solicitação do S3 GET para que a função possa editar dados PII recuperados de um ponto de acesso do S3. Ao criar e configurar um ponto de acesso do S3 Object Lambda, você deve especificar a função do Lambda de redação para invocar e fornecer o contexto de evento no formato JSON como parâmetros personalizados para o Lambda usar.

O contexto do evento fornece informações sobre a solicitação que está sendo feita no evento passado do S3 Object Lambda para o Lambda. Para obter mais informações sobre todos os campos no contexto do evento, consulte Formato e uso de contexto de evento.

Para criar um ponto de acesso do S3 Object Lambda

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Object Lambda access points (Pontos de acesso do Object Lambda).
3. Na página Object Lambda Access Points (Pontos de acesso do Object Lambda), escolha Create Object Lambda Access Point (Criar ponto de acesso do Object Lambda).
4. Para Nome do Ponto de acesso Lambda do objeto, informe o nome que você deseja usar para o ponto de acesso Lambda do objeto (por exemplo, **`tutorial-pii-object-lambda-accesspoint`**).
5. Para Supporting Access Point (Ponto de acesso de suporte), informe ou procure o ponto de acesso padrão criado na Etapa 3 (por exemplo, **`tutorial-pii-access-point`**) e, em seguida, escolha Choose supporting Access Point (Escolher ponto de acesso de suporte).

6. Para recuperar objetos do bucket do S3 para que a função do Lambda processe, selecione GetObject em S3 APIs (APIs do S3).
7. Para Invoke Lambda function (Chamar função Lambda), você pode escolher qualquer uma das duas opções a seguir para este tutorial.
   - Escolha Choose from functions in your account (Escolher das funções de sua conta) e escolha a função Lambda que você implantou na Etapa 4 (por exemplo, **`serverlessrepo-ComprehendPiiRedactionS3ObjectLambda`**) da lista suspensa Lambda function (Função Lambda).
   - Escolha Enter ARN (Inserir ARN) e depois informe o Nome do recurso da Amazon (ARN) da função Lambda que você criou na Etapa 4.
8. Para Lambda function version (Versão da função Lambda), escolha $LATEST (a versão mais recente da função Lambda que você implantou na Etapa 4).
9. (Opcional) Se precisar da função Lambda para reconhecer e processar solicitações GET com cabeçalhos de intervalo e número de peça, selecione Lambda function supports requests using range (A função Lambda suporta solicitações usando intervalo) e Lambda function supports requests using part numbers (A função Lambda suporta solicitações usando números de parte). Caso contrário, desmarque essas duas caixas de seleção.

   Para obter mais informações sobre como usar números de intervalo ou de parte com o S3 Object Lambda, consulte Trabalhar com cabeçalhos Range e partNumber.
10. (Opcional) Em Payload - optional (Carga útil - opcional), adicione um texto JSON para fornecer informações adicionais à sua função Lambda.

    Uma carga útil é um texto JSON opcional que você pode fornecer à sua função do Lambda como entrada para todas as chamadas provenientes de um ponto de acesso do S3 Object Lambda específico. Para personalizar os comportamentos de vários pontos de acesso Lambda do objeto que chamam a mesma função do Lambda, você pode configurar cargas úteis com diferentes parâmetros, estendendo, assim, a flexibilidade da função do Lambda.

    Para obter mais informações sobre carga útil, consulte Formato e uso de contexto de evento.
11. (Opcional) Para Métricas de solicitação – opcional, escolha Desativar ou Ativar para adicionar o monitoramento do Amazon S3 ao ponto de acesso Lambda do objeto. As métricas de solicitação são cobradas na taxa padrão do Amazon CloudWatch. Para obter mais informações, consulte Preço do CloudWatch.
12. Em Object Lambda Access Point policy - optional (Política do ponto de acesso do Object Lambda - opcional), mantenha a configuração padrão.

(Opcional) Você pode definir uma política de recursos. Essa política de recursos concede permissão da API `GetObject` para usar o ponto de acesso do Object Lambda especificado.

13. Mantenha as configurações restantes definidas conforme os padrões e escolha Create Object Lambda Access Point (Criar ponto de acesso do Object Lambda).

Etapa 6: usar o ponto de acesso do S3 Object Lambda para recuperar o arquivo editado

Agora, o S3 Object Lambda está pronto para editar dados de PII do seu arquivo original.

Para usar o ponto de acesso do S3 Object Lambda para recuperar o arquivo editado

Quando você solicita para recuperar um arquivo por meio do ponto de acesso do S3 Object Lambda, você faz uma chamada de API `GetObject` para o S3 Object Lambda. O S3 Object Lambda chama a função Lambda para editar seus dados de PII e retorna os dados transformados como a resposta à chamada de API `GetObject` do S3 padrão.

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Object Lambda access points (Pontos de acesso do Object Lambda).
3. Na página Pontos de acesso do Object Lambda, escolha o ponto de acesso do S3 Object Lambda que você criou na Etapa 5 (por exemplo, **`tutorial-pii-object-lambda-accesspoint`**).
4. Na guia Objetos do ponto de acesso do S3 Object Lambda, selecione o arquivo que tem o mesmo nome (por exemplo, `tutorial.txt`) daquele que você carregou no bucket do S3 na Etapa 2.

   Esse arquivo deve conter todos os dados transformados.
5. Para exibir os dados transformados, escolha Open (Abrir) ou Download (Baixar).

   Você deve ser capaz de ver o arquivo editado, conforme mostrado no exemplo a seguir.

```
Hello *********. Your AnyCompany Financial Services,
LLC credit card account ******************** has a minimum payment
of $24.53 that is due by *********. Based on your autopay settings,
we will withdraw your payment on the due date from your
bank account ********** with the routing number *********.
```

```
Your latest statement was mailed to **********.
After your payment is received, you will receive a confirmation
text message at ***********.
If you have questions about your bill, AnyCompany Customer Service
is available by phone at *********** or
email at **********.
```

Etapa 7: limpar

Se você editou seus dados por meio do S3 Object Lambda apenas como um exercício de aprendizado, exclua os recursos da AWS que você alocou para que não haja mais encargos.

Subetapas

- Excluir o ponto de acesso do Object Lambda
- Exclua o ponto de acesso do S3
- Excluir a função Lambda
- Excluir o grupo de logs do CloudWatch
- Exclua o arquivo original no bucket de origem do S3
- Exclua o bucket de origem do S3
- Exclua a função do IAM para a função Lambda
- Exclua a política gerenciada pelo cliente para o usuário do IAM
- Excluir o usuário do IAM

Excluir o ponto de acesso do Object Lambda

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Object Lambda access points (Pontos de acesso do Object Lambda).
3. Na página Pontos de acesso do Object Lambda, escolha o botão de opção à esquerda do ponto de acesso do S3 Object Lambda que você criou na Etapa 5 (por exemplo, **`tutorial-pii-object-lambda-accesspoint`**).
4. Escolha Excluir.

5. Confirme se deseja excluir o ponto de acesso do Lambda, inserindo o nome no campo de texto exibido e escolha Excluir.

Exclua o ponto de acesso do S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação, escolha Access Points (Pontos de acesso).
3. Navegue até o ponto de acesso que você criou na Etapa 3 (por exemplo, **`tutorial-pii-access-point`**) e escolha o botão de opção ao lado do nome do ponto de acesso.
4. Escolha Excluir.
5. Confirme se deseja excluir o ponto de acesso inserindo o nome no campo de texto exibido e escolha Delete (Excluir).

Excluir a função Lambda

1. No console do AWS Lambda em https://console.aws.amazon.com/lambda/, escolha Functions (Funções) no painel de navegação à esquerda.
2. Escolha a função que você criou na Etapa 4 (por exemplo, **`serverlessrepo-ComprehendPiiRedactionS3ObjectLambda`**).
3. Escolha Ações e, em seguida, escolha Excluir.
4. Na caixa de diálogo Delete function (Excluir função), escolha Delete (Excluir).

Excluir o grupo de logs do CloudWatch

1. Abra o console do CloudWatch em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação esquerdo, escolha Log groups (Grupos de log).
3. Localize o grupo de logs cujo nome termina com a função Lambda que você criou na Etapa 4 (por exemplo, **`serverlessrepo-ComprehendPiiRedactionS3ObjectLambda`**).
4. Escolha Actions (Ações) e Delete log group(s) (Excluir grupo(s) de log).
5. Na caixa de diálogo Delete log group(s) (Excluir grupo(s) de logs), escolha Delete (Excluir).

Exclua o arquivo original no bucket de origem do S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets.
3. Na lista Bucket name (Nome do bucket), escolha o nome do bucket para o qual você carregou o arquivo original na Etapa 2 (por exemplo, **`tutorial-bucket`**).
4. Marque a caixa de seleção à esquerda do nome do objeto que você deseja excluir (por exemplo, `tutorial.txt`).
5. Escolha Excluir.
6. Na página Delete objects (Excluir objetos) na seção Permanently delete objects? (Excluir objetos permanentemente?), confirme se deseja excluir este objeto informando **`permanently delete`** na caixa de texto.
7. Escolha Delete objects (Excluir objetos).

Exclua o bucket de origem do S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets.
3. Na lista de Buckets, escolha o botão de opção ao lado do nome do bucket que você criou na Etapa 1 (por exemplo, **`tutorial-bucket`**).
4. Escolha Excluir.
5. Na página Delete bucket (Excluir bucket), confirme se deseja excluir o bucket inserindo o nome do bucket no campo de texto e escolha Delete bucket (Excluir bucket).

Exclua a função do IAM para a função Lambda

1. Faça login no AWS Management Console e abra o console do IAM, em https://console.aws.amazon.com/iam/.
2. No painel de navegação esquerdo, escolha Roles (Funções) e marque a caixa de seleção ao lado do nome da função que você deseja excluir. O nome da função começa com o nome da função Lambda que você implantou na Etapa 4 (por exemplo, **`serverlessrepo-ComprehendPiiRedactionS3ObjectLambda`**).

3. Escolha Excluir.
4. Na caixa de diálogo Delete (Excluir), informe o nome da função no campo de entrada de texto para confirmar a exclusão. Em seguida, selecione Excluir.

Exclua a política gerenciada pelo cliente para o usuário do IAM

1. Faça login no AWS Management Console e abra o console do IAM, em https://console.aws.amazon.com/iam/.
2. No painel de navegação à esquerda, escolha Políticas.
3. Na página Policies (Políticas), insira o nome da política gerenciada pelo cliente que você criou em Prerequisites (Pré-requisitos) (por exemplo, **`tutorial-serverless-application-repository`**) na caixa de pesquisa para filtrar a lista de políticas. Selecione o botão de opção ao lado do nome da política que você deseja excluir.
4. Escolha Ações e, em seguida, escolha Excluir.
5. Confirme se deseja excluir esta política, inserindo seu nome no campo de texto exibido e escolha Delete (Excluir).

Excluir o usuário do IAM

1. Faça login no AWS Management Console e abra o console do IAM, em https://console.aws.amazon.com/iam/.
2. No painel de navegação esquerdo, escolha Users (Usuários) e marque a caixa de seleção ao lado do nome do usuário que você deseja excluir.
3. Na parte superior da página, escolha Delete (Excluir).
4. Na caixa de diálogo Delete ***`user name`***? (Excluir nome de usuário?), insira o nome de usuário no campo de entrada de texto para confirmar a exclusão do usuário. Escolha Excluir.

Próximas etapas

Depois de concluir este tutorial, você pode explorar ainda mais os seguintes casos de uso relacionados:

- Você pode criar vários pontos de acesso do S3 Object Lambda e habilitá-los com funções do Lambda pré-criadas que são configuradas de forma diferente para editar tipos específicos de PII, dependendo das necessidades de negócios dos assessores de dados.

Cada tipo de usuário assume um perfil do IAM e só tem acesso a um ponto de acesso do S3 Object Lambda (gerenciado por meio de políticas do IAM). Depois, anexe cada função do Lambda `ComprehendPiiRedactionS3ObjectLambda` configurada para um caso de uso de edição diferente para um ponto de acesso do S3 Object Lambda diferente. Para cada ponto de acesso do S3 Object Lambda, você pode ter um ponto de acesso do S3 de suporte para ler dados de um bucket do S3 que armazena o conjunto de dados compartilhado.

Para obter mais informações sobre como criar uma política de bucket do S3 que conceda aos usuários a leitura do bucket somente por meio dos pontos de acesso do S3, consulte Configurar políticas do IAM para uso de pontos de acesso.

Para obter mais informações sobre como conceder permissão de usuário para acessar a função do Lambda, o ponto de acesso S3 e o ponto de acesso do S3 Object Lambda, consulte Configurar políticas do IAM para pontos de acesso do Object Lambda.

- Você pode criar sua própria função Lambda e usar o S3 Object Lambda com sua função Lambda personalizada para atender às suas necessidades de dados específicas.

  Por exemplo, para explorar vários valores de dados, você pode usar o S3 Object Lambda e sua própria função Lambda que usa Recursos do Amazon Comprehend, como reconhecimento de entidade, reconhecimento de frase-chave, análise de sentimento e classificação de documentos, para processar dados. Você também pode usar o S3 Object Lambda junto com oAmazon Comprehend Medical, um serviço de PNL qualificado para HIPAA, para analisar e extrair dados com reconhecimento de contexto.

  Para obter mais informações sobre como transformar dados com o S3 Object Lambda e sua própria função Lambda, consulte Tutorial: Como transformar dados para sua aplicação com o S3 Object Lambda.

Depurar e solucionar problemas do S3 Object Lambda

As solicitações para pontos de acesso do Amazon S3 Object Lambda podem resultar em novas respostas de erro quando algo der errado com a invocação ou execução da função do Lambda. Esses erros seguem o mesmo formato que os erros padrão do Amazon S3. Para obter informações sobre erros do S3 Object Lambda, consulte Lista de códigos de erro do S3 Object Lambda na Referência da API do Amazon Simple Storage Service.

Para obter mais informações sobre a depuração geral da função do Lambda, consulte Monitoramento e solução de problemas de aplicações do Lambda no Guia do desenvolvedor do AWS Lambda.

Para obter informações sobre erros padrão do Amazon S3, consulte Respostas de erro na Referência da API do Amazon Simple Storage Service.

Você pode habilitar métricas de solicitação no Amazon CloudWatch para os pontos de acesso do Object Lambda. Essas métricas ajudam você a monitorar a performance operacional do seu ponto de acesso. Você pode habilitar métricas de solicitação durante ou após a criação de um ponto de acesso do Object Lambda. Para obter mais informações, consulte Métricas de solicitação do S3 Object Lambda no CloudWatch.

Para obter registros em log mais granulares sobre solicitações feitas aos seus pontos de acesso do Object Lambda, é possível ativar eventos de dados do AWS CloudTrail. Para obter mais informações, consulte Registro eventos de dados em logs para trilhas no Guia do usuário do AWS CloudTrail.

Para tutoriais do S3 Object Lambda, consulte o seguinte:

- Tutorial: Como transformar dados para sua aplicação com o S3 Object Lambda
- Tutorial: Detectar e editar dados PII com o S3 Object Lambda e o Amazon Comprehend
- Tutorial: Using S3 Object Lambda to dynamically watermark images as they are retrieved (Tutorial: Como usar o S3 Object Lambda para colocar marca d'água em imagens de maneira dinâmica à medida que são recuperadas)

Para obter mais informações sobre pontos de acesso padrão, consulte Gerenciar o acesso a conjuntos de dados compartilhados com pontos de acesso.

Para obter informações sobre como trabalhar com buckets, consulte Visão geral dos buckets de uso geral. Para obter mais informações sobre como trabalhar com objetos, consulte Visão geral de objetos Amazon S3.

Executar operações de objetos em massa com o Operações em Lote

Você pode usar operações em lote do S3 para executar operações em lote de grande escala em objetos do Amazon S3. As operações em lote do S3 podem executar uma única operação em

listas de objetos do Amazon S3 especificadas. Um único trabalho pode realizar uma operação especificada em bilhões de objetos contendo exabytes de dados. O Amazon S3 monitora o progresso, envia notificações e armazena um relatório de conclusão detalhado de todas as ações, fornecendo uma experiência totalmente gerenciada, auditável e sem servidor. É possível usar o recurso Operações em Lote do S3 por meio do console do Amazon S3, da AWS CLI, de SDKs da AWS ou da API REST do Amazon S3.

Use as operações em lote do S3 para copiar objetos e definir tags de objetos ou listas de controle de acesso (ACLs). Também é possível iniciar restaurações de objetos no S3 Glacier Flexible Retrieval ou invocar uma função do AWS Lambda para executar ações personalizadas usando seus objetos. É possível executar essas operações em uma lista personalizada de objetos ou usar um relatório do Amazon S3 Inventory para facilitar a geração de listas de objetos. O recurso Operações em Lote do Amazon S3 usa as mesmas operações da API do Amazon S3 que você já utiliza com o Amazon S3.

> **Note**
>
> Para obter mais informações sobre o uso da classe de armazenamento Amazon S3 Express One Zone com buckets de diretório, consulte S3 Express One Zone e Trabalhar com buckets de diretório. Para obter mais informações sobre o uso da funcionalidade Operações em Lote com a classe S3 Express One Zone e buckets de diretório, consulte Usar a funcionalidade Operações em Lote com buckets de diretório.

Conceitos básicos sobre operações em lote do S3

Você pode usar operações em lote do S3 para executar operações em lote de grande escala em objetos do Amazon S3. As operações em lote do S3 podem executar uma única operação ou ação em listas de objetos do Amazon S3 que você especificar.

Terminologia

Esta seção usa os termos manifestos, trabalhos, operações e tarefas. Confira suas definições abaixo:

Manifesto

Um manifesto é um objeto do Amazon S3 que contém as chaves de objeto em que você deseja que o Amazon S3 atue. Se quiser criar um trabalho de operações em lote, você deverá fornecer um manifesto. O manifesto gerado pelo usuário deve conter o nome do bucket, a chave de objeto

e, opcionalmente, a versão de cada objeto. Se você fornecer um manifesto gerado pelo usuário, ele deverá estar na forma de um relatório da funcionalidade Inventário Amazon S3 ou um arquivo CSV.

Você pode instruir o Amazon S3 a gerar um manifesto automaticamente com base nos critérios de filtro de objetos especificados ao criar um trabalho. Essa opção está disponível para trabalhos de Replicação em Lote do S3 criados no console do Amazon S3 ou para qualquer tipo de trabalho criado usando a AWS Command Line Interface (AWS CLI), SDKs da AWS ou a API REST do Amazon S3.

Trabalho

Um trabalho é a unidade básica de trabalho para operações em lote do S3. Uma tarefa contém todas as informações necessárias para executar a operação especificada nos objetos listados no manifesto. Depois que você tiver fornecido essas informações e solicitado o início do trabalho, ele executará a operação para cada objeto no manifesto.

Operação

A operação é o tipo de ação da API, como copiar objetos, que você deseja que o trabalho de operações em lote execute. Cada trabalho executa um único tipo de operação em todos os objetos especificados no manifesto.

Tarefa

Uma tarefa é a unidade de execução para um trabalho. Uma tarefa representa uma única chamada para uma operação de API do AWS Lambda ou do Amazon S3 a fim de executar a operação do trabalho em um único objeto. Ao longo da vida útil de um trabalho, as operações em lote do S3 criam uma tarefa para cada objeto especificado no manifesto.

Como funciona um trabalho de operações em lote do S3

Um trabalho é a unidade básica de trabalho para operações em lote do S3. Uma tarefa contém todas as informações necessárias para executar a operação especificada em uma lista de objetos. Para criar um trabalho, dê uma lista de objetos às operações em lote do S3 e especifique a ação a ser realizada neles.

Para obter informações sobre as operações compatíveis com o S3 Batch Operations, consulte Operações suportadas pelo S3 Batch Operations.

Um trabalho em lote realiza a operação especificada em cada objeto incluído em seu manifesto. Um manifesto lista os objetos que você deseja que um trabalho em lote processe e ele é armazenado

como um objeto em um bucket. Você pode usar um relatório de Catalogar e analisar seus dados com o Inventário S3 formatado em CSV como um manifesto, o que facilita a criação de grandes listas de objetos localizados em um bucket. Também é possível especificar um manifesto em um formato CSV simples que permite realizar operações em lotem em uma lista personalizada de objetos contidos em um único bucket.

Depois de criar um trabalho, o Amazon S3 processará a lista de objetos no manifesto e executará a operação especificada em cada objeto. Enquanto um trabalho está em execução, é possível monitorar o andamento de maneira programática ou por meio do console do Amazon S3. Também é possível configurar uma tarefa para gerar um relatório de conclusão quando ele termina. O relatório de conclusão descreve os resultados de cada tarefa executada pelo trabalho. Para obter mais informações sobre como monitorar trabalhos, consulte Gerenciar trabalhos de operações em lote do S3.

Há custos associados ao recurso Operações em Lote do S3. Você recebe cobrança pela criação de trabalhos no recurso Operações em Lote, inclusive trabalhos que são cancelados antes da conclusão. Para obter mais informações, consulte Preço do Amazon S3.

Por padrão, os trabalhos do recurso Operações em Lote do S3 podem processar até 4 bilhões de objetos para todas as operações. Especificamente os trabalhos de cópia, marcação de objetos, bloqueio de objetos, invocação de uma função do AWS Lambda e replicação em lote podem comportar até 20 bilhões de objetos. Há um limite de seis trabalhos ativos de replicação em lote por conta da AWS. Para começar a criar um trabalho de operações em lote, consulte Criar um trabalho de operações em lote do S3.

Tutorial Operações em lote do S3

Os tutoriais a seguir apresentam procedimentos completos para algumas tarefas de operações em lote.

- Tutorial: vídeos de transcodificação em lote com o Operações em Lote do S3

Conceder permissões para operações em lote

Antes de criar e executar trabalhos do S3 Batch Operations, você deve conceder as permissões necessárias. Para criar um trabalho do Amazon S3 Batch Operations, a permissão de usuário `s3:CreateJob` é necessária. A mesma entidade que cria o trabalho também deve ter a permissão `iam:PassRole` para passar o perfil do AWS Identity and Access Management (IAM) especificado para o trabalho ao Operações em Lote.

Para obter informações gerais sobre como especificar recursos do IAM, consulte Elementos de política JSON do IAM: Resource no Guia do usuário do IAM. As seções a seguir fornecem informações sobre como criar uma função do IAM e anexar políticas.

Tópicos

- Criar uma função do IAM das operações em lote do S3
- Anexar políticas de permissões

Criar uma função do IAM das operações em lote do S3

O Amazon S3 deve ter permissão para executar o S3 Batch Operations em seu nome. Conceda essas permissões por meio de uma função do AWS Identity and Access Management (IAM). Esta seção fornece exemplos das políticas de permissões e confiança usadas ao criar uma função do IAM. Para obter mais informações, consulte Funções do IAM no Guia do usuário do IAM. Veja exemplos em Controlar permissões para o Operações em Lote usando tags de trabalho e Copiar objetos usando o S3 Batch Operations.

Em suas políticas do IAM, você também pode usar chaves de condição para filtrar permissões de acesso para trabalhos de operações em lote do S3. Consulte mais informações e uma lista completa das chaves de condição específicas do Amazon S3 em Actions, resources, and condition keys for Amazon S3 na Referência de autorização do serviço.

Para ter mais informações sobre as permissões referentes a operações de API do S3 de acordo com os tipos de recurso do S3, consulte Permissões obrigatórias para operações de API do Amazon S3.

Política de confiança

Para permitir que o principal do serviço de operações em lote do S3 assuma a função do IAM, anexe a política de confiança a seguir à função.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service":"batchoperations.s3.amazonaws.com"
         },
         "Action":"sts:AssumeRole"
      }
```

```
    ]
}
```

Anexar políticas de permissões

Dependendo do tipo de operação, é possível anexar uma das seguintes políticas:

Antes de configurar as permissões, observe o seguinte:

- Independentemente da operação, o Amazon S3 precisa de permissão para ler o objeto do manifesto no seu bucket do S3 e, opcionalmente, gerar um relatório para o bucket. Portanto, todas as políticas a seguir incluem essas permissões.
- Para manifestos de relatório do Amazon S3 Inventory, as operações em lote do S3 necessitam de permissão de leitura para o objeto manifest.json e todos os arquivos de dados CSV associados.
- Permissões específicas da versão, como `s3:GetObjectVersion`, somente são necessárias ao especificar o ID de versão dos objetos.
- Se você estiver executando o S3 Batch Operations em objetos criptografados, a função do IAM também deverá ter acesso às chaves do AWS KMS usadas para criptografá-las.
- Se você enviar um manifesto de relatório de inventário criptografado com o AWS KMS, a política do IAM deverá incluir as permissões `"kms:Decrypt"` e `"kms:GenerateDataKey"` para o objeto manifest.json e todos os arquivos de dados CSV associados.
- Se o trabalho de operações em lote gerar um manifesto em um bucket com listas de controle de acesso (ACLs) habilitadas e estiver em outra Conta da AWS, você deverá conceder a permissão `s3:PutObjectAcl` na política do IAM do perfil do IAM configurado para o trabalho em lote. Se você não incluir essa permissão, o trabalho em lote falhará com o erro `Error occurred when preparing manifest: Failed to write manifest`.

Copiar objetos: PutObject

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:PutObject",
                "s3:PutObjectAcl",
                "s3:PutObjectTagging"
            ],
```

```
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:GetObjectAcl",
                "s3:GetObjectTagging",
                "s3:ListBucket"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-source-bucket",
                "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*"
            ]
        }
    ]
}
```

Substituir a marcação de objetos: PutObjectTagging

```
{
  "Version":"2012-10-17",
  "Statement":[
```

```
    {
      "Effect":"Allow",
      "Action":[
        "s3:PutObjectTagging",
        "s3:PutObjectVersionTagging"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
      ]
    },
    {
      "Effect":"Allow",
      "Action":[
        "s3:PutObject"
      ],
      "Resource":[
        "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*"
      ]
    }
  ]
}
```

Excluir a marcação de objetos: DeleteObjectTagging

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
              "s3:DeleteObjectTagging",
              "s3:DeleteObjectVersionTagging"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
```

```
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*"
            ]
        }
    ]
}
```

Substituir a lista de controle de acesso: PutObjectAcl

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "s3:PutObjectAcl",
        "s3:PutObjectVersionAcl"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
```

```
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
      ]
    },
    {
      "Effect":"Allow",
      "Action":[
        "s3:PutObject"
      ],
      "Resource":[
        "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*"
      ]
    }
  ]
}
```

Restaurar objetos: RestoreObject

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
          "s3:RestoreObject"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
      ]
    },
    {
      "Effect":"Allow",
      "Action":[
        "s3:PutObject"
      ],
```

```
      "Resource":[
        "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*"
      ]
    }
  ]
}
```

Aplicar retenção do Bloqueio de Objetos: PutObjectRetention

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:GetBucketObjectLockConfiguration",
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-destination-bucket"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObjectRetention",
                "s3:BypassGovernanceRetention"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject"
```

```
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*"
            ]
        }
    ]
}
```

Aplicar retenção legal do Bloqueio de Objetos: PutObjectLegalHold

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:GetBucketObjectLockConfiguration",
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-destination-bucket"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "s3:PutObjectLegalHold",
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject"
            ],
            "Resource": [
```

```
                "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*"
            ]
        }
    ]
}
```

Replicar objetos existentes: InitiateReplication com um manifesto gerado pelo S3

Use essa política se estiver usando e armazenando um manifesto gerado pelo S3. Consulte mais informações sobre o uso de operações em lote para replicação de objetos existentes em Replicar objetos existentes com o Replicação em Lote.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Action":[
            "s3:InitiateReplication"
         ],
         "Effect":"Allow",
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
         ]
      },
      {
         "Action":[
            "s3:GetReplicationConfiguration",
            "s3:PutInventoryConfiguration"
         ],
         "Effect":"Allow",
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-source-bucket"
         ]
      },
      {
         "Action":[
            "s3:GetObject",
            "s3:GetObjectVersion"
         ],
         "Effect":"Allow",
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
         ]
```

```
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3:PutObject"
         ],
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*",
            "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
         ]
      }
   ]
}
```

Replicar objetos existentes: InitiateReplication com um manifesto do usuário

Use essa política se estiver usando um manifesto fornecido pelo usuário. Consulte mais informações sobre o uso de Operações em Lote para replicação de objetos existentes em Replicar objetos existentes com o Replicação em Lote.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Action":[
            "s3:InitiateReplication"
         ],
         "Effect":"Allow",
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
         ]
      },
      {
         "Action":[
            "s3:GetObject",
            "s3:GetObjectVersion"
         ],
         "Effect":"Allow",
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
         ]
      },
      {
```

```
         "Effect":"Allow",
         "Action":[
            "s3:PutObject"
         ],
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*"
         ]
      }
   ]
}
```

Criar um trabalho de operações em lote do S3

Com a funcionalidade Operações em Lote do Amazon S3, você pode executar operações em lote em grande escala em uma lista de objetos específicos do Amazon S3. Esta seção descreve as informações necessárias para criar um trabalho do Operações em lote do S3 e os resultados de uma solicitação `CreateJob`. Ela também fornece instruções para criar um trabalho de Operações em Lote usando o console do Amazon S3, a AWS Command Line Interface (AWS CLI) e o AWS SDK para Java.

Ao criar um trabalho do S3 Batch Operations, você pode solicitar um relatório de conclusão para todas as tarefas ou somente para aquelas que apresentaram falha. Contanto que pelo menos uma tarefa tenha sido invocada com êxito, a funcionalidade Operações em Lote do S3 gera um relatório para tarefas que foram concluídas, que falharam ou que foram canceladas. Para obter mais informações, consulte Exemplos: relatórios de conclusão de operações em lote do S3.

Tópicos

- Elementos da solicitação de trabalho de Operações em lote
- Especificar um manifesto

Elementos da solicitação de trabalho de Operações em lote

Para criar um trabalho de operações em lote do S3, você deve fornecer as seguintes informações:

Operação

Especifique a operação que deseja que as operações em lote do S3 execute nos objetos no manifesto. Cada tipo de operação aceita parâmetros específicos para essa operação. A

funcionalidade Operações em Lote possibilita a execução de uma operação em lote, com os mesmos resultados da operação executada individualmente em cada objeto.

Manifesto

O manifesto é uma lista de todos os objetos em que você deseja que a funcionalidade Operações em Lote do S3 execute a ação especificada. Você pode usar os seguintes métodos para especificar um manifesto para um trabalho de Operações em Lote:

- Crie manualmente sua própria lista de objetos personalizada em formato CSV.
- Escolha um relatório do Catalogar e analisar seus dados com o Inventário S3 existente em formato CSV.
- Instruir a funcionalidade Operações em Lote para que gere um manifesto automaticamente com base nos critérios de filtro de objetos especificados ao criar um trabalho. Essa opção está disponível para trabalhos de replicação em lote criados no console do Amazon S3 ou para qualquer tipo de trabalho criado usando a AWS CLI, SDKs da AWS ou a API REST do Amazon S3.

> **Note**
>
> - Independentemente de como você especifica o manifesto, a lista em si deve ser armazenada em um bucket de uso geral. A funcionalidade Operações em Lote não pode importar manifestos existentes nem salvar manifestos gerados em buckets de diretório. No entanto, os objetos descritos no manifesto podem ser armazenados em buckets de diretório. Para obter mais informações, consulte Directory buckets.
> - Se os objetos no manifesto estiverem em um bucket com versionamento, especificar os IDs de versão dos objetos instruirá a funcionalidade Operações em Lote a realizar a operação em uma versão específica. Se nenhum ID de versão for especificado, a funcionalidade Operações em Lote realizará a operação na versão mais recente dos objetos. Se o manifesto incluir um campo de ID de versão, você deverá fornecer um ID de versão para todos os objetos no manifesto.

Para obter mais informações, consulte Especificar um manifesto.

Priority

Use prioridades de trabalho para indicar a prioridade relativa desse trabalho em relação a outros em execução na conta. Um número maior indica uma prioridade mais alta.

As prioridades de trabalho só têm significado em relação às prioridades definidas para outros trabalhos na mesma conta e região. Você pode escolher qualquer sistema de numeração adequado para você. Por exemplo, talvez você queira atribuir a todos os trabalhos Restaurar (`RestoreObject`) uma prioridade 1, a todos os trabalhos de Copiar (`CopyObject`) uma prioridade 2 e a todos os trabalhos de Substituir listas de controle de acesso (ACLs) (`PutObjectAcl`) uma prioridade 3.

A funcionalidade Operações em Lote do S3 prioriza trabalhos em ordem numérica, mas o rigor dessa ordem não é garantido. Por isso, não use prioridades de trabalho para garantir que um trabalho comece ou termine antes de outro. Caso precise garantir uma ordem rigorosa, aguarde a conclusão de uma tarefa para iniciar a próxima.

RoleArn

Especifique uma função do AWS Identity and Access Management (IAM) para executar o trabalho. A função do IAM usada deve ter permissões suficientes para realizar a operação especificada no trabalho. Por exemplo, para executar um trabalho `CopyObject`, o perfil do IAM deve ter a permissão `s3:GetObject` para o bucket de origem e a permissão `s3:PutObject` para o bucket de destino. A função também precisa de permissões para ler o manifesto e gravar o relatório de conclusão do trabalho.

Para obter mais informações sobre funções do IAM, consulte Funções do IAM no Manual do usuário do IAM.

Para obter mais informações sobre as permissões do Amazon S3, consulte Ações de políticas para o Amazon S3.

> **Note**
>
> Os trabalhos de Operações em Lote que realizam ações em buckets de diretório exigem permissões específicas. Para obter mais informações, consulte AWS Identity and Access Management (IAM) for S3 Express One Zone.

Relatório

Especifique se deseja que as operações em lote do S3 gerem um relatório de conclusão. Caso solicite um relatório de conclusão do trabalho, você deve fornecer os parâmetros para o relatório neste elemento. As informações necessárias incluem o seguinte]:

- O bucket no qual você deseja armazenar o relatório.

> **Note**
>
> O relatório deve ser armazenado em um bucket de uso geral. A funcionalidade Operações em Lote não pode salvar relatórios em buckets de diretório. Para obter mais informações, consulte Directory buckets.

- O formato do relatório
- Se você deseja que o relatório inclua os detalhes de todas as tarefas ou apenas das tarefas que apresentaram falha.
- Uma string de prefixo opcional.

> **Note**
>
> Os relatórios de conclusão são sempre criptografados com a criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3).

Tags (opcional)

Você pode rotular e controlar o acesso aos trabalhos de operações em lote do S3 adicionando tags. Você pode usar etiquetas para identificar quem é responsável por um trabalho de Operações em Lote ou para controlar como os usuários interagem com os trabalhos de Operações em Lote. A presença de marcações de trabalho pode conceder ou limitar a capacidade do usuário de cancelar um trabalho, ativar um trabalho no estado de confirmação ou alterar o nível de prioridade de um trabalho. Por exemplo, você pode conceder a um usuário permissão para invocar a operação `CreateJob`, desde que o trabalho seja criado com a etiqueta `"Department=Finance"`.

Você pode criar trabalhos com tags anexadas a eles e pode adicionar tags a trabalhos depois de criá-los.

Para obter mais informações, consulte the section called “Usar tags”.

Description (opcional)

Para rastrear e monitorar seu trabalho, você também pode fornecer uma descrição de até 256 caracteres. O Amazon S3 inclui essa descrição sempre que retorna informações sobre um trabalho ou exibe detalhes do trabalho no console do Amazon S3. É possível classificar e filtrar os trabalhos com facilidade de acordo com as descrições atribuídas. As descrições não precisam ser

exclusivas, de maneira que você possa usar descrições como categorias (por exemplo, "Tarefas de cópia de log semanais") para ajudar a rastrear grupos de tarefas semelhantes.

Especificar um manifesto

Um manifesto é um objeto do Amazon S3 que contém as chaves de objeto em que você deseja que o Amazon S3 atue. Você pode fornecer um manifesto de uma das seguintes maneiras:

- Crie um arquivo de manifesto manualmente.
- Use um manifesto existente.
- Instruir a funcionalidade Operações em Lote para que gere um manifesto automaticamente com base nos critérios de filtro de objetos especificados ao criar um trabalho. Essa opção está disponível para trabalhos de replicação em lote criados no console do Amazon S3 ou para qualquer tipo de trabalho criado usando a AWS CLI, SDKs da AWS ou a API REST do Amazon S3.

> **Note**
>
> - O recurso Operações em Lote do Amazon S3 não permite a geração de manifestos entre regiões.
> - Independentemente de como você especifica o manifesto, a lista em si deve ser armazenada em um bucket de uso geral. A funcionalidade Operações em Lote não pode importar manifestos existentes nem salvar manifestos gerados em buckets de diretório. No entanto, os objetos descritos no manifesto podem ser armazenados em buckets de diretório. Para obter mais informações, consulte Directory buckets.

Criar um arquivo de manifesto

Para criar um arquivo de manifesto manualmente, especifique a chave de objeto do manifesto, a ETag (etiqueta de entidade) e o ID da versão opcional em uma lista em formato CSV. O conteúdo do manifesto deve estar codificado em URL.

Por padrão, o Amazon S3 usa criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3) automaticamente para criptografar um manifesto carregado para um bucket do Amazon S3. Os manifestos que usam a criptografia no servidor com chaves fornecidas pelo cliente (SSE-

C) não são compatíveis. Manifestos que usam criptografia no lado do servidor com chaves do AWS Key Management Service (AWS KMS) (SSE-KMS) só são compatíveis quando usam relatórios de inventário no formato CSV. Usar um manifesto criado manualmente com o AWS KMS não é compatível.

O manifesto deve conter o nome do bucket, a chave de objeto e, opcionalmente, a versão de cada objeto. Qualquer outro campo no manifesto não é usado pelas operações em lote do S3.

> **Note**
>
> Se os objetos no manifesto estiverem em um bucket com versionamento, especificar os IDs de versão dos objetos instruirá a funcionalidade Operações em Lote a realizar a operação em uma versão específica. Se nenhum ID de versão for especificado, a funcionalidade Operações em Lote realizará a operação na versão mais recente dos objetos. Se o manifesto incluir um campo de ID de versão, você deverá fornecer um ID de versão para todos os objetos no manifesto.

Veja a seguir um exemplo de manifesto no formato CSV sem os IDs de versão.

```
amzn-s3-demo-bucket1,objectkey1
amzn-s3-demo-bucket1,objectkey2
amzn-s3-demo-bucket1,objectkey3
amzn-s3-demo-bucket1,photos/jpgs/objectkey4
amzn-s3-demo-bucket1,photos/jpgs/newjersey/objectkey5
amzn-s3-demo-bucket1,object%20key%20with%20spaces
```

Veja a seguir um exemplo de manifesto em formato CSV que inclui IDs de versão.

```
amzn-s3-demo-bucket1,objectkey1,PZ9ibn9D5lP6p298B7S9_ceqx1n5EJ0p
amzn-s3-demo-bucket1,objectkey2,YY_ouuAJByNW1LRBfFMfxMge7XQWxMBF
amzn-s3-demo-bucket1,objectkey3,jbo9_jhdPEyB4RrmOxWS0kU0EoNrU_oI
amzn-s3-demo-bucket1,photos/jpgs/objectkey4,6EqlikJJxLTsHsnbZbSRffn24_eh5Ny4
amzn-s3-demo-bucket1,photos/jpgs/newjersey/objectkey5,imHf3FAiRsvBW_EHB8GOu.NHunHO1gVs
amzn-s3-demo-bucket1,object%20key%20with%20spaces,9HkPvDaZY5MVbMhn6TMn1YTb5ArQAo3w
```

Especificar um arquivo de manifesto existente

É possível especificar um arquivo de manifesto na solicitação de criação de um trabalho usando um dos seguintes formatos:

- Relatório da funcionalidade Inventário Amazon S3: deve ser um relatório da funcionalidade Inventário Amazon S3 em formato CSV. É necessário especificar o arquivo `manifest.json` associado ao relatório de inventário. Para obter mais informações sobre relatórios de inventário, consulte Catalogar e analisar seus dados com o Inventário S3. Se o relatório de inventário incluir IDs de versões, o recurso Operações em lote do S3 operará nas versões especificadas do objeto.

  > **Note**
  >
  > - A funcionalidade Operações em Lote do S3 oferece suporte a relatórios de inventário em CSV criptografados com SSE-KMS.
  > - Se você enviar um manifesto de relatório de inventário criptografado com SSE-KMS, a política do IAM deverá incluir as permissões `"kms:Decrypt"` e `"kms:GenerateDataKey"` para o objeto `manifest.json` e todos os arquivos de dados CSV associados.

- Arquivo CSV: cada linha no arquivo deve incluir o nome do bucket, a chave do objeto e, opcionalmente, a versão do objeto. As chaves de objeto devem ser codificadas em URL conforme mostrado nos exemplos a seguir. O manifesto deve incluir ou omitir IDs de versão para todos os objetos. Para obter mais informações sobre o formato de manifesto CSV, consulte JobManifestSpec na Referência da API do Amazon Simple Storage Service.

  > **Note**
  >
  > A funcionalidade Operações em Lote do S3 não oferece suporte a arquivos de manifesto em CSV criptografados com SSE-KMS.

> **Important**
>
> Ao usar um manifesto criado manualmente e um bucket com versionamento, recomendamos especificar os IDs de versão dos objetos. Quando você cria um trabalho, o recurso Operações em lote do S3 analisa todo o manifesto antes de executar o trabalho. No entanto, ele não tira snapshots do estado do bucket.
> Como os manifestos podem conter bilhões de objetos, os trabalhos podem levar muito tempo para serem executados, o que pode afetar a versão de um objeto em que o trabalho atua. Suponha que você substitua um objeto por uma nova versão enquanto um trabalho estiver em execução e não especifique o ID de versão desse objeto. Nesse caso, o Amazon S3

realizará a operação na versão mais recente do objeto, não na versão que existia quando você criou o trabalho. A única maneira de evitar esse comportamento é especificar o ID de versão do objeto listado no manifesto.

Gerar um manifesto automaticamente

Você pode instruir o Amazon S3 a gerar um manifesto automaticamente com base nos critérios de filtro de objetos especificados ao criar um trabalho. Essa opção está disponível para trabalhos de replicação em lote criados no console do Amazon S3 ou para qualquer tipo de trabalho criado usando a AWS CLI, SDKs da AWS ou a API REST do Amazon S3. Para obter mais informações sobre replicação em lote, consulte Replicar objetos existentes com o Replicação em Lote.

Para gerar um manifesto automaticamente, especifique os seguintes elementos como parte da solicitação de criação de trabalho:

- Informações sobre o bucket que contém seus objetos de origem, incluindo o proprietário do bucket e o nome do recurso da Amazon (ARN).
- Informações sobre a saída do manifesto, incluindo um sinalizador para criar um arquivo de manifesto, o proprietário do bucket de saída, o ARN, o prefixo, o formato do arquivo e o tipo de criptografia.
- Critérios opcionais para filtrar objetos por data de criação, nome da chave, tamanho e classe de armazenamento. No caso de trabalhos de replicação, você também pode usar tags para filtrar objetos.

Critérios de filtro de objetos

Para filtrar a lista de objetos a serem incluídos em um manifesto gerado automaticamente, você pode especificar os critérios a seguir. Para obter mais informações, consulte JobManifestGeneratorFilter na Referência da API do Amazon S3.

CreatedAfter

Se fornecido, o manifesto gerado incluirá somente objetos de bucket de origem que foram criados após esse período.

CreatedBefore

Se fornecido, o manifesto gerado incluirá somente objetos de bucket de origem que foram criados antes desse período.

EligibleForReplication

Se fornecido, o manifesto gerado só incluirá os objetos que estiverem qualificados para replicação de acordo com a configuração de replicação no bucket de origem.

KeyNameConstraint

Se fornecido, o manifesto gerado incluirá somente os objetos do bucket de origem cujas chaves de objeto correspondam às restrições de string especificadas para MatchAnySubstring, MatchAnyPrefix e MatchAnySuffix.

MatchAnySubstring: se fornecido, o manifesto gerado incluirá objetos se a string especificada aparecer em qualquer lugar dentro da string da chave do objeto.

MatchAnyPrefix: se fornecido, o manifesto gerado incluirá objetos se a string especificada aparecer no início da string da chave do objeto.

MatchAnySuffix: se fornecido, o manifesto gerado incluirá objetos se a string especificada aparecer no final da string da chave do objeto.

MatchAnyStorageClass

Se fornecido, o manifesto gerado incluirá somente os objetos do bucket de origem que estiverem armazenados com a classe de armazenamento especificada.

ObjectReplicationStatuses

Se fornecido, o manifesto gerado só incluirá os objetos do bucket de origem que tenham um dos status de replicação especificados.

ObjectSizeGreaterThanBytes

Se fornecido, o manifesto gerado só incluirá os objetos do bucket de origem cujo tamanho de arquivo for maior que o número especificado de bytes.

ObjectSizeLessThanBytes

Se fornecido, o manifesto gerado só incluirá os objetos do bucket de origem cujo tamanho de arquivo for menor que o número especificado de bytes.

> **Note**
>
> Não é possível clonar a maioria dos trabalhos que têm manifestos gerados automaticamente. Os trabalhos de replicação em lote podem ser clonados, exceto quando usam os

critérios de filtro de manifesto `KeyNameConstraint`, `MatchAnyStorageClass`, `ObjectSizeGreaterThanBytes` ou `ObjectSizeLessThanBytes`.

A sintaxe para especificar os critérios do manifesto varia de acordo com o método usado para criar o trabalho. Para obter exemplos, consulte Criar um trabalho.

Criar um trabalho

Você pode criar trabalhos de Operações em Lote do S3 usando o console do Amazon S3, a AWS CLI, AWS SDKs ou a API REST do Amazon S3.

Para obter mais informações sobre como criar uma solicitação de trabalho, consulte Elementos da solicitação de trabalho de Operações em lote.

Pré-requisitos

Antes de criar um trabalho de Operações em Lote, confirme se você configurou as permissões relevantes. Para obter mais informações, consulte Conceder permissões para operações em lote.

Usar o console do S3

Para criar um trabalho em lote

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Na barra de navegação na parte superior da página, escolha o nome da Região da AWS exibida no momento. Em seguida, escolha a região onde você deseja criar o trabalho.

   > **Note**
   >
   > Para operações de cópia, você deve criar o trabalho na mesma região que o bucket de destino. Para todas as outras operações, você deve criar o trabalho na mesma região que os objetos arquivados no manifesto.

3. Selecione Operações em lotes no painel de navegação do console do Amazon S3.
4. Escolha Criar trabalho.
5. Visualize a Região da AWS onde você deseja criar o trabalho.
6. Em Formato do manifesto, escolha o tipo de objeto do manifesto a ser usado.

- Se você selecionar S3 inventory report (Relatório de inventário do S3), insira o caminho para o objeto manifest.json gerado pelo Amazon S3 como parte do relatório de inventário em formato CSV e, opcionalmente, o ID de versão do objeto do manifesto a ser usado, se não for a mais recente.
- Se você selecionar CSV, insira o caminho para o objeto do manifesto formatado em CSV. O objeto do manifesto deve seguir o formato descrito no console. Opcionalmente, inclua o ID de versão do objeto do manifesto que deseja usar, se não for a mais recente.

> **Note**
>
> O console do Amazon S3 oferece suporte à geração automática de manifestos somente para trabalhos de replicação em lote. Para todos os outros tipos de trabalho, se você quiser que o Amazon S3 gere um manifesto automaticamente com base nos critérios de filtro especificados, deverá configurar o trabalho usando a AWS CLI, AWS SDKs ou a API REST do Amazon S3.

7. Escolha Próximo.
8. Em Operation (Operação), selecione a operação a ser executada em todos os objetos no manifesto. Preencha as informações da operação escolhida e, depois, selecione Next (Próximo).
9. Preencha as informações para Configure additional options (Configurar opções adicionais) e, depois, selecione Next (Próximo).
10. Em Review (Revisão), verifique as configurações. Se precisar fazer alterações, escolha Previous (Anterior). Caso contrário, selecione Criar trabalho.

Como usar o AWS CLI

Para criar o trabalho de operações em lote com a AWS CLI, escolha um dos exemplos a seguir, dependendo se você está especificando um manifesto existente ou gerando um manifesto automaticamente.

Specify manifest

O exemplo a seguir mostra como usar a AWS CLI para criar um trabalho `S3PutObjectTagging` do Operações em Lote do S3 que atua em objetos listados em um arquivo de manifesto existente.

Como criar um trabalho **`S3PutObjectTagging`** de operações em lote especificando um manifesto

1. Use os comandos a seguir para criar um perfil do AWS Identity and Access Management (IAM), depois crie uma política do IAM para atribuir as permissões relevantes. O perfil e a política a seguir concedem permissão ao Amazon S3 para adicionar etiquetas de objeto, que serão necessárias quando você criar o trabalho em uma etapa posterior.

   a. Use o exemplo de comando a seguir para criar um perfil do IAM para usar a funcionalidade Operações em Lote. Para usar esse exemplo de comando, substitua *`S3BatchJobRole`* pelo nome que você deseja dar ao perfil.

```
aws iam create-role \
 --role-name S3BatchJobRole \
 --assume-role-policy-document '{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service":"batchoperations.s3.amazonaws.com"
         },
         "Action":"sts:AssumeRole"
      }
   ]
}'
```

   Registre o nome de recurso da Amazon (ARN) da função. Você precisará do ARN ao criar trabalhos.

   b. Use o exemplo de comando a seguir para criar uma política do IAM com as permissões necessárias e anexe-a ao perfil do IAM que você criou na etapa anterior. Para obter mais informações sobre as permissões necessárias, consulte Conceder permissões para operações em lote.

> **Note**
>
> Os trabalhos de Operações em Lote que realizam ações em buckets de diretório exigem permissões específicas. Para obter mais informações, consulte AWS Identity and Access Management (IAM) for S3 Express One Zone.

Para usar esse exemplo de comando, substitua *user input placeholders* da seguinte forma:

- Substitua *S3BatchJobRole* pelo nome do seu perfil do IAM. Garanta que esse nome corresponda ao nome que você usou anteriormente.
- Substitua *PutObjectTaggingBatchJobPolicy* pelo nome que você deseja atribuir à política do IAM.
- Substitua *amzn-s3-demo-destination-bucket* pelo nome do bucket que contém os objetos aos quais você deseja aplicar etiquetas.
- Substitua *amzn-s3-demo-manifest-bucket* pelo nome do bucket que contém o manifesto.
- Substitua *amzn-s3-demo-completion-report-bucket* pelo nome do bucket ao qual você deseja que o relatório de conclusão seja entregue.

```
aws iam put-role-policy \
  --role-name S3BatchJobRole \
  --policy-name PutObjectTaggingBatchJobPolicy \
  --policy-document '{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "s3:PutObjectTagging",
        "s3:PutObjectVersionTagging"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetBucketLocation"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-manifest-bucket",
        "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
```

```
      ]
    },
    {
      "Effect":"Allow",
      "Action":[
        "s3:PutObject",
        "s3:GetBucketLocation"
      ],
      "Resource":[
        "arn:aws:s3:::amzn-s3-demo-completion-report-bucket",
        "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*"
      ]
    }
  ]
}'
```

2. Use o exemplo de comando a seguir para criar um trabalho `S3PutObjectTagging`.

   O arquivo `manifest.csv` fornece uma lista de buckets e valores de chave de objeto. O trabalho aplica as etiquetas específicas aos objetos identificados no manifesto. O `ETag` é o ETag do objeto `manifest.csv`, que você pode obter no console do Amazon S3. Essa solicitação especifica o parâmetro `no-confirmation-required` para que você possa executar o trabalho sem precisar confirmá-lo com o comando `update-job-status`. Para obter mais informações, consulte create-job na Referência de comandos da AWS CLI.

   Para usar esse exemplo de comando, substitua os *`user input placeholders`* por suas próprias informações. Substitua *`IAM-role`* pelo ARN do perfil do IAM que você criou anteriormente.

```
aws s3control create-job \
    --region us-west-2 \
    --account-id acct-id \
    --operation '{"S3PutObjectTagging": { "TagSet": [{"Key":"keyOne",
 "Value":"ValueOne"}] }}' \
    --manifest '{"Spec":{"Format":"S3BatchOperations_CSV_20180820","Fields":
["Bucket","Key"]},"Location":{"ObjectArn":"arn:aws:s3:::amzn-s3-demo-manifest-
bucket/manifest.csv","ETag":"60e460c9d1046e73f7dde5043ac3ae85"}}' \
    --report '{"Bucket":"arn:aws:s3:::amzn-s3-demo-
completion-report-bucket","Prefix":"final-reports",
 "Format":"Report_CSV_20180820","Enabled":true,"ReportScope":"AllTasks"}' \
    --priority 42 \
    --role-arn IAM-role \
```

```
    --client-request-token $(uuidgen) \
    --description "job description" \
    --no-confirmation-required
```

Em resposta, o Amazon S3 retorna um ID de trabalho (por exemplo, `00e123a4-c0d8-41f4-a0eb-b46f9ba5b07c`). Você precisará do ID do trabalho para identificar, monitorar e modificar o trabalho.

Generate manifest

O exemplo a seguir mostra como criar um trabalho `S3DeleteObjectTagging` de Operações em Lote do S3 que gera automaticamente um manifesto com base em critérios de filtro de objetos. Esses critérios incluem a data de criação, o nome da chave, o tamanho, a classe de armazenamento e etiquetas.

Como criar um trabalho **`S3DeleteObjectTagging`** de operações em lote gerando um manifesto

1. Use os comandos a seguir para criar um perfil do AWS Identity and Access Management (IAM), depois crie uma política do IAM para atribuir as permissões. O perfil e a política a seguir concedem permissão ao Amazon S3 para excluir etiquetas de objeto, que serão necessárias quando você criar o trabalho em uma etapa posterior.

   a. Use o exemplo de comando a seguir para criar um perfil do IAM para usar a funcionalidade Operações em Lote. Para usar esse exemplo de comando, substitua *S3BatchJobRole* pelo nome que você deseja dar ao perfil.

```
aws iam create-role \
 --role-name S3BatchJobRole \
 --assume-role-policy-document '{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service":"batchoperations.s3.amazonaws.com"
         },
         "Action":"sts:AssumeRole"
      }
   ]
```

```
}'
```

Registre o nome de recurso da Amazon (ARN) da função. Você precisará do ARN ao criar trabalhos.

b. Use o exemplo de comando a seguir para criar uma política do IAM com as permissões necessárias e anexe-a ao perfil do IAM que você criou na etapa anterior. Para obter mais informações sobre as permissões necessárias, consulte Conceder permissões para operações em lote.

> **Note**
>
> Os trabalhos de Operações em Lote que realizam ações em buckets de diretório exigem permissões específicas. Para obter mais informações, consulte AWS Identity and Access Management (IAM) for S3 Express One Zone.

Para usar esse exemplo de comando, substitua *`user input placeholders`* da seguinte forma:

- Substitua *`S3BatchJobRole`* pelo nome do seu perfil do IAM. Garanta que esse nome corresponda ao nome que você usou anteriormente.
- Substitua *`DeleteObjectTaggingBatchJobPolicy`* pelo nome que você deseja atribuir à política do IAM.
- Substitua *`amzn-s3-demo-destination-bucket`* pelo nome do bucket que contém os objetos aos quais você deseja aplicar etiquetas.
- Substitua *`amzn-s3-demo-manifest-bucket`* pelo nome do bucket onde deseja salvar o manifesto.
- Substitua *`amzn-s3-demo-completion-report-bucket`* pelo nome do bucket ao qual você deseja que o relatório de conclusão seja entregue.

```
aws iam put-role-policy \
  --role-name S3BatchJobRole \
  --policy-name DeleteObjectTaggingBatchJobPolicy \
  --policy-document '{
  "Version":"2012-10-17",
  "Statement":[
    {
```

```
      "Effect":"Allow",
      "Action":[
        "s3:DeleteObjectTagging",
        "s3:DeleteObjectVersionTagging"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
    },
    {
      "Effect":"Allow",
      "Action":[
        "s3:PutInventoryConfiguration"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-manifest-bucket",
        "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
      ]
    },
    {
      "Effect":"Allow",
      "Action":[
        "s3:PutObject",
        "s3:ListBucket"
      ],
      "Resource":[
        "arn:aws:s3:::amzn-s3-demo-completion-report-bucket",
        "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*",
        "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
      ]
    }
  ]
}'
```

2. Use o exemplo de comando a seguir para criar o trabalho `S3DeleteObjectTagging`.

Neste exemplo, os valores na seção `--report` especificam o bucket, o prefixo, o formato e o escopo do relatório de trabalho que será gerado. A seção `--manifest-generator` especifica informações sobre o bucket de origem que contém os objetos sobre os quais o trabalho atuará, informações sobre a lista de saída do manifesto que será gerada para o trabalho e critérios de filtro para restringir o escopo de objetos a serem incluídos no manifesto por data de criação, restrições de nome, tamanho e classe de armazenamento. O comando também especifica a prioridade do trabalho, o perfil do IAM e a Região da AWS.

Para obter mais informações, consulte create-job na Referência de comandos da AWS CLI.

Para usar esse exemplo de comando, substitua os *`user input placeholders`* por suas próprias informações. Substitua *`IAM-role`* pelo ARN do perfil do IAM que você criou anteriormente.

```
aws s3control create-job \
    --account-id 012345678901 \
    --operation '{
        "S3DeleteObjectTagging": {}
    }' \
    --report '{
        "Bucket":"arn:aws:s3:::amzn-s3-demo-completion-report-bucket",
        "Prefix":"reports",
        "Format":"Report_CSV_20180820",
        "Enabled":true,
        "ReportScope":"AllTasks"
    }' \
    --manifest-generator '{
        "S3JobManifestGenerator": {
          "ExpectedBucketOwner": "012345678901",
          "SourceBucket": "arn:aws:s3:::amzn-s3-demo-source-bucket",
          "EnableManifestOutput": true,
          "ManifestOutputLocation": {
            "ExpectedManifestBucketOwner": "012345678901",
            "Bucket": "arn:aws:s3:::amzn-s3-demo-manifest-bucket",
            "ManifestPrefix": "prefix",
            "ManifestFormat": "S3InventoryReport_CSV_20211130"
          },
          "Filter": {
            "CreatedAfter": "2023-09-01",
            "CreatedBefore": "2023-10-01",
            "KeyNameConstraint": {
```

```
            "MatchAnyPrefix": [
              "prefix"
            ],
            "MatchAnySuffix": [
              "suffix"
            ]
          },
          "ObjectSizeGreaterThanBytes": 100,
          "ObjectSizeLessThanBytes": 200,
          "MatchAnyStorageClass": [
            "STANDARD",
            "STANDARD_IA"
          ]
        }
      }
    }' \
    --priority 2 \
    --role-arn IAM-role \
    --region us-east-1
```

Em resposta, o Amazon S3 retorna um ID de trabalho (por exemplo, `00e123a4-c0d8-41f4-a0eb-b46f9ba5b07c`). Você precisará desse ID de trabalho para identificar, monitorar e modificar o trabalho.

Como usar o AWS SDK para Java

Para criar o trabalho de operações em lote com a AWS SDK para Java, escolha um dos exemplos a seguir, dependendo se você está especificando um manifesto existente ou gerando um manifesto automaticamente.

Specify manifest

O exemplo a seguir mostra como criar um trabalho `S3PutObjectTagging` de Operações em Lote do S3 que atua em objetos listados em um arquivo de manifesto existente. Para usar esse exemplo, substitua os *`user input placeholders`* por suas próprias informações.

Example

```
package aws.example.s3control;
```

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import com.amazonaws.services.s3control.model.*;

import java.util.UUID;
import java.util.ArrayList;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class CreateJob {
    public static void main(String[] args) {
        String accountId = "Account ID";
        String iamRoleArn = "IAM Role ARN";
        String reportBucketName = "arn:aws:s3:::amzn-s3-demo-completion-report-
bucket";
        String uuid = UUID.randomUUID().toString();

        ArrayList tagSet = new ArrayList<S3Tag>();
        tagSet.add(new S3Tag().withKey("keyOne").withValue("ValueOne"));


        try {
            JobOperation jobOperation = new JobOperation()
                    .withS3PutObjectTagging(new S3SetObjectTaggingOperation()
                            .withTagSet(tagSet)
                    );

            JobManifest manifest = new JobManifest()
                    .withSpec(new JobManifestSpec()
                            .withFormat("S3BatchOperations_CSV_20180820")
                            .withFields(new String[]{
                                    "Bucket", "Key"
                            }))
                    .withLocation(new JobManifestLocation()
                            .withObjectArn("arn:aws:s3:::my_manifests/manifest.csv")
                            .withETag("60e460c9d1046e73f7dde5043ac3ae85"));
            JobReport jobReport = new JobReport()
                    .withBucket(reportBucketName)
                    .withPrefix("reports")
                    .withFormat("Report_CSV_20180820")
                    .withEnabled(true)
```

```
                    .withReportScope("AllTasks");

            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(US_WEST_2)
                    .build();

            s3ControlClient.createJob(new CreateJobRequest()
                    .withAccountId(accountId)
                    .withOperation(jobOperation)
                    .withManifest(manifest)
                    .withReport(jobReport)
                    .withPriority(42)
                    .withRoleArn(iamRoleArn)
                    .withClientRequestToken(uuid)
                    .withDescription("job description")
                    .withConfirmationRequired(false)
            );

        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Generate manifest

O exemplo a seguir mostra como criar um trabalho `s3PutObjectCopy` de Operações em Lote do S3 que gera automaticamente um manifesto com base em critérios de filtro de objetos, incluindo a data de criação, o nome da chave e o tamanho. Para usar esse exemplo, substitua os *`user input placeholders`* por suas próprias informações.

Example

```
        package aws.example.s3control;

    import com.amazonaws.AmazonServiceException;
```

```
    import com.amazonaws.SdkClientException;
    import com.amazonaws.auth.profile.ProfileCredentialsProvider;
    import com.amazonaws.services.s3control.AWSS3Control;
    import com.amazonaws.services.s3control.AWSS3ControlClient;
    import com.amazonaws.services.s3control.model.CreateJobRequest;
    import com.amazonaws.services.s3control.model.CreateJobResult;
    import com.amazonaws.services.s3control.model.JobManifestGenerator;
    import com.amazonaws.services.s3control.model.JobManifestGeneratorFilter;
    import com.amazonaws.services.s3control.model.JobOperation;
    import com.amazonaws.services.s3control.model.JobReport;
    import com.amazonaws.services.s3control.model.KeyNameConstraint;
    import com.amazonaws.services.s3control.model.S3JobManifestGenerator;
    import com.amazonaws.services.s3control.model.S3ManifestOutputLocation;
    import com.amazonaws.services.s3control.model.S3SetObjectTaggingOperation;
    import com.amazonaws.services.s3control.model.S3Tag;

    import java.time.Instant;
    import java.util.Date;
    import java.util.UUID;
    import java.util.ArrayList;

    import static com.amazonaws.regions.Regions.US_WEST_2;

    public class test {
        public static void main(String[] args) {
            String accountId = "012345678901";
            String iamRoleArn = "arn:aws:iam::012345678901:role/ROLE";
            String sourceBucketName = "arn:aws:s3:::amzn-s3-demo-source-bucket";
            String reportBucketName = "arn:aws:s3:::amzn-s3-demo-completion-report-
bucket";
            String manifestOutputBucketName = "arn:aws:s3:::amzn-s3-demo-manifest-
bucket";
            String uuid = UUID.randomUUID().toString();
            long minimumObjectSize = 100L;

            ArrayList<S3Tag> tagSet = new ArrayList<>();
            tagSet.add(new S3Tag().withKey("keyOne").withValue("ValueOne"));

            ArrayList<String> prefixes = new ArrayList<>();
            prefixes.add("s3KeyStartsWith");

            try {
                JobOperation jobOperation = new JobOperation()
                        .withS3PutObjectTagging(new S3SetObjectTaggingOperation()
```

```
                                .withTagSet(tagSet)
                        );
                S3ManifestOutputLocation manifestOutputLocation = new
S3ManifestOutputLocation()
                        .withBucket(manifestOutputBucketName)
                        .withManifestPrefix("manifests")
                        .withExpectedManifestBucketOwner(accountId)
                        .withManifestFormat("S3InventoryReport_CSV_20211130");

                JobManifestGeneratorFilter jobManifestGeneratorFilter = new
JobManifestGeneratorFilter()
                        .withEligibleForReplication(true)
                        .withKeyNameConstraint(
                                new KeyNameConstraint()
                                        .withMatchAnyPrefix(prefixes))
                        .withCreatedBefore(Date.from(Instant.now()))
                        .withObjectSizeGreaterThanBytes(minimumObjectSize);

                S3JobManifestGenerator s3JobManifestGenerator = new
S3JobManifestGenerator()
                        .withEnableManifestOutput(true)
                        .withManifestOutputLocation(manifestOutputLocation)
                        .withFilter(jobManifestGeneratorFilter)
                        .withSourceBucket(sourceBucketName);

                JobManifestGenerator jobManifestGenerator = new
JobManifestGenerator()
                        .withS3JobManifestGenerator(s3JobManifestGenerator);

                JobReport jobReport = new JobReport()
                        .withBucket(reportBucketName)
                        .withPrefix("reports")
                        .withFormat("Report_CSV_20180820")
                        .withEnabled(true)
                        .withReportScope("AllTasks");

                AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                        .withCredentials(new ProfileCredentialsProvider())
                        .withRegion(US_WEST_2)
                        .build();

                CreateJobResult createJobResult = s3ControlClient.createJob(new
CreateJobRequest()
                        .withAccountId(accountId)
```

```
                        .withOperation(jobOperation)
                        .withManifestGenerator(jobManifestGenerator)
                        .withReport(jobReport)
                        .withPriority(42)
                        .withRoleArn(iamRoleArn)
                        .withClientRequestToken(uuid)
                        .withDescription("job description")
                        .withConfirmationRequired(true)
                );

                System.out.println("Created job " + createJobResult.getJobId());

            } catch (AmazonServiceException e) {
                // The call was transmitted successfully, but Amazon S3 couldn't
process
                // it and returned an error response.
                e.printStackTrace();
            } catch (SdkClientException e) {
                // Amazon S3 couldn't be contacted for a response, or the client
                // couldn't parse the response from Amazon S3.
                e.printStackTrace();
            }
        }
    }
```

Uso da API REST

Você pode usar a API REST para criar um trabalho do Batch Operations. Para obter mais informações, consulte CreateJob na Referência da API do Amazon Simple Storage Service.

Respostas do trabalho

Se a solicitação `CreateJob` for bem-sucedida, o Amazon S3 retornará um ID de trabalho. O ID de trabalho é um identificador exclusivo gerado pelo Amazon S3 automaticamente para que você possa identificar as operações em lote e monitorar o status do trabalho.

Quando você cria um trabalho pela AWS CLI, por AWS SDKs ou pela API REST, é possível definir a funcionalidade Operações em Lote do S3 para que comece a processar o trabalho automaticamente. O trabalho é executado assim que fica pronto em vez de aguardar o processamento de trabalhos de prioridade mais alta.

Ao criar um trabalho por meio do console do Amazon S3, você deve examinar os detalhes e confirmar se deseja executá-lo antes que a funcionalidade Operações em Lote comece a processá-lo. Se uma tarefa permanecer no estado suspenso por mais de 30 dias, ela apresentará falha.

Operações suportadas pelo S3 Batch Operations

Você pode usar operações em lote do S3 para executar operações em lote de grande escala em objetos do Amazon S3. As operações em lote do S3 podem executar uma única operação em listas de objetos do Amazon S3 especificadas. Um único trabalho pode realizar uma operação especificada em bilhões de objetos contendo exabytes de dados. O Amazon S3 monitora o progresso, envia notificações e armazena um relatório de conclusão detalhado de todas as ações, fornecendo uma experiência totalmente gerenciada, auditável e sem servidor. É possível usar o recurso Operações em Lote do S3 por meio do console do Amazon S3, da AWS CLI, de SDKs da AWS ou da API REST do Amazon S3.

As operações em lote do S3 oferece suporte às seguintes operações:

Copiar objetos

Você pode usar o Operações em Lote do Amazon S3 para executar operações em lote de grande escala em objetos do Amazon S3. A operação Copiar do Operações em Lote copia cada objeto especificado no manifesto. É possível copiar objetos em um bucket na mesma Região da AWS ou em um bucket em outra região. O recurso Operações em lote do S3 é compatível com a maioria das opções disponíveis no Amazon S3 para copiar objetos. Essas opções incluem a configuração de metadados de objetos e permissões e a alteração da classe de armazenamento de um objeto.

É possível usar a operação Copiar para copiar objetos não criptografados existentes e gravá-los de volta no mesmo bucket que os objetos criptografados. Para obter mais informações, consulte Criptografia de objetos existentes com o Amazon S3 Batch Operations.

Ao copiar objetos, você pode alterar o algoritmo de soma de verificação usado para calcular a soma de verificação do objeto. Se os objetos não tiverem uma soma de verificação adicional calculada, você também poderá adicionar uma especificando o algoritmo de soma de verificação a ser usado pelo Amazon S3. Para obter mais informações, consulte Verificar a integridade do objeto no Amazon S3.

Consulte mais informações sobre como copiar objetos no Amazon S3, bem como parâmetros obrigatórios e opcionais em Copiar, mover e renomear objetos neste guia e em CopyObject na Referência de API do Amazon Simple Storage Service.

Restrições e limitações

Quando você usa a operação Copiar do Operações em Lote, as seguintes restrições e limitações se aplicam:

- Todos os objetos de origem devem estar em um só bucket.
- Todos os objetos de destino devem estar em um só bucket.
- Você deve ler todas as permissões para o bucket de origem e gravar permissões para o bucket de destino.
- Os objetos a serem copiados devem ter até 5 GB.
- Ao tentar copiar objetos das classes S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive para a classe de armazenamento S3 Standard, primeiro você deverá restaurar esses objetos. Para obter mais informações, consulte Restaurar um objeto arquivado.
- É necessário criar trabalhos Copiar do Operações em Lote na região de destino, que é a região para a qual você pretende copiar os objetos.
- Todas as opções `CopyObject` são compatíveis, exceto para verificações condicionais em tags de entidade (ETags) e criptografia do lado do servidor com chaves de criptografia fornecidas pelo cliente (SSE-C).
- Se o bucket de destino não tiver versionamento, você deverá substituir os objetos que têm os mesmos nomes de chave.
- Os objetos não são necessariamente copiados na mesma ordem em que são listados no manifesto. Para buckets com versionamento, se preservar a ordem de versão atual ou não atual for importante, copie todas as versões não atuais primeiro. Em seguida, após a conclusão do primeiro trabalho, copie as versões atuais em um trabalho subsequente.
- A cópia de objetos na classe Reduced Redundancy Storage (RRS) não é compatível.
- Um único trabalho de cópia do recurso Operações em Lote pode comportar um manifesto com até 20 bilhões de objetos.

Copiar objetos usando o S3 Batch Operations

Você pode usar o Operações em Lote do Amazon S3 para executar operações em lote de grande escala em objetos do Amazon S3. É possível usar o Operações em Lote do S3 para criar um trabalho Copiar (`CopyObject`) para copiar objetos dentro da mesma conta ou para uma conta de destino diferente.

Os exemplos a seguir mostram como armazenar e usar um manifesto que está em uma conta diferente. O primeiro exemplo mostra como você pode usar o Inventário Amazon S3 para entregar o relatório de inventário à conta de destino para uso durante a criação do trabalho. O segundo exemplo mostra como usar um manifesto de valores separados por vírgula (CSV) na conta de origem ou de destino. O terceiro exemplo mostra como usar a operação Copiar para habilitar chaves de bucket do S3 para objetos que foram criptografados com a criptografia do lado do servidor com chaves do AWS Key Management Service (AWS KMS) (SSE-KMS).

Exemplos de operação de cópia

- Uso de um relatório de inventário para copiar objetos entre Contas da AWS
- Uso de um manifesto CSV para copiar objetos entre Contas da AWS
- Usar o Operações em Lote para habilitar chaves de bucket do S3 para SSE-KMS

Uso de um relatório de inventário para copiar objetos entre Contas da AWS

Você pode usar o Operações em Lote do Amazon S3 para executar operações em lote de grande escala em objetos do Amazon S3. É possível usar o Operações em Lote do S3 para criar um trabalho Copiar (`CopyObject`) para copiar objetos dentro da mesma conta ou para uma conta de destino diferente.

Você pode usar o Inventário Amazon S3 para criar um relatório de inventário e usá-lo para criar uma lista (manifesto) de objetos a serem copiados com o Operações em Lote do S3. Para obter mais informações sobre como usar um manifesto CSV na conta de origem ou destino, consulte the section called “Uso de um manifesto CSV para copiar objetos entre Contas da AWS”.

O inventário do Amazon S3 gera inventários dos objetos em um bucket. A lista resultante é publicada em um arquivo de saída. O bucket do qual foi feito o inventário é chamado de bucket de origem e o bucket no qual o relatório de inventário é armazenado é chamado de bucket de destino.

O relatório do Amazon S3 Inventory pode ser configurado para ser entregue a outra Conta da AWS. Fazer isso permite que o Operações em Lote do S3 leia o relatório de inventário quando o trabalho é criado na conta de destino.

Para obter mais informações sobre os buckets de origem e destino do inventário do Amazon S3, consulte Buckets de origem e destino.

A maneira mais fácil de configurar um inventário é usando o console do Amazon S3, mas você também pode usar a API REST do Amazon S3, a AWS Command Line Interface (AWS CLI) ou SDKs da AWS.

O procedimento de console a seguir contém as etapas de alto nível para configurar permissões para um trabalho de operações em lote do S3. Neste procedimento, você copia objetos de uma conta de origem para uma conta de destino, com o relatório de inventário armazenado na conta de destino.

Como configurar o Amazon S3 Inventory para buckets de origem e de destino que são de propriedade de diferentes contas

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets.
3. Escolha (ou crie) um bucket de manifesto de destino para armazenar o relatório de inventário. Neste procedimento, a conta de destino é a conta que possui tanto o bucket de manifesto de destino como o bucket no qual os objetos são copiados.
4. Configure um relatório de inventário para um bucket de origem. Para obter informações sobre como usar o console para configurar um inventário ou sobre como criptografar um arquivo de lista de inventário, consulte Configurar o inventário do Amazon S3.

   Ao configurar o relatório de inventário, você especifica o bucket de destino no qual deseja que a lista seja armazenada. O relatório de inventário para o bucket de origem é publicado no bucket de destino. Neste procedimento, a conta de origem é a conta que possui o bucket de origem.

   Selecione CSV para o formato de saída.

   Ao inserir informações para o bucket de destino, selecione Buckets in another account (Buckets em outra conta). Em seguida, insira o nome do bucket do manifesto de destino. Se preferir, você poderá inserir o ID da conta de destino.

   Após salvar a configuração do inventário, o console exibirá uma mensagem semelhante à seguinte:

   O Amazon S3 não conseguiu criar uma política de bucket no bucket de destino. Peça para o proprietário do bucket de destino adicionar a política de bucket a seguir a fim de permitir que o Amazon S3 insira dados nele.

   O console exibirá, então, uma política de bucket que pode ser usada para o bucket de destino.
5. Copie a política do bucket de destino que aparece no console.
6. Na conta de destino, adicione a política de bucket copiada ao bucket do manifesto de destino no qual o relatório de inventário está armazenado.

7. Crie uma função na conta de destino baseada na política de confiança do recurso Operações em lote do S3. Consulte mais informações sobre essa política de confiança em Política de confiança.

   Consulte mais informações sobre como criar um perfil em Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do usuário do IAM.

   Insira um nome para o perfil (o perfil do exemplo a seguir usa o nome *BatchOperationsDestinationRoleCOPY*). Escolha o serviço S3 e selecione o caso de uso Operações em Lote do S3, que aplica a política de confiança ao perfil.

   Em seguida, selecione Create policy (Criar política) para anexar a política a seguir à função. Para usar essa política, substitua os *user input placeholders* por suas próprias informações.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowBatchOperationsDestinationObjectCOPY",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:PutObjectVersionAcl",
        "s3:PutObjectAcl",
        "s3:PutObjectVersionTagging",
        "s3:PutObjectTagging",
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetObjectAcl",
        "s3:GetObjectTagging",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectVersionTagging"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-destination-bucket/*",
        "arn:aws:s3:::amzn-s3-demo-source-bucket/*",
        "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
      ]
    }
  ]
```

```
}
```

A função usa a política para conceder ao `batchoperations.s3.amazonaws.com` permissão para ler o manifesto no bucket de destino. Ele também concede permissões a objetos `GET`, listas de controle de acesso (ACLs), tags e versões no bucket do objeto de origem. Além disso, ela concede permissões a objetos `PUT`, ACLs, tags e versões no bucket do objeto de destino.

8. Na conta de origem, crie uma política de bucket para o bucket de origem que concede o perfil que você criou na etapa anterior para objetos `GET`, ACLs, tags e versões no bucket de origem. Esta etapa permite que as operações em lote do S3 obtenham objetos do bucket de origem por meio da função de confiança.

   Veja a seguir um exemplo da política de bucket para a conta de origem. Para usar essa política, substitua os *`user input placeholders`* por suas próprias informações.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowBatchOperationsSourceObjectCOPY",
      "Effect": "Allow",
      "Principal": {
        "AWS":
 "arn:aws:iam::DestinationAccountNumber:role/BatchOperationsDestinationRoleCOPY"
      },
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetObjectAcl",
        "s3:GetObjectTagging",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectVersionTagging"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
    }
  ]
}
```

9. Depois que o relatório de inventário estiver disponível, crie um trabalho de Copiar (`CopyObject`) do Operações em Lote do S3 na conta de destino e escolha o relatório de inventário no bucket do manifesto de destino. Você precisa do ARN para o perfil do IAM que criou na conta de destino.

Para obter informações gerais sobre como criar uma tarefa, consulte Criar um trabalho de operações em lote do S3.

Consulte informações sobre a criação de um trabalho usando o console em Criar um trabalho de operações em lote do S3.

Uso de um manifesto CSV para copiar objetos entre Contas da AWS

Você pode usar o Operações em Lote do Amazon S3 para executar operações em lote de grande escala em objetos do Amazon S3. É possível usar o Operações em Lote do S3 para criar um trabalho Copiar (`CopyObject`) para copiar objetos dentro da mesma conta ou para uma conta de destino diferente.

É possível usar um manifesto CSV armazenado na conta de origem para copiar objetos nas Contas da AWS com o S3 Batch Operations. Para usar um relatório de inventário S3 como manifesto, consulte the section called “Uso de um relatório de inventário para copiar objetos entre Contas da AWS”.

Para ter um exemplo do formato CSV para arquivos de manifesto, consulte the section called “Criar um arquivo de manifesto”.

O procedimento a seguir mostra como configurar permissões ao usar um trabalho de Operações em Lote do S3 para copiar objetos de uma conta de origem para uma conta de destino com um arquivo de manifesto CSV armazenado na conta de origem.

Como usar um manifesto CSV para copiar objetos nas Contas da AWS

1. Crie um perfil do AWS Identity and Access Management (IAM) na conta de destino baseado na política de confiança do recurso Operações em Lote do S3. Neste procedimento, a conta de destino é a conta para a qual os objetos estão sendo copiados.

   Para obter mais informações sobre a política de confiança, consulte Política de confiança.

   Consulte mais informações sobre como criar um perfil em Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do usuário do IAM.

   Se você criar o perfil usando o console, insira um nome para o perfil (o perfil de exemplo a seguir usa o nome *`BatchOperationsDestinationRoleCOPY`*). Escolha o serviço S3 e selecione o caso de uso Operações em Lote do S3, que aplica a política de confiança ao perfil.

Em seguida, selecione Create policy (Criar política) para anexar a política a seguir à função. Para usar essa política, substitua os *user input placeholders* por suas próprias informações.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowBatchOperationsDestinationObjectCOPY",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:PutObjectVersionAcl",
        "s3:PutObjectAcl",
        "s3:PutObjectVersionTagging",
        "s3:PutObjectTagging",
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetObjectAcl",
        "s3:GetObjectTagging",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectVersionTagging"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-destination-bucket/*",
        "arn:aws:s3:::amzn-s3-demo-source-bucket/*",
        "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
      ]
    }
  ]
}
```

Com o uso da política, a função concede permissão ao `batchoperations.s3.amazonaws.com` para ler o manifesto no bucket do manifesto de origem. Ela concede permissões a objetos `GET`, listas de controle de acesso (ACLs), tags e versões no bucket do objeto de origem. Ela também concede permissões a objetos `PUT`, ACLs, tags e versões no bucket do objeto de destino.

2. Na conta de origem, crie uma política para o bucket que contém o manifesto para conceder ao perfil que você criou na etapa anterior permissões para objetos `GET` e versões no bucket do manifesto de origem.

Esta etapa permite que as Operações em Lote do S3 leiam o manifesto usando o perfil confiável. Aplique a política de bucket ao bucket que contém o manifesto.

Veja a seguir um exemplo da política de bucket para ser aplicada ao bucket do manifesto de origem. Para usar essa política, substitua os *user input placeholders* por suas próprias informações.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowBatchOperationsSourceManfiestRead",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::DestinationAccountNumber:user/ConsoleUserCreatingJob",

 "arn:aws:iam::DestinationAccountNumber:role/BatchOperationsDestinationRoleCOPY"
        ]
      },
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
    }
  ]
}
```

Esta poítica também concede ao usuário de um console que está criando uma tarefa na conta de destino as mesmas permissões no bucket do manifesto de origem por meio da mesma política de bucket.

3. Na conta de origem, crie uma política para o bucket de origem que conceda ao perfil que você criou permissões para objetos GET, ACLs, tags e versões no bucket de objeto de origem. O Operações em lote do S3 pode então obter objetos do bucket de origem por meio da função confiável.

   Veja a seguir um exemplo da política de bucket para o bucket que contém os objetos de origem. Para usar essa política, substitua os *user input placeholders* por suas próprias informações.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowBatchOperationsSourceObjectCOPY",
      "Effect": "Allow",
      "Principal": {
        "AWS":
 "arn:aws:iam::DestinationAccountNumber:role/BatchOperationsDestinationRoleCOPY"
      },
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetObjectAcl",
        "s3:GetObjectTagging",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectVersionTagging"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
    }
  ]
}
```

4. Crie um trabalho de operações em lote do S3 na conta de destino. Você precisa do nome de recurso da Amazon (ARN) para a função que criou na conta de destino. Para obter mais informações sobre como criar um trabalho, consulte Criar um trabalho de operações em lote do S3.

Usar o Operações em Lote para habilitar chaves de bucket do S3 para SSE-KMS

As chaves de bucket do S3 reduzem o custo da criptografia do lado do servidor com o AWS Key Management Service (AWS KMS) (SSE-KMS), diminuindo assim o tráfego de solicitações do Amazon S3 para o AWS KMS. Para obter mais informações, consulte Redução do custo do SSE-KMS com chaves de bucket do Amazon S3 e Configurando seu bucket para usar uma chave de bucket do S3 com SSE-KMS para novos objetos. Ao executar uma operação `CopyObject` usando a API REST, SDKs da AWS ou a AWS CLI, você pode habilitar ou desabilitar uma chave de bucket do S3 no nível do objeto adicionando o cabeçalho de solicitação `x-amz-server-side-encryption-bucket-key-enabled` com um valor `true` ou `false`.

Quando você configura uma chave de bucket do S3 para um objeto usando uma operação `CopyObject`, o Amazon S3 atualiza somente as configurações para esse objeto. As configurações da chave de bucket S3 para o bucket de destino não são alteradas. Se você enviar uma solicitação `CopyObject` para um objeto criptografado pelo AWS KMS em um bucket com as chaves de bucket do S3 habilitadas, as operações no nível do objeto vão usar automaticamente as chaves de bucket do S3, a menos que você desabilite as chaves no cabeçalho da solicitação. Se você não especificar uma chave de bucket do S3 para seu objeto, o Amazon S3 aplicará as configurações da chave de bucket do S3 para o bucket de destino ao objeto.

Para criptografar objetos existentes do Amazon S3, você pode usar o Operações em Lote do S3. É possível usar a operação Copy do Batch Operations para copiar objetos não criptografados existentes e gravá-los de volta no mesmo bucket que os objetos criptografados. Consulte mais informações em Encrypting objects with Amazon S3 Batch Operations no Blog de armazenamento da AWS.

No exemplo a seguir, você usa a operação Copiar do Operações em Lote para habilitar chaves de bucket do S3 em objetos existentes. Para obter mais informações, consulte the section called "Configuração de uma chave de bucket do S3 para um objeto".

Tópicos

- Considerações sobre o uso do Operações em Lote do S3 para criptografar objetos com chaves de bucket do S3 habilitadas
- Pré-requisitos
- Etapa 1: obter a lista de objetos usando o Amazon S3 Inventory
- Etapa 2: Filtrar sua lista de objetos com S3 Select
- Etapa 3: Configurar e executar o trabalho do S3 Batch Operations

Considerações sobre o uso do Operações em Lote do S3 para criptografar objetos com chaves de bucket do S3 habilitadas

Considere os seguintes problemas ao usar o Operações em Lote do S3 para criptografar objetos com chaves de bucket do S3 habilitadas:

- Você será cobrado por trabalhos, objetos e solicitações das Operações em Lote do S3, além de quaisquer encargos associados à operação que as Operações em Lote do S3 executa em seu nome, como transferência de dados, solicitações e outras cobranças. Para obter mais informações, consulte Definição de preço do Amazon S3.

- Se você usar um bucket versionado, cada trabalho do S3 Batch Operations executado criará novas versões criptografadas de seus objetos. Ele também mantém as versões anteriores sem chave do bucket do S3 configurada. Para excluir as versões antigas, configure uma política de expiração do ciclo de vida do S3 para versões não atuais, conforme descrito em Elementos de configuração do ciclo de vida.
- A operação de cópia cria novos objetos com novas datas de criação, o que pode afetar ações do ciclo de vida, como arquivamento. Se você copiar todos os objetos em seu bucket, todas as novas cópias terão datas de criação idênticas ou semelhantes. Para identificar esses objetos e criar regras de ciclo de vida diferentes para vários subconjuntos de dados, considere o uso de tags de objeto.

Pré-requisitos

Antes de configurar os objetos para usar uma chave de bucket do S3, consulte Alterações na observação antes de habilitar uma chave de bucket do S3.

Para usar esse exemplo, é necessário ter uma Conta da AWS e pelo menos um bucket do S3 para manter os arquivos de trabalho e os resultados criptografados. Você também pode achar grande parte da documentação existente do S3 Batch Operations útil, incluindo os seguintes tópicos:

- Conceitos básicos sobre operações em lote do S3
- Criar um trabalho de operações em lote do S3
- Operações suportadas pelo S3 Batch Operations
- Gerenciar trabalhos de operações em lote do S3

Etapa 1: obter a lista de objetos usando o Amazon S3 Inventory

Para começar, identifique o bucket do S3 que contém os objetos a serem criptografados e obtenha uma lista de seu conteúdo. Um relatório do Amazon S3 Inventory é a maneira mais conveniente e acessível de fazer isso. O relatório fornece a lista dos objetos em um bucket, juntamente com os metadados associados. Nessa etapa, o bucket de origem é o bucket inventariado, e o bucket de destino é o bucket onde você armazena o arquivo de relatório de inventário. Para obter mais informações sobre os buckets de origem e destino do inventário do Amazon S3, consulte Catalogar e analisar seus dados com o Inventário S3.

A maneira mais fácil de configurar um inventário é usando o AWS Management Console. Mas você também pode usar a API REST, AWS Command Line Interface (AWS CLI) ou AWS SDKs.

Antes de seguir essas etapas, faça login no console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/. Se você encontrar erros de permissão negada, adicione uma política de bucket ao bucket de destino. Para obter mais informações, consulte Conceder permissões para o Inventário do S3 e análises do S3.

Para obter uma lista de objetos usando o S3 Inventory

1. Abra o console do Amazon S3, em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, selecione Buckets e escolha um bucket que contém objetos para criptografar.
3. Na guia Management (Gerenciamento), navegue para a seção Inventory configurations (Configurações de inventário) e escolha Create inventory configuration (Criar configuração de inventário).
4. Dê um nome ao seu novo inventário, insira o nome do bucket S3 de destino e, opcionalmente, crie um prefixo de destino para que o Amazon S3 atribua objetos nesse bucket.
5. Em Output format (Formato de saída), escolha CSV.
6. (Opcional) Na seção Campos adicionais: opcional, selecione Criptografia e quaisquer outros campos de relatórios de seu interesse. Defina a frequência das entregas de relatório como Daily (Diariamente) para que o primeiro relatório seja entregue ao seu bucket mais cedo.
7. Selecione Create (Criar) para salvar suas configurações.

O Amazon S3 pode demorar até 48 horas para entregar o primeiro relatório, portanto, verifique quando o primeiro relatório chegar. Depois de receber seu primeiro relatório, vá para a próxima etapa para filtrar o conteúdo do relatório do Inventário S3. Se não desejar mais receber relatórios de inventário para esse bucket, exclua a configuração do S3 Inventory. Caso contrário, o Amazon S3 continuará entregando relatórios em uma programação diária ou semanal.

Uma lista de inventário não é uma única visualização point-in-time de todos os objetos. As listas de inventário são um snapshot de contínuo de itens do bucket que são consistentes no final (ou seja, a lista pode não incluir os objetos adicionados ou excluídos recentemente). A combinação do S3 Inventory e S3 Batch Operations funciona melhor quando você trabalha com objetos estáticos ou com um conjunto de objetos criado há dois ou mais dias. Para trabalhar com dados mais recentes, use a operação de API ListObjectsV2 (GET bucket) para criar a lista de objetos manualmente. Se necessário, repita o processo nos próximos dias ou até que o relatório de inventário mostre o status desejado para todos os objetos.

Etapa 2: Filtrar sua lista de objetos com S3 Select

Depois de receber o relatório do Inventário S3, você poderá filtrar o conteúdo do relatório para listar somente os objetos que não estão criptografados com chaves de bucket do S3 habilitadas. Se quiser que todos os objetos do bucket sejam criptografados com chaves de bucket do S3 habilitadas, você poderá ignorar esta etapa. No entanto, filtrar seu relatório do Inventário S3 nessa fase economiza o tempo e as despesas de criptografar novamente os objetos que já foram criptografados com chaves de bucket do S3 habilitadas.

Embora as etapas a seguir mostrem como filtrar usando o Amazon S3 Select, você também pode usar o Amazon Athena. Para decidir qual ferramenta usar, consulte o arquivo `manifest.json` de relatório do S3 Inventory. Esse arquivo lista o número de arquivos de dados associados a esse relatório. Se o número for grande, use o Amazon Athena porque ele é executado em vários objetos do S3, enquanto o S3 Select funciona em um objeto de cada vez. Consulte mais informações sobre como usar o Amazon S3 e o Athena em conjunto em Consulta do Amazon S3 Inventory com o Amazon Athena e “Using Athena” na publicação Encrypting objects with Amazon S3 Batch Operations do Blog de armazenamento da AWS.

Como filtrar o relatório do Inventário S3 usando o S3 Select

1. Abra o arquivo `manifest.json` do seu relatório de inventário e observe a seção `fileSchema` do JSON. Isso informa a consulta que você executa nos dados.

   O seguinte JSON é um arquivo `manifest.json` de exemplo para um inventário em formato CSV em um bucket com versionamento habilitado. Dependendo de como você configurou seu relatório de inventário, seu manifesto pode parecer diferente.

```
  {
    "sourceBucket": "batchoperationsdemo",
    "destinationBucket": "arn:aws:s3:::amzn-s3-demo-destination-bucket",
    "version": "2021-05-22",
    "creationTimestamp": "1558656000000",
    "fileFormat": "CSV",
    "fileSchema": "Bucket, Key, VersionId, IsLatest, IsDeleteMarker,
 BucketKeyStatus",
    "files": [
      {
        "key": "demoinv/batchoperationsdemo/DemoInventory/data/009a40e4-
f053-4c16-8c75-6100f8892202.csv.gz",
        "size": 72691,
        "MD5checksum": "c24c831717a099f0ebe4a9d1c5d3935c"
```

```
      }
    ]
}
```

Se o versionamento não estiver ativado no bucket, ou se você optar por executar o relatório para as versões mais recentes, o `fileSchema` é `Bucket`, `Key` e `BucketKeyStatus`.

Se o versionamento estiver habilitado, dependendo de como você configurou o relatório de inventário, o `fileSchema` poderá incluir o seguinte: `Bucket`, `Key`, `VersionId`, `IsLatest`, `IsDeleteMarker`, `BucketKeyStatus`. Portanto, preste atenção às colunas 1, 2, 3 e 6 ao executar a consulta.

As Operações em Lote do S3 precisam do bucket, da chave e do ID da versão como entradas para executar o trabalho, além do campo pelo qual pesquisar, que é o `BucketKeyStatus`. Você não precisa do campo `VersionID`, mas é útil especificar o campo `VersionID` quando você opera em um bucket com versionamento. Para obter mais informações, consulte Trabalhar com objetos em um bucket com versionamento habilitado.

2. Localize os arquivos de dados para o relatório de inventário. O objeto `manifest.json` lista os arquivos de dados em files (arquivos).
3. Depois de localizar e selecionar o arquivo de dados no console do S3, escolha Actions (Ações) e, em seguida, Query with S3 Select (Consulta com o S3 Select).
4. Mantenha os campos predefinidos CSV, Comma (Vírgula) e GZIP selecionados e escolha Next (Avançar).
5. Para revisar o formato do relatório de inventário antes de prosseguir, escolha Show file preview (Mostrar visualização do arquivo).
6. Insira as colunas a serem referenciadas no campo de expressão SQL. Depois, escolha Run SQL (Executar SQL). A expressão a seguir retorna as colunas 1 a 3 para todos os objetos sem chave de bucket do S3 configurada.

```
select s._1, s._2, s._3 from s3object s where s._6 = 'DISABLED'
```

Estes são resultados de exemplo.

```
batchoperationsdemo,0100059%7Ethumb.jpg,lsrtIxksLu0R0ZkYPL.LhgD5caTYn6vu
batchoperationsdemo,0100074%7Ethumb.jpg,sd2M60g6Fdazoi6D5kNARIE7KzUibmHR
batchoperationsdemo,0100075%7Ethumb.jpg,TLYESLnl1mXD5c4BwiOIinqFrktddkoL
batchoperationsdemo,0200147%7Ethumb.jpg,amufzfMi_fEw0Rs99rxR_HrDFlE.l3Y0
batchoperationsdemo,0301420%7Ethumb.jpg,9qGU2SEscL.C.c_sK89trmXYIwooABSh
```

```
      batchoperationsdemo,0401524%7Ethumb.jpg,ORnEWNuB1QhHrrYAGFsZhbyvEYJ3DUor
      batchoperationsdemo,200907200065HQ
%7Ethumb.jpg,d8LgvIVjbDR5mUVwW6pu9ahTfReyn5V4
      batchoperationsdemo,200907200076HQ
%7Ethumb.jpg,XUT25d7.gK40u_GmnupdaZg3BVx2jN40
      batchoperationsdemo,201103190002HQ
%7Ethumb.jpg,z.2sVRh0myqVi0BuIrngWlsRPQdb7qOS
```

7. Faça download dos resultados, salve-os em um formato CSV e faça seu upload para o Amazon S3 como sua lista de objetos para o trabalho do S3 Batch Operations.
8. Se você tiver vários arquivos de manifesto, execute Query woth S3 Select (Consulta com o S3 Select) neles também. Dependendo do tamanho dos resultados, você pode combinar as listas e executar um único trabalho do S3 Batch Operations ou executar cada lista como um trabalho separado. Para decidir o número de trabalhos a executar, considere o preço de executar cada trabalho do Operações em Lote do S3.

Etapa 3: Configurar e executar o trabalho do S3 Batch Operations

Agora que tem suas listas CSV filtradas de objetos do S3, você pode iniciar o trabalho do Operações em Lote do S3 para criptografar os objetos com chaves de bucket do S3 habilitadas.

Um trabalho refere-se coletivamente à lista (manifesto) de objetos fornecidos, à operação executada e aos parâmetros especificados. A maneira mais fácil de criptografar esse conjunto de objetos com chaves de bucket do S3 habilitadas é usando a operação Copiar e especificando o mesmo prefixo de destino dos objetos listados no manifesto. Em um bucket sem versionamento, essa operação substitui os objetos existentes. Em um bucket com o versionamento ativado, essa operação cria uma versão mais recente e criptografada dos objetos.

Como parte da cópia dos objetos, especifique se o Amazon S3 deve criptografar os objetos com a criptografia SSE-KMS. Esse trabalho copia os objetos para que todos os objetos mostrem uma data de criação atualizada após a conclusão, independentemente de quando você os adicionou originalmente ao Amazon S3. Especifique também as outras propriedades do seu conjunto de objetos como parte do trabalho do S3 Batch Operations, incluindo tags de objeto e classe de armazenamento.

Subetapas

- Definir sua política do IAM
- Configurar sua função do IAM do Batch Operations

- Habilitar chaves de bucket do S3 para um bucket existente
- Criar seu trabalho do Batch Operations
- Executar seu trabalho do Batch Operations

Definir sua política do IAM

1. Abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação à esquerda, escolha Política e Criar política.
3. Selecione a guia JSON. SelecioneEdit policy (Editar política) e adicione a política do IAM de exemplo que aparece no bloco de código a seguir.

   Depois de copiar o exemplo de política no console do IAM, substitua o seguinte:

   a. Substitua *amzn-s3-demo-source-bucket* pelo nome do bucket de origem para copiar objetos dele.
   b. Substitua *amzn-s3-demo-destination-bucket* pelo nome do bucket de destino para copiar objetos nele.
   c. Substitua *amzn-s3-demo-manifest-bucket*/*manifest-key* pelo nome do objeto de manifesto.
   d. Substitua *amzn-s3-demo-completion-report-bucket* pelo nome do bucket onde deseja salvar os relatórios de conclusão.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CopyObjectsToEncrypt",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:PutObjectTagging",
        "s3:PutObjectAcl",
        "s3:PutObjectVersionTagging",
        "s3:PutObjectVersionAcl",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
```

```
        "s3:GetObjectVersionAcl",
        "s3:GetObjectVersionTagging"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-source-bucket/*",
        "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
      ]
    },
    {
      "Sid": "ReadManifest",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-manifest-bucket/manifest-key"
    },
    {
      "Sid": "WriteReport",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*"
    }
  ]
}
```

4. Escolha Next: Tags (Próximo: tags).
5. Adicione quaisquer tags desejadas (opcional) e escolha Next: Review (Próximo: Revisão).
6. Adicione um nome para a política e, opcionalmente, uma descrição. Em seguida, escolha Create policy (Criar política).
7. Selecione Review policy (Revisar política) e, em seguida, escolha, Save changes (Salvar alterações).
8. Com sua política do S3 Batch Operations agora concluída, o console retorna você à página Policies (Políticas) do IAM. Filtre o nome da política, escolha o botão à esquerda do nome da política, escolha o botão Policy actions (Ações da política) e escolha Attach (Anexar).

   Para anexar a política recém-criada a uma função do IAM, selecione os usuários, grupos ou funções apropriados em sua conta e escolha Attach policy (Anexar política). Isso levará você de volta ao console do IAM.

Configurar sua função do IAM do Batch Operations

1. No painel de navegação do console do IAM, selecione Perfis e escolha Criar perfil.
2. Selecione AWS service (Serviço da AWS), S3 e Operações em Lote do S3). Então, escolha Próximo: Permissões.
3. Comece a inserir o nome da política do IAM que acabou de criar. Marque a caixa de seleção ao lado do nome da política quando ela for exibida e escolha Next: Tags (Próximo: Tags).
4. (Opcional) Adicione tags ou mantenha os campos de chave e valor em branco para este exercício. Selecione Next: Review.
5. Insira um nome de função e aceite a descrição padrão ou adicione a sua própria. Selecione Create role.
6. Certifique-se de que o usuário que está criando o trabalho tenha as permissões no exemplo a seguir.

   Substitua *account-id* por seu ID da Conta da AWS e *IAM-role-name* pelo nome que você planeja aplicar ao perfil do IAM que você criará na etapa de criação do trabalho das Operações em Lote posteriormente. Para obter mais informações, consulte Conceder permissões para operações em lote.

```
{
"Sid": "AddIamPermissions",
"Effect": "Allow",
"Action": [
"iam:GetRole",
"iam:PassRole"
],
"Resource": "arn:aws:iam::account-id:role/IAM-role-name"
}
```

Habilitar chaves de bucket do S3 para um bucket existente

1. Abra o console do Amazon S3, em https://console.aws.amazon.com/s3/.
2. Na lista Buckets, escolha o bucket para o qual você deseja ativar uma chave de bucket do S3.
3. Escolha Properties (Propriedades).
4. Em Default encryption (Criptografia padrão), escolha Edit (Editar).

5. Em Tipo de criptografia, você pode escolher entre Chaves gerenciadas do Amazon S3 (SSE-S3) e Chave do AWS Key Management Service (SSE-KMS).
6. Se você escolheu chave do AWS Key Management Service (SSE-KMS), em AWS KMS key, poderá especificar a chave do AWS KMS por meio de uma das opções a seguir.

   - Para selecionar entre uma lista de chaves do KMS disponíveis, selecione Escolher entre suas chaves do AWS KMS. Na lista de chaves disponíveis, selecione uma chave do KMS de criptografia simétrica na mesma região que seu bucket. A chave gerenciada pela AWS (`aws/s3`) e as chaves gerenciadas pelo cliente são exibidas na lista.
   - Para inserir o ARN da chave do KMS, selecione Inserir ARN da chave do AWS KMS e insira o ARN da chave do KMS no campo exibido.
   - Para criar uma chave gerenciada pelo cliente no console do AWS KMS, selecione Criar uma chave do KMS.
7. Em Bucket key (Chave do bucket), escolha Enable (Habilitar) e, em seguida, escolha Save changes (Salvar alterações).

Agora que a chave de bucket do S3 está habilitada no nível do bucket, os objetos carregados, modificados ou copiados nesse bucket herdarão essa configuração de criptografia por padrão. Isso inclui objetos copiados usando Operações em Lote do Amazon S3.

Criar seu trabalho do Batch Operations

1. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação, escolha S3 Batch Operations e, em seguida, escolha Create Job (Criar trabalho).
3. Selecione a Region (Região) onde você armazena seus objetos e escolha CSV como o tipo de manifesto.
4. Insira o caminho ou navegue para o arquivo de manifesto CSV criado anteriormente a partir dos resultados do S3 Select (ou Athena). Se o manifesto contiver IDs de versão, marque essa caixa. Escolha Next (Próximo).
5. Selecione a operação Copy (Copiar) e escolha o bucket de destino da cópia. Você pode manter a criptografia no lado do servidor desabilitada. Desde que o destino do bucket tenha o recurso de chaves de bucket do S3 habilitado, a operação de cópia aplicará chaves de bucket do S3 no bucket de destino.

6. (Opcional) Escolha uma classe de armazenamento e os outros parâmetros conforme desejado. Os parâmetros especificados nesta etapa se aplicam a todas as operações executadas nos objetos listados no manifesto. Escolha Próximo.
7. Para a criptografia no lado do servidor, siga estas etapas:

   a. Em Criptografia do lado do servidor, selecione uma das seguintes opções:

      - Para manter as configurações de bucket para a criptografia padrão de objetos no lado do servidor ao armazená-los no Amazon S3, selecione Não especificar uma chave de criptografia. Desde que o destino do bucket tenha o recurso de chaves de bucket do S3 ativado, a operação de cópia aplicará uma chave de bucket do S3 ao bucket de destino.

        > **Note**
        >
        > Se a política de bucket para o destino especificado exigir que os objetos sejam criptografados antes de armazená-los no Amazon S3, você deverá especificar uma chave de criptografia. Caso contrário, ocorrerá uma falha na cópia de objetos no destino.

      - Para criptografar objetos antes de armazená-los no Amazon S3, selecione Especificar uma chave de criptografia.

   b. Em Configurações de criptografia, se você selecionar Especificar uma chave de criptografia, deverá escolher Usar configurações do bucket de destino para criptografia padrão ou Substituir configurações do bucket de destino para criptografia padrão.

   c. Se você selecionar Substituir configurações do bucket de destino para criptografia padrão, deverá definir as configurações de criptografia a seguir.

      i. Em Tipo de criptografia, você deve escolher Chaves gerenciadas do Amazon S3 (SSE-S3) ou Chave do AWS Key Management Service (SSE-KMS). A SSE-S3 usa uma das criptografias de bloco mais fortes: o padrão de criptografia avançada de 256 bits (AES-256) para criptografar cada objeto. A SSE-KMS oferece mais controle sobre sua chave. Para obter mais informações, consulte Usar a criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3) e Usar criptografia do lado do servidor com o AWS KMS (SSE-KMS).

      ii. Se você selecionar chave do AWS Key Management Service (SSE-KMS), em AWS KMS key, poderá especificar sua AWS KMS key por meio de uma das opções a seguir.

- Para escolher em uma lista de chaves do KMS disponíveis, selecione Escolher entre suas AWS KMS keys e, depois, escolha uma chave do KMS de criptografia simétrica na mesma região que seu bucket. A chave gerenciada pela AWS (`aws/s3`) e as chaves gerenciadas pelo cliente são exibidas na lista.
- Para inserir o ARN da chave do KMS, selecione Inserir ARN da chave do AWS KMS e insira o ARN da chave do KMS no campo exibido.
- Para criar uma chave gerenciada pelo cliente no console do AWS KMS, selecione Criar uma chave do KMS.

iii. Em Bucket key (Chave do bucket), escolha Enable (Ativar). A operação de cópia aplicará uma chave do bucket do S3 no bucket de destino.

8. Dê uma descrição ao seu trabalho (ou mantenha o padrão), defina seu nível de prioridade, escolha um tipo de relatório e especifique o Path to completion report destination (Caminho para destino do relatório de conclusão).
9. Na seção Permissions (Permissões), certifique-se de escolher a função do IAM do Batch Operations definida anteriormente. Escolha Next (Próximo).
10. Em Review (Revisão), verifique as configurações. Se precisar fazer alterações, escolha Previous (Anterior). Depois de confirmar as configurações do Batch Operations, escolha Create job (Criar trabalho).

    Para obter mais informações, consulte Criar um trabalho de operações em lote do S3.

Executar seu trabalho do Batch Operations

O assistente de configuração retorna você automaticamente à seção S3 Batch Operations do console do Amazon S3. Suas novas transições de trabalho do estado New (Novo) para o estado Preparing (Preparação) como S3 inicia o processo. Durante o estado de preparação, o S3 lê o manifesto do trabalho, verifica se há erros e calcula o número de objetos.

1. Escolha o botão de atualização no console do Amazon S3 para verificar o progresso. Dependendo do tamanho do manifesto, a leitura pode levar minutos ou horas.
2. Quando o S3 termina de ler o manifesto do trabalho, o trabalho é movido para o estado Awaiting your confirmation (Aguardando sua confirmação). Escolha o botão de opção à esquerda da ID do trabalho e escolha Run job (Executar trabalho).
3. Verifique as configurações do trabalho e escolha Run job (Executar trabalho) no canto inferior direito.

Depois que o trabalho começar a ser executado, você poderá escolher o botão de atualizar para verificar o andamento na exibição do painel do console ou selecionando o trabalho específico.

4. Quando o trabalho é concluído, você pode exibir as contagens de objetos Successful (Com êxito) e Failed (Com falha) para confirmar que tudo foi executado conforme esperado. Se você ativou relatórios de trabalhos, verifique o relatório do trabalho para saber a causa exata de qualquer operação com falha.

   Você também pode executar essas etapas usando a AWS CLI, AWS SDKs ou a API REST do Amazon S3. Para obter mais informações sobre como rastrear o status de um trabalho e os relatórios de conclusão, consulte Monitoramento de relatórios de status e conclusão.

Para obter exemplos que mostram a operação de cópia com tags usando a AWS CLI e o AWS SDK para Java, consulte Criar um trabalho do Operações em lote com tags de trabalho usadas para rotulagem.

Invocar função do AWS Lambda

Você pode usar o Operações em Lote do Amazon S3 para executar operações em lote de grande escala em objetos do Amazon S3. A operação do Operações em Lote da função Invocar do AWS Lambda inicia as funções do AWS Lambda para executar ações personalizadas em objetos que estão listados em um manifesto. Esta seção descreve como criar uma função do Lambda para uso com as operações em lote do S3 e como criar um trabalho para chamar a função. O trabalho de Operações em lote do S3 usa a operação `LambdaInvoke` para executar uma função do Lambda em cada objeto listado em um manifesto.

Você pode trabalhar com o Operações em Lote do S3 usando o console do Amazon S3, a AWS Command Line Interface (AWS CLI), SDKs da AWS ou a API REST do Amazon S3. Para obter mais informações sobre como usar o Lambda, consulte Conceitos básicos do AWS Lambda no Guia do desenvolvedor do AWS Lambda.

As seções a seguir explicam como começar a usar as operações em lote do S3 com o Lambda.

Tópicos

- Usar o Lambda com o Operações em Lote
- Criar uma função do Lambda para uso com operações em lote do S3
- Criar um trabalho de operações em lote do S3 que chama uma função do Lambda
- Fornecer informações em nível de tarefa em manifestos do Lambda

- Tutorial Operações em lote do S3

Usar o Lambda com o Operações em Lote

Ao usar o S3 Batch Operations com o AWS Lambda, crie novas funções do Lambda especificamente para uso com o S3 Batch Operations. Não é possível reutilizar funções baseadas em eventos do Amazon S3 existentes com operações em lote do S3. As funções de eventos só podem receber mensagens; elas não retornam mensagens. As funções do Lambda usadas com operações em lote do S3 devem aceitar e retornar mensagens. Para obter mais informações sobre como usar o Lambda com eventos do Amazon S3, consulte Uso do AWS Lambda com o Amazon S3 no Guia do desenvolvedor do AWS Lambda.

Crie um trabalho de operações em lote do S3 que chame a função do Lambda. O trabalho executa a mesma função do Lambda em todos os objetos listados no manifesto. É possível controlar quais versões da função do Lambda usar durante o processamento dos objetos no manifesto. As operações em lote do S3 são compatíveis com nomes de recursos da Amazon (ARNs) não qualificados, aliases e versões específicas. Para obter mais informações, consulte Introdução ao versionamento do AWS Lambda no Guia do desenvolvedor do AWS Lambda.

Se você fornecer ao trabalho de operações em lote do S3 um ARN de função que usa um alias ou o qualificador `$LATEST`, e atualizar a versão indicada por um deles, as operações em lote do S3 começarão a chamar a nova versão dessa função do Lambda. Isso pode ser útil quando você quer atualizar a funcionalidade durante um trabalho grande. Se você não quer que o Operações em Lote do S3 altere a versão usada, forneça a versão específica no parâmetro `FunctionARN` ao criar o trabalho.

Um único trabalho do AWS Lambda com o recurso Operações em Lote do S3 pode comportar um manifesto com até 20 bilhões de objetos.

Usar o Lambda e o Operações em Lote com buckets de diretório

Os buckets de diretório são um tipo de bucket do Amazon S3 projetado para workloads ou aplicações essenciais à performance que requerem latência consistente inferior a dez milissegundos. Para obter mais informações, consulte Directory buckets.

Há requisitos especiais para usar a funcionalidade Operações em Lote para invocar funções do Lambda que atuam em buckets de diretório. Por exemplo, você deve estruturar a solicitação do Lambda usando um esquema JSON atualizado e especificar InvocationSchemaVersion 2.0 (não 1.0) ao criar o trabalho. Esse esquema atualizado permite que você especifique pares

opcionais de chave e valor para UserArguments, que você pode usar para modificar determinados parâmetros de funções do Lambda existentes. Consulte mais informações em Automate object processing in Amazon S3 directory buckets with S3 Batch Operations and AWS Lambda no Blog de armazenamento da AWS.

Códigos de resultado e resposta

A funcionalidade Operações em Lote do S3 invoca a função do Lambda com uma ou mais chaves, cada uma com um `TaskID` associado. A funcionalidade Operações em Lote do S3 espera um código de resultado por chave das funções do Lambda. Todos os IDs de tarefas enviados na solicitação que não forem retornados com um código de resultado por chave receberão o código de resultado do campo `treatMissingKeysAs`. `treatMissingKeysAs` é um campo de solicitação opcional e o padrão é `TemporaryFailure`. A tabela a seguir contém os outros códigos de resultado e valores possíveis para o campo `treatMissingKeysAs`.

Código de resposta	Descrição
`Succeeded`	A tarefa foi concluída normalmente. Se você solicitou um relatório de conclusão do trabalho, a string do resultado da tarefa será incluída no relatório.
`TemporaryFailure`	A tarefa sofreu uma falha temporária e será redirecionada antes da conclusão do trabalho. A string de resultado é ignorada. Se esse for o redirecionamento final, a mensagem de erro será incluída no relatório final.
`PermanentFailure`	A tarefa sofreu uma falha permanente. Se você solicitou um relatório de conclusão do trabalho, a tarefa será marcada como `Failed` e incluirá a string da mensagem de erro. As strings de resultado de tarefas com falha são ignoradas.

Criar uma função do Lambda para uso com operações em lote do S3

Essa seção fornece um exemplo de permissões do AWS Identity and Access Management (IAM) que devem ser usadas com a função do Lambda. Ela também contém um exemplo de função do Lambda

para uso com operações em lote do S3. Se você nunca criou uma função do Lambda antes, consulte Tutorial: Como usar um trigger do Amazon S3 para invocar uma função do AWS Lambda no Guia do desenvolvedor do AWS Lambda.

Crie funções do Lambda especificamente para uso com as operações em lote do S3. Não é possível reutilizar funções do Lambda baseadas em eventos do Amazon S3, pois as funções do Lambda que são usadas para o Operações em Lote do S3 devem aceitar e mostrar campos de dados especiais.

> **Important**
>
> Funções do AWS Lambda escritas em Java aceitam interfaces de manipulador RequestHandler ou RequestStreamHandler. No entanto, para oferecer suporte ao formato de solicitação e resposta do S3 Batch Operations, o AWS Lambda requer a interface `RequestStreamHandler` para serialização e desserialização personalizadas de uma solicitação e resposta. Essa interface permite que o Lambda passe um InputStream e um OutputStream para o método Java `handleRequest`.
>
> Use a interface `RequestStreamHandler` ao usar funções do Lambda com operações em lote do S3. Se você usar uma interface `RequestHandler`, o trabalho em lote falhará com "Invalid JSON returned in Lambda payload (JSON inválido retornado no payload do Lambda)" no relatório de conclusão.
>
> Para obter mais informações, consulte Interfaces do manipulador no Guia do usuário do AWS Lambda.

Exemplo de permissões do IAM

Veja a seguir exemplos das permissões do IAM necessárias para usar uma função do Lambda com operações em lote do S3.

Example Política de confiança de operações em lote do S3

Veja a seguir um exemplo da política de confiança que pode ser usada para a função do IAM de operações em lote. Essa função do IAM é especificada quando você cria o trabalho e concede às operações em lote permissão para assumir a função do IAM.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
```

```
            "Principal": {
                "Service": "batchoperations.s3.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Example Política do IAM do Lambda

Veja a seguir um exemplo de uma política do IAM que concede permissão às operações em lote do S3 para chamar a função do Lambda e ler o manifesto de entrada.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "BatchOperationsLambdaPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion",
                "s3:PutObject",
                "lambda:InvokeFunction"
            ],
            "Resource": "*"
        }
    ]
}
```

Exemplo de solicitação e resposta

Esta seção fornece exemplos de solicitação e resposta para a função do Lambda.

Example Solicitação

Veja a seguir um exemplo do JSON de uma solicitação para a função do Lambda.

```
{
    "invocationSchemaVersion": "1.0",
    "invocationId": "YXNkbGZqYWRmaiBhc2RmdW9hZHNmZGpmaGFzbGtkaGZza2RmaAo",
    "job": {
        "id": "f3cc4f60-61f6-4a2b-8a21-d07600c373ce"
```

```
    },
    "tasks": [
        {
            "taskId": "dGFza2lkZ29lc2hlcmUK",
            "s3Key": "customerImage1.jpg",
            "s3VersionId": "1",
            "s3BucketArn": "arn:aws:s3:us-east-1:0123456788:amzn-s3-demo-bucket1"
        }
    ]
}
```

Example Resposta

Veja a seguir um exemplo do JSON de uma resposta para a função do Lambda.

```
{
  "invocationSchemaVersion": "1.0",
  "treatMissingKeysAs" : "PermanentFailure",
  "invocationId" : "YXNkbGZqYWRmaiBhc2RmdW9hZHNmZGpmaGFzbGtkaGZza2RmaAo",
  "results": [
    {
      "taskId": "dGFza2lkZ29lc2hlcmUK",
      "resultCode": "Succeeded",
      "resultString": "[\"Mary Major", \"John Stiles\"]"
    }
  ]
}
```

Exemplo de função do Lambda para operações em lote do S3

O exemplo Lambda em Python a seguir remove um marcador de exclusão de um objeto versionado.

Como mostra o exemplo, as chaves das operações em lote do S3 são codificadas por URL. Para usar o Amazon S3 com outros produtos da AWS, é importante que seu URL decodifique a chave passada pelo S3 Batch Operations.

```
import logging
from urllib import parse
import boto3
from botocore.exceptions import ClientError

logger = logging.getLogger(__name__)
logger.setLevel("INFO")
```

```
s3 = boto3.client("s3")


def lambda_handler(event, context):
    """
    Removes a delete marker from the specified versioned object.

    :param event: The S3 batch event that contains the ID of the delete marker
                  to remove.
    :param context: Context about the event.
    :return: A result structure that Amazon S3 uses to interpret the result of the
             operation. When the result code is TemporaryFailure, S3 retries the
             operation.
    """
    # Parse job parameters from Amazon S3 batch operations
    invocation_id = event["invocationId"]
    invocation_schema_version = event["invocationSchemaVersion"]

    results = []
    result_code = None
    result_string = None

    task = event["tasks"][0]
    task_id = task["taskId"]

    try:
        obj_key = parse.unquote(task["s3Key"], encoding="utf-8")
        obj_version_id = task["s3VersionId"]
        bucket_name = task["s3BucketArn"].split(":")[-1]

        logger.info(
            "Got task: remove delete marker %s from object %s.", obj_version_id,
 obj_key
        )

        try:
            # If this call does not raise an error, the object version is not a delete
            # marker and should not be deleted.
            response = s3.head_object(
                Bucket=bucket_name, Key=obj_key, VersionId=obj_version_id
            )
            result_code = "PermanentFailure"
            result_string = (
```

```
                f"Object {obj_key}, ID {obj_version_id} is not " f"a delete marker."
            )

            logger.debug(response)
            logger.warning(result_string)
        except ClientError as error:
            delete_marker = error.response["ResponseMetadata"]["HTTPHeaders"].get(
                "x-amz-delete-marker", "false"
            )
            if delete_marker == "true":
                logger.info(
                    "Object %s, version %s is a delete marker.", obj_key,
obj_version_id
                )
                try:
                    s3.delete_object(
                        Bucket=bucket_name, Key=obj_key, VersionId=obj_version_id
                    )
                    result_code = "Succeeded"
                    result_string = (
                        f"Successfully removed delete marker "
                        f"{obj_version_id} from object {obj_key}."
                    )
                    logger.info(result_string)
                except ClientError as error:
                    # Mark request timeout as a temporary failure so it will be
retried.
                    if error.response["Error"]["Code"] == "RequestTimeout":
                        result_code = "TemporaryFailure"
                        result_string = (
                            f"Attempt to remove delete marker from  "
                            f"object {obj_key} timed out."
                        )
                        logger.info(result_string)
                    else:
                        raise
            else:
                raise ValueError(
                    f"The x-amz-delete-marker header is either not "
                    f"present or is not 'true'."
                )
    except Exception as error:
        # Mark all other exceptions as permanent failures.
        result_code = "PermanentFailure"
```

```
        result_string = str(error)
        logger.exception(error)
    finally:
        results.append(
            {
                "taskId": task_id,
                "resultCode": result_code,
                "resultString": result_string,
            }
        )
    return {
        "invocationSchemaVersion": invocation_schema_version,
        "treatMissingKeysAs": "PermanentFailure",
        "invocationId": invocation_id,
        "results": results,
    }
```

Criar um trabalho de operações em lote do S3 que chama uma função do Lambda

Ao criar um trabalho de operações em lote do S3 para chamar uma função do Lambda, forneça o seguinte:

- O ARN da função do Lambda (que pode incluir o alias da função ou o número de uma versão específica)
- Uma função do IAM com permissão para invocar a função
- O parâmetro de ação `LambdaInvokeFunction`

Para obter mais informações sobre como criar um trabalho de operações em lote do S3, consulte Criar um trabalho de operações em lote do S3 e Operações suportadas pelo S3 Batch Operations.

O exemplo a seguir cria um trabalho do Operações em Lote do S3 que invoca uma função do Lambda usando a AWS CLI. Para usar esse exemplo, substitua os *`user input placeholders`* por suas próprias informações.

```
aws s3control create-job
    --account-id account-id
```

```
    --operation  '{"LambdaInvoke": { "FunctionArn": "arn:aws:lambda:region:account-
id:function:LambdaFunctionName" } }'
    --manifest '{"Spec":{"Format":"S3BatchOperations_CSV_20180820","Fields":
["Bucket","Key"]},"Location":{"ObjectArn":"arn:aws:s3:::amzn-s3-demo-manifest-
bucket","ETag":"ManifestETag"}}'
    --report '{"Bucket":"arn:aws:s3:::amzn-s3-demo-
bucket","Format":"Report_CSV_20180820","Enabled":true,"Prefix":"ReportPrefix","ReportScope":"Al
    --priority 2
    --role-arn arn:aws:iam::account-id:role/BatchOperationsRole
    --region region
    --description "Lambda Function"
```

Fornecer informações em nível de tarefa em manifestos do Lambda

Ao usar funções do AWS Lambda com o Operações em Lote do S3, talvez você queira que dados adicionais acompanhem cada tarefa em que são operados. Por exemplo, você pode querer fornecer uma chave de objeto de origem e uma nova chave de objeto. A função do Lambda pode copiar a chave de origem em um novo bucket do S3 com um novo nome. Por padrão, o Operações em Lote permite especificar apenas o bucket de destino e uma lista de chaves de origem no manifesto de entrada do trabalho. Os exemplos a seguir descrevem como você pode incluir dados adicionais no manifesto para poder executar funções do Lambda mais complexas.

Para especificar parâmetros por chave no manifesto de operações em lote do S3 para usar no código da função do Lambda, use o seguinte formato JSON codificado por URL. O campo `key` é passado para a função do Lambda como se fosse uma chave de objeto do Amazon S3. Porém, ele pode ser interpretado pela função do Lambda como contendo outros valores ou várias chaves, conforme mostrado nos exemplos a seguir.

> **Note**
>
> O número máximo de caracteres para o campo `key` no manifesto é 1.024.

Example – Manifesto que substitui as “chaves do Amazon S3” por strings JSON

A versão codificada por URL deve ser fornecida para operações em lote do S3.

```
amzn-s3-demo-bucket,{"origKey": "object1key", "newKey": "newObject1Key"}
amzn-s3-demo-bucket,{"origKey": "object2key", "newKey": "newObject2Key"}
amzn-s3-demo-bucket,{"origKey": "object3key", "newKey": "newObject3Key"}
```

Example – Manifesto codificado por URL

Essa versão codificada por URL deve ser fornecida para operações em lote do S3. A versão não codificada em URL não funciona.

```
amzn-s3-demo-bucket,%7B%22origKey%22%3A%20%22object1key%22%2C%20%22newKey%22%3A
%20%22newObject1Key%22%7D
amzn-s3-demo-bucket,%7B%22origKey%22%3A%20%22object2key%22%2C%20%22newKey%22%3A
%20%22newObject2Key%22%7D
amzn-s3-demo-bucket,%7B%22origKey%22%3A%20%22object3key%22%2C%20%22newKey%22%3A
%20%22newObject3Key%22%7D
```

Example função do Lambda com formato de manifesto que grava resultados no relatório de trabalho

Esse exemplo de manifesto codificado em URL contém chaves de objeto delimitadas por pipe para que a função do Lambda a seguir analise.

```
amzn-s3-demo-bucket,object1key%7Clower
amzn-s3-demo-bucket,object2key%7Cupper
amzn-s3-demo-bucket,object3key%7Creverse
amzn-s3-demo-bucket,object4key%7Cdelete
```

Essa função do Lambda mostra como analisar uma tarefa delimitada por pipe que é codificada no manifesto do Operações em Lote do S3. A tarefa indica qual operação de revisão é aplicada ao objeto especificado.

```
import logging
from urllib import parse
import boto3
from botocore.exceptions import ClientError

logger = logging.getLogger(__name__)
logger.setLevel("INFO")

s3 = boto3.resource("s3")


def lambda_handler(event, context):
    """
    Applies the specified revision to the specified object.

    :param event: The Amazon S3 batch event that contains the ID of the object to
```

```
                revise and the revision type to apply.
    :param context: Context about the event.
    :return: A result structure that Amazon S3 uses to interpret the result of the
             operation.
    """
    # Parse job parameters from Amazon S3 batch operations
    invocation_id = event["invocationId"]
    invocation_schema_version = event["invocationSchemaVersion"]

    results = []
    result_code = None
    result_string = None

    task = event["tasks"][0]
    task_id = task["taskId"]
    # The revision type is packed with the object key as a pipe-delimited string.
    obj_key, revision = parse.unquote(task["s3Key"], encoding="utf-8").split("|")
    bucket_name = task["s3BucketArn"].split(":")[-1]

    logger.info("Got task: apply revision %s to %s.", revision, obj_key)

    try:
        stanza_obj = s3.Bucket(bucket_name).Object(obj_key)
        stanza = stanza_obj.get()["Body"].read().decode("utf-8")
        if revision == "lower":
            stanza = stanza.lower()
        elif revision == "upper":
            stanza = stanza.upper()
        elif revision == "reverse":
            stanza = stanza[::-1]
        elif revision == "delete":
            pass
        else:
            raise TypeError(f"Can't handle revision type '{revision}'.")

        if revision == "delete":
            stanza_obj.delete()
            result_string = f"Deleted stanza {stanza_obj.key}."
        else:
            stanza_obj.put(Body=bytes(stanza, "utf-8"))
            result_string = (
                f"Applied revision type '{revision}' to " f"stanza {stanza_obj.key}."
            )
```

```
        logger.info(result_string)
        result_code = "Succeeded"
    except ClientError as error:
        if error.response["Error"]["Code"] == "NoSuchKey":
            result_code = "Succeeded"
            result_string = (
                f"Stanza {obj_key} not found, assuming it was deleted "
                f"in an earlier revision."
            )
            logger.info(result_string)
        else:
            result_code = "PermanentFailure"
            result_string = (
                f"Got exception when applying revision type '{revision}' "
                f"to {obj_key}: {error}."
            )
            logger.exception(result_string)
    finally:
        results.append(
            {
                "taskId": task_id,
                "resultCode": result_code,
                "resultString": result_string,
            }
        )
    return {
        "invocationSchemaVersion": invocation_schema_version,
        "treatMissingKeysAs": "PermanentFailure",
        "invocationId": invocation_id,
        "results": results,
    }
```

Tutorial Operações em lote do S3

O tutorial a seguir apresenta procedimentos completos para algumas tarefas do recurso Operações em Lote com o Lambda. Nesse tutorial, você aprenderá a configurar o Operações em Lote para invocar uma função do Lambda para transcodificação em lote de vídeos armazenados em um bucket de origem do S3. A função do Lambda chama o AWS Elemental MediaConvert para transcodificar os vídeos.

- Tutorial: vídeos de transcodificação em lote com o Operações em Lote do S3

Substituir todas as tags de objeto

Você pode usar o Operações em Lote do Amazon S3 para executar operações em lote de grande escala em objetos do Amazon S3. A operação Substituir todas as tags de objeto substitui as tags de objeto em cada objeto listado no manifesto. A tag de objeto do é um par de strings chave-valor que pode ser usado para armazenar metadados sobre um objeto.

Para criar um trabalho Substituir todas as tags de objeto, forneça um conjunto de tags que pretende aplicar. As Operações em lote do Amazon S3 aplica o mesmo conjunto de tags a cada objeto. O conjunto de tags que você fornece substitui os conjuntos de tags já associados aos objetos no manifesto. O Operações em Lote do S3 não permite adicionar tags a objeto, deixando as tags existentes no lugar.

Se os objetos em seu manifesto estiverem em um bucket versionado, você pode aplicar o conjunto de tags a versões específicas de cada objeto. Para fazer isso, especifique um ID de versão para cada objeto no manifesto. Se você não incluir um ID de versão para nenhum objeto, o Operações em Lote do S3 aplica o conjunto de tags à versão mais recente de cada objeto. Para obter mais informações sobre o recurso Operações em lote, consulte Especificar um manifesto.

Consulte mais informações sobre a marcação de objetos em Categorizar seu armazenamento usando tags neste guia e em PutObjectTagging, GetObjectTagging e DeleteObjectTagging na Referência de API do Amazon Simple Storage Service.

Para criar um trabalho Substituir todas as tags de objeto usando o console, consulte Criar um trabalho de operações em lote do S3.

Restrições e limitações

Quando você usa o Operações em Lote para substituir tags de objeto, as seguintes restrições e limitações se aplicam:

- O perfil do AWS Identity and Access Management (IAM) que você especifica para executar o trabalho de operações em lote deve ter permissões para executar a operação `PutObjectTagging` subjacente. Consulte mais informações sobre as permissões necessárias em PutObjectTagging na Referência da API do Amazon Simple Storage Service.

- O Operações em Lote do S3 usa a operação PutObjectTagging do Amazon S3 para aplicar tags a cada objeto no manifesto. Todas as restrições e limitações que se aplicam à operação subjacente também se aplicam a trabalhos das Operações em lote do S3.
- Um único trabalho de substituição de todas as tags de objeto pode comportar um manifesto com até 20 bilhões de objetos.

Excluir todas as tags de objeto

Você pode usar o Operações em Lote do Amazon S3 para executar operações em lote de grande escala em objetos do Amazon S3. A operação Excluir todas as tags de objeto remove todos os conjuntos de tags de objeto do Amazon S3 atualmente associados aos objetos listados no manifesto. O Operações em Lote do S3 não permite a exclusão de tags de objeto enquanto mantém outras tags no lugar.

Se os objetos no manifesto estiverem em um bucket versionado, você poderá remover os conjuntos de tags de uma versão específica de um objeto. Para fazer isso, você deve especificar um ID de versão para cada objeto no manifesto. Se você não incluir um ID de versão para um objeto, as Operações em lote do S3 removerão o conjunto de tags da versão mais recente de cada objeto. Para obter mais informações sobre o recurso Operações em lote, consulte Especificar um manifesto.

Consulte mais detalhes sobre a marcação de objetos em Categorizar seu armazenamento usando tags neste guia e em PutObjectTagging, GetObjectTagging e DeleteObjectTagging na Referência de API do Amazon Simple Storage Service.

> **Warning**
>
> A execução deste trabalho remove todos os conjuntos de tags de objeto em cada objeto listado no manifesto.

Para usar o console a fim de criar um trabalho de Excluir todas as tags de objeto, consulte Criar um trabalho de operações em lote do S3.

Restrições e limitações

Quando você usa o Operações em Lote para excluir tags de objeto, as seguintes restrições e limitações se aplicam:

- O perfil do AWS Identity and Access Management (IAM) que você especificar para executar o trabalho deverá ter permissões para executar a operação `DeleteObjectTagging` do Amazon S3 subjacente. Para obter mais informações, consulte DeleteObjectTagging na Referência da API do Amazon Simple Storage Service.
- O Operações em Lote do S3 usam a operação DeleteObjectTagging do Amazon S3 para remover os conjuntos de tags de cada objeto no manifesto. Todas as restrições e limitações que se aplicam à operação subjacente também se aplicam a trabalhos das Operações em lote do S3.
- Um único trabalho de exclusão da marcação de objetos pode comportar um manifesto com até 20 bilhões de objetos.

Substituir lista de controle de acesso (ACL)

Você pode usar o Operações em Lote do Amazon S3 para executar operações em lote de grande escala em objetos do Amazon S3. A operação Substituir lista de controle de acesso (ACL) substitui as listas de controle de acesso (ACLs) para cada objeto listado no manifesto. Ao usar ACLs, é possível definir quem pode acessar o objeto e quais ações podem ser executadas.

> **Note**
>
> A maioria dos casos de uso modernos no Amazon S3 não exige mais o uso de ACLs. Recomendamos manter as ACLs desabilitadas, exceto em circunstâncias incomuns em que seja necessário controlar o acesso para cada objeto individualmente. Com as ACLs desabilitadas, é possível usar políticas para controlar o acesso a todos os objetos no bucket, independentemente de quem carregou os objetos para o bucket. Para obter mais informações, consulte Controlar a propriedade de objetos e desabilitar ACLs para seu bucket.

O Operações em Lote do S3 é compatível com ACLs personalizadas que você define e com ACLs pré-configuradas fornecidas pelo Amazon S3 com um conjunto predefinido de permissões de acesso.

Se os objetos em seu manifesto estiverem em um bucket versionado, é possível aplicar as ACLs a versões específicas de cada objeto. Para fazer isso, especifique um ID de versão para cada objeto no manifesto. Se você não incluir um ID de versão para um objeto, o Operações em Lote do S3 aplicará a ACL à versão mais recente do objeto.

Consulte mais informações sobre ACLs no Amazon S3 em Visão geral da lista de controle de acesso (ACL).

Bloqueio de acesso público do S3

Se quiser limitar o acesso público a todos os objetos em um bucket, recomendamos usar o Bloqueio de Acesso Público do Amazon S3 em vez de usar o Operações em Lote do S3 para aplicar ACLS. O Block Public Access pode limitar o acesso público a cada bucket ou à conta com uma única operação simples, que entra em vigor rapidamente. Esse comportamento torna o Bloqueio de Acesso Público do Amazon S3 uma melhor opção caso seu objetivo seja controlar o acesso público a todos os objetos em um bucket ou uma conta. Use o Operações em Lote do S3 somente quando precisar aplicar uma ACL personalizada a cada objeto no manifesto. Para obter mais informações sobre o S3 Block Public Access, consulte Bloquear o acesso público ao armazenamento do Amazon S3.

Propriedade de objeto do S3

Se os objetos no manifesto estiverem em um bucket que usa a configuração Aplicada pelo proprietário do bucket para Propriedade de Objetos, a operação Substituir lista de controle de acesso (ACL) poderá especificar apenas ACLs do objeto que concedem controle total ao proprietário do bucket. Nesse caso, a operação Substituir lista de controle de acesso (ACL) não pode conceder permissões de ACL de objeto a outros grupos ou Contas da AWS. Para obter mais informações, consulte Controlar a propriedade de objetos e desabilitar ACLs para seu bucket.

Restrições e limitações

Quando você usa o Operações em Lote para substituir ACLs, as seguintes restrições e limitações se aplicam:

- O perfil do AWS Identity and Access Management (IAM) especificado para executar o trabalho Substituir lista de controle de acesso (ACL) deve ter permissões para executar a operação `PutObjectAcl` subjacente do Amazon S3. Consulte mais informações sobre as permissões necessárias em PutObjectAcl na Referência da API do Amazon Simple Storage Service.
- O S3 Batch Operations usa a operação `PutObjectAcl` do Amazon S3 para aplicar a ACL especificada a cada objeto no manifesto. Portanto, todas as restrições e limitações que se aplicam à operação `PutObjectAcl` subjacente também se aplicam a trabalhos Substituir lista de controle de acesso (ACL) do Operações em Lote do S3.
- Um único trabalho de substituição da lista de controle de acesso pode comportar um manifesto com até 20 bilhões de objetos.

Restaurar objetos com operações em lote

Você pode usar o Operações em Lote do Amazon S3 para executar operações em lote de grande escala em objetos do Amazon S3. A operação Restaurar inicia solicitações de restauração dos objetos arquivados do Amazon S3 listados no manifesto. Os objetos a seguir devem ser restaurados para que possam ser acessados em tempo real:

- Objetos arquivados nas classes de armazenamento S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive
- Objetos arquivados por meio da classe de armazenamento do S3 Intelligent-Tiering nos níveis Acesso de arquivamento ou Acesso de arquivamento profundo

O uso de uma operação Restaurar (S3InitiateRestoreObjectOperation) no trabalho do Operações em Lote do S3 resulta em uma solicitação `RestoreObject` para cada objeto especificado no manifesto.

> **Important**
>
> O trabalho Restaurar só inicia a solicitação para restaurar objetos. As Operações em lote do S3 relatam o trabalho como concluído para cada objeto depois que a solicitação é iniciada para aquele objeto. O Amazon S3 não atualiza o trabalho nem o notificará quando os objetos tiverem sido restaurados. No entanto, é possível usar notificações de eventos do S3 para receber notificações quando os objetos estiverem disponíveis no Amazon S3. Para obter mais informações, consulte Notificações de eventos do Amazon S3.

Ao criar um trabalho de Restaurar os seguintes argumentos estão disponíveis:

ExpirationInDays

Esse argumento especifica por quanto tempo o objeto do S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive permanecerá disponível no Amazon S3. Os trabalhos de Restaurar voltados para objetos do S3 Glacier Flexible Retrieval e do S3 Glacier Deep Archive exigem que você defina `ExpirationInDays` como 1 ou superior.

> **Important**
>
> Não defina `ExpirationInDays` ao criar trabalhos de operação de Restaurar voltados a objetos dos níveis S3 Intelligent-Tiering Archive Access e Deep Archive Access. Os

objetos nos níveis de acesso de arquivo S3 Intelligent-Tiering não estão sujeitos a uma data de validade da restauração; portanto, especificar `ExpirationInDays` provoca uma falha na solicitação `RestoreObject`.

GlacierJobTier

O Amazon S3 pode restaurar objetos usando um destes três diferentes níveis de recuperação: `EXPEDITED`, `STANDARD` e `BULK`. No entanto, o recurso Operações em lote do S3 suporta apenas os níveis de recuperação `STANDARD` e `BULK`. Para receber mais informações sobre as diferenças entre os níveis de recuperação, consulte Noções básicas sobre as opções de recuperação de arquivos.

Para receber mais informações sobre preço para cada nível, consulte a seção Solicitações e recuperações de dados na página Definição de preço do Amazon S3.

Diferenças na restauração por meio do S3 Glacier e do S3 Intelligent-Tiering

A restauração de arquivos arquivados das classes de armazenamento S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive difere da restauração de arquivos da classe de armazenamento S3 Intelligent-Tiering nos níveis Acesso de arquivamento ou Acesso de arquivamento profundo.

- Quando você restaura do S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive, uma cópia temporária do objeto é criada. O Amazon S3 exclui essa cópia após o término do valor especificado no argumento `ExpirationInDays`. Depois que essa cópia temporária for excluída, será preciso enviar uma solicitação de restauração adicional para acessar o objeto.
- Ao restaurar objetos arquivados do S3 Intelligent-Tiering, não especifique o argumento `ExpirationInDays`. Quando você restaura um objeto do nível S3 Intelligent-Tiering Archive Access ou Deep Archive Access, o objeto faz a transição de volta ao nível S3 Intelligent-Tiering Frequent Access. Após no mínimo 90 dias consecutivos sem acesso, o objeto transita automaticamente para o nível Archive Access. Depois de um período mínimo de 180 dias consecutivos sem acesso, o objeto é movido automaticamente ao nível Deep Archive Access.
- Os trabalhos de operações em lote podem operar em objetos das classes de armazenamento S3 Glacier Flexible Retrieval e S3 Glacier Deep Archive ou em objetos dos níveis S3 Intelligent-Tiering Archive Access e Deep Archive Access. As operações em lote não podem operar nos dois tipos de objetos arquivados no mesmo trabalho. Para restaurar objetos de ambos os tipos, você deve criar trabalhos de Operações em lote separados.

Sobrepor restaurações

Se o trabalho S3InitiateRestoreObjectOperation tentar restaurar um objeto que já esteja em processo de restauração, o Operações em Lote do S3 procederá da maneira indicada a seguir.

A operação de restauração será bem-sucedida para o objeto se uma das seguintes condições for verdadeira:

- Quando comparado à solicitação de restauração já em andamento, o valor `ExpirationInDays` desse trabalho é o mesmo, e o valor `GlacierJobTier` é mais rápido.
- A solicitação de restauração anterior já foi concluída, e o objeto está disponível no momento. Nesse caso, as operações em lote atualizam a data de validade do objeto restaurado para coincidir com o valor `ExpirationInDays` especificado na solicitação de restauração em andamento.

A operação apresenta falha para o objeto se uma das seguintes condições for verdadeira:

- A solicitação de restauração já em andamento ainda não foi concluída, e a duração da restauração para esse trabalho (especificada pelo valor `ExpirationInDays`) é diferente da duração da restauração especificada na solicitação de restauração em andamento.
- O nível de restauração para esse trabalho (especificado pelo valor `GlacierJobTier`) é o mesmo ou é mais lento do que o nível especificado na solicitação de restauração em andamento.

Limitações

Os trabalhos `S3InitiateRestoreObjectOperation` têm as seguintes limitações:

- Você deve criar o trabalho na mesma região que os objetos arquivados.
- O Operações em Lote do S3 não é compatível com o nível de recuperação `EXPEDITED`.
- Um único trabalho de restauração de operações em lote pode comportar um manifesto com até 4 bilhões de objetos.

Para obter mais informações sobre a restauração de objetos, consulte Restaurar um objeto arquivado.

Retenção do Bloqueio de objetos do S3

Você pode usar o Operações em Lote do Amazon S3 para executar operações em lote de grande escala em objetos do Amazon S3. É possível usar a operação de Retenção de Bloqueio de

objetos para aplicar datas de retenção para seus objetos usando o modo de governança ou de conformidade. Esses modos de retenção aplicam níveis diferentes de proteção. É possível aplicar qualquer modo de retenção a qualquer versão de objeto. Datas de retenção, como retenções legais, impedem que um objeto seja substituído ou excluído. O Amazon S3 armazena a opção reter até a data especificada nos metadados do objeto e protege a versão especificada da versão do objeto até que o período de retenção expire.

É possível usar o Operações em Lote do S3 com o Bloqueio de Objetos para gerenciar as datas de retenção de muitos objetos do Amazon S3 de uma só vez. Especifique a lista de objetos de destino no manifesto e envie o manifesto para o Operações em Lote para conclusão. Para obter mais informações, consulte Bloqueio de objetos do S3 the section called “Períodos de retenção”.

As datas de retenção de trabalhos de operações em lote do S3 com datas de retenção é executado até que a conclusão, o cancelamento ou um estado de falha seja atingido. Recomendamos usar o Operações em Lote do S3 e a retenção do Bloqueio de Objetos do S3 ao adicionar, alterar ou remover a data de retenção de muitos objetos com uma única solicitação.

As operações em lote verificam se o bloqueio de objetos está habilitado no bucket antes de processar qualquer chave no manifesto. Para executar as operações e a validação, o Operações em Lote precisa das permissões `s3:GetBucketObjectLockConfiguration` e `s3:PutObjectRetention` em um perfil do AWS Identity and Access Management (IAM) para permitir que o Operações em Lote chame o Bloqueio de Objetos em seu nome. Para obter mais informações, consulte the section called “Considerações sobre a funcionalidade Bloqueio de Objetos”.

Consulte informações sobre como usar essa operação com a API REST em `S3PutObjectRetention` na operação CreateJob da Referência de API do Amazon Simple Storage Service.

Consulte um exemplo da AWS Command Line Interface (AWS CLI) de como usar essa operação em the section called “Usar operações em lote com retenção de bloqueio de objetos”. Para ver um exemplo de AWS SDK para Java, consulte the section called “Usar operações em lote com retenção de bloqueio de objetos”.

Restrições e limitações

Quando você usa o Operações em Lote para aplicar períodos de retenção do Bloqueio de Objetos, as seguintes restrições e limitações se aplicam:

- O Operações em Lote do S3 não faz alterações no nível doesn't bucket.

- O versionamento e o bloqueio de objetos do S3 devem ser configurados no bucket em que o trabalho é executado.
- Todos os objetos listados no manifesto devem estar no mesmo bucket.
- A operação funciona na versão mais recente do objeto, a menos que uma versão seja explicitamente especificada no manifesto.
- Você precisa da permissão `s3:PutObjectRetention` no perfil do IAM para usar um trabalho de Retenção de Bloqueio de objetos.
- A permissão `s3:GetBucketObjectLockConfiguration` do IAM é necessária para confirmar se o Bloqueio de Objetos está habilitado para o bucket do S3 no qual o trabalho está sendo realizado.
- Só é possível estender o período de retenção de objetos com datas de retenção do modo `COMPLIANCE` aplicadas, e esse período de retenção não pode ser reduzido.
- Um único trabalho de retenção do Bloqueio de Objetos do S3 pode comportar um manifesto com até 20 bilhões de objetos.

Retenção legal do Bloqueio de objetos do S3

Você pode usar o Operações em Lote do Amazon S3 para executar operações em lote de grande escala em objetos do Amazon S3. É possível usar a operação de retenção legal do Bloqueio de Objetos para colocar uma retenção legal em uma versão de objeto. Assim como a definição de um período de retenção, uma retenção legal evita que uma versão do objeto seja substituída ou excluída. Porém, uma retenção legal não tem um período de retenção associado e permanecerá em vigor até ser removida.

Você pode usar o Operações em lote do S3 com o Bloqueio de objetos para adicionar retenções legais a muitos objetos do Amazon S3 de uma só vez. Para fazer isso, especifique uma lista de objetos de destino no manifesto e envie essa lista ao Operações em Lote. O trabalho de Retenção legal do Bloqueio de Objetos do Operações em Lote do S3 é executado até a conclusão, até o cancelamento ou até que um estado de falha seja atingido.

O Operações em Lote do S3 verifica se o Bloqueio de Objetos está habilitado no bucket do S3 antes de processar qualquer objeto no manifesto. Para executar as operações de objeto e a validação no nível do bucket, o Operações em Lote do S3 precisa de `s3:PutObjectLegalHold` e `s3:GetBucketObjectLockConfiguration` em um perfil do AWS Identity and Access Management (IAM). Essas permissões possibilitam que o Operações em Lote do S3 chame o Bloqueio de Objetos do S3 em seu nome.

Ao criar um trabalho do Operações em Lote do S3 para remover a retenção legal, você só precisa especificar `Off` como o status de retenção legal. Para obter mais informações, consulte the section called “Considerações sobre a funcionalidade Bloqueio de Objetos”.

Consulte informações sobre como usar essa operação com a API REST do Amazon S3 em `S3PutObjectLegalHold` na operação CreateJob na Referência da API do Amazon Simple Storage Service.

Consulte um exemplo de como usar essa operação em Usar o AWS SDK for Java.

Restrições e limitações

Quando você usa o Operações em Lote para aplicar ou remover uma retenção legal do Bloqueio de Objetos, as seguintes restrições e limitações se aplicam:

- O Operações em Lote do S3 não faz alterações no nível doesn't bucket.
- Todos os objetos listados no manifesto devem estar no mesmo bucket.
- O versionamento e o bloqueio de objetos do S3 devem ser configurados no bucket em que o trabalho é executado.
- A operação Retenção legal do Bloqueio de Objetos funciona na versão mais recente do objeto, a menos que uma versão seja explicitamente especificada no manifesto.
- A permissão `s3:PutObjectLegalHold` é necessária no perfil do IAM para adicionar ou remover uma retenção legal de objetos.
- A permissão `s3:GetBucketObjectLockConfiguration` do IAM é necessária para confirmar se o Bloqueio de Objetos do S3 está habilitado para o bucket do S3 no qual o trabalho está sendo realizado.
- Um único trabalho de retenção jurídica do Bloqueio de Objetos do S3 pode comportar um manifesto com até 20 bilhões de objetos.

- Copiar objetos
- Invocar função do AWS Lambda
- Substituir todas as tags de objeto
- Excluir todas as tags de objeto
- Substituir lista de controle de acesso (ACL)
- Restaurar objetos com operações em lote
- Retenção do Bloqueio de objetos do S3

- Retenção legal do Bloqueio de objetos do S3
- Replicar objetos existentes com o Replicação em Lote

Gerenciar trabalhos de operações em lote do S3

O Amazon S3 oferece um conjunto de ferramentas robusto para ajudar a gerenciar trabalhos do S3 Batch Operations após a criação deles. Esta seção descreve as operações que você pode usar para gerenciar e rastrear trabalhos usando o console do Amazon S3, a AWS Command Line Interface (AWS CLI), SDKs da AWS ou a API REST do Amazon S3.

Tópicos

- Usar o console do Simple Storage Service (Amazon S3) para gerenciar trabalhos do S3 Batch Operations
- Listar trabalhos
- Visualizar detalhes do trabalho
- Atribuir prioridade aos trabalhos

Usar o console do Simple Storage Service (Amazon S3) para gerenciar trabalhos do S3 Batch Operations

Usar o console para gerenciar seus trabalhos do S3 Batch Operations. Por exemplo, é possível:

- Exibir trabalhos ativos e enfileirados
- Alterar a prioridade de um trabalho
- Confirmar e executar um trabalho
- Clonar um trabalho
- Cancelar um trabalho

Para gerenciar trabalhos do S3 Batch Operations usando o console

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação esquerdo, escolha Batch Operations (Operações em lote).
3. Escolha o trabalho específico que você deseja gerenciar.

Listar trabalhos

Você pode recuperar uma lista dos seus trabalhos de operações em lote do S3. Ela inclui os trabalhos ainda não concluídos, bem como os concluídos nos últimos 90 dias. A lista inclui informações para cada trabalho, como ID, descrição, prioridade, status atual e número de tarefas que foram bem-sucedidas e que apresentaram falha. Você pode filtrar a lista por status. Ao recuperar uma lista pelo console, você também pode pesquisar os trabalhos por descrição ou ID e filtrá-los por Região da AWS.

Obter uma lista de trabalhos **`Active`** e **`Complete`**

O exemplo de AWS CLI a seguir obtém uma lista de trabalhos `Active` e `Complete`. Para usar esse exemplo, substitua os *`user input placeholders`* por suas próprias informações.

```
aws s3control list-jobs \
    --region us-west-2 \
    --account-id account-id \
    --job-statuses '["Active","Complete"]' \
    --max-results 20
```

Para obter mais informações e exemplos, consulte list-jobs na Referência de comandos da AWS CLI.

Visualizar detalhes do trabalho

Se quiser mais informações sobre um trabalho do Operações em Lote do Amazon S3 que pode ser recuperado listando trabalhos, você poderá visualizar todos os detalhes de um único trabalho. É possível ver detalhes dos trabalhos que ainda não foram concluídos ou dos que foram concluídos nos últimos 90 dias. Além das informações retornadas em uma lista de trabalhos, os detalhes de um trabalho individual incluem outros itens, como:

- Os parâmetros da operação
- Detalhes sobre o manifesto
- Informações sobre o relatório de conclusão (se você configurou um ao criar o trabalho)
- O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que você atribuiu para executar o trabalho

Exibindo os detalhes de um trabalho individual, você acessa toda a configuração de um trabalho. Para visualizar os detalhes de um trabalho, você pode usar o console do Amazon S3 ou a AWS Command Line Interface (AWS CLI).

Ter a descrição de um trabalho de Operações em Lote do S3 no console do Amazon S3

Como visualizar a descrição de um trabalho de Operações em Lote usando o console

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação esquerdo, escolha Batch Operations (Operações em lote).
3. Escolha o ID do trabalho específico para visualizar os detalhes.

Ter a descrição de um trabalho de Operações em Lote do S3 no AWS CLI

O exemplo a seguir obtém a descrição de um trabalho de Operações em Lote do S3 usando a AWS CLI. Para usar o comando a seguir, substitua os *`user input placeholders`* por suas próprias informações.

```
aws s3control describe-job \
--region us-west-2 \
--account-id account-id \
--job-id 00e123a4-c0d8-41f4-a0eb-b46f9ba5b07c
```

Para obter mais informações e exemplos, consulte describe-job na Referência de comandos da AWS CLI.

Atribuir prioridade aos trabalhos

Você pode atribuir a cada trabalho do Operações em Lote do Amazon S3 uma prioridade numérica, que pode ser qualquer inteiro positivo. O Operações em Lote do S3 prioriza trabalhos de acordo com a prioridade atribuída. Os trabalhos com prioridade mais alta (ou um valor inteiro mais alto para o parâmetro de prioridade) são avaliados primeiro. A prioridade é determinada em ordem decrescente. Por exemplo, uma fila de tarefas com valor de prioridade 10 tem preferência de programação em relação a uma fila com valor de prioridade 1.

É possível alterar a prioridade do trabalho enquanto ele está sendo executado. Se você enviar um novo trabalho com uma prioridade mais alta enquanto um trabalho estiver em execução, o trabalho de menor prioridade poderá ser pausado para permitir a execução do trabalho de maior prioridade.

Alterar a prioridade de um trabalho não afeta a velocidade de processamento dele.

> **Note**
>
> O Operações em Lote do S3 respeita as prioridades de trabalhos com o melhor esforço. Embora os trabalhos com prioridades mais altas normalmente tenham precedência sobre os de prioridades mais baixas, o Amazon S3 não garante a classificação rígida dos trabalhos.

Usar o console do S3

Como atualizar a prioridade de trabalhos no console do Amazon S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação esquerdo, escolha Batch Operations (Operações em lote).
3. Selecione o trabalho específico que você deseja gerenciar.
4. Escolha Actions (Ações). Na lista suspensa, escolha Update priority (Atualizar prioridade).

Como usar o AWS CLI

O exemplo a seguir atualiza a prioridade do trabalho usando a AWS CLI. Um número maior indica uma prioridade de execução mais alta. Para usar o comando a seguir, substitua os *`user input placeholders`* por suas próprias informações.

```
aws s3control update-job-priority \
    --region us-west-2 \
    --account-id account-id \
    --priority 98 \
    --job-id 00e123a4-c0d8-41f4-a0eb-b46f9ba5b07c
```

Como usar o AWS SDK para Java

O exemplo a seguir atualiza a prioridade de um trabalho do S3 Batch Operations usando o AWS SDK para Java.

Para obter mais informações sobre prioridade de trabalhos, consulte Atribuir prioridade aos trabalhos.

Example

```
package aws.example.s3control;


import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import com.amazonaws.services.s3control.model.UpdateJobPriorityRequest;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class UpdateJobPriority {
    public static void main(String[] args) {
        String accountId = "Account ID";
        String jobId = "00e123a4-c0d8-41f4-a0eb-b46f9ba5b07c";

        try {
            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(US_WEST_2)
                    .build();

            s3ControlClient.updateJobPriority(new UpdateJobPriorityRequest()
                    .withAccountId(accountId)
                    .withJobId(jobId)
                    .withPriority(98));

        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Monitoramento de relatórios de status e conclusão

Com o S3 Batch Operations, você pode exibir e atualizar o status do trabalho, adicionar notificações e registro em log, rastrear falhas de trabalho e gerar relatórios de conclusão.

Tópicos

- Status de trabalhos
- Atualizar status do trabalho
- Notificações e registro em log
- Monitorar falhas nos trabalhos
- Relatórios de conclusão
- Monitorar um trabalho de operações em lote do S3 no Amazon EventBridge por meio do AWS CloudTrail
- Exemplos: relatórios de conclusão de operações em lote do S3

Status de trabalhos

Depois de criar um trabalho, ele passa por diversos status. A tabela a seguir descreve os status e as possíveis transições entre eles.

Status	Descrição	Transições
`New`	Ao ser criado, o trabalho ganha o status `New`.	Um trabalho passa automaticamente para o estado `Preparing` quando o Amazon S3 começa a processar o objeto do manifesto.
`Preparing`	O Amazon S3 está processando o objeto do manifesto e outros parâmetros do trabalho para configurar e executar o trabalho.	O trabalho passa automaticamente para o estado `Ready` depois que o Amazon S3 termina de processar o manifesto e outros parâmetros. Então, o trabalho está pronto para começar a

Status	Descrição	Transições
		executar a operação especificada nos objetos listados no manifesto. Se o trabalho exigir confirmação antes da execução, como ao criar um trabalho usando o console do Amazon S3, ele passará do estado `Preparing` para `Suspended`. Ele permanece no estado `Suspended` até que você confirme que deseja executá-lo.
`Suspended`	O trabalho exige confirmação, mas você ainda não confirmou que deseja executá-lo. Somente os trabalhos criados pelo console do Amazon S3 exigem confirmação. Um trabalho criado pelo console entra no estado `Suspended` imediatamente depois de `Preparing`. Depois de confirmar que deseja executar o trabalho e ele entra no estado `Ready`, ele não retorna mais a `Suspended`.	Depois de confirmar que deseja executar o trabalho, o status muda para `Ready`.

Status	Descrição	Transições
`Ready`	O Amazon S3 está pronto para executar as operações do objeto solicitadas.	Um trabalho passa automatic amente para `Active` quando o Amazon S3 começa a executá-lo. O tempo que o trabalho permanece no estado `Ready` depende do fato de outros trabalhos de maior prioridade estarem sendo executados e do tempo necessários para conclui-los.
`Active`	O Amazon S3 está executand o a operação solicitada nos objetos listados no manifesto . Enquanto um trabalho está no status `Active`, é possível monitorar seu progresso usando o console do Amazon S3 ou a operação `DescribeJ ob` por meio da API REST, AWS CLI ou AWS SDKs.	Um trabalho sai do estado `Active` quando para de executar operações nos objetos. Esse comportamento pode acontecer automatic amente, como quando um trabalho é concluído com êxito ou apresenta falha. Ou esse comportamento pode ocorrer como resultado de ações do usuário, como ao cancelar um trabalho. O estado que o trabalho passa a apresenta r depende do motivo da transição.
`Pausing`	O trabalho está passando de outro estado para `Paused`.	O trabalho passa automatic amente para `Paused` quando o estado `Pausing` é concluído .

Status	Descrição	Transições
`Paused`	O trabalho pode assumir o estado `Paused` se você enviar outro trabalho de maior prioridade enquanto o atual está sendo executado.	O trabalho `Paused` volta automaticamente para `Active` depois que os trabalhos de prioridade mais alta que estavam bloqueando sua execução são concluídos, suspensos ou falham.
`Complete`	O trabalho terminou a execução da operação solicitada em todos os objetos do manifesto. A operação pode ter sido concluída com êxito ou ter apresentado falha para cada objeto. Se você configurar a criação do relatório de conclusão, o relatório estará disponível assim que o trabalho estiver em `Complete`.	`Complete` é um estado terminal. Quando um trabalho atinge `Complete`, ele não muda mais de estado.
`Cancelling`	O trabalho está passando para o estado `Cancelled` .	O trabalho passa automatic amente para `Cancelled` quando o estado `Cancellin g` é concluído.
`Cancelled`	Você solicitou que o trabalho fosse cancelado e o Operações em Lote do S3 fez o cancelamento com sucesso. O trabalho não enviará novas solicitações ao Amazon S3.	`Cancelled` é um estado terminal. Quando o trabalho atinge `Cancelled` , ele não muda mais de estado.

Status	Descrição	Transições
`Failing`	O trabalho está passando para o estado `Failed`.	O trabalho passa automatic amente para `Failed` quando o estado `Failing` é concluído .
`Failed`	O trabalho apresentou falha e não está mais em execução. Para obter mais informações sobre falhas em trabalhos, consulte Monitorar falhas nos trabalhos.	`Failed` é um estado terminal. Quando o trabalho atinge `Failed`, ele não muda mais de estado.

Atualizar status do trabalho

Os exemplos da AWS CLI e do AWS SDK para Java a seguir atualizam o status de um trabalho do Operações em Lote. Consulte mais informações sobre como usar o console do Amazon S3 para gerenciar trabalhos do Operações em lote em Usar o console do Simple Storage Service (Amazon S3) para gerenciar trabalhos do S3 Batch Operations.

Como usar o AWS CLI

Para usar os comandos a seguir, substitua os *`user input placeholders`* por suas próprias informações.

- Se você não tiver especificado o parâmetro `--no-confirmation-required` no comando `create-job`, o trabalho permanecerá em um estado suspenso até você confirmar o trabalho definindo o status dele como `Ready`. O Amazon S3 torna o trabalho qualificado para execução.

```
aws s3control update-job-status \
    --region us-west-2 \
    --account-id 123456789012 \
    --job-id 00e123a4-c0d8-41f4-a0eb-b46f9ba5b07c \
    --requested-job-status 'Ready'
```

- Para cancelar o trabalho, defina o status do trabalho como `Cancelled`.

```
aws s3control update-job-status \
```

```
    --region us-west-2 \
    --account-id 123456789012 \
    --job-id 00e123a4-c0d8-41f4-a0eb-b46f9ba5b07c \
    --status-update-reason "No longer needed" \
    --requested-job-status Cancelled
```

Usar o AWS SDK for Java

O exemplo a seguir atualiza o status de um trabalho do Operações em Lote do S3 usando o AWS SDK para Java.

Para obter mais informações sobre o status de trabalhos, consulte Monitoramento de relatórios de status e conclusão.

Example

```
package aws.example.s3control;


import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import com.amazonaws.services.s3control.model.UpdateJobStatusRequest;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class UpdateJobStatus {
    public static void main(String[] args) {
        String accountId = "Account ID";
        String jobId = "00e123a4-c0d8-41f4-a0eb-b46f9ba5b07c";

        try {
            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(US_WEST_2)
                    .build();

            s3ControlClient.updateJobStatus(new UpdateJobStatusRequest()
                    .withAccountId(accountId)
```

```
                    .withJobId(jobId)
                    .withRequestedJobStatus("Ready"));

        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Notificações e registro em log

Além de solicitar relatórios de conclusão, você também pode capturar, revisar e auditar as atividades de operações em lote usando o AWS CloudTrail. Como o Operações em Lote usa operações de API existentes do Amazon S3 para realizar tarefas, essas tarefas também emitem os mesmos eventos que emitiriam se você as chamasse diretamente. Portanto, você pode monitorar e registrar o andamento do trabalho e todas as tarefas usando as mesmas ferramentas de notificação, registro em log e auditoria, além dos processos já usados com o Amazon S3. Para obter mais informações, consulte os exemplos nas seções a seguir.

> **Note**
>
> O Operações em Lote gera eventos de gerenciamento e dados no CloudTrail durante a execução do trabalho. O volume desses eventos é escalado com o número de chaves no manifesto de cada trabalho. Consulte mais informações na página Definição de preço do AWS CloudTrail, que inclui exemplos de como a definição de preço muda dependendo do número de trilhas que você configurou na conta. Para saber como configurar e registrar em log eventos para atender às suas necessidades, consulte Criar sua primeira trilha no Guia do usuário do AWS CloudTrail.

Para obter mais informações sobre eventos do Amazon S3, consulte Notificações de eventos do Amazon S3.

Monitorar falhas nos trabalhos

Se uma operação em lote do S3 encontrar um problema que o impeça de ser executado com êxito, como não ser capaz de ler o manifesto especificado, o trabalho falhará. Quando um trabalho falha, ele gera um ou mais códigos de falha ou motivos de falha. O Operações em Lote do S3 armazena os códigos e os motivos da falha com o trabalho para que você possa visualizá-los solicitando os detalhes do trabalho. Caso você tenha solicitado um relatório de conclusão para o trabalho, os códigos e os motivos de falha também são exibidos.

Para evitar que trabalhos executem um grande número de operações malsucedidas, o Amazon S3 impõe um limite de falhas por tarefa em cada trabalho de operações em lote. O Amazon S3 monitora a taxa de falhas das tarefas depois que o trabalho executa pelo menos 1.000 tarefas. Se, a qualquer momento, a taxa de falha (o número de tarefas que falharam em proporção ao número total de tarefas executadas) exceder 50%, o trabalho vai falhar. Se o trabalho falhar porque excedeu o limite de falhas da tarefa, você poderá identificar a causa das falhas. Por exemplo, você pode ter incluído por acidente alguns objetos no manifesto que não existem no bucket especificado. Depois de corrigir os erros, você pode reenviar o trabalho.

> **Note**
>
> O Operações em Lote do S3 funciona de maneira assíncrona e não necessariamente executa tarefas na ordem em que os objetos estão listados no manifesto. Portanto, não é possível usar a ordem do manifesto para determinar quais tarefas dos objetos foram bem-sucedidas e quais falharam. Em vez disso, examine o relatório de conclusão do trabalho (caso você tenha solicitado um) ou exiba os logs de evento do AWS CloudTrail para ajudar a determinar a origem das falhas.

Relatórios de conclusão

Ao criar um trabalho, você solicita um relatório de conclusão. Desde que o Operações em Lote do S3 invoque com êxito pelo menos uma tarefa, o Amazon S3 gerará um relatório de conclusão depois que o trabalho concluir a execução de tarefas, falhar ou ser cancelado. Configure o relatório de conclusão para incluir todas as tarefas ou somente tarefas com falha.

O relatório de conclusão inclui a configuração do trabalho, o status e as informações de cada tarefa, inclusive a chave e a versão do objeto, status, códigos de erro e descrições de eventuais erros. Os relatórios de conclusão oferecem uma maneira fácil de visualizar os resultados das tarefas em um

formato consolidado, sem a necessidade de configurações adicionais. Os relatórios de conclusão são criptografados usando a criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3). Para obter um exemplo de um relatório de conclusão, consulte Exemplos: relatórios de conclusão de operações em lote do S3.

Mesmo que você não configure um relatório de conclusão, ainda poderá monitorar e auditar o trabalho e suas tarefas usando o CloudTrail e o Amazon CloudWatch. Para obter mais informações, consulte os tópicos a seguir.

Tópicos

- Monitorar um trabalho de operações em lote do S3 no Amazon EventBridge por meio do AWS CloudTrail
- Exemplos: relatórios de conclusão de operações em lote do S3

Monitorar um trabalho de operações em lote do S3 no Amazon EventBridge por meio do AWS CloudTrail

A atividade do trabalho de operações em lote do Amazon S3 é registrada como eventos no AWS CloudTrail. Você pode criar uma regra personalizada no Amazon EventBridge e enviar esses eventos para o recurso de notificação de destino de sua escolha, como o Amazon Simple Notification Service (Amazon SNS).

> **Note**
>
> O Amazon EventBridge é a maneira preferida de gerenciar seus eventos. O Amazon CloudWatch Events e o EventBridge são o mesmo serviço subjacente e API, mas o EventBridge oferece mais recursos. As alterações feitas no CloudWatch ou no EventBridge aparecem em cada console. Para obter mais informações, consulte o Guia do usuário do Amazon EventBridge.

Exemplos de rastreamento

- Eventos de operações em lote do S3 registrados no CloudTrail
- Regra do EventBridge para rastrear eventos de trabalhos de operações em lote do S3

Eventos de operações em lote do S3 registrados no CloudTrail

Quando um trabalho de operações em lote é criado, ele é gravado como um evento `JobCreated` no CloudTrail. À medida que o trabalho é executado, ele muda de estado durante o processamento e outros eventos `JobStatusChanged` são registrados no CloudTrail. Você pode visualizar esses eventos no console do CloudTrail. Para obter mais informações sobre o CloudTrail, consulte o Guia do usuário do AWS CloudTrail.

> **Note**
>
> Somente eventos `status-change` de trabalho de operações em lote do S3 são registrados no CloudTrail.

Example — evento de conclusão de trabalho de operações em lote do S3 registrado pelo CloudTrail

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "accountId": "123456789012",
        "invokedBy": "s3.amazonaws.com"
    },
    "eventTime": "2020-02-05T18:25:30Z",
    "eventSource": "s3.amazonaws.com",
    "eventName": "JobStatusChanged",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "s3.amazonaws.com",
    "userAgent": "s3.amazonaws.com",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "f907577b-bf3d-4c53-b9ed-8a83a118a554",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "recipientAccountId": "123412341234",
    "serviceEventDetails": {
        "jobId": "d6e58ec4-897a-4b6d-975f-10d7f0fb63ce",
        "jobArn": "arn:aws:s3:us-west-2:181572960644:job/
d6e58ec4-897a-4b6d-975f-10d7f0fb63ce",
        "status": "Complete",
        "jobEventId": "b268784cf0a66749f1a05bce259804f5",
        "failureCodes": [],
        "statusChangeReason": []
    }
```

```
}
```

Regra do EventBridge para rastrear eventos de trabalhos de operações em lote do S3

O exemplo a seguir mostra como criar uma regra no Amazon EventBridge para capturar eventos do S3 Batch Operations registrados pelo AWS CloudTrail para um destino escolhido por você.

Para fazer isso, você cria uma regra seguindo todas as etapas em Criação de regras do EventBridge que reagem aos eventos. Cole a política de padrão de evento personalizada de operações em lote do S3, quando aplicável, e selecione o serviço de destino de sua escolha.

Política de padrão de evento personalizado de operações em lote do S3

```
{
    "source": [
        "aws.s3"
    ],
    "detail-type": [
        "AWS Service Event via CloudTrail"
    ],
    "detail": {
        "eventSource": [
            "s3.amazonaws.com"
        ],
        "eventName": [
            "JobCreated",
            "JobStatusChanged"
        ]
    }
}
```

Os exemplos a seguir são dois eventos de operações em lote que foram enviados para o Amazon Simple Queue Service (Amazon SQS) a partir de uma regra de evento do EventBridge. Um trabalho de operações em lote passa por vários estados diferentes durante o processamento (`New`, `Preparing`, `Active` etc.), portanto, você pode esperar receber várias mensagens para cada trabalho.

Example – Evento de exemplo JobCreated

```
{
    "version": "0",
```

```
    "id": "51dc8145-541c-5518-2349-56d7dffdf2d8",
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.s3",
    "account": "123456789012",
    "time": "2020-02-27T15:25:49Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "11112223334444",
            "invokedBy": "s3.amazonaws.com"
        },
        "eventTime": "2020-02-27T15:25:49Z",
        "eventSource": "s3.amazonaws.com",
        "eventName": "JobCreated",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "s3.amazonaws.com",
        "userAgent": "s3.amazonaws.com",
        "eventID": "7c38220f-f80b-4239-8b78-2ed867b7d3fa",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "jobId": "e849b567-5232-44be-9a0c-40988f14e80c",
            "jobArn": "arn:aws:s3:us-east-1:181572960644:job/
e849b567-5232-44be-9a0c-40988f14e80c",
            "status": "New",
            "jobEventId": "f177ff24f1f097b69768e327038f30ac",
            "failureCodes": [],
            "statusChangeReason": []
        }
    }
}
```

Example – Evento JobStatusChanged de conclusão de trabalho

```
{
  "version": "0",
  "id": "c8791abf-2af8-c754-0435-fd869ce25233",
  "detail-type": "AWS Service Event via CloudTrail",
  "source": "aws.s3",
  "account": "123456789012",
  "time": "2020-02-27T15:26:42Z",
```

```
  "region": "us-east-1",
  "resources": [],
  "detail": {
    "eventVersion": "1.05",
    "userIdentity": {
      "accountId": "1111222233334444",
      "invokedBy": "s3.amazonaws.com"
    },
    "eventTime": "2020-02-27T15:26:42Z",
    "eventSource": "s3.amazonaws.com",
    "eventName": "JobStatusChanged",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "s3.amazonaws.com",
    "userAgent": "s3.amazonaws.com",
    "eventID": "0238c1f7-c2b0-440b-8dbd-1ed5e5833afb",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "serviceEventDetails": {
      "jobId": "e849b567-5232-44be-9a0c-40988f14e80c",
      "jobArn": "arn:aws:s3:us-east-1:181572960644:job/
e849b567-5232-44be-9a0c-40988f14e80c",
      "status": "Complete",
      "jobEventId": "51f5ac17dba408301d56cd1b2c8d1e9e",
      "failureCodes": [],
      "statusChangeReason": []
    }
  }
}
```

Exemplos: relatórios de conclusão de operações em lote do S3

Ao criar uma trabalho de operações em lote do S3, você pode solicitar um relatório de conclusão para todas as tarefas ou somente para aquelas que apresentaram falha. Contanto que pelo menos uma tarefa tenha sido invocada com êxito, as operações em lote do S3 geram um relatório para tarefas que foram concluídas, que falharam ou que foram canceladas.

O relatório de conclusão contém informações adicionais de cada tarefa, inclusive a chave e a versão do objeto, status, códigos de erro e descrições de qualquer erro. A descrição dos erros para cada tarefa com falha pode ser usada para diagnosticar problemas durante a criação de trabalhos, como permissões.

> **Note**
>
> Os relatórios de conclusão são sempre criptografados com chaves gerenciadas pelo Amazon S3 (SSE-S3).

Example – Arquivo de resultado do manifesto de nível superior

O arquivo `manifest.json` de nível superior contém os locais de cada relatório bem-sucedido e (se a tarefa apresentou qualquer falha) o local de relatórios com falha, conforme mostrado no exemplo a seguir.

```
{
    "Format": "Report_CSV_20180820",
    "ReportCreationDate": "2019-04-05T17:48:39.725Z",
    "Results": [
        {
            "TaskExecutionStatus": "succeeded",
            "Bucket": "my-job-reports",
            "MD5Checksum": "83b1c4cbe93fc893f54053697e10fd6e",
            "Key": "job-f8fb9d89-a3aa-461d-bddc-ea6a1b131955/
results/6217b0fab0de85c408b4be96aeaca9b195a7daa5.csv"
        },
        {
            "TaskExecutionStatus": "failed",
            "Bucket": "my-job-reports",
            "MD5Checksum": "22ee037f3515975f7719699e5c416eaa",
            "Key": "job-f8fb9d89-a3aa-461d-bddc-ea6a1b131955/results/
b2ddad417e94331e9f37b44f1faf8c7ed5873f2e.csv"
        }
    ],
    "ReportSchema": "Bucket, Key, VersionId, TaskStatus, ErrorCode, HTTPStatusCode,
 ResultMessage"
}
```

Example – Relatórios de tarefas com falha

Relatórios de tarefas com falha contêm as seguintes informações para todas as tarefas com falha:

- `Bucket`
- `Key`

- `VersionId`
- `TaskStatus`
- `ErrorCode`
- `HTTPStatusCode`
- `ResultMessage`

O exemplo de relatório a seguir mostra um caso no qual a função do AWS Lambda atingiu o tempo limite, fazendo com que as falhas excedessem o limite de falhas. Ela foi então marcado como um `PermanentFailure`.

```
amzn-s3-demo-bucket1,image_14975,,failed,200,PermanentFailure,"Lambda returned
 function error: {""errorMessage"":""2019-04-05T17:35:21.155Z 2845ca0d-38d9-4c4b-
abcf-379dc749c452 Task timed out after 3.00 seconds""}"
amzn-s3-demo-bucket1,image_15897,,failed,200,PermanentFailure,"Lambda returned
 function error: {""errorMessage"":""2019-04-05T17:35:29.610Z 2d0a330b-de9b-425f-
b511-29232fde5fe4 Task timed out after 3.00 seconds""}"
amzn-s3-demo-bucket1,image_14819,,failed,200,PermanentFailure,"Lambda returned
 function error: {""errorMessage"":""2019-04-05T17:35:22.362Z fcf5efde-74d4-4e6d-b37a-
c7f18827f551 Task timed out after 3.00 seconds""}"
amzn-s3-demo-bucket1,image_15930,,failed,200,PermanentFailure,"Lambda returned
 function error: {""errorMessage"":""2019-04-05T17:35:29.809Z 3dd5b57c-4a4a-48aa-8a35-
cbf027b7957e Task timed out after 3.00 seconds""}"
amzn-s3-demo-bucket1,image_17644,,failed,200,PermanentFailure,"Lambda
 returned function error: {""errorMessage"":""2019-04-05T17:35:46.025Z
 10a764e4-2b26-4d8c-9056-1e1072b4723f Task timed out after 3.00 seconds""}"
amzn-s3-demo-bucket1,image_17398,,failed,200,PermanentFailure,"Lambda returned
 function error: {""errorMessage"":""2019-04-05T17:35:44.661Z 1e306352-4c54-4eba-
aee8-4d02f8c0235c Task timed out after 3.00 seconds""}"
```

Example – Relatório de tarefas bem-sucedidas

Os relatórios de tarefas bem-sucedidas contêm o seguinte para as tarefas bem-sucedidas:

- `Bucket`
- `Key`
- `VersionId`
- `TaskStatus`
- `ErrorCode`

- `HTTPStatusCode`
- `ResultMessage`

No exemplo a seguir, a função do Lambda copiou com êxito o objeto do Amazon S3 para outro bucket. A resposta retornada do Amazon S3 é passada de volta para operações em lote do S3 e, em seguida, é gravada no relatório de conclusão final.


```
amzn-s3-demo-bucket1,image_17775,,succeeded,200,,"{u'CopySourceVersionId':
 'xVR78haVKlRnurYofbTfYr3ufYbktF8h', u'CopyObjectResult': {u'LastModified':
 datetime.datetime(2019, 4, 5, 17, 35, 39, tzinfo=tzlocal()), u'ETag':
 '""fe66f4390c50f29798f040d7aae72784""'}, 'ResponseMetadata': {'HTTPStatusCode':
 200, 'RetryAttempts': 0, 'HostId': 'nXNaClIMxEJzWNmeMNQV2KpjbaCJLn0OGoXWZpuVOFS/
iQYWxb3QtTvzX9SVfx2lA3oTKLwImKw=', 'RequestId': '3ED5852152014362', 'HTTPHeaders':
 {'content-length': '234', 'x-amz-id-2': 'nXNaClIMxEJzWNmeMNQV2KpjbaCJLn0OGoXWZpuVOFS/
iQYWxb3QtTvzX9SVfx2lA3oTKLwImKw=', 'x-amz-copy-source-version-id':
 'xVR78haVKlRnurYofbTfYr3ufYbktF8h', 'server': 'AmazonS3', 'x-amz-request-id':
 '3ED5852152014362', 'date': 'Fri, 05 Apr 2019 17:35:39 GMT', 'content-type':
 'application/xml'}}}"
amzn-s3-demo-bucket1,image_17763,,succeeded,200,,"{u'CopySourceVersionId':
 '6HjOUSim4Wj6BTcbxToXW44pSZ.40pwq', u'CopyObjectResult': {u'LastModified':
 datetime.datetime(2019, 4, 5, 17, 35, 39, tzinfo=tzlocal()),
 u'ETag': '""fe66f4390c50f29798f040d7aae72784""'}, 'ResponseMetadata':
 {'HTTPStatusCode': 200, 'RetryAttempts': 0, 'HostId': 'GiCZNYr8LHd/
Thyk6beTRP96IGZk2sYxujLe13TuuLpq6U2RD3we0YoluuIdm1PRvkMwnEW1aFc=', 'RequestId':
 '1BC9F5B1B95D7000', 'HTTPHeaders': {'content-length': '234', 'x-amz-id-2':
 'GiCZNYr8LHd/Thyk6beTRP96IGZk2sYxujLe13TuuLpq6U2RD3we0YoluuIdm1PRvkMwnEW1aFc=', 'x-
amz-copy-source-version-id': '6HjOUSim4Wj6BTcbxToXW44pSZ.40pwq', 'server': 'AmazonS3',
 'x-amz-request-id': '1BC9F5B1B95D7000', 'date': 'Fri, 05 Apr 2019 17:35:39 GMT',
 'content-type': 'application/xml'}}}"
amzn-s3-demo-bucket1,image_17860,,succeeded,200,,"{u'CopySourceVersionId':
 'm.MDD0g_QsUnYZ8TBzVFrp.TmjN8PJyX', u'CopyObjectResult': {u'LastModified':
 datetime.datetime(2019, 4, 5, 17, 35, 40, tzinfo=tzlocal()), u'ETag':
 '""fe66f4390c50f29798f040d7aae72784""'}, 'ResponseMetadata': {'HTTPStatusCode':
 200, 'RetryAttempts': 0, 'HostId': 'F9ooZOgpE5g9sNgBZxjdiPHqB4+0DNWgj3qbsir
+sKai4fv7rQEcF2fBN1VeeFc2WH45a9ygb2g=', 'RequestId': '8D9CA56A56813DF3', 'HTTPHeaders':
 {'content-length': '234', 'x-amz-id-2': 'F9ooZOgpE5g9sNgBZxjdiPHqB4+0DNWgj3qbsir
+sKai4fv7rQEcF2fBN1VeeFc2WH45a9ygb2g=', 'x-amz-copy-source-version-id':
 'm.MDD0g_QsUnYZ8TBzVFrp.TmjN8PJyX', 'server': 'AmazonS3', 'x-amz-request-id':
 '8D9CA56A56813DF3', 'date': 'Fri, 05 Apr 2019 17:35:40 GMT', 'content-type':
 'application/xml'}}}"
```

Controlar o acesso e rotular trabalhos usando tags

Você pode rotular e controlar o acesso aos trabalhos de operações em lote do S3 adicionando tags. As tags podem ser usadas para identificar quem é responsável por um trabalho de operações em lote. A presença de marcações de trabalho pode conceder ou limitar a capacidade do usuário de cancelar um trabalho, ativar um trabalho no estado de confirmação ou alterar o nível de prioridade de um trabalho. Você pode criar trabalhos com tags anexadas a eles e pode adicionar tags aos trabalhos depois que eles são criados. Cada tag é um par de chave-valor que pode ser incluído quando você cria o trabalho ou atualizado posteriormente.

> **Warning**
>
> Garanta que as tags de trabalho não contenham informações confidenciais ou dados pessoais.

Considere o seguinte exemplo de marcação: suponha que você deseja que seu departamento financeiro crie um trabalho de operações em lote. Você pode escrever uma política do AWS Identity and Access Management (IAM) que permita que um usuário invoque `CreateJob`, desde que o trabalho seja criado com a tag `Department` atribuída ao valor `Finance`. Além disso, você pode anexar essa política a todos os usuários que são membros do departamento de Finanças.

Continuando com este exemplo, você pode escrever uma política que permita que um usuário atualize a prioridade de qualquer trabalho que tenha as tags desejadas ou cancele qualquer trabalho que tenha essas tags. Para obter mais informações, consulte the section called “Controlar permissões”.

Você pode adicionar tags a novos trabalhos de operações em lote do S3 ao criá-los ou adicionar tags a trabalhos existentes.

Observe as seguintes restrições de tag:

- Você pode associar até 50 tags a um trabalho, desde que elas tenham chaves de tag exclusivas.
- Um chave de tag pode ter até 128 caracteres Unicode e os valores de tag podem ter até 256 caracteres Unicode.
- As chaves e os valores diferenciam letras maiúsculas de minúsculas.

Para obter mais informações sobre restrições de tags, consulte Restrições de tags definidas pelo usuário no Guia do usuário do Gerenciamento de Faturamento e Custos da AWS.

Operações de API relacionadas à marcação de trabalhos de operações em lote do S3

O Amazon S3 oferece suporte às seguintes operações de API específicas para a marcação de trabalhos de operações em lote do S3:

- GetJobTagging: mostra o conjunto de tags associado a um trabalho do Operações em Lote.
- PutJobTagging: substitui o conjunto de tags associado a um trabalho. Há dois cenários distintos de gerenciamento de tags de trabalho de operações em lote do S3 usando essa ação de API:
  - O trabalho não tem tags: você pode adicionar um conjunto de tags a um trabalho (o trabalho não tem tags anteriores).
  - O trabalho tem um conjunto de tags existentes: para modificar o conjunto de tags existente, é possível substituí-lo ou fazer alterações nele recuperando o conjunto de tags existente usando GetJobTagging, modificar esse conjunto de tags e usar essa ação de API para substituir a tag definida pela que você modificou.

    > **Note**
    >
    > Se você enviar essa solicitação com o conjunto de tags vazio, o Operações em lote do S3 excluirá o conjunto de tags existente no objeto. Se você usar esse método, receberá a cobrança por uma solicitação de nível 1 (PUT). Para obter mais informações, consulte Definição de preço do Amazon S3.
    >
    > Para excluir tags existentes do trabalho de Operações em lote, a ação `DeleteJobTagging` é preferida porque ela obtém o mesmo resultado sem incorrer em encargos.

- DeleteJobTagging: exclui o conjunto de tags associado a um trabalho de operações em lote.

Criar um trabalho do Operações em lote com tags de trabalho usadas para rotulagem

É possível rotular e controlar o acesso aos trabalhos do Operações em Lote do Amazon S3 adicionando tags. As tags podem ser usadas para identificar quem é responsável por um trabalho de operações em lote. Você pode criar trabalhos com tags anexadas a eles e pode adicionar tags aos trabalhos depois que eles são criados. Para obter mais informações, consulte the section called “Usar tags”.

Usar a AWS CLI

O exemplo da AWS CLI a seguir cria um trabalho `S3PutObjectCopy` do S3 Batch Operations usando tags de trabalho como rótulos para o trabalho.

1. Selecione a ação ou `OPERATION` que deseja que o trabalho de operações em lote execute e escolha `TargetResource`.

```
read -d '' OPERATION <<EOF
{
  "S3PutObjectCopy": {
    "TargetResource": "arn:aws:s3:::amzn-s3-demo-destination-bucket"
  }
}
EOF
```

2. Identifique as `TAGS` que você deseja para o trabalho. Nesse caso, você aplica duas tags, `department` e `FiscalYear`, com os valores `Marketing` e `2020`, respectivamente.

```
read -d '' TAGS <<EOF
[
  {
    "Key": "department",
    "Value": "Marketing"
  },
  {
    "Key": "FiscalYear",
    "Value": "2020"
  }
]
EOF
```

3. Especifique o `MANIFEST` para o trabalho de operações em lote.

```
read -d '' MANIFEST <<EOF
{
  "Spec": {
    "Format": "EXAMPLE_S3BatchOperations_CSV_20180820",
    "Fields": [
      "Bucket",
      "Key"
    ]
  },
```

```
  "Location": {
    "ObjectArn": "arn:aws:s3:::amzn-s3-demo-manifest-bucket/example_manifest.csv",
    "ETag": "example-5dc7a8bfb90808fc5d546218"
  }
}
EOF
```

4. Configure o REPORT para o trabalho de operações em lote.

```
read -d '' REPORT <<EOF
{
  "Bucket": "arn:aws:s3:::amzn-s3-demo-completion-report-bucket",
  "Format": "Example_Report_CSV_20180820",
  "Enabled": true,
  "Prefix": "reports/copy-with-replace-metadata",
  "ReportScope": "AllTasks"
}
EOF
```

5. Execute a ação `create-job` para criar o trabalho de operações em lote com entradas definidas nas etapas anteriores.

```
aws \
    s3control create-job \
    --account-id 123456789012 \
    --manifest "${MANIFEST//$'\n'}" \
    --operation "${OPERATION//$'\n'/}" \
    --report "${REPORT//$'\n'}" \
    --priority 10 \
    --role-arn arn:aws:iam::123456789012:role/batch-operations-role \
    --tags "${TAGS//$'\n'/}" \
    --client-request-token "$(uuidgen)" \
    --region us-west-2 \
    --description "Copy with Replace Metadata";
```

Usar o AWS SDK for Java

Example

O exemplo a seguir cria um trabalho do S3 Batch Operations com tags usando o AWS SDK para Java.

```
public String createJob(final AWSS3ControlClient awss3ControlClient) {
    final String manifestObjectArn = "arn:aws:s3:::amzn-s3-demo-manifest-bucket/
manifests/10_manifest.csv";
    final String manifestObjectVersionId = "example-5dc7a8bfb90808fc5d546218";

    final JobManifestLocation manifestLocation = new JobManifestLocation()
            .withObjectArn(manifestObjectArn)
            .withETag(manifestObjectVersionId);

    final JobManifestSpec manifestSpec =
            new
 JobManifestSpec().withFormat(JobManifestFormat.S3InventoryReport_CSV_20161130);

    final JobManifest manifestToPublicApi = new JobManifest()
            .withLocation(manifestLocation)
            .withSpec(manifestSpec);

    final String jobReportBucketArn = "arn:aws:s3:::amzn-s3-demo-completion-report-
bucket";
    final String jobReportPrefix = "example-job-reports";

    final JobReport jobReport = new JobReport()
            .withEnabled(true)
            .withReportScope(JobReportScope.AllTasks)
            .withBucket(jobReportBucketArn)
            .withPrefix(jobReportPrefix)
            .withFormat(JobReportFormat.Report_CSV_20180820);

    final String lambdaFunctionArn = "arn:aws:lambda:us-
west-2:123456789012:function:example-function";

    final JobOperation jobOperation = new JobOperation()
            .withLambdaInvoke(new
 LambdaInvokeOperation().withFunctionArn(lambdaFunctionArn));

    final S3Tag departmentTag = new
 S3Tag().withKey("department").withValue("Marketing");
    final S3Tag fiscalYearTag = new S3Tag().withKey("FiscalYear").withValue("2020");

    final String roleArn = "arn:aws:iam::123456789012:role/example-batch-operations-
role";
    final Boolean requiresConfirmation = true;
    final int priority = 10;
```

```
    final CreateJobRequest request = new CreateJobRequest()
            .withAccountId("123456789012")
            .withDescription("Test lambda job")
            .withManifest(manifestToPublicApi)
            .withOperation(jobOperation)
            .withPriority(priority)
            .withRoleArn(roleArn)
            .withReport(jobReport)
            .withTags(departmentTag, fiscalYearTag)
            .withConfirmationRequired(requiresConfirmation);

    final CreateJobResult result = awss3ControlClient.createJob(request);

    return result.getJobId();
}
```

Excluir as tags de um trabalho do Operações em lote do S3

Você pode usar esses exemplos para excluir as tags de um trabalho do Operações em Lote do Amazon S3.

Usar a AWS CLI

O exemplo a seguir exclui as tags de um trabalho do Batch Operations usando a AWS CLI.

```
aws \
    s3control delete-job-tagging \
    --account-id 123456789012 \
    --job-id Example-e25a-4ed2-8bee-7f8ed7fc2f1c \
    --region us-east-1
```

Excluir as tags de um trabalho de operações em lote

Example

O exemplo a seguir exclui as tags de um trabalho do S3 Batch Operations usando o AWS SDK para Java.

```
public void deleteJobTagging(final AWSS3ControlClient awss3ControlClient,
                             final String jobId) {
    final DeleteJobTaggingRequest deleteJobTaggingRequest = new
 DeleteJobTaggingRequest()
```

```
            .withJobId(jobId);

    final DeleteJobTaggingResult deleteJobTaggingResult =
                awss3ControlClient.deleteJobTagging(deleteJobTaggingRequest);
}
```

Adicionar tags a um trabalho existente do Operações em Lote

Você pode usar a operação de API PutJobTagging para adicionar tags aos trabalhos existentes do Operações em Lote do Amazon S3. Para obter mais informações, veja os exemplos a seguir:

Usar a AWS CLI

Veja a seguir um exemplo de uso de `s3control put-job-tagging` para adicionar tags aos trabalhos do Operações em Lote do S3 usando a AWS CLI. Para usar os exemplos, substitua *`user input placeholders`* por suas próprias informações.

> **Note**
>
> Se você enviar essa solicitação com o conjunto de tags vazio, o Operações em Lote excluirá o conjunto de tags existente no objeto. No entanto, se você usar essa abordagem, receberá cobrança por uma solicitação de nível 1 (PUT). Para obter mais informações, consulte Preço do Amazon S3.
>
> Em vez disso, para excluir tags existentes do trabalho do Operações em Lote, recomendamos usar a operação `DeleteJobTagging` porque ela consegue o mesmo resultado sem incorrer em cobranças.

1. Identifique as TAGS que você deseja para o trabalho. Nesse caso, você aplica duas tags, *`department`* e *`FiscalYear`*, com os valores *`Marketing`* e *`2020`*, respectivamente.

```
read -d '' TAGS <<EOF
[
  {
    "Key": "department",
    "Value": "Marketing"
  },
  {
    "Key": "FiscalYear",
    "Value": "2020"
  }
```

```
]
EOF
```

2. Execute o seguinte comando `put-job-tagging` com os parâmetros exigidos:

```
aws \
    s3control put-job-tagging \
    --account-id 123456789012 \
    --tags "${TAGS//$'\n'/}" \
    --job-id Example-e25a-4ed2-8bee-7f8ed7fc2f1c \
    --region us-east-1
```

Usar o AWS SDK para Java

Example

O exemplo a seguir coloca as tags de um trabalho do Operações em Lote do S3 usando o AWS SDK para Java.

```
public void putJobTagging(final AWSS3ControlClient awss3ControlClient,
                          final String jobId) {
    final S3Tag departmentTag = new
 S3Tag().withKey("department").withValue("Marketing");
    final S3Tag fiscalYearTag = new S3Tag().withKey("FiscalYear").withValue("2020");

    final PutJobTaggingRequest putJobTaggingRequest = new PutJobTaggingRequest()
            .withJobId(jobId)
            .withTags(departmentTag, fiscalYearTag);

    final PutJobTaggingResult putJobTaggingResult =
 awss3ControlClient.putJobTagging(putJobTaggingRequest);
}
```

Obter as tags de um trabalho do Operações em lote S3

Para recuperar as tags de um trabalho do Operações em Lote do Amazon S3, você pode usar a operação de API `GetJobTagging`. Para obter mais informações, veja os exemplos a seguir:

Usar a AWS CLI

O exemplo a seguir obtém as tags de um trabalho do Batch Operations usando a AWS CLI. Para usar esse exemplo, substitua os *`user input placeholders`* por suas próprias informações.

```
aws \
    s3control get-job-tagging \
    --account-id 123456789012 \
    --job-id Example-e25a-4ed2-8bee-7f8ed7fc2f1c \
    --region us-east-1
```

Usar o AWS SDK for Java

Example

O exemplo a seguir obtém as tags de um trabalho do S3 Batch Operations usando a AWS SDK para Java.

```
public List<S3Tag> getJobTagging(final AWSS3ControlClient awss3ControlClient,
                                 final String jobId) {
    final GetJobTaggingRequest getJobTaggingRequest = new GetJobTaggingRequest()
            .withJobId(jobId);

    final GetJobTaggingResult getJobTaggingResult =
            awss3ControlClient.getJobTagging(getJobTaggingRequest);

    final List<S3Tag> tags = getJobTaggingResult.getTags();

    return tags;
}
```

Controlar permissões para o Operações em Lote usando tags de trabalho

Para ajudar a gerenciar trabalhos do Operações em Lote do Amazon S3, você pode adicionar tags de trabalho. Com tags de trabalho, você pode controlar o acesso aos seus trabalhos de operações em lote e impor que as tags sejam aplicadas quando qualquer trabalho for criado.

Você pode aplicar até 50 tags de trabalho a cada trabalho de operações em lote. O uso de tags permite que você defina políticas detalhadas para restringir o conjunto de usuários que podem editar o trabalho. As tags de trabalho podem conceder ou limitar a capacidade do usuário de cancelar um trabalho, ativar um trabalho no estado de confirmação ou alterar o nível de prioridade de um trabalho. Além disso, você pode impor que as tags sejam aplicadas a todos os novos trabalhos e especificar os pares de chave-valor permitidos para as tags. Você pode expressar todas essas condições usando a linguagem de política do AWS Identity and Access Management (IAM). Consulte mais informações em Actions, resources, and condition keys for Amazon S3 na Referência de autorização do serviço.

Para ter mais informações sobre as permissões referentes a operações de API do S3 de acordo com os tipos de recurso do S3, consulte Permissões obrigatórias para operações de API do Amazon S3.

O exemplo a seguir mostra como você pode usar tags de trabalho de operações em lote do S3 para conceder aos usuários permissão para criar e editar somente os trabalhos executados em um departamento específico (por exemplo, o departamento Finanças ou Conformidade). Você também pode atribuir trabalhos com base no estágio de desenvolvimento ao qual eles estão relacionados, como QA ou Produção.

Neste exemplo, você usa tags de trabalho do Operações em Lote do S3 nas políticas do IAM para conceder aos usuários permissão para criar e editar apenas os trabalhos que estão sendo executados no departamento deles. Você atribui trabalhos com base no estágio de desenvolvimento ao qual eles estão relacionados, como QA ou Produção.

Os exemplos a seguir usam os seguintes departamentos, com cada um usando o Operações em Lote de maneiras diferentes:

- Finanças
- Conformidade
- Business Intelligence
- Engenharia

Tópicos

- Controlar o acesso atribuindo tags a usuários e recursos
- Marcar trabalhos de operações em lote por estágio e impor limites na prioridade do trabalho

Controlar o acesso atribuindo tags a usuários e recursos

Nesse cenário, os administradores estão usando o controle de acesso baseado em atributos (ABAC). ABAC é uma estratégia de autorização do IAM que define permissões anexando etiquetas a usuários e recursos da AWS.

Os usuários e os trabalhos recebem uma das seguintes tags de departamento:

Chave: valor

- `department : Finance`
- `department : Compliance`

- `department : BusinessIntelligence`
- `department : Engineering`

> **Note**
>
> As chaves e os valores de tags de trabalho diferenciam maiúsculas de minúsculas.

Usando a estratégia de controle de acesso ABAC, você concede a um usuário no departamento de finanças permissão para criar e gerenciar trabalhos de Operações em Lote do S3 em seu departamento associando a etiqueta `department=Finance` ao usuário.

Além disso, você pode anexar uma política gerenciada ao usuário do IAM que permite que qualquer usuário em sua empresa crie ou modifique trabalhos de operações em lote do S3 dentro de seus respectivos departamentos.

A política neste exemplo inclui três instruções de política:

- A primeira instrução na política permite que o usuário crie um trabalho de operações em lote desde que a solicitação de criação de trabalho inclua uma tag de trabalho que corresponda ao respectivo departamento. Isso é expresso usando a sintaxe `"${aws:PrincipalTag/department}"`, que é substituída pela etiqueta de departamento do usuário no momento da avaliação da política. A condição é satisfeita quando o valor fornecido para a tag de departamento na solicitação (`"aws:RequestTag/department"`) corresponde ao departamento do usuário.
- A segunda instrução na política permite que os usuários alterem a prioridade dos trabalhos ou atualizem o status de um trabalho, desde que o trabalho que o usuário está atualizando corresponda ao departamento do usuário.
- A terceira instrução permite que um usuário atualize as tags de um trabalho de operações em lote a qualquer momento por meio de uma solicitação `PutJobTagging`, desde que (1) sua tag de departamento seja preservada e (2) o trabalho que está atualizando esteja dentro de seu departamento.

```
{
      "Version": "2012-10-17",
      "Statement": [
            {
                  "Effect": "Allow",
                  "Action": "s3:CreateJob",
```

```
                "Resource": "*",
                "Condition": {
                      "StringEquals": {
                            "aws:RequestTag/department": "${aws:PrincipalTag/
department}"
                }
            }
        },
            {
                "Effect": "Allow",
                "Action": [
                      "s3:UpdateJobPriority",
                      "s3:UpdateJobStatus"
            ],
                "Resource": "*",
                "Condition": {
                      "StringEquals": {
                            "aws:ResourceTag/department": "${aws:PrincipalTag/
department}"
                }
            }
        },
            {
                "Effect": "Allow",
                "Action": "s3:PutJobTagging",
                "Resource": "*",
                "Condition": {
                      "StringEquals": {
                            "aws:RequestTag/department": "${aws:PrincipalTag/
department}",
                            "aws:ResourceTag/department": "${aws:PrincipalTag/
department}"
                }
            }
        }
    ]
}
```

Marcar trabalhos de operações em lote por estágio e impor limites na prioridade do trabalho

Todos os trabalhos de operações em lote do S3 têm uma prioridade numérica, que o Amazon S3 usa para decidir em que ordem executar os trabalhos. Para este exemplo, você restringe a prioridade

máxima que a maioria dos usuários pode atribuir a trabalhos, com intervalos de prioridade mais altos reservados para um conjunto limitado de usuários privilegiados, da seguinte forma:

- Intervalo de prioridade do estágio de QA (baixa): 1–100
- Intervalo de prioridade do estágio de produção (alta): 1–300

Para fazer isso, introduza um novo conjunto de tags representando o estágio do trabalho:

Chave: valor

- `stage : QA`
- `stage : Production`

Criar e atualizar trabalhos de baixa prioridade em um departamento

Esta política introduz duas novas restrições à criação e atualização de trabalhos de operações em lote do S3, além da restrição baseada em departamento:

- Ele permite que os usuários criem ou atualizem trabalhos em seu departamento com uma nova condição que requer que o trabalho inclua a tag `stage=QA`.
- Ele permite que os usuários criem ou atualizem a prioridade de um trabalho até uma nova prioridade máxima de 100.

```
{
        "Version": "2012-10-17",
        "Statement": [
        {
        "Effect": "Allow",
        "Action": "s3:CreateJob",
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "aws:RequestTag/department": "${aws:PrincipalTag/department}",
                "aws:RequestTag/stage": "QA"
            },
            "NumericLessThanEquals": {
                "s3:RequestJobPriority": 100
            }
        }
```

```
    },
    {
        "Effect": "Allow",
        "Action": [
            "s3:UpdateJobStatus"
        ],
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "aws:ResourceTag/department": "${aws:PrincipalTag/department}"
            }
        }
    },
    {
        "Effect": "Allow",
        "Action": "s3:UpdateJobPriority",
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "aws:ResourceTag/department": "${aws:PrincipalTag/department}",
                "aws:ResourceTag/stage": "QA"
            },
            "NumericLessThanEquals": {
                "s3:RequestJobPriority": 100
            }
        }
    },
    {
        "Effect": "Allow",
        "Action": "s3:PutJobTagging",
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "aws:RequestTag/department" : "${aws:PrincipalTag/department}",
                "aws:ResourceTag/department": "${aws:PrincipalTag/department}",
                "aws:RequestTag/stage": "QA",
                "aws:ResourceTag/stage": "QA"
            }
        }
    },
    {
        "Effect": "Allow",
        "Action": "s3:GetJobTagging",
        "Resource": "*"
```

```
    }
    ]
}
```

Criar e atualizar trabalhos de alta prioridade em um departamento

Um pequeno número de usuários pode exigir a capacidade de criar trabalhos de alta prioridade em QA ou Produção. Para dar suporte a essa necessidade, crie uma política gerenciada adaptada da política de baixa prioridade na seção anterior.

Essa política faz o seguinte:

- Permite que os usuários criem ou atualizem trabalhos em seu departamento com a tag `stage=QA` ou `stage=Production`.
- Permite que os usuários criem ou atualizem a prioridade de um trabalho até um máximo de 300.

```
{
      "Version": "2012-10-17",
      "Statement": [
          {
                "Effect": "Allow",
                "Action": "s3:CreateJob",
                "Resource": "*",
                "Condition": {
                      "ForAnyValue:StringEquals": {
                            "aws:RequestTag/stage": [
                                  "QA",
                                  "Production"
                    ]
                },
                      "StringEquals": {
                            "aws:RequestTag/department": "${aws:PrincipalTag/
department}"
                },
                      "NumericLessThanEquals": {
                            "s3:RequestJobPriority": 300
                }
             }
        },
          {
                "Effect": "Allow",
                "Action": [
```

```
                    "s3:UpdateJobStatus"
            ],
                "Resource": "*",
                "Condition": {
                    "StringEquals": {
                        "aws:ResourceTag/department": "${aws:PrincipalTag/
department}"
                }
            }
        },
          {
                "Effect": "Allow",
                "Action": "s3:UpdateJobPriority",
                "Resource": "*",
                "Condition": {
                    "ForAnyValue:StringEquals": {
                        "aws:ResourceTag/stage": [
                            "QA",
                            "Production"
                    ]
                },
                    "StringEquals": {
                        "aws:ResourceTag/department": "${aws:PrincipalTag/
department}"
                },
                    "NumericLessThanEquals": {
                        "s3:RequestJobPriority": 300
                }
            }
        },
          {
                "Effect": "Allow",
                "Action": "s3:PutJobTagging",
                "Resource": "*",
                "Condition": {
                    "StringEquals": {
                        "aws:RequestTag/department": "${aws:PrincipalTag/
department}",
                        "aws:ResourceTag/department": "${aws:PrincipalTag/
department}"
                },
                    "ForAnyValue:StringEquals": {
                        "aws:RequestTag/stage": [
                            "QA",
```

```
                                "Production"
                    ],
                            "aws:ResourceTag/stage": [
                                "QA",
                                "Production"
                    ]
                }
            }
        }
    ]
}
```

Gerenciar o Bloqueio de objetos do S3 usando o Operações em lote do S3

Você pode usar operações em lote do S3 para executar operações em lote de grande escala em objetos do Amazon S3. As operações em lote do S3 podem executar uma única operação em listas de objetos do Amazon S3 especificadas. Um único trabalho pode realizar uma operação especificada em bilhões de objetos contendo exabytes de dados. O Amazon S3 monitora o progresso, envia notificações e armazena um relatório de conclusão detalhado de todas as ações, fornecendo uma experiência totalmente gerenciada, auditável e sem servidor. É possível usar o recurso Operações em Lote do S3 por meio do console do Amazon S3, da AWS CLI, de SDKs da AWS ou da API REST do Amazon S3.

Com o bloqueio de objetos do S3, você também pode colocar uma retenção legal em uma versão de objeto. Assim como a definição de um período de retenção, uma retenção legal evita que uma versão do objeto seja substituída ou excluída. No entanto, uma retenção legal não tem um período de retenção associado e permanece em vigor até ser removida. Para obter mais informações, consulte Retenção legal do Bloqueio de objetos do S3.

Para adicionar retenções legais a vários objetos do Amazon S3 de uma só vez usando o Operações em Lote do S3 com o Bloqueio de Objetos, consulte os tópicos a seguir.

Tópicos

- Habilitar o Bloqueio de objetos do S3 usando o Operações em lote do S3
- Definir a retenção do Bloqueio de Objetos usando o Operações em Lote
- Usar operações em lote do S3 com o modo de conformidade de retenção do bloqueio de objetos do S3
- Usar operações em lote do S3 com modo de governança de retenção de bloqueio de objetos do S3

- Usar o Operações em Lote do S3 para desativar retenções legais do Bloqueio de Objetos do S3

Habilitar o Bloqueio de objetos do S3 usando o Operações em lote do S3

É possível usar o Operações em Lote do Amazon S3 com o Bloqueio de Objetos do S3 para gerenciar a retenção ou habilitar uma retenção legal para vários objetos do Amazon S3 de uma só vez. Especifique a lista de objetos de destino no manifesto e envie-a para as operações em lote para conclusão. Para obter mais informações, consulte the section called “Retenção do Bloqueio de objetos” e the section called “Retenção legal do Bloqueio de objetos”.

Os exemplos a seguir mostram como criar um perfil do AWS Identity and Access Management (IAM) com permissões do Operações em Lote do S3 e atualizar as permissões do perfil para criar trabalhos que habilitem o Bloqueio de Objetos. Você também deve ter um manifesto `CSV` que identifica os objetos para o trabalho do Operações em Lote do S3. Para obter mais informações, consulte the section called “Especificar um manifesto”.

Para usar os exemplos a seguir, substitua *`user input placeholders`* por suas próprias informações.

Como usar o AWS CLI

1. Crie uma função do IAM e atribua permissões de operações em lote do S3 para executar.

   Esta etapa é necessária para todos os trabalhos de operações em lote do S3.

```
export AWS_PROFILE='aws-user'

read -d '' batch_operations_trust_policy <<EOF
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "batchoperations.s3.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
```

```
}
EOF
aws iam create-role --role-name batch_operations-objectlock \
--assume-role-policy-document "${batch_operations_trust_policy}"
```

2. Configure operações em lote do S3 com bloqueio de objeto do S3 para executar.

   Nesta etapa, permita que a função faça o seguinte:

   a. Execute o bloqueio de objeto no bucket do S3 que contém os objetos de destino nos quais você deseja que as operações em lote sejam executadas.

   b. Leia o bucket do S3 no qual estão localizados o arquivo CSV de manifesto e os objetos.

   c. Grave os resultados do trabalho de operações em lote do S3 no bucket de relatórios.

```
read -d '' batch_operations_permissions <<EOF
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:GetBucketObjectLockConfiguration",
            "Resource": [
                "arn:aws:s3:::{{amzn-s3-demo-manifest-bucket}}"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion",
                "s3:GetBucketLocation"
            ],
            "Resource": [
                "arn:aws:s3:::{{amzn-s3-demo-manifest-bucket}}/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetBucketLocation"
            ],
```

```
            "Resource": [
                "arn:aws:s3:::{{amzn-s3-demo-completion-report-bucket}}/*"
            ]
        }
    ]
}
EOF

aws iam put-role-policy --role-name batch_operations-objectlock \
--policy-name object-lock-permissions \
--policy-document "${batch_operations_permissions}"
```

Usar o AWS SDK for Java

Os exemplos a seguir mostram como criar um perfil do IAM com permissões do Operações em Lote do S3 e atualizar as permissões de perfil para criar trabalhos que habilitem o Bloqueio de Objetos usando o AWS SDK para Java. Você também deve ter um manifesto CSV identificando os objetos para o trabalho de operações em lote do S3. Para obter mais informações, consulte the section called “Especificar um manifesto”.

Siga estas etapas:

1. Crie uma função do IAM e atribua permissões de operações em lote do S3 para executar. Esta etapa é necessária para todos os trabalhos de operações em lote do S3.
2. Configure operações em lote do S3 com bloqueio de objeto do S3 para executar.

   Permita que a função faça o seguinte:

   1. Execute o bloqueio de objeto no bucket do S3 que contém os objetos de destino nos quais você deseja que as operações em lote sejam executadas.
   2. Leia o bucket do S3 no qual estão localizados o arquivo CSV de manifesto e os objetos.
   3. Grave os resultados do trabalho de operações em lote do S3 no bucket de relatórios.

```
public void createObjectLockRole() {
    final String roleName = "batch_operations-object-lock";

    final String trustPolicy = "{" +
            "  \"Version\": \"2012-10-17\", " +
            "  \"Statement\": [ " +
```

```
            "    { " +
            "      \"Effect\": \"Allow\", " +
            "      \"Principal\": { " +
            "        \"Service\": [" +
            "          \"batchoperations.s3.amazonaws.com\"" +
            "        ]" +
            "      }, " +
            "      \"Action\": \"sts:AssumeRole\" " +
            "    } " +
            "  ]" +
            "}";

    final String bopsPermissions = "{" +
            "    \"Version\": \"2012-10-17\"," +
            "    \"Statement\": [" +
            "        {" +
            "            \"Effect\": \"Allow\"," +
            "            \"Action\": \"s3:GetBucketObjectLockConfiguration\"," +
            "            \"Resource\": [" +
            "                \"arn:aws:s3:::amzn-s3-demo-manifest-bucket\"" +
            "            ]" +
            "        }," +
            "        {" +
            "            \"Effect\": \"Allow\"," +
            "            \"Action\": [" +
            "                \"s3:GetObject\"," +
            "                \"s3:GetObjectVersion\"," +
            "                \"s3:GetBucketLocation\"" +
            "            ]," +
            "            \"Resource\": [" +
            "                \"arn:aws:s3:::amzn-s3-demo-manifest-bucket/*\"" +
            "            ]" +
            "        }," +
            "        {" +
            "            \"Effect\": \"Allow\"," +
            "            \"Action\": [" +
            "                \"s3:PutObject\"," +
            "                \"s3:GetBucketLocation\"" +
            "            ]," +
            "            \"Resource\": [" +
            "                \"arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*\""
 +
            "            ]" +
            "        }" +
```

```
            "    ]" +
            "}";

    final AmazonIdentityManagement iam =
            AmazonIdentityManagementClientBuilder.defaultClient();

    final CreateRoleRequest createRoleRequest = new CreateRoleRequest()
            .withAssumeRolePolicyDocument(bopsPermissions)
            .withRoleName(roleName);

    final CreateRoleResult createRoleResult = iam.createRole(createRoleRequest);

    final PutRolePolicyRequest putRolePolicyRequest = new PutRolePolicyRequest()
            .withPolicyDocument(bopsPermissions)
            .withPolicyName("batch_operations-permissions")
            .withRoleName(roleName);

    final PutRolePolicyResult putRolePolicyResult =
 iam.putRolePolicy(putRolePolicyRequest);
}
```

Definir a retenção do Bloqueio de Objetos usando o Operações em Lote

É possível usar o Operações em Lote do Amazon S3 com o Bloqueio de Objetos do S3 para gerenciar a retenção de vários objetos do Amazon S3 de uma só vez. Especifique a lista de objetos de destino no manifesto e envie-a para as operações em lote para conclusão. Para obter mais informações, consulte the section called “Retenção do Bloqueio de objetos” e the section called “Retenção legal do Bloqueio de objetos”.

Os exemplos a seguir mostram como criar um perfil do AWS Identity and Access Management (IAM) com permissões do Operações em Lote do S3 e atualizar as permissões do perfil para incluir as permissões `s3:PutObjectRetention` de modo que possa executar a retenção do Bloqueio de Objetos do S3 nos objetos do bucket do manifesto. Você também deve ter um manifesto `CSV` que identifica os objetos para o trabalho do Operações em Lote do S3. Para obter mais informações, consulte the section called “Especificar um manifesto”.

Para usar os exemplos a seguir, substitua *`user input placeholders`* por suas próprias informações.

Como usar o AWS CLI

O exemplo AWS CLI a seguir mostra como usar o Operações em Lote para aplicar a retenção do Bloqueio de Objetos do S3 a vários objetos.

```
export AWS_PROFILE='aws-user'

read -d '' retention_permissions <<EOF
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObjectRetention"
            ],
            "Resource": [
                "arn:aws:s3:::{{amzn-s3-demo-manifest-bucket}}/*"
            ]
        }
    ]
}
EOF

aws iam put-role-policy --role-name batch_operations-objectlock --policy-
name retention-permissions --policy-document "${retention_permissions}"
```

Usar o AWS SDK para Java

O exemplo AWS SDK para Java a seguir mostra como usar o Operações em Lote para aplicar a retenção do Bloqueio de Objetos do S3 a vários objetos.

```
public void allowPutObjectRetention() {
    final String roleName = "batch_operations-object-lock";

    final String retentionPermissions = "{" +
            "    \"Version\": \"2012-10-17\"," +
            "    \"Statement\": [" +
            "        {" +
            "            \"Effect\": \"Allow\"," +
            "            \"Action\": [" +
            "                \"s3:PutObjectRetention\"" +
            "            ]," +
```

```
            "            \"Resource\": [" +
            "                \"arn:aws:s3:::amzn-s3-demo-manifest-bucket*\"" +
            "            ]" +
            "        }" +
            "    ]" +
            "}";

    final AmazonIdentityManagement iam =
            AmazonIdentityManagementClientBuilder.defaultClient();

    final PutRolePolicyRequest putRolePolicyRequest = new PutRolePolicyRequest()
            .withPolicyDocument(retentionPermissions)
            .withPolicyName("retention-permissions")
            .withRoleName(roleName);

    final PutRolePolicyResult putRolePolicyResult =
 iam.putRolePolicy(putRolePolicyRequest);
}
```

Usar operações em lote do S3 com o modo de conformidade de retenção do bloqueio de objetos do S3

O exemplo a seguir baseia-se nos exemplos anteriores de criação de uma política de confiança e na definição de permissões de configuração do Operações em lote do S3 e Bloqueio de objetos do S3 em seus objetos. Este exemplo define o modo de retenção como `COMPLIANCE` e `retain until date` como 1.º de janeiro de 2025. Esse exemplo cria um trabalho que visa objetos no bucket de manifesto e relata os resultados no bucket de relatórios identificado.

Para usar os exemplos a seguir, substitua *`user input placeholders`* por suas próprias informações.

Como usar o AWS CLI

Os exemplos da AWS CLI a seguir mostram como usar o Operações em Lote para aplicar o modo de conformidade de retenção do Bloqueio de Objetos do S3 a vários objetos.

Example – Definir o modo de conformidade de retenção do Bloqueio de Objetos do S3 em vários objetos

```
export AWS_PROFILE='aws-user'
export AWS_DEFAULT_REGION='us-west-2'
export ACCOUNT_ID=123456789012
```

```
export ROLE_ARN='arn:aws:iam::123456789012:role/batch_operations-objectlock'

read -d '' OPERATION <<EOF
{
  "S3PutObjectRetention": {
    "Retention": {
      "RetainUntilDate":"2025-01-01T00:00:00",
      "Mode":"COMPLIANCE"
    }
  }
}
EOF

read -d '' MANIFEST <<EOF
{
  "Spec": {
    "Format": "S3BatchOperations_CSV_20180820",
    "Fields": [
      "Bucket",
      "Key"
    ]
  },
  "Location": {
    "ObjectArn": "arn:aws:s3:::amzn-s3-demo-manifest-bucket/compliance-objects-
manifest.csv",
    "ETag": "Your-manifest-ETag"
  }
}
EOF

read -d '' REPORT <<EOF
{
  "Bucket": "arn:aws:s3:::ReportBucket",
  "Format": "Report_CSV_20180820",
  "Enabled": true,
  "Prefix": "amzn-s3-demo-completion-report-bucket/compliance-objects-batch-
operations",
  "ReportScope": "AllTasks"
}
EOF

aws \
    s3control create-job \
    --account-id "${ACCOUNT_ID}" \
```

```
    --manifest "${MANIFEST//$'\n'}" \
    --operation "${OPERATION//$'\n'/}" \
    --report "${REPORT//$'\n'}" \
    --priority 10 \
    --role-arn "${ROLE_ARN}" \
    --client-request-token "$(uuidgen)" \
    --region "${AWS_DEFAULT_REGION}" \
    --description "Set compliance retain-until to 1 Jul 2030";
```

Example – Estender o **`retain until date`** do modo de **`COMPLIANCE`** para 15 de janeiro de 2025

O exemplo a seguir estende a `retain until date` do modo de `COMPLIANCE` para 15 de janeiro de 2025.

```
export AWS_PROFILE='aws-user'
export AWS_DEFAULT_REGION='us-west-2'
export ACCOUNT_ID=123456789012
export ROLE_ARN='arn:aws:iam::123456789012:role/batch_operations-objectlock'

read -d '' OPERATION <<EOF
{
  "S3PutObjectRetention": {
    "Retention": {
      "RetainUntilDate":"2025-01-15T00:00:00",
      "Mode":"COMPLIANCE"
    }
  }
}
EOF

read -d '' MANIFEST <<EOF
{
  "Spec": {
    "Format": "S3BatchOperations_CSV_20180820",
    "Fields": [
      "Bucket",
      "Key"
    ]
  },
  "Location": {
    "ObjectArn": "arn:aws:s3:::amzn-s3-demo-manifest-bucket/compliance-objects-
manifest.csv",
    "ETag": "Your-manifest-ETag"
```

```
  }
}
EOF

read -d '' REPORT <<EOF
{
  "Bucket": "arn:aws:s3:::amzn-s3-demo-completion-report-bucket",
  "Format": "Report_CSV_20180820",
  "Enabled": true,
  "Prefix": "reports/compliance-objects-batch_operations",
  "ReportScope": "AllTasks"
}
EOF

aws \
    s3control create-job \
    --account-id "${ACCOUNT_ID}" \
    --manifest "${MANIFEST//$'\n'}" \
    --operation "${OPERATION//$'\n'/}" \
    --report "${REPORT//$'\n'}" \
    --priority 10 \
    --role-arn "${ROLE_ARN}" \
    --client-request-token "$(uuidgen)" \
    --region "${AWS_DEFAULT_REGION}" \
    --description "Extend compliance retention to 15 Jan 2025";
```

Usar o AWS SDK for Java

Os exemplos da AWS SDK para Java a seguir mostram como usar o Operações em Lote para aplicar o modo de conformidade de retenção do Bloqueio de Objetos do S3 a vários objetos.

Example – Definir o modo de retenção como COMPLIANCE e o prazo de retenção para 1.º de janeiro de 2025

```
public String createComplianceRetentionJob(final AWSS3ControlClient awss3ControlClient)
 throws ParseException {
    final String manifestObjectArn = "arn:aws:s3:::amzn-s3-demo-manifest-bucket/
compliance-objects-manifest.csv";
    final String manifestObjectVersionId = "your-object-version-Id";

    final JobManifestLocation manifestLocation = new JobManifestLocation()
            .withObjectArn(manifestObjectArn)
            .withETag(manifestObjectVersionId);
```

```
    final JobManifestSpec manifestSpec =
            new JobManifestSpec()
                    .withFormat(JobManifestFormat.S3BatchOperations_CSV_20180820)
                    .withFields("Bucket", "Key");

    final JobManifest manifestToPublicApi = new JobManifest()
            .withLocation(manifestLocation)
            .withSpec(manifestSpec);

    final String jobReportBucketArn = "arn:aws:s3:::amzn-s3-demo-completion-report-
bucket";
    final String jobReportPrefix = "reports/compliance-objects-bops";

    final JobReport jobReport = new JobReport()
            .withEnabled(true)
            .withReportScope(JobReportScope.AllTasks)
            .withBucket(jobReportBucketArn)
            .withPrefix(jobReportPrefix)
            .withFormat(JobReportFormat.Report_CSV_20180820);

    final SimpleDateFormat format = new SimpleDateFormat("dd/MM/yyyy");
    final Date janFirst = format.parse("01/01/2025");

    final JobOperation jobOperation = new JobOperation()
            .withS3PutObjectRetention(new S3SetObjectRetentionOperation()
                    .withRetention(new S3Retention()
                            .withMode(S3ObjectLockRetentionMode.COMPLIANCE)
                            .withRetainUntilDate(janFirst)));

    final String roleArn = "arn:aws:iam::123456789012:role/batch_operations-object-
lock";
    final Boolean requiresConfirmation = true;
    final int priority = 10;

    final CreateJobRequest request = new CreateJobRequest()
            .withAccountId("123456789012")
            .withDescription("Set compliance retain-until to 1 Jan 2025")
            .withManifest(manifestToPublicApi)
            .withOperation(jobOperation)
            .withPriority(priority)
            .withRoleArn(roleArn)
            .withReport(jobReport)
            .withConfirmationRequired(requiresConfirmation);
```

```
    final CreateJobResult result = awss3ControlClient.createJob(request);

    return result.getJobId();
}
```

Example – Estender o **`retain until date`** do modo **`COMPLIANCE`**

O exemplo a seguir estende o `retain until date` do modo de `COMPLIANCE` para 15 de janeiro de 2025.

```
public String createExtendComplianceRetentionJob(final AWSS3ControlClient
 awss3ControlClient) throws ParseException {
    final String manifestObjectArn = "arn:aws:s3:::amzn-s3-demo-manifest-bucket/
compliance-objects-manifest.csv";
    final String manifestObjectVersionId = "15ad5ba069e6bbc465c77bf83d541385";

    final JobManifestLocation manifestLocation = new JobManifestLocation()
            .withObjectArn(manifestObjectArn)
            .withETag(manifestObjectVersionId);

    final JobManifestSpec manifestSpec =
            new JobManifestSpec()
                    .withFormat(JobManifestFormat.S3BatchOperations_CSV_20180820)
                    .withFields("Bucket", "Key");

    final JobManifest manifestToPublicApi = new JobManifest()
            .withLocation(manifestLocation)
            .withSpec(manifestSpec);

    final String jobReportBucketArn = "arn:aws:s3:::amzn-s3-demo-completion-report-
bucket";
    final String jobReportPrefix = "reports/compliance-objects-batch_operations";

    final JobReport jobReport = new JobReport()
            .withEnabled(true)
            .withReportScope(JobReportScope.AllTasks)
            .withBucket(jobReportBucketArn)
            .withPrefix(jobReportPrefix)
            .withFormat(JobReportFormat.Report_CSV_20180820);

    final SimpleDateFormat format = new SimpleDateFormat("dd/MM/yyyy");
    final Date jan15th = format.parse("15/01/2025");
```

```
    final JobOperation jobOperation = new JobOperation()
            .withS3PutObjectRetention(new S3SetObjectRetentionOperation()
                    .withRetention(new S3Retention()
                            .withMode(S3ObjectLockRetentionMode.COMPLIANCE)
                            .withRetainUntilDate(jan15th)));

    final String roleArn = "arn:aws:iam::123456789012:role/batch_operations-object-
lock";
    final Boolean requiresConfirmation = true;
    final int priority = 10;

    final CreateJobRequest request = new CreateJobRequest()
            .withAccountId("123456789012")
            .withDescription("Extend compliance retention to 15 Jan 2025")
            .withManifest(manifestToPublicApi)
            .withOperation(jobOperation)
            .withPriority(priority)
            .withRoleArn(roleArn)
            .withReport(jobReport)
            .withConfirmationRequired(requiresConfirmation);

    final CreateJobResult result = awss3ControlClient.createJob(request);

    return result.getJobId();
}
```

Usar operações em lote do S3 com modo de governança de retenção de bloqueio de objetos do S3

O exemplo a seguir baseia-se nos exemplos anteriores de criação de uma política de confiança e na definição de permissões de configuração de operações em lote do S3 e bloqueio de objetos do S3. Esse exemplo mostra como aplicar a vários objetos a governança de retenção do Bloqueio de Objetos do S3 com `retain until date` de 30 de janeiro de 2025. Ele cria um trabalho de operações em lote que usa o bucket de manifesto e relata os resultados no bucket de relatórios.

Para usar os exemplos a seguir, substitua *`user input placeholders`* por suas próprias informações.

Como usar o AWS CLI

Os exemplos da AWS CLI a seguir mostram como usar o Operações em Lote para aplicar o modo de governança de retenção do Bloqueio de Objetos do S3 a vários objetos.

Example – Aplicar a governança de retenção do Bloqueio de Objetos do S3 a vários objetos com o prazo de retenção de 30 de janeiro de 2025

```
export AWS_PROFILE='aws-user'
export AWS_DEFAULT_REGION='us-west-2'
export ACCOUNT_ID=123456789012
export ROLE_ARN='arn:aws:iam::123456789012:role/batch_operations-objectlock'

read -d '' OPERATION <<EOF
{
  "S3PutObjectRetention": {
    "Retention": {
      "RetainUntilDate":"2025-01-30T00:00:00",
      "Mode":"GOVERNANCE"
    }
  }
}
EOF

read -d '' MANIFEST <<EOF
{
  "Spec": {
    "Format": "S3BatchOperations_CSV_20180820",
    "Fields": [
      "Bucket",
      "Key"
    ]
  },
  "Location": {
    "ObjectArn": "arn:aws:s3:::amzn-s3-demo-manifest-bucket/governance-objects-
manifest.csv",
    "ETag": "Your-manifest-ETag"
  }
}
EOF

read -d '' REPORT <<EOF
{
```

```
  "Bucket": "arn:aws:s3:::amzn-s3-demo-completion-report-bucketT",
  "Format": "Report_CSV_20180820",
  "Enabled": true,
  "Prefix": "reports/governance-objects",
  "ReportScope": "AllTasks"
}
EOF

aws \
    s3control create-job \
    --account-id "${ACCOUNT_ID}" \
    --manifest "${MANIFEST//$'\n'}" \
    --operation "${OPERATION//$'\n'/}" \
    --report "${REPORT//$'\n'}" \
    --priority 10 \
    --role-arn "${ROLE_ARN}" \
    --client-request-token "$(uuidgen)" \
    --region "${AWS_DEFAULT_REGION}" \
    --description "Put governance retention";
```

Example – Ignorar a governança de retenção em vários objetos

O exemplo a seguir baseia-se nos exemplos anteriores de criação de uma política de confiança e na definição de permissões de configuração de operações em lote do S3 e bloqueio de objetos do S3. Ele mostra como ignorar a governança de retenção em vários objetos e cria um trabalho de operações em lote que usa o bucket de manifestos e relata os resultados no bucket de relatórios.

```
export AWS_PROFILE='aws-user'

read -d '' bypass_governance_permissions <<EOF
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:BypassGovernanceRetention"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
            ]
        }
    ]
```

```
}
EOF

aws iam put-role-policy --role-name batch-operations-objectlock --policy-name bypass-
governance-permissions --policy-document "${bypass_governance_permissions}"

export AWS_PROFILE='aws-user'
export AWS_DEFAULT_REGION='us-west-2'
export ACCOUNT_ID=123456789012
export ROLE_ARN='arn:aws:iam::123456789012:role/batch_operations-objectlock'

read -d '' OPERATION <<EOF
{
  "S3PutObjectRetention": {
    "BypassGovernanceRetention": true,
    "Retention": {
    }
  }
}
EOF

read -d '' MANIFEST <<EOF
{
  "Spec": {
    "Format": "S3BatchOperations_CSV_20180820",
    "Fields": [
      "Bucket",
      "Key"
    ]
  },
  "Location": {
    "ObjectArn": "arn:aws:s3:::amzn-s3-demo-manifest-bucket/governance-objects-
manifest.csv",
    "ETag": "Your-manifest-ETag"
  }
}
EOF

read -d '' REPORT <<EOF
{
  "Bucket": "arn:aws:s3:::amzn-s3-demo-completion-report-bucket",
  "Format": "Report_CSV_20180820",
  "Enabled": true,
  "Prefix": "reports/batch_operations-governance",
```

```
  "ReportScope": "AllTasks"
}
EOF

aws \
    s3control create-job \
    --account-id "${ACCOUNT_ID}" \
    --manifest "${MANIFEST//$'\n'}" \
    --operation "${OPERATION//$'\n'/}" \
    --report "${REPORT//$'\n'}" \
    --priority 10 \
    --role-arn "${ROLE_ARN}" \
    --client-request-token "$(uuidgen)" \
    --region "${AWS_DEFAULT_REGION}" \
    --description "Remove governance retention";
```

Usar o AWS SDK for Java

O exemplo a seguir baseia-se nos exemplos anteriores de criação de uma política de confiança e na definição de permissões de configuração de operações em lote do S3 e bloqueio de objetos do S3. Esse exemplo mostra como aplicar a vários objetos a governança de retenção do Bloqueio de Objetos do S3 com `retain until date` definido como 30 de janeiro de 2025. Esse exemplo cria um trabalho de operações em lote que usa o bucket de manifesto e relata os resultados no bucket de relatórios.

Example – Aplicar a governança de retenção do Bloqueio de Objetos do S3 a vários objetos com o prazo de retenção de 30 de janeiro de 2025

```
public String createGovernanceRetentionJob(final AWSS3ControlClient awss3ControlClient)
 throws ParseException {
    final String manifestObjectArn = "arn:aws:s3:::amzn-s3-demo-manifest-bucket/
governance-objects-manifest.csv";
    final String manifestObjectVersionId = "15ad5ba069e6bbc465c77bf83d541385";

    final JobManifestLocation manifestLocation = new JobManifestLocation()
            .withObjectArn(manifestObjectArn)
            .withETag(manifestObjectVersionId);

    final JobManifestSpec manifestSpec =
            new JobManifestSpec()
                    .withFormat(JobManifestFormat.S3BatchOperations_CSV_20180820)
                    .withFields("Bucket", "Key");
```

```
    final JobManifest manifestToPublicApi = new JobManifest()
            .withLocation(manifestLocation)
            .withSpec(manifestSpec);

    final String jobReportBucketArn = "arn:aws:s3:::amzn-s3-demo-completion-report-
bucket";
    final String jobReportPrefix = "reports/governance-objects";

    final JobReport jobReport = new JobReport()
            .withEnabled(true)
            .withReportScope(JobReportScope.AllTasks)
            .withBucket(jobReportBucketArn)
            .withPrefix(jobReportPrefix)
            .withFormat(JobReportFormat.Report_CSV_20180820);

    final SimpleDateFormat format = new SimpleDateFormat("dd/MM/yyyy");
    final Date jan30th = format.parse("30/01/2025");

    final JobOperation jobOperation = new JobOperation()
            .withS3PutObjectRetention(new S3SetObjectRetentionOperation()
                    .withRetention(new S3Retention()
                            .withMode(S3ObjectLockRetentionMode.GOVERNANCE)
                            .withRetainUntilDate(jan30th)));

    final String roleArn = "arn:aws:iam::123456789012:role/batch_operations-object-
lock";
    final Boolean requiresConfirmation = true;
    final int priority = 10;

    final CreateJobRequest request = new CreateJobRequest()
            .withAccountId("123456789012")
            .withDescription("Put governance retention")
            .withManifest(manifestToPublicApi)
            .withOperation(jobOperation)
            .withPriority(priority)
            .withRoleArn(roleArn)
            .withReport(jobReport)
            .withConfirmationRequired(requiresConfirmation);

    final CreateJobResult result = awss3ControlClient.createJob(request);

    return result.getJobId();
```

```
}
```

Example – Ignorar a governança de retenção em vários objetos

O exemplo a seguir baseia-se nos exemplos anteriores de criação de uma política de confiança e na definição de permissões de configuração de operações em lote do S3 e bloqueio de objetos do S3. Esse exemplo mostra como ignorar a governança de retenção em vários objetos e cria um trabalho de operações em lote que usa o bucket de manifesto e relata os resultados no bucket de relatórios.

```
public void allowBypassGovernance() {
    final String roleName = "batch_operations-object-lock";

    final String bypassGovernancePermissions = "{" +
            "    \"Version\": \"2012-10-17\"," +
            "    \"Statement\": [" +
            "        {" +
            "            \"Effect\": \"Allow\"," +
            "            \"Action\": [" +
            "                \"s3:BypassGovernanceRetention\"" +
            "            ]," +
            "            \"Resource\": [" +
            "                \"arn:aws:s3:::amzn-s3-demo-manifest-bucket/*\"" +
            "            ]" +
            "        }" +
            "    ]" +
            "}";

    final AmazonIdentityManagement iam =
            AmazonIdentityManagementClientBuilder.defaultClient();

    final PutRolePolicyRequest putRolePolicyRequest = new PutRolePolicyRequest()
            .withPolicyDocument(bypassGovernancePermissions)
            .withPolicyName("bypass-governance-permissions")
            .withRoleName(roleName);

    final PutRolePolicyResult putRolePolicyResult =
 iam.putRolePolicy(putRolePolicyRequest);
}
public String createRemoveGovernanceRetentionJob(final AWSS3ControlClient
 awss3ControlClient) {
    final String manifestObjectArn = "arn:aws:s3:::amzn-s3-demo-manifest-bucket/
governance-objects-manifest.csv";
    final String manifestObjectVersionId = "15ad5ba069e6bbc465c77bf83d541385";
```

```
    final JobManifestLocation manifestLocation = new JobManifestLocation()
            .withObjectArn(manifestObjectArn)
            .withETag(manifestObjectVersionId);

    final JobManifestSpec manifestSpec =
            new JobManifestSpec()
                    .withFormat(JobManifestFormat.S3BatchOperations_CSV_20180820)
                    .withFields("Bucket", "Key");

    final JobManifest manifestToPublicApi = new JobManifest()
            .withLocation(manifestLocation)
            .withSpec(manifestSpec);

    final String jobReportBucketArn = "arn:aws:s3:::amzn-s3-demo-completion-report-
bucket";
    final String jobReportPrefix = "reports/batch_operations-governance";

    final JobReport jobReport = new JobReport()
            .withEnabled(true)
            .withReportScope(JobReportScope.AllTasks)
            .withBucket(jobReportBucketArn)
            .withPrefix(jobReportPrefix)
            .withFormat(JobReportFormat.Report_CSV_20180820);

    final JobOperation jobOperation = new JobOperation()
            .withS3PutObjectRetention(new S3SetObjectRetentionOperation()
                    .withRetention(new S3Retention()));

    final String roleArn = "arn:aws:iam::123456789012:role/batch_operations-object-
lock";
    final Boolean requiresConfirmation = true;
    final int priority = 10;

    final CreateJobRequest request = new CreateJobRequest()
            .withAccountId("123456789012")
            .withDescription("Remove governance retention")
            .withManifest(manifestToPublicApi)
            .withOperation(jobOperation)
            .withPriority(priority)
            .withRoleArn(roleArn)
            .withReport(jobReport)
            .withConfirmationRequired(requiresConfirmation);
```

```
    final CreateJobResult result = awss3ControlClient.createJob(request);

    return result.getJobId();
}
```

Usar o Operações em Lote do S3 para desativar retenções legais do Bloqueio de Objetos do S3

O exemplo a seguir baseia-se nos exemplos anteriores de criação de uma política de confiança e na definição de permissões de configuração de operações em lote do S3 e bloqueio de objetos do S3. Esse exemplo mostra como desabilitar a retenção legal do Bloqueio de Objetos em objetos usando o Operações em Lote.

O exemplo primeiro atualiza a função para conceder permissões `s3:PutObjectLegalHold`, cria um trabalho de operações em lote que desativa (remove) a retenção legal dos objetos identificados no manifesto e, depois, cria um relatório.

Para usar os exemplos a seguir, substitua *`user input placeholders`* por suas próprias informações.

Como usar o AWS CLI

Os exemplos da AWS CLI a seguir mostram como usar o Operações em Lote para desativar retenções legais do Bloqueio de Objetos do S3 em vários objetos.

Example – Atualiza o perfil para conceder permissões **`s3:PutObjectLegalHold`**

```
export AWS_PROFILE='aws-user'

read -d '' legal_hold_permissions <<EOF
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObjectLegalHold"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
            ]
```

```
        }
    ]

EOF

aws iam put-role-policy --role-name batch_operations-objectlock --policy-name legal-
hold-permissions --policy-document "${legal_hold_permissions}"
```

Example – Desativar retenção legal

O exemplo a seguir desativa a retenção legal.

```
export AWS_PROFILE='aws-user'
export AWS_DEFAULT_REGION='us-west-2'
export ACCOUNT_ID=123456789012
export ROLE_ARN='arn:aws:iam::123456789012:role/batch_operations-objectlock'

read -d '' OPERATION <<EOF
{
  "S3PutObjectLegalHold": {
    "LegalHold": {
      "Status":"OFF"
    }
  }
}
EOF

read -d '' MANIFEST <<EOF
{
  "Spec": {
    "Format": "S3BatchOperations_CSV_20180820",
    "Fields": [
      "Bucket",
      "Key"
    ]
  },
  "Location": {
    "ObjectArn": "arn:aws:s3:::amzn-s3-demo-manifest-bucket/legalhold-object-
manifest.csv",
    "ETag": "Your-manifest-ETag"
  }
}
EOF
```

```
read -d '' REPORT <<EOF
{
  "Bucket": "arn:aws:s3:::amzn-s3-demo-completion-report-bucket",
  "Format": "Report_CSV_20180820",
  "Enabled": true,
  "Prefix": "reports/legalhold-objects-batch_operations",
  "ReportScope": "AllTasks"
}
EOF

aws \
    s3control create-job \
    --account-id "${ACCOUNT_ID}" \
    --manifest "${MANIFEST//$'\n'}" \
    --operation "${OPERATION//$'\n'/}" \
    --report "${REPORT//$'\n'}" \
    --priority 10 \
    --role-arn "${ROLE_ARN}" \
    --client-request-token "$(uuidgen)" \
    --region "${AWS_DEFAULT_REGION}" \
    --description "Turn off legal hold";
```

Usar o AWS SDK for Java

Os exemplos da AWS SDK para Java a seguir mostram como usar o Operações em Lote para desativar retenções legais do Bloqueio de Objetos do S3 em vários objetos.

Example – Atualiza o perfil para conceder permissões **`s3:PutObjectLegalHold`**

```
public void allowPutObjectLegalHold() {
    final String roleName = "batch_operations-object-lock";

    final String legalHoldPermissions = "{" +
            "    \"Version\": \"2012-10-17\"," +
            "    \"Statement\": [" +
            "        {" +
            "            \"Effect\": \"Allow\"," +
            "            \"Action\": [" +
            "                \"s3:PutObjectLegalHold\"" +
            "            ]," +
            "            \"Resource\": [" +
            "                \"arn:aws:s3:::amzn-s3-demo-manifest-bucket/*\"" +
            "            ]" +
```

```
            "        }" +
            "    ]" +
            "}";

    final AmazonIdentityManagement iam =
            AmazonIdentityManagementClientBuilder.defaultClient();

    final PutRolePolicyRequest putRolePolicyRequest = new PutRolePolicyRequest()
            .withPolicyDocument(legalHoldPermissions)
            .withPolicyName("legal-hold-permissions")
            .withRoleName(roleName);

    final PutRolePolicyResult putRolePolicyResult =
 iam.putRolePolicy(putRolePolicyRequest);
}
```

Example – Desativar retenção legal

Use o exemplo abaixo se quiser desativar a retenção legal.

```
public String createLegalHoldOffJob(final AWSS3ControlClient awss3ControlClient) {
    final String manifestObjectArn = "arn:aws:s3:::amzn-s3-demo-manifest-bucket/
legalhold-object-manifest.csv";
    final String manifestObjectVersionId = "15ad5ba069e6bbc465c77bf83d541385";

    final JobManifestLocation manifestLocation = new JobManifestLocation()
            .withObjectArn(manifestObjectArn)
            .withETag(manifestObjectVersionId);

    final JobManifestSpec manifestSpec =
            new JobManifestSpec()
                    .withFormat(JobManifestFormat.S3BatchOperations_CSV_20180820)
                    .withFields("Bucket", "Key");

    final JobManifest manifestToPublicApi = new JobManifest()
            .withLocation(manifestLocation)
            .withSpec(manifestSpec);

    final String jobReportBucketArn = "arn:aws:s3:::amzn-s3-demo-completion-report-
bucket";
    final String jobReportPrefix = "reports/legalhold-objects-batch_operations";

    final JobReport jobReport = new JobReport()
            .withEnabled(true)
```

```
            .withReportScope(JobReportScope.AllTasks)
            .withBucket(jobReportBucketArn)
            .withPrefix(jobReportPrefix)
            .withFormat(JobReportFormat.Report_CSV_20180820);

    final JobOperation jobOperation = new JobOperation()
            .withS3PutObjectLegalHold(new S3SetObjectLegalHoldOperation()
                    .withLegalHold(new S3ObjectLockLegalHold()
                            .withStatus(S3ObjectLockLegalHoldStatus.OFF)));

    final String roleArn = "arn:aws:iam::123456789012:role/batch_operations-object-
lock";
    final Boolean requiresConfirmation = true;
    final int priority = 10;

    final CreateJobRequest request = new CreateJobRequest()
            .withAccountId("123456789012")
            .withDescription("Turn off legal hold")
            .withManifest(manifestToPublicApi)
            .withOperation(jobOperation)
            .withPriority(priority)
            .withRoleArn(roleArn)
            .withReport(jobReport)
            .withConfirmationRequired(requiresConfirmation);

    final CreateJobResult result = awss3ControlClient.createJob(request);

    return result.getJobId();
}
```

Tutorial: vídeos de transcodificação em lote com o Operações em Lote do S3

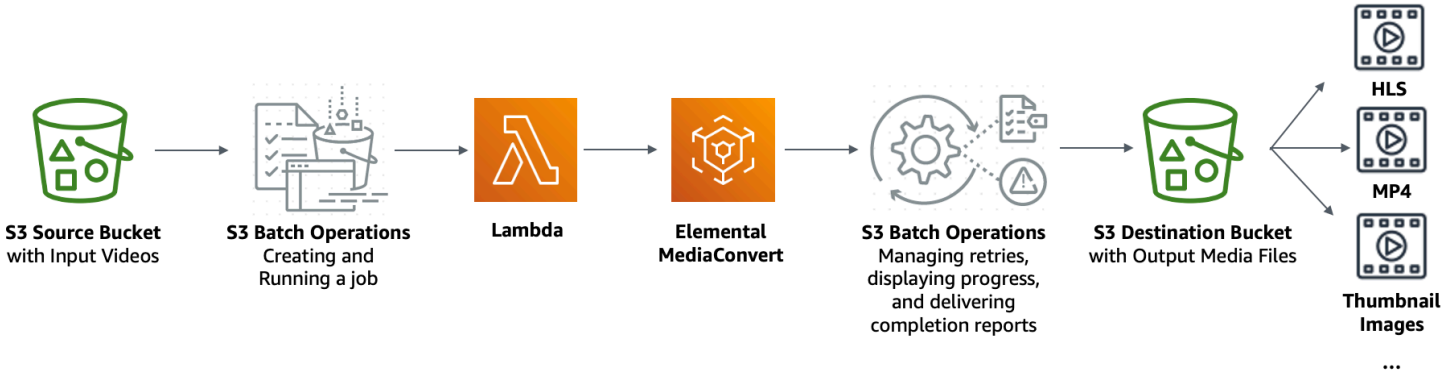
Os consumidores de vídeo usam dispositivos de todas as formas, tamanhos e épocas para desfrutar de conteúdo de mídia. Essa grande variedade de dispositivos representa um desafio para criadores e distribuidores de conteúdo. Em vez um formato de tamanho único, os vídeos precisam abranger uma ampla variedade de tamanhos, formatos e bitrates. Essa tarefa de conversão é ainda mais desafiadora quando você tem um grande número de vídeos a serem convertidos.

A AWS oferece um método para construir uma arquitetura escalável e distribuída que faz o seguinte:

- Ingere vídeos de entrada

- Processa os vídeos para reprodução em uma ampla variedade de dispositivos
- Armazena os arquivos de mídia transcodificados
- Fornece os arquivos de mídia de saída para atender à demanda

Quando você tem extensos repositórios de vídeo armazenados no Amazon S3, pode transcodificar esses vídeos de seus formatos na fonte para vários tipos de arquivo, no tamanho, resolução e formato necessários para um determinado player ou dispositivo de vídeo. Mais especificamente, as operações em lote do S3 fornecem uma solução para chamar as funções do AWS Lambda para vídeos de entrada existentes em um bucket de origem do S3. Depois, as funções do Lambda chamam o AWS Elemental MediaConvert para realizar tarefas de transcodificação de vídeo em grande escala. Os arquivos de mídia de saída convertidos são armazenados em um bucket de destino do S3.



Objetivo

Neste tutorial, você aprenderá como configurar as operações em lote do S3 para chamar uma função Lambda para transcodificação em lote de vídeos armazenados em um bucket de origem do S3. A função Lambda chama o MediaConvert para transcodificar os vídeos. As saídas para cada vídeo no bucket de origem do S3 são as seguintes:

- Um fluxo de bitrate adaptativa HTTP Live Streaming (HLS) para reprodução em dispositivos de vários tamanhos e larguras de banda variáveis
- Um arquivo de vídeo MP4
- Imagens em miniatura coletadas em intervalos

Tópicos

- Pré-requisitos

- Etapa 1: Criar um bucket do S3 para os arquivos de mídia de saída
- Etapa 2: criar uma função do IAM para MediaConvert
- Etapa 3: criar uma função do IAM para a função Lambda
- Etapa 4: Criar uma função do Lambda para transcodificação de vídeo
- Etapa 5: Configurar o inventário do Amazon S3 para seu bucket de origem do S3
- Etapa 6: criar uma função do IAM para operações em lote do S3
- Etapa 7: criar e executar um trabalho de operações em lote do S3
- Etapa 8: Conferir os arquivos de mídia de saída do bucket de destino do S3
- Etapa 9: limpar
- Próximas etapas

Pré-requisitos

Antes de iniciar este tutorial, você deve ter um bucket de origem do Amazon S3 (por exemplo, *`amzn-s3-demo-source-bucket`*) com vídeos a serem transcodificados já armazenados nele.

Você pode dar ao bucket outro nome, se desejar. Para obter mais informações sobre os nomes de bucket do Amazon S3, consulte Regras de nomenclatura de buckets de uso geral.

Para o bucket de origem do S3, mantenha as configurações relacionadas a Block Public Access settings for this bucket (Configurações de bloquear acesso público a este bucket) definidas com os padrões (Block all public access (Bloquear todo o acesso público) está habilitado). Para obter mais informações, consulte Criar um bucket de uso geral.

Para obter mais informações sobre como carregar vídeos para o bucket de origem do S3, consulte Fazer upload de objetos. Se você for carregar muitos arquivos de vídeo grandes para o S3, pode ser interessante usar o Amazon S3 Transfer Acceleration para configurar transferências de arquivos rápidas e seguras. O Transfer Acceleration pode acelerar o carregamento de vídeo no seu bucket do S3 para transferências de longa distância de vídeos maiores. Para obter mais informações, consulte Configurar transferências de arquivos rápidas e seguras usando o Amazon S3 Transfer Acceleration.

Etapa 1: Criar um bucket do S3 para os arquivos de mídia de saída

Nesta etapa, você cria um bucket de destino do S3 para armazenar os arquivos de mídia de saída convertidos. Você também cria uma configuração CORS (Cross Origin Resource Sharing) para permitir acesso de origem cruzada aos arquivos de mídia transcodificados armazenados no bucket de destino do S3.

Subetapas

- Criar um bucket para os arquivos de mídia de saída
- Para adicionar uma configuração CORS a um bucket de saída do S3

Criar um bucket para os arquivos de mídia de saída

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets.
3. Escolha Criar bucket.
4. Em Bucket name (Nome do bucket), insira um nome para o seu bucket (por exemplo, *amzn-s3-demo-destination-bucket1*).
5. Em Region (Região), escolha a Região da AWS onde deseja que o bucket resida.
6. Para garantir o acesso público aos arquivos de mídia de saída, em Block Public Access settings for this bucket (Configurações de bloqueio de acesso público para este bucket), desmarque Block all public access (Bloquear todo acesso público).

   > **Warning**
   >
   > Antes de concluir esta etapa, revise Bloquear o acesso público ao armazenamento do Amazon S3 para garantir que você entenda e aceite os riscos envolvidos em permitir o acesso público. Quando você desativa as configurações Block Public Access (Bloquear acesso público) para tornar seu bucket público, qualquer pessoa na Internet pode acessá-lo. Recomendamos que você bloqueie todo o acesso público aos seus buckets. Se você não quiser limpar as configurações de Block Public Access (Bloquear acesso público), pode usar o Amazon CloudFront para entregar os arquivos de mídia transcodificados aos visualizadores (usuários finais). Para obter mais informações, consulte Tutorial: Hospedagem de transmissão sob demanda com o Amazon S3, Amazon CloudFront e Amazon Route 53.

7. Marque a caixa de seleção ao lado de I acknowledge that the current settings might result in this bucket and the objects within becoming public (Eu reconheço que as configurações atuais podem fazem com que o bucket e os objetos fiquem públicos.)
8. Mantenha as configurações restantes definidas conforme os padrões.
9. Escolha Criar bucket.

Para adicionar uma configuração CORS a um bucket de saída do S3

Uma configuração de CORS JSON define uma maneira para as aplicações Web clientes (players de vídeo neste contexto) que são carregadas em um domínio reproduzirem os arquivos de mídia de saída transcodificados em um domínio diferente.

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets.
3. Na lista Buckets, escolha o nome do bucket que você criou antes (por exemplo, *amzn-s3-demo-destination-bucket1*).
4. Escolha a aba Permissões.
5. Na seção Cross-origin resource sharing (CORS) (Compartilhamento de recursos de origem cruzada (CORS)) escolha Edit (Editar).
6. Na caixa de texto de configuração de CORS, copie e cole a seguinte configuração de CORS.

   A configuração do CORS deve estar no formato JSON. Neste exemplo, o atributo `AllowedOrigins` usa o caractere curinga (*) para especificar todas as origens. Se você souber qual é a sua origem específica, pode restringir o atributo `AllowedOrigins` ao URL do seu player específico. Para obter mais informações sobre esse e outros atributos, consulte Elementos de uma configuração de CORS.

```
[
    {
        "AllowedOrigins": [
            "*"
        ],
        "AllowedMethods": [
            "GET"
        ],
        "AllowedHeaders": [
            "*"
        ],
        "ExposeHeaders": []

    }
]
```

7. Escolha Salvar alterações.

Etapa 2: criar uma função do IAM para MediaConvert

Para usar o AWS Elemental MediaConvert para transcodificar vídeos de entrada armazenados no bucket do S3, você deve ter um perfil de serviço do AWS Identity and Access Management (IAM) para conceder ao MediaConvert permissões para ler e gravar arquivos de vídeo entre os buckets de origem e de destino do S3. Quando você executa trabalhos de transcodificação, o console do MediaConvert usa essa função.

Para criar uma função do IAM para MediaConvert

1. Crie uma função do IAM com um nome de função que você escolhe (por exemplo, **`tutorial-mediaconvert-role`**). Para criar essa função, siga as etapas em Criar função do MediaConvert no IAM (console) no Guia do usuário do AWS Elemental MediaConvert.
2. Depois de criar a função do IAM para o MediaConvert, na lista Roles (Funções), escolha o nome da função para o MediaConvert que você criou (por exemplo, **`tutorial-mediaconvert-role`**).
3. Na página Summary (Resumo), copie o Role ARN (ARN da função) (que começa com `arn:aws:iam::`) e salve o ARN para uso posterior.

   Para obter mais informações sobre os ARNs, consulte Amazon Resource Names (ARNs) (Nomes de recurso da Amazon (ARNs) em AWS General Reference (Referência geral).

Etapa 3: criar uma função do IAM para a função Lambda

Para transcodificar vídeos em lote com o MediaConvert e operações em lote do S3, você usa uma função do Lambda para conectar esses dois serviços para converter vídeos. Essa função do Lambda precisa ter uma função do IAM que conceda permissões à função do Lambda para acessar o MediaConvert e as operações em lote do S3.

Subetapas

- Criar uma função do IAM para sua função Lambda
- Incorpore uma política em linha para a função do IAM da sua função Lambda

Criar uma função do IAM para sua função Lambda

1. Faça login no AWS Management Console e abra o console do IAM, em https://console.aws.amazon.com/iam/.

2. No painel de navegação à esquerda, escolha Roles (Funções) e Create role (Criar função).
3. Escolha o tipo de função AWS service (serviço da WS) e em Common use cases (Casos de uso comuns), escolha Lambda.
4. Escolha Próximo: Permissões.
5. Na página Attach Permissions policies (Anexar políticas de permissões), insira **`AWSLambdaBasicExecutionRole`** na caixa Filter policies (Filtrar políticas). Para anexar a política gerenciada AWSLambdaBasicExecutionRole a esta função para conceder permissões de gravação a Amazon CloudWatch Logs, marque a caixa de seleção ao lado de AWSLambdaBasicExecutionRole.
6. Escolha Próximo.
7. Em Nome do perfil, insira **`tutorial-lambda-transcode-role`**.
8. (Opcional) Adicione etiquetas à política gerenciada.
9. Selecione Criar perfil.

Incorpore uma política em linha para a função do IAM da sua função Lambda

Para conceder permissões para o recurso do MediaConvert que é necessário para que a função do Lambda seja executada, você deve usar uma política em linha.

1. Faça login no AWS Management Console e abra o console do IAM, em https://console.aws.amazon.com/iam/.
2. No painel de navegação à esquerda, selecione Perfis.
3. Na lista Roles (Funções), escolha o nome da função do IAM que você criou antes para a sua função do Lambda (por exemplo, **`tutorial-lambda-transcode-role`**).
4. Escolha a guia Permissions (Permissões).
5. Escolha Add inline policy (Adicionar política em linha).
6. Escolha a guia JSON e copie e cole a política JSON a seguir.

   Na política JSON, substitua o valor de `Resource` do ARN do exemplo pelo ARN da função do IAM para o MediaConvert que você criou na Etapa 2 (por exemplo, **`tutorial-mediaconvert-role`**).

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Action": [
                "logs:CreateLogGroup",
                "logs:CreateLogStream",
                "logs:PutLogEvents"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "Logging"
        },
        {
            "Action": [
                "iam:PassRole"
            ],
            "Resource": [
                "arn:aws:iam::111122223333:role/tutorial-mediaconvert-role"
            ],
            "Effect": "Allow",
            "Sid": "PassRole"
        },
        {
            "Action": [
                "mediaconvert:*"
            ],
            "Resource": [
                "*"
            ],
            "Effect": "Allow",
            "Sid": "MediaConvertService"
        },
        {
            "Action": [
                "s3:*"
            ],
            "Resource": [
                "*"
            ],
            "Effect": "Allow",
            "Sid": "S3Service"
        }
    ]
}
```

7. Escolha Revisar política.

8. Em Nome, insira **`tutorial-lambda-policy`**.
9. Escolha Create Policy.

   Após a criação de uma política em linha, ela é automaticamente incorporada à função do IAM de sua função Lambda.

Etapa 4: Criar uma função do Lambda para transcodificação de vídeo

Nesta seção do tutorial, você constrói uma função do Lambda usando o SDK for Python para integrar com as operações em lote do S3 e o MediaConvert. Para iniciar a transcodificação dos vídeos já armazenados no bucket de origem do S3, você executa um trabalho de operações em lote do S3 que invoca diretamente a função do Lambda para cada vídeo no bucket de origem do S3. Em seguida, a função Lambda envia um trabalho de transcodificação de cada vídeo para MediaConvert.

Subetapas

- Grave o código de função Lambda e crie um pacote de implantação
- Crie uma função Lambda com uma função de execução (console)
- Implante sua função Lambda com arquivos .zip e configure a função Lambda (console)

Grave o código de função Lambda e crie um pacote de implantação

1. Na sua máquina local, crie uma pasta denominada `batch-transcode`.
2. Na pasta `batch-transcode`, crie um arquivo com as configurações de trabalho de JSON. Por exemplo, use as configurações fornecidas nesta seção e dê ao arquivo o nome de `job.json`.

   Um arquivo `job.json` especifica o seguinte:

   - Quais arquivos devem ser transcodificados
   - Como você deseja transcodificar seus vídeos de entrada
   - Quais arquivos de mídia de saída você deseja criar
   - Como dar nomes aos arquivos transcodificados
   - Onde salvar os arquivos transcodificados
   - Quais recursos avançados aplicar e assim por diante

Neste tutorial, usamos o arquivo `job.json` a seguir para criar as seguintes saídas para cada vídeo no bucket de origem do S3:

- Um fluxo de bitrate adaptativa HTTP Live Streaming (HLS) para reprodução em dispositivos de diversos tamanhos e diferentes larguras de banda
- Um arquivo de vídeo MP4
- Imagens em miniatura coletadas em intervalos

Este exemplo de arquivo `job.json` usa bitrare variável definia por qualidade (QVCR - Quality-Defined Variable Bitrate) para otimizar a qualidade do vídeo. A saída HTTP Live Streaming (HLS) é compatível com Apple (áudio de vídeo não mixado, duração de segmento de 6 segundos e qualidade de vídeo otimizada por QVBR automática).

Se você não quiser usar as configurações de exemplo fornecidas aqui, pode gerar uma especificação de `job.json` baseada em seu caso de uso. Para garantir a consistência em todas as saídas, certifique-se de que os arquivos de entrada tenham configurações de vídeo e áudio semelhantes. Para arquivos de entrada com diferentes configurações de vídeo e áudio, crie automações separadas (configurações de `job.json` exclusivas). Para obter mais informações, consulte Exemplos de configuração de trabalhos do AWS Elemental MediaConvert em JSON no Guia do usuário do AWS Elemental MediaConvert.

```
{
  "OutputGroups": [
    {
      "CustomName": "HLS",
      "Name": "Apple HLS",
      "Outputs": [
        {
          "ContainerSettings": {
            "Container": "M3U8",
            "M3u8Settings": {
              "AudioFramesPerPes": 4,
              "PcrControl": "PCR_EVERY_PES_PACKET",
              "PmtPid": 480,
              "PrivateMetadataPid": 503,
              "ProgramNumber": 1,
              "PatInterval": 0,
              "PmtInterval": 0,
```

```
            "TimedMetadata": "NONE",
            "VideoPid": 481,
            "AudioPids": [
              482,
              483,
              484,
              485,
              486,
              487,
              488,
              489,
              490,
              491,
              492
            ]
          }
        },
        "VideoDescription": {
          "Width": 640,
          "ScalingBehavior": "DEFAULT",
          "Height": 360,
          "TimecodeInsertion": "DISABLED",
          "AntiAlias": "ENABLED",
          "Sharpness": 50,
          "CodecSettings": {
            "Codec": "H_264",
            "H264Settings": {
              "InterlaceMode": "PROGRESSIVE",
              "NumberReferenceFrames": 3,
              "Syntax": "DEFAULT",
              "Softness": 0,
              "GopClosedCadence": 1,
              "GopSize": 2,
              "Slices": 1,
              "GopBReference": "DISABLED",
              "MaxBitrate": 1200000,
              "SlowPal": "DISABLED",
              "SpatialAdaptiveQuantization": "ENABLED",
              "TemporalAdaptiveQuantization": "ENABLED",
              "FlickerAdaptiveQuantization": "DISABLED",
              "EntropyEncoding": "CABAC",
              "FramerateControl": "INITIALIZE_FROM_SOURCE",
              "RateControlMode": "QVBR",
              "CodecProfile": "MAIN",
```

```
                "Telecine": "NONE",
                "MinIInterval": 0,
                "AdaptiveQuantization": "HIGH",
                "CodecLevel": "AUTO",
                "FieldEncoding": "PAFF",
                "SceneChangeDetect": "TRANSITION_DETECTION",
                "QualityTuningLevel": "SINGLE_PASS_HQ",
                "FramerateConversionAlgorithm": "DUPLICATE_DROP",
                "UnregisteredSeiTimecode": "DISABLED",
                "GopSizeUnits": "SECONDS",
                "ParControl": "INITIALIZE_FROM_SOURCE",
                "NumberBFramesBetweenReferenceFrames": 2,
                "RepeatPps": "DISABLED"
              }
            },
            "AfdSignaling": "NONE",
            "DropFrameTimecode": "ENABLED",
            "RespondToAfd": "NONE",
            "ColorMetadata": "INSERT"
          },
          "OutputSettings": {
            "HlsSettings": {
              "AudioGroupId": "program_audio",
              "AudioRenditionSets": "program_audio",
              "SegmentModifier": "$dt$",
              "IFrameOnlyManifest": "EXCLUDE"
            }
          },
          "NameModifier": "_360"
        },
        {
          "ContainerSettings": {
            "Container": "M3U8",
            "M3u8Settings": {
              "AudioFramesPerPes": 4,
              "PcrControl": "PCR_EVERY_PES_PACKET",
              "PmtPid": 480,
              "PrivateMetadataPid": 503,
              "ProgramNumber": 1,
              "PatInterval": 0,
              "PmtInterval": 0,
              "TimedMetadata": "NONE",
              "TimedMetadataPid": 502,
              "VideoPid": 481,
```

```
            "AudioPids": [
              482,
              483,
              484,
              485,
              486,
              487,
              488,
              489,
              490,
              491,
              492
            ]
          }
        },
        "VideoDescription": {
          "Width": 960,
          "ScalingBehavior": "DEFAULT",
          "Height": 540,
          "TimecodeInsertion": "DISABLED",
          "AntiAlias": "ENABLED",
          "Sharpness": 50,
          "CodecSettings": {
            "Codec": "H_264",
            "H264Settings": {
              "InterlaceMode": "PROGRESSIVE",
              "NumberReferenceFrames": 3,
              "Syntax": "DEFAULT",
              "Softness": 0,
              "GopClosedCadence": 1,
              "GopSize": 2,
              "Slices": 1,
              "GopBReference": "DISABLED",
              "MaxBitrate": 3500000,
              "SlowPal": "DISABLED",
              "SpatialAdaptiveQuantization": "ENABLED",
              "TemporalAdaptiveQuantization": "ENABLED",
              "FlickerAdaptiveQuantization": "DISABLED",
              "EntropyEncoding": "CABAC",
              "FramerateControl": "INITIALIZE_FROM_SOURCE",
              "RateControlMode": "QVBR",
              "CodecProfile": "MAIN",
              "Telecine": "NONE",
              "MinIInterval": 0,
```

```
                "AdaptiveQuantization": "HIGH",
                "CodecLevel": "AUTO",
                "FieldEncoding": "PAFF",
                "SceneChangeDetect": "TRANSITION_DETECTION",
                "QualityTuningLevel": "SINGLE_PASS_HQ",
                "FramerateConversionAlgorithm": "DUPLICATE_DROP",
                "UnregisteredSeiTimecode": "DISABLED",
                "GopSizeUnits": "SECONDS",
                "ParControl": "INITIALIZE_FROM_SOURCE",
                "NumberBFramesBetweenReferenceFrames": 2,
                "RepeatPps": "DISABLED"
              }
            },
            "AfdSignaling": "NONE",
            "DropFrameTimecode": "ENABLED",
            "RespondToAfd": "NONE",
            "ColorMetadata": "INSERT"
          },
          "OutputSettings": {
            "HlsSettings": {
              "AudioGroupId": "program_audio",
              "AudioRenditionSets": "program_audio",
              "SegmentModifier": "$dt$",
              "IFrameOnlyManifest": "EXCLUDE"
            }
          },
          "NameModifier": "_540"
        },
        {
          "ContainerSettings": {
            "Container": "M3U8",
            "M3u8Settings": {
              "AudioFramesPerPes": 4,
              "PcrControl": "PCR_EVERY_PES_PACKET",
              "PmtPid": 480,
              "PrivateMetadataPid": 503,
              "ProgramNumber": 1,
              "PatInterval": 0,
              "PmtInterval": 0,
              "TimedMetadata": "NONE",
              "VideoPid": 481,
              "AudioPids": [
                482,
                483,
```

```
                484,
                485,
                486,
                487,
                488,
                489,
                490,
                491,
                492
              ]
            }
          },
          "VideoDescription": {
            "Width": 1280,
            "ScalingBehavior": "DEFAULT",
            "Height": 720,
            "TimecodeInsertion": "DISABLED",
            "AntiAlias": "ENABLED",
            "Sharpness": 50,
            "CodecSettings": {
              "Codec": "H_264",
              "H264Settings": {
                "InterlaceMode": "PROGRESSIVE",
                "NumberReferenceFrames": 3,
                "Syntax": "DEFAULT",
                "Softness": 0,
                "GopClosedCadence": 1,
                "GopSize": 2,
                "Slices": 1,
                "GopBReference": "DISABLED",
                "MaxBitrate": 5000000,
                "SlowPal": "DISABLED",
                "SpatialAdaptiveQuantization": "ENABLED",
                "TemporalAdaptiveQuantization": "ENABLED",
                "FlickerAdaptiveQuantization": "DISABLED",
                "EntropyEncoding": "CABAC",
                "FramerateControl": "INITIALIZE_FROM_SOURCE",
                "RateControlMode": "QVBR",
                "CodecProfile": "MAIN",
                "Telecine": "NONE",
                "MinIInterval": 0,
                "AdaptiveQuantization": "HIGH",
                "CodecLevel": "AUTO",
                "FieldEncoding": "PAFF",
```

```
                "SceneChangeDetect": "TRANSITION_DETECTION",
                "QualityTuningLevel": "SINGLE_PASS_HQ",
                "FramerateConversionAlgorithm": "DUPLICATE_DROP",
                "UnregisteredSeiTimecode": "DISABLED",
                "GopSizeUnits": "SECONDS",
                "ParControl": "INITIALIZE_FROM_SOURCE",
                "NumberBFramesBetweenReferenceFrames": 2,
                "RepeatPps": "DISABLED"
              }
            },
            "AfdSignaling": "NONE",
            "DropFrameTimecode": "ENABLED",
            "RespondToAfd": "NONE",
            "ColorMetadata": "INSERT"
          },
          "OutputSettings": {
            "HlsSettings": {
              "AudioGroupId": "program_audio",
              "AudioRenditionSets": "program_audio",
              "SegmentModifier": "$dt$",
              "IFrameOnlyManifest": "EXCLUDE"
            }
          },
          "NameModifier": "_720"
        },
        {
          "ContainerSettings": {
            "Container": "M3U8",
            "M3u8Settings": {}
          },
          "AudioDescriptions": [
            {
              "AudioSourceName": "Audio Selector 1",
              "CodecSettings": {
                "Codec": "AAC",
                "AacSettings": {
                  "Bitrate": 96000,
                  "CodingMode": "CODING_MODE_2_0",
                  "SampleRate": 48000
                }
              }
            }
          ],
          "OutputSettings": {
```

```
            "HlsSettings": {
              "AudioGroupId": "program_audio",
              "AudioTrackType": "ALTERNATE_AUDIO_AUTO_SELECT_DEFAULT"
            }
          },
          "NameModifier": "_audio"
        }
      ],
      "OutputGroupSettings": {
        "Type": "HLS_GROUP_SETTINGS",
        "HlsGroupSettings": {
          "ManifestDurationFormat": "INTEGER",
          "SegmentLength": 6,
          "TimedMetadataId3Period": 10,
          "CaptionLanguageSetting": "OMIT",
          "Destination": "s3://EXAMPLE-BUCKET/HLS/",
          "DestinationSettings": {
            "S3Settings": {
              "AccessControl": {
                "CannedAcl": "PUBLIC_READ"
              }
            }
          },
          "TimedMetadataId3Frame": "PRIV",
          "CodecSpecification": "RFC_4281",
          "OutputSelection": "MANIFESTS_AND_SEGMENTS",
          "ProgramDateTimePeriod": 600,
          "MinSegmentLength": 0,
          "DirectoryStructure": "SINGLE_DIRECTORY",
          "ProgramDateTime": "EXCLUDE",
          "SegmentControl": "SEGMENTED_FILES",
          "ManifestCompression": "NONE",
          "ClientCache": "ENABLED",
          "StreamInfResolution": "INCLUDE"
        }
      }
    },
    {
      "CustomName": "MP4",
      "Name": "File Group",
      "Outputs": [
        {
          "ContainerSettings": {
            "Container": "MP4",
```

```
            "Mp4Settings": {
              "CslgAtom": "INCLUDE",
              "FreeSpaceBox": "EXCLUDE",
              "MoovPlacement": "PROGRESSIVE_DOWNLOAD"
            }
          },
          "VideoDescription": {
            "Width": 1280,
            "ScalingBehavior": "DEFAULT",
            "Height": 720,
            "TimecodeInsertion": "DISABLED",
            "AntiAlias": "ENABLED",
            "Sharpness": 100,
            "CodecSettings": {
              "Codec": "H_264",
              "H264Settings": {
                "InterlaceMode": "PROGRESSIVE",
                "ParNumerator": 1,
                "NumberReferenceFrames": 3,
                "Syntax": "DEFAULT",
                "Softness": 0,
                "GopClosedCadence": 1,
                "HrdBufferInitialFillPercentage": 90,
                "GopSize": 2,
                "Slices": 2,
                "GopBReference": "ENABLED",
                "HrdBufferSize": 10000000,
                "MaxBitrate": 5000000,
                "ParDenominator": 1,
                "EntropyEncoding": "CABAC",
                "RateControlMode": "QVBR",
                "CodecProfile": "HIGH",
                "MinIInterval": 0,
                "AdaptiveQuantization": "AUTO",
                "CodecLevel": "AUTO",
                "FieldEncoding": "PAFF",
                "SceneChangeDetect": "ENABLED",
                "QualityTuningLevel": "SINGLE_PASS_HQ",
                "UnregisteredSeiTimecode": "DISABLED",
                "GopSizeUnits": "SECONDS",
                "ParControl": "SPECIFIED",
                "NumberBFramesBetweenReferenceFrames": 3,
                "RepeatPps": "DISABLED",
                "DynamicSubGop": "ADAPTIVE"
```

```
            }
          },
          "AfdSignaling": "NONE",
          "DropFrameTimecode": "ENABLED",
          "RespondToAfd": "NONE",
          "ColorMetadata": "INSERT"
        },
        "AudioDescriptions": [
          {
            "AudioTypeControl": "FOLLOW_INPUT",
            "AudioSourceName": "Audio Selector 1",
            "CodecSettings": {
              "Codec": "AAC",
              "AacSettings": {
                "AudioDescriptionBroadcasterMix": "NORMAL",
                "Bitrate": 160000,
                "RateControlMode": "CBR",
                "CodecProfile": "LC",
                "CodingMode": "CODING_MODE_2_0",
                "RawFormat": "NONE",
                "SampleRate": 48000,
                "Specification": "MPEG4"
              }
            },
            "LanguageCodeControl": "FOLLOW_INPUT",
            "AudioType": 0
          }
        ]
      }
    ],
    "OutputGroupSettings": {
      "Type": "FILE_GROUP_SETTINGS",
      "FileGroupSettings": {
        "Destination": "s3://EXAMPLE-BUCKET/MP4/",
        "DestinationSettings": {
          "S3Settings": {
            "AccessControl": {
              "CannedAcl": "PUBLIC_READ"
            }
          }
        }
      }
    }
  },
```

```
    {
      "CustomName": "Thumbnails",
      "Name": "File Group",
      "Outputs": [
        {
          "ContainerSettings": {
            "Container": "RAW"
          },
          "VideoDescription": {
            "Width": 1280,
            "ScalingBehavior": "DEFAULT",
            "Height": 720,
            "TimecodeInsertion": "DISABLED",
            "AntiAlias": "ENABLED",
            "Sharpness": 50,
            "CodecSettings": {
              "Codec": "FRAME_CAPTURE",
              "FrameCaptureSettings": {
                "FramerateNumerator": 1,
                "FramerateDenominator": 5,
                "MaxCaptures": 500,
                "Quality": 80
              }
            },
            "AfdSignaling": "NONE",
            "DropFrameTimecode": "ENABLED",
            "RespondToAfd": "NONE",
            "ColorMetadata": "INSERT"
          }
        }
      ],
      "OutputGroupSettings": {
        "Type": "FILE_GROUP_SETTINGS",
        "FileGroupSettings": {
          "Destination": "s3://EXAMPLE-BUCKET/Thumbnails/",
          "DestinationSettings": {
            "S3Settings": {
              "AccessControl": {
                "CannedAcl": "PUBLIC_READ"
              }
            }
          }
        }
      }
```

```
    }
  ],
  "AdAvailOffset": 0,
  "Inputs": [
    {
      "AudioSelectors": {
        "Audio Selector 1": {
          "Offset": 0,
          "DefaultSelection": "DEFAULT",
          "ProgramSelection": 1
        }
      },
      "VideoSelector": {
        "ColorSpace": "FOLLOW"
      },
      "FilterEnable": "AUTO",
      "PsiControl": "USE_PSI",
      "FilterStrength": 0,
      "DeblockFilter": "DISABLED",
      "DenoiseFilter": "DISABLED",
      "TimecodeSource": "EMBEDDED",
      "FileInput": "s3://EXAMPLE-INPUT-BUCKET/input.mp4"
    }
  ]
}
```

3. Na pasta `batch-transcode`, crie um arquivo com uma função Lambda. Você pode usar o seguinte exemplo Python e nomear o arquivo `convert.py`.

   As operações em lote do S3 enviam dados de tarefa específicos para uma função do Lambda e requerem os dados do resultado de volta. Para obter exemplos de solicitação e resposta para a função do Lambda, informações sobre códigos de resposta e de resultados, e exemplos de funções do Lambda para operações em lote do S3, consulte Invocar função do AWS Lambda.

```
import json
import os
from urllib.parse import urlparse
import uuid
import boto3

"""
When you run an S3 Batch Operations job, your job
invokes this Lambda function. Specifically, the Lambda function is
```

```
invoked on each video object listed in the manifest that you specify
for the S3 Batch Operations job in Step 5.

Input parameter "event": The S3 Batch Operations event as a request
                         for the Lambda function.

Input parameter "context": Context about the event.

Output: A result structure that Amazon S3 uses to interpret the result
        of the operation. It is a job response returned back to S3 Batch
 Operations.
"""
def handler(event, context):

    invocation_schema_version = event['invocationSchemaVersion']
    invocation_id = event['invocationId']
    task_id = event['tasks'][0]['taskId']

    source_s3_key = event['tasks'][0]['s3Key']
    source_s3_bucket = event['tasks'][0]['s3BucketArn'].split(':::')[-1]
    source_s3 = 's3://' + source_s3_bucket + '/' + source_s3_key

    result_list = []
    result_code = 'Succeeded'
    result_string = 'The input video object was converted successfully.'

    # The type of output group determines which media players can play
    # the files transcoded by MediaConvert.
    # For more information, see Creating outputs with AWS Elemental MediaConvert.
    output_group_type_dict = {
        'HLS_GROUP_SETTINGS': 'HlsGroupSettings',
        'FILE_GROUP_SETTINGS': 'FileGroupSettings',
        'CMAF_GROUP_SETTINGS': 'CmafGroupSettings',
        'DASH_ISO_GROUP_SETTINGS': 'DashIsoGroupSettings',
        'MS_SMOOTH_GROUP_SETTINGS': 'MsSmoothGroupSettings'
    }

    try:
        job_name = 'Default'
        with open('job.json') as file:
            job_settings = json.load(file)

        job_settings['Inputs'][0]['FileInput'] = source_s3
```

```
        # The path of each output video is constructed based on the values of
        # the attributes in each object of OutputGroups in the job.json file.
        destination_s3 = 's3://{0}/{1}/{2}' \
            .format(os.environ['amzn-s3-demo-destination-bucket'],
                    os.path.splitext(os.path.basename(source_s3_key))[0],
                    os.path.splitext(os.path.basename(job_name))[0])

        for output_group in job_settings['OutputGroups']:
            output_group_type = output_group['OutputGroupSettings']['Type']
            if output_group_type in output_group_type_dict.keys():
                output_group_type = output_group_type_dict[output_group_type]
                output_group['OutputGroupSettings'][output_group_type]
['Destination'] = \
                    "{0}{1}".format(destination_s3,
                                    urlparse(output_group['OutputGroupSettings']
[output_group_type]['Destination']).path)
            else:
                raise ValueError("Exception: Unknown Output Group Type {}."
                                 .format(output_group_type))

        job_metadata_dict = {
            'assetID': str(uuid.uuid4()),
            'application': os.environ['Application'],
            'input': source_s3,
            'settings': job_name
        }

        region = os.environ['AWS_DEFAULT_REGION']
        endpoints = boto3.client('mediaconvert', region_name=region) \
            .describe_endpoints()
        client = boto3.client('mediaconvert', region_name=region,
                              endpoint_url=endpoints['Endpoints'][0]['Url'],
                              verify=False)

        try:
            client.create_job(Role=os.environ['MediaConvertRole'],
                              UserMetadata=job_metadata_dict,
                              Settings=job_settings)
        # You can customize error handling based on different error codes that
        # MediaConvert can return.
        # For more information, see MediaConvert error codes.
        # When the result_code is TemporaryFailure, S3 Batch Operations retries
        # the task before the job is completed. If this is the final retry,
        # the error message is included in the final report.
```

```
        except Exception as error:
            result_code = 'TemporaryFailure'
            raise

    except Exception as error:
        if result_code != 'TemporaryFailure':
            result_code = 'PermanentFailure'
        result_string = str(error)

    finally:
        result_list.append({
            'taskId': task_id,
            'resultCode': result_code,
            'resultString': result_string,
        })

    return {
        'invocationSchemaVersion': invocation_schema_version,
        'treatMissingKeyAs': 'PermanentFailure',
        'invocationId': invocation_id,
        'results': result_list
    }
```

4. Para criar um pacote de implantação com `convert.py` e `job.json` como um arquivo `.zip`, denominado `lambda.zip` em seu terminal local, abra a pasta `batch-transcode` que você criou antes e execute o comando a seguir.

   Para usuários do macOS, execute o seguinte comando:

   ```
   zip -r lambda.zip convert.py job.json
   ```

   Para usuários do Windows, execute os seguintes comandos:

   ```
   powershell Compress-Archive convert.py lambda.zip
   ```

   ```
   powershell Compress-Archive -update job.json lambda.zip
   ```

Crie uma função Lambda com uma função de execução (console)

1. Abra o console AWS Lambda em https://console.aws.amazon.com/lambda/.

2. No painel de navegação à esquerda, escolha Functions (Funções).
3. Escolha Create function (Criar função).
4. Escolha Author from scratch (Criar do zero).
5. Em Basic information (Informações básicas), faça o seguinte:
   a. Em Function name (Nome da função), insira **`tutorial-lambda-convert`**.
   b. Em Runtime, selecione Python 3.13.
6. Escolha Change default execution role (Alterar a função de execução padrão) e, em Execution role (Função de execução), escolha Use an existing role (Usar uma função existente).
7. Em Exiting role (Função de saída), escolha o nome da função do IAM que você criou para sua função do Lambda na Etapa 3 (por exemplo, **`tutorial-lambda-transcode-role`**).
8. Mantenha as configurações restantes definidas conforme os padrões.
9. Escolha Create function (Criar função).

Implante sua função Lambda com arquivos .zip e configure a função Lambda (console)

1. Na seção Code Source (Código-fonte) da página da função do Lambda que você criou (por exemplo, **`tutorial-lambda-convert`**), escolha Upload from (Carregar de) e depois .zip file (arquivo .zip).
2. Selecione Upload (Carregar) para selecionar seu arquivo `.zip` local.
3. Selecione o arquivo `lambda.zip` que você criou antes e escolha Open (Abrir).
4. Escolha Salvar.
5. Na seção Runtime settings (Configurações do tempo de execução), escolha Edit (Editar).
6. Para informar ao tempo de execução do Lambda qual método de handler em seu código de função do Lambda deve invocar, insira no campo **`convert.handler`** Handler.

   Ao configurar uma função em Python, o valor da configuração do handler é o nome do arquivo e o nome do módulo do handler exportado, separados por um ponto (`.`). Por exemplo, `convert.handler` chama o método `handler` definido no arquivo `convert.py`.
7. Escolha Salvar.
8. Em sua página da função Lambda, escolha a guia Configuration (Configuração). No painel de navegação esquerdo na guia Configuration (Configuração), escolha Environment variables (Variáveis de ambiente) e, depois, escolha Edit (Editar).

9. Escolha Add environment variable (Adicionar variável de ambiente). Em seguida, insira a Key (Chave) e o Value (Valor) especificados para cada uma das seguintes variáveis de ambiente:

   - Key (Chave): **`DestinationBucket`** Value (Valor): **`amzn-s3-demo-destination-bucket1`**

     Este valor é o bucket do S3 para os arquivos de mídia de saída que você criou na Etapa 1.

   - Key (Chave): **`MediaConvertRole`** Value (Valor): **`arn:aws:iam::`*`111122223333`*`:role/tutorial-mediaconvert-role`**

     Este valor é o ARN da função do IAM para MediaConvert que você criou na Etapa 2. Certifique-se de substituir esse ARN pelo ARN real da sua função do IAM.

   - Key (Chave): **`Application`** Value (Valor): **`Batch-Transcoding`**

     Esse valor é o nome da sua aplicação.

10. Escolha Salvar.

11. (Opcional) Na guia Configuration (Configuração), na seção General configuration (Configuração geral) do painel de navegação à esquerda, escolha Edit (Editar). No campo Timeout (Tempo limite), insira **`2`** min **`0`** segundos. Selecione Salvar.

    Timeout (Tempo limite) é a quantidade de tempo durante a qual o Lambda permite que uma função seja executada entes de interrompê-la. O padrão é 3 segundos. O preço é baseado na quantidade de memória configurada e na quantidade de tempo em que o código é executado. Para obter mais informações, consulte Preços do AWS Lambda.

Etapa 5: Configurar o inventário do Amazon S3 para seu bucket de origem do S3

Depois de configurar a função de transcodificação do Lambda, crie um trabalho de operações em lote do S3 para transcodificar um conjunto de vídeos. Primeiro, você precisa de uma lista de objetos de vídeo de entrada nos quais deseja que as operações em lote do S3 executem a ação de transcodificação especificada. Para obter uma lista de objetos de vídeo de entrada, você pode gerar um relatório de inventário do S3 para o bucket de origem do S3 (por exemplo, *`amzn-s3-demo-source-bucket`*).

Subetapas

- Crie e configure um bucket para relatórios de inventário do S3 para vídeos de entrada
- Configure o inventário do Amazon S3 para o bucket de origem de vídeo do S3

- Confira o relatório de inventário para o seu bucket de origem de vídeo S3

Crie e configure um bucket para relatórios de inventário do S3 para vídeos de entrada

Para armazenar relatórios de inventário do S3 que listam os objetos do bucket de origem do S3, você precisa criar um bucket de destino de inventário do S3 e depois configurar uma política de bucket para que o bucket grave os arquivos de inventário no bucket de origem do S3.

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets.
3. Escolha Criar bucket.
4. Em Bucket name (Nome do bucket), insira um nome para o seu bucket (por exemplo, *amzn-s3-demo-destination-bucket2*).
5. Em Região da AWS, escolha a Região da AWS na qual você deseja que o bucket resida.

   O bucket de destino do inventário deve estar na mesma Região da AWS que o bucket de origem para o qual você está configurando o inventário do S3. O bucket de destino do inventário pode estar em uma Conta da AWS diferente.
6. Em Block Public Access settings for this bucket (Configurações de bloquear acesso público para este bucket), mantenha as configurações padrão (Block all public access (Bloquear todo acesso público) está habilitado).
7. Mantenha as configurações restantes definidas conforme os padrões.
8. Escolha Criar bucket.
9. Na lista de Buckets, escolha o nome do bucket que você acabou de criar (por exemplo, *amzn-s3-demo-destination-bucket2*).
10. Para conceder permissão ao Amazon S3 para gravar dados para os relatórios de inventário no bucket de destino de inventário do S3, escolha a guia Permissions (Permissões).
11. Role para baixo até a seção Bucket policy (Política de bucket) e escolha Edit (Editar). A página Bucket policy (Política de bucket) se abre.
12. Para conceder permissões para o inventário do S3, no campo Policy (Política), cole a seguinte política de bucket.

    Substitua os três valores do exemplo pelos seguintes valores:

- O nome do bucket criado para armazenar os relatórios de inventário (por exemplo, *amzn-s3-demo-destination-bucket2*).
- O nome do bucket de origem que armazena os vídeos de entrada (por exemplo, *amzn-s3-demo-source-bucket*).
- O ID da Conta da AWS que você usou para criar o bucket de origem do vídeo S3 (por exemplo, *111122223333*).

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"InventoryAndAnalyticsExamplePolicy",
      "Effect":"Allow",
      "Principal": {"Service": "s3.amazonaws.com"},
      "Action":"s3:PutObject",
      "Resource":["arn:aws:s3:::amzn-s3-demo-destination-bucket2/*"],
      "Condition": {
          "ArnLike": {
              "aws:SourceArn": "arn:aws:s3:::amzn-s3-demo-source-bucket"
           },
         "StringEquals": {
             "aws:SourceAccount": "111122223333",
             "s3:x-amz-acl": "bucket-owner-full-control"
          }
       }
    }
  ]
}
```

13. Escolha Salvar alterações.

Configure o inventário do Amazon S3 para o bucket de origem de vídeo do S3

Para gerar uma lista de arquivos simples de objetos de vídeo e metadados, você deve configurar o inventário do S3 para o seu bucket de origem de vídeo do S3. Esses relatórios programados podem incluir todos os objetos no bucket ou objetos agrupados por um prefixo compartilhado. Neste tutorial, o relatório de inventário do S3 inclui todos os objetos de vídeo em seu bucket de origem do S3.

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets.
3. Para configurar um relatório de inventário do S3 dos vídeos de entrada no bucket de origem do S3, na seção Buckets, escolha o nome do bucket de origem do S3 (por exemplo, *amzn-s3-demo-source-bucket*).
4. Escolha a guia Management.
5. Role para baixo até a seção Inventory configurations (Configurações de inventário), e escolha Create Inventory configuration (Criar configuração de inventário).
6. Para Inventory configuration name (Nome da configuração de inventário), insira um nome (por exemplo, **tutorial-inventory-config**).
7. Em Inventory scope (Escopo do inventário), escolha Current version only (Somente versão atual) para Object versions (Versões do objeto) e mantenha as outras configurações de Inventary scope(Escopo do inventário) definidas com os padrões para este tutorial.
8. Na seção Report details (Detalhes do relatório), para Destination bucket (Bucket de destino), escolha This account (Esta conta).
9. Para Destination (Destino), escolha Browse S3 (Procurar no S3) e escolha o bucket de destino que você criou antes para salvar os relatórios de inventário (por exemplo, *amzn-s3-demo-destination-bucket2*). Em seguida, escolha Choose path (Escolher caminho).

   O bucket de destino do inventário deve estar na mesma Região da AWS que o bucket de origem para o qual você está configurando o inventário do S3. O bucket de destino do inventário pode estar em uma Conta da AWS diferente.

   No campo de bucket de Destination (Destino), a Destination bucket permission (Permissão do bucket de destino) é adicionada à política de bucket de destino para permitir que o Amazon S3 coloque dados nesse bucket de destino do inventário. Para obter mais informações, consulte Criação de uma política de bucket de destino.
10. Em Frequency (Frequência), escolha Daily (Diária).
11. Em Output format (Formato de saída), escolha CSV.
12. Em Status, escolha Enabled (Habilitado).
13. Em Server-side encryption (Criptografia do lado do servidor), escolha Disable (Desabilitar) para este tutorial.

Para obter mais informações, consulte Configurar um inventário usando o console do S3 e Conceder permissão para que o Amazon S3 use a sua chave gerenciada pelo cliente para criptografia.

14. Na seção Additional fields - optional (Campos adicionais - opcionais), escolha Size (Tamanho), Last modified (Última modificação) e Storage class (Classe de armazenamento).
15. Escolha Criar.

Para obter mais informações, consulte Configurar um inventário usando o console do S3.

Confira o relatório de inventário para o seu bucket de origem de vídeo S3

Quando um relatório de inventário é publicado, os arquivos manifestos são enviados para o bucket de destino do S3.

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets.
3. Na lista de Buckets, escolha o nome do bucket de origem de vídeo (por exemplo, *amzn-s3-demo-source-bucket*).
4. Escolha Management (Gerenciamento).
5. Para ver se o relatório de inventário do S3 está pronto para você poder criar um trabalho de operações em lote do S3 na Etapa 7, em Inventory configurations (Configurações do inventário), confira se o botão Create job from manifest (Criar trabalho a partir do manifesto) está habilitado.

   > **Note**
   >
   > O primeiro relatório de inventário pode demorar até 48 horas para ser entregue. Se o botão Create job from manifest (Criar trabalho do manifesto) estiver desativado, o primeiro relatório de inventário não foi entregue. Espere até que o primeiro relatório de inventário seja entregue e o botão Create job from manifest (Criar trabalho a partir do manifesto) esteja habilitado para criar um trabalho de operações em lote do S3 na Etapa 7.

6. Para conferir um relatório de inventário do S3 (`manifest.json`), na coluna Destination (Destino), escolha o nome do bucket de destino do inventário que você criou antes para armazenar relatórios de inventário (por exemplo, *amzn-s3-demo-destination-bucket2*).

7. Na guia Objects (Objetos), escolha a pasta existente com o nome do seu bucket de origem do S3 (por exemplo, *amzn-s3-demo-source-bucket*). Em seguida, escolha o nome que você inseriu em Inventory configuration name (Nome da configuração do inventário) quando criou a configuração de inventário antes (por exemplo, **tutorial-inventory-config**).

   Você pode ver uma lista de pastas com as datas de geração dos relatórios como seus nomes.
8. Para conferir o relatório de inventário diário do S3 para uma determinada data, escolha a pasta com um nome de data de geração e depois escolha `manifest.json`.
9. Para verificar os detalhes do relatório de inventário em uma data específica, na página manifesto.json, escolha Download (Baixar) ou Open (Abrir).

Etapa 6: criar uma função do IAM para operações em lote do S3

Para usar as operações em lote do S3 para fazer transcodificação em lote, você deve primeiro criar uma função do IAM para conceder permissões ao Amazon S3 para executar as operações em lote do S3.

Subetapas

- Criar uma política do IAM para operações em lote do S3
- Crie uma função do IAM de operações em lote do S3 e anexe políticas de permissão

Criar uma política do IAM para operações em lote do S3

Você deve criar uma política do IAM que conceda permissão às operações em lote do S3 para ler o manifesto de entrada, invocar a função do Lambda e gravar o relatório de conclusão do trabalho de operações em lote do S3.

1. Faça login no AWS Management Console e abra o console do IAM, em https://console.aws.amazon.com/iam/.
2. No painel de navegação à esquerda, escolha Políticas.
3. Escolha Criar política.
4. Escolha a guia JSON.
5. No campo de texto JSON, cole a política JSON a seguir.

   Na política JSON, substitua os quatro valores do exemplo pelos seguintes valores:

- O nome do bucket de origem que armazena vídeos de entrada (por exemplo, *amzn-s3-demo-source-bucket*).
- O nome do bucket de destino de inventário que você criou na Etapa 5 para armazenar os arquivos `manifest.json` (por exemplo, *amzn-s3-demo-destination-bucket2*).
- O nome do bucket que você criou na Etapa 1 para armazenar arquivos de mídia de saída (por exemplo, *amzn-s3-demo-destination-bucket1*). Neste tutorial, colocamos relatórios de conclusão de trabalho no bucket de destino para arquivos de mídia de saída.
- A função ARN da função Lambda que você criou na Etapa 4. Para localizar e copiar o ARN da função do Lambda, faça o seguinte:
  - Em uma nova guia do navegador, abra a página Functions (Funções) no console do Lambda em https://console.aws.amazon.com/lambda/home#/functions.
  - Na lista de Functions (Funções), escolha o nome da função do Lambda que você criou na Etapa 4 (por exemplo, **`tutorial-lambda-convert`**).
  - Escolha Copy ARN (Copiar ARN).

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "S3Get",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-source-bucket/*",
                "arn:aws:s3:::amzn-s3-demo-destination-bucket2/*"
            ]
        },
        {
            "Sid": "S3PutJobCompletionReport",
            "Effect": "Allow",
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket1/*"
        },
        {
            "Sid": "S3BatchOperationsInvokeLambda",
```

```
            "Effect": "Allow",
            "Action": [
                "lambda:InvokeFunction"
            ],
            "Resource": [
                "arn:aws:lambda:us-west-2:111122223333:function:tutorial-lambda-
convert"
            ]
        }
    ]
}
```

6. Escolha Próximo: etiquetas.
7. Selecione Próximo: revisar.
8. No campo Name (Nome), insira **`tutorial-s3batch-policy`**.
9. Escolha Criar política.

Crie uma função do IAM de operações em lote do S3 e anexe políticas de permissão

1. Faça login no AWS Management Console e abra o console do IAM, em https://console.aws.amazon.com/iam/.
2. No painel de navegação à esquerda, escolha Roles (Funções) e Create role (Criar função).
3. Escolha o tipo de função AWS service (Serviço da AWS) e depois escolha o serviço S3.
4. Em Select your use case (Selecionar seu caso de uso), escolha S3 Batch Operations (Operações em lote do S3).
5. Escolha Próximo.
6. Em Anexar políticas de permissões, insira o nome da política do IAM que você criou antes (por exemplo, **`tutorial-s3batch-policy`**) na caixa de pesquisa para filtrar a lista de políticas. Marque a caixa de seleção ao lado do nome da política (por exemplo, **`tutorial-s3batch-policy`**).
7. Escolha Próximo.
8. Em Nome do perfil, insira **`tutorial-s3batch-role`**.
9. Escolha Create role (Criar função).

   Depois que você cria a função do IAM para as operações em lote do S3, a política de confiança a seguir é anexada automaticamente à função. Essa política de confiança permite que o principal das operações em lote do S3 assuma a função do IAM.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service":"batchoperations.s3.amazonaws.com"
         },
         "Action":"sts:AssumeRole"
      }
   ]
}
```

Etapa 7: criar e executar um trabalho de operações em lote do S3

Para criar um trabalho de operações em lote do S3 para processar os vídeos de entrada no bucket de origem do S3, você deve especificar os parâmetros para esse trabalho específico.

> **Note**
>
> Antes de começar a criar um trabalho de operações em lote do S3, certifique-se de que o botão Create job from manifest (Criar trabalho a partir do manifesto) esteja habilitado. Para obter mais informações, consulte Confira o relatório de inventário para o seu bucket de origem de vídeo S3. Se o botão Create job from manifest (Criar trabalho a partir do manifesto) estiver desabilitado, o primeiro relatório de inventário não foi entregue e você deve esperar até que o botão esteja habilitado. Depois de configurar o inventário do Amazon S3 para o bucket de origem do S3 na Etapa 5, a entrega do primeiro relatório de inventário pode levar até 48 horas.

Subetapas

- Criar um trabalho de operações em lote do S3
- Execute o trabalho de operações em lote do S3 para chamar a função Lambda
- (Opcional) Verificar seu relatório de conclusão
- (Opcional) Monitore cada chamada do Lambda no console do Lambda
- (Opcional) Monitore cada trabalho de transcodificação de vídeo MediaConvert no console do MediaConvert

Criar um trabalho de operações em lote do S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação esquerdo, escolha Batch Operations (Operações em lote).
3. Escolha Criar trabalho.
4. Para Região da AWS, escolha a região onde você deseja criar o trabalho.

   Neste tutorial, para usar o trabalho de operações em lote do S3 para invocar uma função do Lambda, você deve criar o trabalho na mesma região que o bucket de origem de vídeo do S3 onde os objetos referenciados no manifesto estão localizados.
5. Na seção Manifest (Manifesto), faça o seguinte:

   a. Para Manifest format (Formato do manifesto), escolha S3 Inventory report (manifest.json) (Relatório do S3 Inventory [manifest.json]).

   b. Para Manifest object (Objeto de manifesto), escolha Browse S3 (Procurar no S3) para encontrar o bucket que você criou na Etapa 5 para armazenar relatórios de inventário (por exemplo, *amzn-s3-demo-destination-bucket2*). Na página Manifest object, (Objeto de manifesto) navegue pelos nomes de objetos até encontrar um arquivo `manifest.json` para uma data específica. Este arquivo lista as informações sobre todos os vídeos que você deseja transcodificar em lote. Quando encontrar o arquivo `manifest.json` que você deseja usar, escolha o botão de opção ao lado dele. Em seguida, escolha Choose path (Escolher caminho).

   c. (Opcional) Para Manifest object version ID - optional (ID da versão do objeto de manifesto - opcional) insira o ID de versão do objeto de manifesto se quiser usar uma versão que não seja a mais recente.
6. Escolha Próximo.
7. Para usar a função do Lambda para transcodificar todos os objetos listados no arquivo `manifest.json` selecionado, em Operation type (Tipo de operação), escolha Invoke AWS Lambda function (Invocar função do IAM).
8. Na seção Invoke Lambda Function (Invocar função do Lambda), faça o seguinte:

   a. Escolha Choose from functions in your account (Escolher das funções de sua conta).

   b. Para Lambda function (Função do Lambda), escolha a função do Lambda que você criou na Etapa 4 (por exemplo, **`tutorial-lambda-convert`**).

c. Para Lambda function version (Versão da função do Lambda), mantenha o valor padrão $LATER.

9. Escolha Próximo. A página Configure additional options (Configurar opções adicionais) se abre.
10. Na seção Additional options (Opções adicionais), mantenha as configurações padrão.

    Para obter mais informações sobre essas opções, consulte Elementos da solicitação de trabalho de Operações em lote.
11. Na seção Completion report (Relatório de conclusão) para Path to completion report destination (Caminho para o destino do relatório de conclusão), escolha Browse S3 (Procurar no S3). Encontre o nome do bucket para armazenar os arquivos de mídia de saída que você criou na Etapa 1 (por exemplo, *amzn-s3-demo-destination-bucket1*). Escolha o botão de opção ao lado do nome desse bucket. Em seguida, escolha Choose path (Escolher caminho).

    Para as demais configurações de Relatório de conclusão, mantenha os padrões. Para obter mais informações sobre conclusão de configurações do relatório, consulte Elementos da solicitação de trabalho de Operações em lote. Um relatório de conclusão mantém um registro dos detalhes do trabalho e das operações executadas.
12. Em Permissions (Permissões), escolha Choose from existing IAM roles (Escolher entre as funções do IAM existentes). Para IAM role (Função do IAM), escolha a função do IAM para seu trabalho de operações em lote do S3 que você criou na Etapa 6 (por exemplo, **`tutorial-s3batch-role`**).
13. Escolha Próximo.
14. Na página Review (Revisão), revise as configurações. Depois, escolha Create Job (Criar trabalho).

    Depois que o S3 termina de ler o manifesto do trabalho de operações em lote do S3, ele define o Status do trabalho como Awaiting your confirmation to run (Aguardando sua confirmação para ser executado). Para ver as atualizações do status do trabalho, atualize a página. Você não pode executar seu trabalho até que o status dele seja Awaiting your confirmation to run (Aguardando sua confirmação para ser executado).

Execute o trabalho de operações em lote do S3 para chamar a função Lambda

Execute seu trabalho de operações em lote para chamar sua função Lambda para transcodificação de vídeo. Se o trabalho falhar, você pode conferir o relatório da conclusão para identificar a causa.

Para executar o trabalho de operações em lote do S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação esquerdo, escolha Batch Operations (Operações em lote).
3. Na lista Jobs (Trabalhos), escolha a opção Job ID (ID do trabalho) na primeira linha, que é o trabalho das operações em lote do S3 que você criou antes.
4. Escolha Run job (Executar trabalho).
5. Revise os parâmetros do job novamente e confirme se o valor para Total objects listed in manifest (Total de objeto listados no manifesto) é o mesmo do número de objetos no manifesto. Em seguida, selecione Run job (Executar trabalho).

   A página de trabalho de operações em lote do S3 é aberta.
6. Depois que o trabalho começar a execução, em sua página de trabalho em Status, verifique o andamento de seu trabalho de operações em lote do S3, como Status, % Complete (% de conclusão), Total succeeded (rate) (Total com êxito [taxa]), Total failed (rate) (Total com falha [taxa]), Date terminated (Data de término) e Reason for termination (Motivo do término).

   Quando o trabalho de operações em lote do S3 for concluído, visualize os dados na página do trabalho para confirmar que o trabalho foi concluído conforme esperado.

   Se mais de 50% das operações de objeto do trabalho das operações em lote do S3 falharem após mais de 1.000 tentativas, o trabalho automaticamente falha. Para conferir o relatório de conclusão para identificar a causa das falhas, consulte o procedimento opcional abaixo.

(Opcional) Verificar seu relatório de conclusão

Você pode usar o relatório de conclusão para determinar quais objetos falharam e a causa das falhas.

Para conferir o relatório de conclusão para obter detalhes sobre os objetos que falharam

1. Na página do trabalho de operações em lote do S3, role para baixo até a seção Completion report (Relatório de conclusão) e escolha o link em Completion report destination (Destino do relatório de conclusão).

   A página do bucket de destino de saída do S3 se abre.

2. Na guia Objects (Objetos), escolha a pasta que tem um nome que termina com o ID do trabalho de operações em lote do S3 que você criou antes.
3. Escolha results/ (resultados/).
4. Marque a caixa de seleção próxima ao arquivo `.csv`.
5. Para visualizar o relatório de trabalhos, escolha Open (Abrir) ou Download (Baixar).

(Opcional) Monitore cada chamada do Lambda no console do Lambda

Depois que o trabalho de operações em lote do S3 começa a ser executado, o trabalho invoca a função do Lambda para cada objeto de vídeo de entrada. O S3 grava logs de cada chamada do Lambda no CloudWatch Logs. Você pode usar o painel de monitoramento do console do Lambda para monitorar sua função Lambda.

1. Abra o console AWS Lambda em https://console.aws.amazon.com/lambda/.
2. No painel de navegação à esquerda, escolha Functions (Funções).
3. Na lista Functions (Funções), escolha o nome da função do Lambda que você criou na Etapa 4 (por exemplo, **`tutorial-lambda-convert`**).
4. Escolha a guia Monitor (Monitorar).
5. Em Metrics (Métricas), consulte as métricas de tempo de execução para sua função Lambda.
6. Em Logs, visualize dados de log para cada chamada do Lambda por meio do CloudWatch Logs Insights

> **Note**
>
> Quando você usa as operações em lote do S3 com uma função Lambda, essa função Lambda é chamada em cada objeto. Se o trabalho de operações em lote do S3 for grande, ele poderá chamar várias funções Lambda ao mesmo tempo, causando um pico na simultaneidade do Lambda.
> Cada Conta da AWS tem uma cota de simultaneidade do Lambda por região. Para obter mais informações, consulte Escalabilidade de função do AWS Lambda no Guia do desenvolvedor do AWS Lambda. Uma prática recomendada para usar funções Lambda com operações em lote do S3 é definir um limite de simultaneidade na própria função Lambda. Definir um limite de simultaneidade evita que seu trabalho consuma a maior parte de sua simultaneidade do Lambda e potencialmente restrinja a utilização de

outras funções em sua conta. Para obter mais informações, consulte Gerenciamento de simultaneidade reservada do Lambda no Guia do desenvolvedor do AWS Lambda.

(Opcional) Monitore cada trabalho de transcodificação de vídeo MediaConvert no console do MediaConvert

Um trabalho do MediaConvert se encarrega da transcodificação de um arquivo de mídia. Quando o trabalho de operações em lote do S3 invoca sua função do Lambda para cada vídeo, cada invocação da função do Lambda cria um trabalho de transcodificação do MediaConvert para cada vídeo de entrada.

1. Faça login no AWS Management Console e abra o console do MediaConvert em https://console.aws.amazon.com/mediaconvert/.
2. Se a página introdutória MediaConvert for exibida, escolha Get started (Conceitos básicos).
3. Na lista de Jobs (Trabalhos), visualize cada linha para monitorar a tarefa de transcodificação para cada vídeo de entrada.
4. Identifique a linha de um trabalho que você deseja conferir e escolha o link Job ID (ID do trabalho) para abrir a página de detalhes do trabalho.
5. Na página Job summary (Resumo do trabalho) em Outputs (Saídas), escolha o link para a saída HLS, MP4 ou miniaturas, dependendo do que é suportado pelo navegador, para ir para o bucket de destino do S3 para os arquivos de mídia de saída.
6. Na pasta correspondente (HLS, MP4 ou Thumbnails [Miniaturas]) do bucket de destino de saída do S3, escolha o nome do objeto de arquivo de mídia de saída.

   A página de details do objeto se abre.
7. Na página de detalhes do objeto, em Object overview (Visão geral do objeto), escolha o link em Object URL (URL do objeto) para assistir ao arquivo de mídia de saída transcodificado.

Etapa 8: Conferir os arquivos de mídia de saída do bucket de destino do S3

Para conferir os arquivos de mídia de saída do bucket de destino do S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets.

3. Na lista Buckets, escolha o nome do bucket de destino do S3 para os arquivos de mídia de saída que você criou na Etapa 1 (por exemplo, *amzn-s3-demo-destination-bucket1*).
4. Na guia Objects (Objetos), cada vídeo de entrada tem uma pasta com o nome do vídeo de entrada. Cada pasta contém os arquivos de mídia de saída transcodificados para um vídeo de entrada.

   Para verificar os arquivos de mídia de saída para um vídeo de entrada, faça o seguinte:

   a. Escolha a pasta com o nome do vídeo de entrada que você deseja conferir.
   b. Escolha a pasta Default/ (Padrão/).
   c. Escolha a pasta para um formato transcodificado (HLS, MP4 ou miniaturas neste tutorial).
   d. Escolha o nome do arquivo de mídia de saída.
   e. Para ver o arquivo transcodificado, na página de detalhes do objeto, escolha o link em Object URL (URL do objeto).

      Os arquivos de mídia de saída no formato HLS são divididos em segmentos curtos. Para reproduzir esses vídeos, incorpore o URL do objeto do arquivo `.m3u8` em um player compatível.

Etapa 9: limpar

Se você transcodificou vídeos usando as operações em lote do S3, o Lambda e o MediaConvert somente como um exercício de aprendizado, exclua os recursos da AWS alocados para que não haja mais encargos.

Subetapas

- Exclua a configuração do inventário do S3 para o bucket de origem do S3
- Excluir a função Lambda
- Excluir o grupo de logs do CloudWatch
- Exclua as funções do IAM junto com as políticas em linha das funções do IAM
- Exclua a política do IAM gerenciada pelo cliente
- Esvaziar os buckets do S3
- Excluir os buckets do S3

Exclua a configuração do inventário do S3 para o bucket de origem do S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets.
3. Na lista de Buckets, selecione o nome do bucket de origem (por exemplo, *amzn-s3-demo-source-bucket*).
4. Escolha a guia Management.
5. Em Inventory configurations (Configurações do inventário), escolha o botão de opção ao lado da configuração de inventário que você criou na Etapa 5 (por exemplo, **tutorial-inventory-config**).
6. Escolha Delete (Excluir) e, em seguida, escolha Confirm (Confirmar).

Excluir a função Lambda

1. Abra o console AWS Lambda em https://console.aws.amazon.com/lambda/.
2. No painel de navegação à esquerda, escolha Functions (Funções).
3. Marque a caixa de seleção ao lado da função que você criou na Etapa 4 (por exemplo, **tutorial-lambda-convert**).
4. Escolha Ações e, em seguida, escolha Excluir.
5. Na caixa de diálogo Delete function (Excluir função), escolha Delete (Excluir).

Excluir o grupo de logs do CloudWatch

1. Abra o console do CloudWatch em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação à esquerda, escolha Logs e, em seguida, escolha Log groups (Grupos de log).
3. Marque a caixa de seleção ao lado do grupo de logs que tem um nome que termina com a função do Lambda que você criou na Etapa 4 (por exemplo, **tutorial-lambda-convert**).
4. Escolha Actions (Ações) e Delete log group(s) (Excluir grupo(s) de log).
5. Na caixa de diálogo Delete log group(s) (Excluir grupo(s) de logs), escolha Delete (Excluir).

Exclua as funções do IAM junto com as políticas em linha das funções do IAM

Para excluir as funções do IAM criadas na Etapa 2, Etapa 3 e Etapa 6, faça o seguinte:

1. Faça login no AWS Management Console e abra o console do IAM, em https://console.aws.amazon.com/iam/.
2. No painel de navegação da esquerda, escolha Roles (Funções) e marque as caixas de seleção ao lado do nome da função que você deseja excluir.
3. Na parte superior da página, escolha Delete (Excluir).
4. Na caixa de diálogo de confirmação, insira a resposta necessária no campo de entrada de texto com base no prompt e escolha Delete (Excluir).

Exclua a política do IAM gerenciada pelo cliente

Para excluir a política do IAM gerenciada pelo cliente que você criou na Etapa 6, faça o seguinte:

1. Faça login no AWS Management Console e abra o console do IAM, em https://console.aws.amazon.com/iam/.
2. No painel de navegação à esquerda, escolha Políticas.
3. Escolha o botão de opção ao lado da política que você criou na Etapa 6 (por exemplo, **`tutorial-s3batch-policy`**). É possível usar a caixa de pesquisa para filtrar a lista de políticas.
4. Escolha Actions (Ações) e, em seguida, escolha Delete (Excluir).
5. Confirme que deseja excluir esta política, inserindo o nome da política no campo de texto, e escolha Delete (Excluir).

Esvaziar os buckets do S3

Para esvaziar os buckets do S3 criados em Pré-requisitos, Etapa 1 e Etapa 5, faça o seguinte:

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets.
3. Na lista Buckets, escolha o botão de opção ao lado do nome do bucket que você deseja esvaziar e depois escolha Empty (Esvaziar).

4. Na página Empty bucket (Esvaziar bucket), confirme se deseja esvaziar o bucket inserindo **`permanently delete`** no campo de texto e depois escolha Empty (Esvaziar).

Excluir os buckets do S3

Para excluir os buckets do S3 criados em Pré-requisitos, Etapa 1 e Etapa 5, faça o seguinte:

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets.
3. Na lista Buckets, escolha o botão de opção ao lado do nome do bucket que você deseja excluir.
4. Escolha Excluir.
5. Na página Delete bucket (Excluir bucket), confirme se deseja excluir o bucket inserindo o nome do bucket no campo de texto e escolha Delete bucket (Excluir bucket).

Próximas etapas

Depois de concluir este tutorial, você poderá explorar outros casos de uso relevantes:

- Você pode usar o Amazon CloudFront para transmitir os arquivos de mídia transcodificados para espectadores em todo o mundo. Para obter mais informações, consulte Tutorial: Hospedagem de transmissão sob demanda com o Amazon S3, Amazon CloudFront e Amazon Route 53.
- Você pode transcodificar vídeos no momento em que os carrega para o bucket de origem do S3. Para fazer isso, você pode configurar um acionador de evento do Amazon S3 que invoca automaticamente a função do Lambda para transcodificar novos objetos no S3 com o MediaConvert. Para obter mais informações, consulte o Tutorial: Uso de um acionador do Amazon S3 para invocar uma função do Lambda no Guia do desenvolvedor do AWS Lambda.

Solução de problemas do Operações em Lote

Os tópicos a seguir listam os erros comuns para ajudar você a solucionar problemas que pode encontrar durante ao trabalhar com o Operações em Lote do Amazon S3.

Para solucionar problemas com o Replicação em Lote do S3, consulte the section called “Erros de replicação em lote”.

Erros comuns

- O relatório do trabalho não é entregue quando há um problema com as permissões ou quando o modo de retenção do Bloqueio de Objetos do S3 está habilitado
- O Operações em Lote apresenta falha em objetos com o erro 400 InvalidRequest: falha na tarefa devido à falta de VersionId
- Crie uma falha de trabalho com a opção de tag de trabalho ativada
- Acesso negado para ler o manifesto

O relatório do trabalho não é entregue quando há um problema com as permissões ou quando o modo de retenção do Bloqueio de Objetos do S3 está habilitado

O erro a seguir ocorrerá se não houver as permissões necessárias ou se o modo de retenção do Bloqueio de Objetos (modo de governança ou modo de conformidade) estiver habilitado no bucket de destino.

Erro: motivos da falha. Não foi possível gravar o relatório do trabalho no bucket de relatórios. Verifique suas permissões.

É necessário configurar o perfil do AWS Identity and Access Management (IAM) e a política de confiança para conceder ao Operações em Lote a permissão `s3:PutObject` para PUT objetos no bucket em que o relatório será entregue. Se não houver essas permissões necessárias, ocorrerá uma falha na entrega do relatório de trabalhos.

Quando um modo de retenção está ativado, o bucket é protegido de gravação única e várias leituras (WORM). O Bloqueio de Objetos com o modo de retenção habilitado no bucket de destino não é compatível; portanto, as tentativas de entrega do relatório de conclusão de trabalhos falham. Para corrigir esse problema, escolha um bucket de destino para seus relatórios de conclusão de trabalhos que não tenha o modo de retenção de bloqueio de objetos ativado.

O Operações em Lote apresenta falha em objetos com o erro 400 InvalidRequest: falha na tarefa devido à falta de VersionId

O exemplo de erro a seguir ocorre se um trabalho de operações em lote estiver executando ações em objetos em um bucket versionado e encontrar um objeto no manifesto com um campo de ID de versão vazio.

Erro: *`bucket_name,prefix/file_name`*,failed,400,InvalidRequest,Falha na tarefa devido à falta de VersionId

Esse erro ocorre porque o campo ID da versão no manifesto é uma string vazia, em vez da string `null` literal.

As operações em lote falharão para aquele objeto ou objetos específicos, mas não para todo o trabalho. Esse problema ocorre se o formato do manifesto estiver configurado para usar IDs de versão durante a operação. Os trabalhos sem versionamento não enfrentam esse problema porque operam somente na versão mais recente de cada objeto e ignoram os IDs de versão no manifesto.

Para corrigir esse problema, converta os IDs de versão vazios em strings `null`. Para obter mais informações, consulte the section called “Converter strings de ID de versão vazias em cadeias de caracteres null”.

Crie uma falha de trabalho com a opção de tag de trabalho ativada

Sem a permissão `s3:PutJobTagging`, a criação de trabalhos de operações em lote com a opção de tag de trabalho ativada causa erros `403 access denied`.

Para criar trabalhos de operações em lote com a opção de tag de trabalho ativada, o usuário do AWS Identity and Access Management (IAM) que está criando o trabalho de operações em lote deve ter a permissão `s3:PutJobTagging` além da permissão `s3:CreateJob`.

Para obter mais informações sobre as permissões necessárias para as operações em lote, consulte the section called “Conceder permissões”.

Acesso negado para ler o manifesto

Se as operações em lote não conseguirem ler o arquivo de manifesto ao tentar criar um trabalho de operações em lote, os seguintes erros poderão ocorrer.

AWS CLI

Motivo da falha A leitura do manifesto é proibida: AccessDenied

Console do Amazon S3

Aviso: não é possível obter a ETag do objeto de manifesto. Especifique um objeto diferente para continuar.

Para resolver esse problema, execute um dos seguintes procedimentos:

- Verifique se o perfil do IAM da Conta da AWS usado para criar o trabalho de operações em lote tem a permissão `s3:GetObject`. O perfil do IAM da conta deve ter a permissão `s3:GetObject` para permitir que o Operações em Lote leia o arquivo de manifesto.

  Para obter mais informações sobre as permissões necessárias para as operações em lote, consulte the section called “Conceder permissões”.
- Verifique os metadados dos objetos do manifesto para ver se há incompatibilidade de acesso com a propriedade do objeto do S3. Para obter mais informações sobre a propriedade de objeto do S3, consulte the section called “Controlar a propriedade do objeto”.
- Verifique se as chaves do AWS Key Management Service (AWS KMS) são usadas para criptografar o arquivo de manifesto.

  O Operações em Lote é compatível com relatórios de inventário CSV criptografados pelo AWS KMS. No entanto, o Operações em Lote não é compatível com arquivos de manifesto CSV criptografados pelo AWS KMS. Para obter mais informações, consulte Configurar o inventário do Amazon S3 e Especificar um manifesto.

Consultar dados no local com o Amazon S3 Select

> **Important**
>
> O Amazon S3 Select não está mais disponível para novos clientes. Os clientes existentes do Amazon S3 Select podem continuar usando o recurso normalmente. Saiba mais

Com o Amazon S3 Select, é possível usar instruções de linguagem de consulta estruturada (SQL) para filtrar o conteúdo de um objeto do Amazon S3 e recuperar somente o subconjunto de dados necessário. Ao usar o Amazon S3 Select para filtrar esses dados, é possível reduzir a quantidade de dados transferidos pelo Amazon S3. Isso reduz o custo e a latência de recuperação desses dados.

O Amazon S3 Select permite que você consulte somente um objeto por vez. Ele funciona em um objeto armazenado em formato CSV, JSON ou Apache Parquet. Ele também funciona em um objeto compactado com GZIP ou BZIP2 (somente para objetos CSV e JSON) e um objeto criptografado do lado do servidor. Você pode especificar o formato dos resultados como CSV ou JSON e determinar como os registros do resultado são delimitados.

Expressões SQL são passadas para o Amazon S3 na solicitação. O Amazon S3 Select é compatível com um subconjunto de SQL. Para obter mais informações sobre os elementos SQL compatíveis com o Amazon S3 Select, consulte Referência SQL para o Amazon S3 Select.

É possível realizar consultas SQL usando o console do Amazon S3, a AWS Command Line Interface (AWS CLI), a operação de API REST `SelectObjectContent` ou os SDKs da AWS.

> **Note**
>
> O console do Amazon S3 limita a quantidade de dados retornados em 40 MB. Para recuperar mais dados, use a AWS CLI ou a API.

Requisitos e limites

Estes são os requisitos para o uso do Amazon S3 Select:

- É necessário ter permissão `s3:GetObject` para o objeto sendo consultado.
- Se o objeto consultado for criptografado por meio da criptografia do lado do servidor com chaves fornecidas pelo cliente (SSE-C), será necessário usar `https` e fornecer a chave de criptografia na solicitação.

Os seguintes limites se aplicam ao usar o Amazon S3 Select:

- O S3 Select pode consultar somente um objeto por solicitação.
- O tamanho máximo de uma expressão SQL é 256 KB.
- O tamanho máximo de um registro na entrada ou no resultado é de 1 MB.
- O Amazon S3 Select só pode emitir dados aninhados usando o formato de saída JSON.
- Não é possível consultar um objeto armazenado nas classes de armazenamento S3 Glacier Flexible Retrieval, S3 Glacier Deep Archive ou Reduced Redundancy Storage (RRS). Também não é possível consultar um objeto armazenado no nível S3 Intelligent-Tiering Archive Access ou S3 Intelligent-Tiering Deep Archive Access. Para obter mais informações sobre classes de armazenamento, consulte Compreender e gerenciar classes de armazenamento do Amazon S3.

Limitações adicionais se aplicam ao usar o Amazon S3 Select com um objeto Parquet:

- O Amazon S3 Select aceita somente a compactação colunar com GZIP ou Snappy. O Amazon S3 Select não aceita a compactação de objetos inteiros no caso de um objeto Parquet.
- O Amazon S3 Select não é compatível com a saída do Parquet. É necessário especificar o formato de saída como CSV ou JSON.
- O tamanho máximo do grupo de linhas não compactadas é 512 MB.
- É necessário usar os tipos de dados especificados no esquema do objeto.
- A seleção em um campo repetido retorna apenas o último valor.

Criar uma solicitação

Ao criar uma solicitação, você fornece detalhes do objeto consultado usando um objeto `InputSerialization`. Forneça detalhes sobre como os resultados serão retornados usando um objeto `OutputSerialization`. Inclua também a expressão SQL que o Amazon S3 usa para filtrar a solicitação.

Para obter mais informações sobre como criar uma solicitação do Amazon S3 Select, consulte SelectObjectContent na Referência de API do Amazon Simple Storage Service. Também é possível um exemplo de código do SDK nas seções a seguir.

Solicitações usando intervalos de verificação

Com o Amazon S3 Select, é possível verificar um subconjunto de um objeto especificando um intervalo de bytes a ser consultado. Esse recurso permite paralelizar a verificação de todo o objeto dividindo o trabalho em solicitações separadas do Amazon S3 Select para uma série de intervalos de verificação não sobrepostos.

Os intervalos de verificação não precisam estar alinhados aos limites de registro. Uma solicitação de intervalo de verificação do Amazon S3 Select é executada no intervalo de bytes especificado. Um registro que começa no intervalo de verificação especificado, mas ultrapassa o intervalo de verificação, será processado pela consulta. Por exemplo, veja abaixo um objeto do Amazon S3 que contém uma série de registros em um formato CSV delimitado por linha:

```
A,B
C,D
D,E
E,F
G,H
I,J
```

Suponha que você esteja usando o parâmetro `ScanRange` do Amazon S3 Select e inicie no (byte) `1` e termine no (byte) `4`. Assim, o intervalo de verificação começaria em "`,`" e faria a verificação até o final do registro, começando em `C`. A solicitação de intervalo de verificação retornará o resultado `C,D` porque esse é o final do registro.

As solicitações de intervalo de verificação do Amazon S3 Select são compatíveis com objetos Parquet, CSV (sem delimitadores entre aspas) ou JSON (somente no modo `LINES`). Os objetos CSV e JSON devem estar descompactados. Para objetos JSON e CSV baseados em linha, quando um intervalo de verificação é especificado como parte da solicitação do Amazon S3 Select, todos os registros que começam no intervalo de verificação são processados. Para objetos Parquet, todos os grupos de linhas que começam no intervalo de verificação solicitado são processados.

As solicitações de intervalo de verificação do Amazon S3 Select estão disponíveis para uso com a AWS CLI, a API do Amazon S3 e AWS SDKs. É possível usar o parâmetro `ScanRange` na solicitação do Seleção do Amazon S3 desse recurso. Para obter mais informações, consulte SelectObjectContent na Referência da API do Amazon Simple Storage Service.

Erros

O Amazon S3 Select retorna um código de erro e uma mensagem de erro associada quando um problema é encontrado ao tentar executar uma consulta. Para obter uma lista de códigos de erro e descrições, consulte a seção Lista de Códigos de erro de conteúdo de objetos SELECT da página Respostas de erro na Referência de APIs do Amazon Simple Storage Service.

Para obter mais informações sobre o Amazon S3 Select, consulte os tópicos a seguir.

Tópicos

- Exemplos de uso do Amazon S3 Select em um objeto
- Referência SQL para o Amazon S3 Select

Exemplos de uso do Amazon S3 Select em um objeto

> **Important**
>
> O Amazon S3 Select não está mais disponível para novos clientes. Os clientes existentes do Amazon S3 Select podem continuar usando o recurso normalmente. Saiba mais

É possível usar o S3 Select para selecionar conteúdo de um objeto usando o console do Amazon S3, a API REST e SDKs da AWS.

Para receber mais informações sobre as funções SQL compatíveis com o S3 Select, consulte Funções SQL.

Usar o console do S3

Como selecionar o conteúdo de um objeto no console do Amazon S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets.
3. Escolha o bucket que contém o objeto do qual você deseja selecionar o conteúdo; depois, escolha o nome do objeto.
4. Escolha Ações de objeto e Consultar com o S3 Select.
5. Defina as Configurações de entrada, com base no formato dos dados de entrada.
6. Defina as Configurações de saída, com base no formato da saída que você deseja receber.
7. Para extrair registros do objeto escolhido, em Consulta SQL, insira os comandos SQL SELECT. Para obter mais informações sobre como escrever comandos SQL, consulte Referência SQL para o Amazon S3 Select.
8. Depois de inserir consultas SQL, escolha Executar consulta SQL. Depois, em Resultados da consulta, é possível ver os resultados das consultas SQL.

Uso da API REST

É possível usar SDKs da AWS para selecionar conteúdo de um objeto. Contudo, se o seu aplicativo exigir, você pode enviar solicitações REST diretamente. Para obter mais informações sobre o formato de solicitação e de resposta, consulte SelectObjectContent.

Uso dos SDKs da AWS

É possível usar o Amazon S3 Select para selecionar parte do conteúdo de um objeto usando o método `selectObjectContent`. Se esse método for bem-sucedido, ele retornará os resultados da expressão SQL.

Java

O código Java a seguir retorna o valor da primeira coluna para cada registro armazenado em um objeto que contém dados armazenados em formato CSV. Ele também solicita que mensagens de `Progress` e `Stats` sejam retornadas. É necessário fornecer um nome de bucket válido e um objeto que contenha dados em formato CSV.

Consulte instruções sobre como criar e testar uma amostra funcional em Getting Started no Guia do desenvolvedor do AWS SDK para Java.

```
package com.amazonaws;

import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.CSVInput;
import com.amazonaws.services.s3.model.CSVOutput;
import com.amazonaws.services.s3.model.CompressionType;
import com.amazonaws.services.s3.model.ExpressionType;
import com.amazonaws.services.s3.model.InputSerialization;
import com.amazonaws.services.s3.model.OutputSerialization;
import com.amazonaws.services.s3.model.SelectObjectContentEvent;
import com.amazonaws.services.s3.model.SelectObjectContentEventVisitor;
import com.amazonaws.services.s3.model.SelectObjectContentRequest;
import com.amazonaws.services.s3.model.SelectObjectContentResult;

import java.io.File;
import java.io.FileOutputStream;
import java.io.InputStream;
import java.io.OutputStream;
import java.util.concurrent.atomic.AtomicBoolean;

import static com.amazonaws.util.IOUtils.copy;

/**
 * This example shows how to query data from S3Select and consume the response in
 the form of an
 * InputStream of records and write it to a file.
 */

public class RecordInputStreamExample {

    private static final String BUCKET_NAME = "${my-s3-bucket}";
    private static final String CSV_OBJECT_KEY = "${my-csv-object-key}";
```

```
    private static final String S3_SELECT_RESULTS_PATH = "${my-s3-select-results-
path}";
    private static final String QUERY = "select s._1 from S3Object s";

    public static void main(String[] args) throws Exception {
        final AmazonS3 s3Client = AmazonS3ClientBuilder.defaultClient();

        SelectObjectContentRequest request = generateBaseCSVRequest(BUCKET_NAME,
 CSV_OBJECT_KEY, QUERY);
        final AtomicBoolean isResultComplete = new AtomicBoolean(false);

        try (OutputStream fileOutputStream = new FileOutputStream(new File
 (S3_SELECT_RESULTS_PATH));
             SelectObjectContentResult result =
 s3Client.selectObjectContent(request)) {
            InputStream resultInputStream =
 result.getPayload().getRecordsInputStream(
                    new SelectObjectContentEventVisitor() {
                        @Override
                        public void visit(SelectObjectContentEvent.StatsEvent event)
                        {
                            System.out.println(
                                    "Received Stats, Bytes Scanned: " +
 event.getDetails().getBytesScanned()
                                            +  " Bytes Processed: " +
 event.getDetails().getBytesProcessed());
                        }

                        /*
                         * An End Event informs that the request has finished
 successfully.
                         */
                        @Override
                        public void visit(SelectObjectContentEvent.EndEvent event)
                        {
                            isResultComplete.set(true);
                            System.out.println("Received End Event. Result is
 complete.");
                        }
                    }
            );

            copy(resultInputStream, fileOutputStream);
        }
```

```
        /*
         * The End Event indicates all matching records have been transmitted.
         * If the End Event is not received, the results may be incomplete.
         */
        if (!isResultComplete.get()) {
            throw new Exception("S3 Select request was incomplete as End Event was
 not received.");
        }
    }

    private static SelectObjectContentRequest generateBaseCSVRequest(String bucket,
 String key, String query) {
        SelectObjectContentRequest request = new SelectObjectContentRequest();
        request.setBucketName(bucket);
        request.setKey(key);
        request.setExpression(query);
        request.setExpressionType(ExpressionType.SQL);

        InputSerialization inputSerialization = new InputSerialization();
        inputSerialization.setCsv(new CSVInput());
        inputSerialization.setCompressionType(CompressionType.NONE);
        request.setInputSerialization(inputSerialization);

        OutputSerialization outputSerialization = new OutputSerialization();
        outputSerialization.setCsv(new CSVOutput());
        request.setOutputSerialization(outputSerialization);

        return request;
    }
}
```

JavaScript

Para obter um exemplo de JavaScript que usa o AWS SDK para JavaScript com a operação de API `SelectObjectContent` do S3 para selecionar registros dos arquivos JSON e CSV armazenados no Amazon S3, consulte a publicação de blog Adição de suporte ao Amazon S3 Select no AWS SDK para JavaScript.

Python

Para obter um exemplo do Python sobre o uso de consultas SQL para pesquisar dados carregados no Amazon S3 como um arquivo de valor separado por vírgulas (CSV) usando o

S3 Select, consulte a publicação do blog Consultar dados sem servidores ou bancos de dados usando o Amazon S3 Select.

Referência SQL para o Amazon S3 Select

> **Important**
>
> O Amazon S3 Select não está mais disponível para novos clientes. Os clientes existentes do Amazon S3 Select podem continuar usando o recurso normalmente. Saiba mais

Essa referência contém uma descrição de elementos de linguagem de consulta estruturada (SQL) que são compatíveis com o Amazon S3 Select.

Tópicos

- Comando SELECT
- Tipos de dados
- Operadores
- Palavras-chave reservadas
- Funções SQL

Comando SELECT

> **Important**
>
> O Amazon S3 Select não está mais disponível para novos clientes. Os clientes existentes do Amazon S3 Select podem continuar usando o recurso normalmente. Saiba mais

O Amazon S3 Select só oferece suporte ao comando SQL `SELECT`. As seguintes cláusulas padrão ANSI são compatíveis com `SELECT`:

- `SELECT` lista
- `FROM`Cláusula
- `WHERE`Cláusula

- `LIMIT`Cláusula

> **Note**
>
> As consultas do Amazon S3 Select não oferecem suporte a subconsultas ou junções no momento.

SELECT lista

A lista `SELECT` nomeia as colunas, as funções e as expressões que a consulta deve retornar. A lista representa o resultado da consulta.

```
SELECT *
SELECT projection1 AS column_alias_1, projection2 AS column_alias_2
```

O primeiro formulário de `SELECT` com o `*` (asterisco) retorna todas as linhas que passaram na cláusula `WHERE`, da maneira como estão. O segundo formulário de `SELECT` cria uma linha com expressões escalares de saída definidas pelo usuário ***projection1*** e ***projection2*** para cada coluna.

FROMCláusula

O Amazon S3 Select oferece suporte aos seguintes formatos de cláusula `FROM`:

```
FROM table_name
FROM table_name alias
FROM table_name AS alias
```

Em cada forma da cláusula `FROM`, `table_name` é o `S3Object` que está sendo consultado. Os usuários provenientes de bancos de dados relacionais tradicionais podem pensar nisso como um esquema de banco de dados que contém várias visualizações em uma tabela.

Seguindo o SQL padrão, a cláusula `FROM` cria linhas filtradas na cláusula `WHERE` e projetadas na lista `SELECT`.

Para objetos JSON armazenados no Seleção do Amazon S3, você também pode usar as seguintes formas da cláusula `FROM`:

```
FROM S3Object[*].path
```

```
FROM S3Object[*].path alias
FROM S3Object[*].path AS alias
```

Com essa forma da cláusula FROM, você pode selecionar entre matrizes ou objetos em um objeto JSON. É possível especificar path usando uma das formas a seguir:

- Por nome (em um objeto): .*name* ou ['*name*']
- Por índice (em uma matriz): [*index*]
- Por caractere curinga (em um objeto): .*
- Por caractere curinga (em uma matriz): [*]

Note

- Essa forma da cláusula FROM funciona apenas com objetos JSON.
- Caracteres curingas sempre emitem pelo menos um registro. Se não houver correspondência com nenhum registro, o Seleção do Amazon S3 emitirá o valor MISSING. Durante a serialização de saída (após a execução da consulta), o Amazon S3 Select substituirá os valores MISSING por registros vazios.
- Funções agregadas (AVG, COUNT, MAX, MIN, and SUM) ignoram valores MISSING.
- Se não fornecer um alias ao usar um caractere curinga, você poderá consultar a linha usando o último elemento do caminho. Por exemplo, você pode selecionar todos os preços em uma lista de livros usando a consulta SELECT price FROM S3Object[*].books[*].price. Se o caminho terminar com um caractere curinga em vez de um nome, você poderá usar o valor _1 para consultar a linha. Por exemplo, em vez de SELECT price FROM S3Object[*].books[*].price, você pode usar a consulta SELECT _1.price FROM S3Object[*].books[*].
- O Amazon S3 Select sempre trata um documento JSON como uma matriz de valores no nível da raiz. Dessa forma, mesmo se o objeto JSON que você estiver consultando tiver apenas um elemento raiz, a cláusula FROM deverá começar com S3Object[*]. No entanto, por razões de compatibilidade, o Amazon S3 Select permite omitir o caractere curinga caso você não inclua um caminho. Dessa forma, a cláusula completa FROM S3Object é equivalente a FROM S3Object[*] as S3Object. Se você incluir um caminho, também deverá usar o caractere curinga. Portanto, FROM S3Object e FROM S3Object[*].*path* são clausulas válidas, mas FROM S3Object.*path* não.

Example

Exemplos:

Exemplo 1

Este exemplo mostra resultados ao usar o seguinte conjunto de dados e consulta:

```
{ "Rules": [ {"id": "1"}, {"expr": "y > x"}, {"id": "2", "expr": "z = DEBUG"} ]}
{ "created": "June 27", "modified": "July 6" }
```

```
SELECT id FROM S3Object[*].Rules[*].id
```

```
{"id":"1"}
{}
{"id":"2"}
{}
```

O Amazon S3 Select produz cada resultado pelos seguintes motivos:

- `{"id":"id-1"}`: `S3Object[0].Rules[0].id` produziu uma correspondência.
- `{}`: `S3Object[0].Rules[1].id` não teve correspondência com um registro. Portanto, o Amazon S3 Select emitiu `MISSING`, que foi, então, alterado para um registro vazio durante a serialização de saída e retornou.
- `{"id":"id-2"}`: `S3Object[0].Rules[2].id` produziu uma correspondência.
- `{}`: `S3Object[1]` não teve correspondência em `Rules`. Portanto, o Amazon S3 Select emitiu `MISSING`, que foi, então, alterado para um registro vazio durante a serialização de saída e retornou.

Se você não quiser que o Seleção do Amazon S3 retorne registros vazios quando não encontrar uma correspondência, você poderá testar o valor `MISSING`. A consulta a seguir retorna os mesmos resultados que a consulta anterior, mas com os valores vazios omitidos:

```
SELECT id FROM S3Object[*].Rules[*].id WHERE id IS NOT MISSING
```

```
{"id":"1"}
{"id":"2"}
```

Exemplo 2

Este exemplo mostra resultados ao usar o seguinte conjunto de dados e consultas:

```
{ "created": "936864000", "dir_name": "important_docs", "files": [ { "name": "." },
 { "name": ".." }, { "name": ".aws" }, { "name": "downloads" } ], "owner": "Amazon
 S3" }
{ "created": "936864000", "dir_name": "other_docs", "files": [ { "name": "." },
 { "name": ".." }, { "name": "my stuff" }, { "name": "backup" } ], "owner": "User" }
```

```
SELECT d.dir_name, d.files FROM S3Object[*] d
```

```
{"dir_name":"important_docs","files":[{"name":"."},{"name":".."},{"name":".aws"},
{"name":"downloads"}]}
{"dir_name":"other_docs","files":[{"name":"."},{"name":".."},{"name":"my stuff"},
{"name":"backup"}]}
```

```
SELECT _1.dir_name, _1.owner FROM S3Object[*]
```

```
{"dir_name":"important_docs","owner":"Amazon S3"}
{"dir_name":"other_docs","owner":"User"}
```

WHERECláusula

A cláusula `WHERE` segue esta sintaxe:

```
WHERE condition
```

A cláusula `WHERE` filtra as linhas com base na *`condition`*. Uma condição é uma expressão com um valor booliano. Somente linhas para as quais a condição é avaliada como `TRUE` são retornadas no resultado.

LIMITCláusula

A cláusula `LIMIT` segue esta sintaxe:

```
LIMIT number
```

A cláusula `LIMIT` limita o número de registros que você deseja que a consulta retorne com base no *`number`*.

Acesso ao atributo

As cláusulas `SELECT` e `WHERE` podem se referir a dados de registro usando um dos métodos nas seções a seguir, dependendo se o arquivo que está sendo consultado está no formato CSV ou JSON.

CSV

- Números da coluna: você pode se referir à coluna Nth de uma linha com o nome da coluna *`_N`*, em que *`N`* é a posição da coluna. A contagem da posição começa em 1. Por exemplo, a primeira coluna é denominada _1 e a segunda coluna é denominada _2.

  Você pode se referir a uma coluna como *`_N`* ou *`alias`*`._`*`N`*. Por exemplo, _2 e `myAlias._2` são maneiras válidas de fazer referência a uma coluna na lista `SELECT` e na cláusula `WHERE`.
- Cabeçalhos da coluna — Para objetos no formato CSV que possuem uma linha de cabeçalho, os cabeçalhos estão disponíveis para a lista `SELECT` e a cláusula `WHERE`. Especificamente, como no SQL tradicional, nas expressões de cláusula `SELECT` e `WHERE`, você pode consultar as colunas por *`alias`*`.`*`column_name`* ou *`column_name`*.

JSON

- Documento — você pode acessar os campos do documentos JSON como *`alias`*`.`*`name`*. Também é possível acessar os campos aninhados, por exemplo, *`alias`*`.`*`name1`*`.`*`name2`*`.`*`name3`*.
- Lista: é possível acessar elementos em uma lista JSON usando índices baseados em zero com o operador `[]`. Por exemplo, você pode acessar o segundo elemento de uma lista como *`alias`*`[1]`. É possível combinar elementos da lista de acesso com campos, por exemplo, *`alias`*`.`*`name1`*`.`*`name2`*`[1].`*`name3`*.
- Exemplos: considere esse objeto JSON como um exemplo de conjunto de dados:

```
{"name": "Susan Smith",
"org": "engineering",
"projects":
    [
     {"project_name":"project1", "completed":false},
     {"project_name":"project2", "completed":true}
    ]
```

```
}
```

Exemplo 1

A consulta a seguir retorna estes resultados:

```
Select s.name from S3Object s
```

```
{"name":"Susan Smith"}
```

Exemplo 2

A consulta a seguir retorna estes resultados:

```
Select s.projects[0].project_name from S3Object s
```

```
{"project_name":"project1"}
```

Diferenciação de letras maiúsculas e minúsculas de cabeçalho e nomes de atributo

Com o Amazon S3 Select, você pode usar aspas duplas para indicar que cabeçalhos de coluna (para objetos CSV) e atributos (para objetos JSON) fazem diferenciação entre letras maiúsculas e minúsculas. Sem as aspas duplas, os cabeçalhos e atributos de objeto não diferenciam letras maiúsculas de minúsculas. Um erro ocorre em casos de ambiguidade.

Os exemplos a seguir são 1) objetos do Amazon S3 no formato CSV com os cabeçalhos de coluna especificados e com `FileHeaderInfo` definido como `"Use"` para a solicitação de consulta; ou 2) objetos do Amazon S3 no formato JSON com os atributos especificados.

Exemplo 1: o objeto consultado tem o cabeçalho ou atributo `NAME`.

- A expressão a seguir retorna com êxito valores do objeto. Como não há aspas, a consulta não diferencia letras maiúsculas de minúsculas.

```
SELECT s.name from S3Object s
```

- A expressão a seguir resulta em um erro 400 `MissingHeaderName`. Como há aspas, a consulta diferencia letras maiúsculas de minúsculas.

```
SELECT s."name" from S3Object s
```

Exemplo 2: o objeto do Amazon S3 que está sendo consultado tem um cabeçalho ou atributo com `NAME` e outro cabeçalho/atributo com `name`.

- A expressão a seguir resulta em um erro 400 `AmbiguousFieldName`. Como não há aspas, a consulta não diferencia letras maiúsculas de minúsculas, mas há duas correspondências, então o erro é gerado.

```
SELECT s.name from S3Object s
```

- A expressão a seguir retorna com êxito valores do objeto. Como há aspas, a consulta diferencia letras maiúsculas de minúsculas, portanto, não há ambiguidade.

```
SELECT s."NAME" from S3Object s
```

Usar palavras-chave reservadas como termos definidos pelo usuário

O Amazon S3 Select possui um conjunto de palavras-chave reservadas que são necessárias para executar as expressões SQL usadas para consultar o conteúdo do objeto. As palavras-chave reservadas incluem nomes de função, tipos de dados, operadores, e assim por diante. Em alguns casos, os termos definidos pelo usuário como os cabeçalhos de coluna (para arquivos CSV) ou os atributos (para objetos JSON) podem entrar em conflito com uma palavra-chave reservada. Quando isso ocorrer, é necessário usar as aspas duplas para indicar que você está usando intencionalmente um termo definido pelo usuário que entra em conflito com uma palavra-chave reservada. Caso contrário, ocorrerá um erro de análise 400.

Para obter a lista completa de palavras-chave reservadas, consulte Palavras-chave reservadas.

O exemplo a seguir é 1) um objeto do Amazon S3 no formato CSV com os cabeçalhos de coluna especificados, com `FileHeaderInfo` definido como `"Use"` para a solicitação de consulta ou 2) um objeto do Amazon S3 no formato JSON com os atributos especificados.

Exemplo: o objeto consultado tem o cabeçalho ou atributo nomeado como `CAST`, que é uma palavra-chave reservada.

- A expressão a seguir retorna com êxito valores do objeto. Como as aspas são usadas na consulta, o S3 Select usa o cabeçalho ou atributo definido pelo usuário.

```
SELECT s."CAST" from S3Object s
```

- A expressão a seguir resulta em um erro de análise 400. Como nenhuma aspa é usada na consulta, CAST colide com uma palavra-chave reservada.

```
SELECT s.CAST from S3Object s
```

Expressões escalares

Na cláusula WHERE e na lista SELECT, você tem expressões escalares SQL, que são expressões que retornam valores escalares. Elas têm o seguinte formato:

- ***literal***

  Um literal SQL.

- ***column_reference***

  Uma referência a uma coluna no formulário *column_name* ou *alias*.*column_name*.

- ***unary_op expression***

  Nesse caso, ***unary_op*** é um operador unário SQL.

- ***expression binary_op expression***

  Nesse caso, ***binary_op*** é um operador binário SQL.

- ***func_name***

  Nesse caso, ***func_name*** é o nome da função escalar a ser invocada.

- ***expression*** [NOT] BETWEEN ***expression*** AND ***expression***

- ***expression*** LIKE ***expression*** [ESCAPE ***expression***]

Tipos de dados

> **Important**
>
> O Amazon S3 Select não está mais disponível para novos clientes. Os clientes existentes do Amazon S3 Select podem continuar usando o recurso normalmente. Saiba mais

O Amazon S3 Select oferece suporte a vários tipos de dados primitivos.

Conversões de tipos de dados

A regra geral é seguir a função `CAST` se for definida. Se `CAST` não estiver definido, todos os dados de entrada serão tratados como uma string. Nesse caso, é necessário converter seus dados de entrada em tipos de dados relevantes quando necessário.

Para obter mais informações sobre a função `CAST`, consulte CAST.

Tipos de dados compatíveis

O Amazon S3 Select oferece suporte ao conjunto a seguir de tipos de dados primitivos.

Nome	Descrição	Exemplos
`bool`	Um valor booliano, `TRUE` ou `FALSE`.	`FALSE`
`int`, `integer`	Um número inteiro assinado de 8 bytes no intervalo de -9.223.372.036.854.775.808 a 9.223.372.036.854.775.807.	`100000`
`string`	Uma string de tamanho variável codificada por UTF8. O limite padrão é de um caractere. O limite máximo de caracteres é 2.147.483.647.	`'xyz'`
`float`	Um número de ponto flutuante de 8 bytes.	`CAST(0.456 AS FLOAT)`
`decimal`, `numeric`	Um número de base 10, com precisão máxima de 38 (ou seja, a quantidade máxima de dígitos significativos) e com uma escala no intervalo de -2^{31} a $2^{31}-1$ (ou seja, o expoente de base 10).	`123.456`

Nome	Descrição	Exemplos
	Note O Amazon S3 Select ignora a escala e a precisão quando as duas são fornecidas ao mesmo tempo.	
`timestamp`	Os carimbos de data/hora representam um momento específico, sempre incluem um deslocamento local e são capazes de oferecer precisão arbitrária. No formato de texto, os carimbos de data/hora seguem a nota W3C sobre formatos de data e hora, mas devem terminar com o literal `T`, se os carimbos de data/hora não forem pelo menos a precisão de dia inteiro. As frações de segundos são permitidas, com pelo menos um dígito de precisão e um máximo ilimitado. Os deslocamentos de hora local podem ser representados como deslocamentos de hora:minuto em UTC ou como o literal `Z` para indicar uma hora local em UTC. Os deslocamentos de horário local são necessários em carimbos de data/hora com hora e não são permitidos em valores de data.	`CAST('2007-04-05T14:30Z' AS TIMESTAMP)`

Tipos compatíveis de Parquet

O Amazon S3 Select é compatível com os seguintes tipos de Parquet.

- `DATE`
- `DECIMAL`
- `ENUM`
- `INT(8)`
- `INT(16)`
- `INT(32)`
- `INT(64)`

- `LIST`

> **Note**
>
> Para a saída do tipo `LIST` do Parquet, o Amazon S3 Select só é compatível com o formato JSON. No entanto, se a consulta limitar os dados a valores simples, o tipo de Parquet `LIST` também poderá ser consultado em formato CSV.

- `STRING`
- Precisão compatível de `TIMESTAMP` (`MILLIS`/`MICROS`/`NANOS`)

> **Note**
>
> Não há compatibilidade com carimbos de data/hora salvos como `INT(96)`. Devido ao intervalo do tipo `INT(64)`, os carimbos de data/hora que usam a unidade `NANOS` só podem representar valores entre `1677-09-21 00:12:43` e `2262-04-11 23:47:16`. Valores fora desse intervalo não podem ser representados com a unidade `NANOS`.

Mapeamento de tipos de Parquet para tipos de dados compatíveis no Amazon S3 Select

Tipos do Parquet	Tipos de dados compatíveis
`DATE`	`timestamp`
`DECIMAL`	`decimal`, `numeric`
`ENUM`	`string`
`INT(8)`	`int`, `integer`
`INT(16)`	`int`, `integer`
`INT(32)`	`int`, `integer`

Tipos do Parquet	Tipos de dados compatíveis
`INT(64)`	`decimal`, `numeric`
`LIST`	Cada tipo de Parquet na lista é mapeado para o tipo de dados correspon dente.
`STRING`	`string`
`TIMESTAMP`	`timestamp`

Operadores

> **Important**
>
> O Amazon S3 Select não está mais disponível para novos clientes. Os clientes existentes do Amazon S3 Select podem continuar usando o recurso normalmente. Saiba mais

O Amazon S3 Select é compatível com os seguintes operadores.

Operadores lógicos

- `AND`
- `NOT`
- `OR`

Operadores de comparação

- `<`
- `>`
- `<=`
- `>=`
- `=`
- `<>`

- `!=`
- `BETWEEN`
- `IN` – Por exemplo: `IN ('a', 'b', 'c')`

Operadores de correspondência de padrões

- `LIKE`
- `_` (corresponde a qualquer caractere)
- `%` (corresponde a qualquer sequência de caracteres)

Operadores unitários

- `IS NULL`
- `IS NOT NULL`

Operadores matemáticos

A adição, a subtração, a multiplicação, a divisão e o módulo são compatíveis, como indicado a seguir:

- `+`
- `-`
- `*`
- `/`
- `%`

Precedência do operador

A tabela a seguir mostra a precedência dos operadores em ordem decrescente.

Operador ou elemento	Capacidade de associação	Obrigatório
-	direita	menos unário

Operador ou elemento	Capacidade de associação	Obrigatório
`*`, `/`, `%`	esquerda	multiplicação, divisão, módulo
`+`, `-`	esquerda	adição, subtração
`IN`		associação de conjunto
`BETWEEN`		contenção de intervalo
`LIKE`		correspondência de padrões de string
`<>`		menor que, maior que
`=`	direita	igualdade, atribuição
`NOT`	direita	negação lógica
`AND`	esquerda	conjunção lógica
`OR`	esquerda	disjunção lógica

Palavras-chave reservadas

> **Important**
>
> O Amazon S3 Select não está mais disponível para novos clientes. Os clientes existentes do Amazon S3 Select podem continuar usando o recurso normalmente. Saiba mais

Veja a seguir a lista de palavras-chave reservadas para o Amazon S3 Select. Essas palavras-chave incluem os nomes de função, tipos de dados, operadores e assim por diante, necessários para executar as expressões SQL usadas para consultar o conteúdo do objeto.

```
absolute
action
add
all
allocate
alter
and
any
are
as
asc
assertion
at
authorization
avg
bag
begin
between
bit
bit_length
blob
bool
boolean
both
by
cascade
cascaded
case
cast
catalog
```

```
char
char_length
character
character_length
check
clob
close
coalesce
collate
collation
column
commit
connect
connection
constraint
constraints
continue
convert
corresponding
count
create
cross
current
current_date
current_time
current_timestamp
current_user
cursor
date
day
deallocate
dec
decimal
declare
default
deferrable
deferred
delete
desc
describe
descriptor
diagnostics
disconnect
distinct
```

```
domain
double
drop
else
end
end-exec
escape
except
exception
exec
execute
exists
external
extract
false
fetch
first
float
for
foreign
found
from
full
get
global
go
goto
grant
group
having
hour
identity
immediate
in
indicator
initially
inner
input
insensitive
insert
int
integer
intersect
interval
```

```
into
is
isolation
join
key
language
last
leading
left
level
like
limit
list
local
lower
match
max
min
minute
missing
module
month
names
national
natural
nchar
next
no
not
null
nullif
numeric
octet_length
of
on
only
open
option
or
order
outer
output
overlaps
pad
```

```
partial
pivot
position
precision
prepare
preserve
primary
prior
privileges
procedure
public
read
real
references
relative
restrict
revoke
right
rollback
rows
schema
scroll
second
section
select
session
session_user
set
sexp
size
smallint
some
space
sql
sqlcode
sqlerror
sqlstate
string
struct
substring
sum
symbol
system_user
table
```

```
temporary
then
time
timestamp
timezone_hour
timezone_minute
to
trailing
transaction
translate
translation
trim
true
tuple
union
unique
unknown
unpivot
update
upper
usage
user
using
value
values
varchar
varying
view
when
whenever
where
with
work
write
year
zone
```

Funções SQL

> **Important**
>
> O Amazon S3 Select não está mais disponível para novos clientes. Os clientes existentes do Amazon S3 Select podem continuar usando o recurso normalmente. Saiba mais

O Amazon S3 Select é compatível com as funções SQL a seguir.

Tópicos

- Funções agregadas
- Funções condicionais
- Funções de conversão
- Funções de data
- Funções de string

Funções agregadas

> **Important**
>
> O Amazon S3 Select não está mais disponível para novos clientes. Os clientes existentes do Amazon S3 Select podem continuar usando o recurso normalmente. Saiba mais

O Amazon S3 Select é compatível com as seguintes funções agregadas.

Função	Tipo de argumento	Tipo de retorno
`AVG(`*`expressio`* *`n`* `)`	`INT`, `FLOAT`, `DECIMAL`	`DECIMAL` para um argumento `INT`, `FLOAT` um argumento de ponto flutuante, caso contrário, é igual ao tipo

Função	Tipo de argumento	Tipo de retorno
		de dados do argumento.
COUNT	-	INT
MAX(*expressio n*)	INT, DECIMAL	O mesmo que o tipo de argumento.
MIN(*expressio n*)	INT, DECIMAL	O mesmo que o tipo de argumento.
SUM(*expressio n*)	INT, FLOAT, DOUBLE, DECIMAL	INT para um argumento INT, FLOAT um argumento de ponto flutuante; do contrário, é igual ao tipo de dados do argumento.

Exemplo de SUM

Para agregar os tamanhos totais de objetos de uma pasta em um relatório do S3 Inventory, use uma expressão SUM.

O relatório do S3 Inventory a seguir é um arquivo CSV compactado com GZIP. Existem três colunas.

- A primeira coluna é o nome do bucket do S3 (*DOC-EXAMPLE-BUCKET*) para o qual o relatório do S3 Inventory se destina.
- A segunda coluna é o nome da chave do objeto que identifica exclusivamente o objeto no bucket.

  O valor *example-folder/* na primeira linha é para a pasta *example-folder*. No Amazon S3, quando você cria uma pasta no bucket, o S3 cria um objeto de 0 byte com uma chave definida como o nome da pasta que você forneceu.

O valor *example-folder/object1* na segunda linha é para o objeto *object1* na pasta *example-folder*.

O valor *example-folder/object2* na terceira linha é para o objeto *object2* na pasta *example-folder*.

Para obter mais informações sobre pastas do S3, consulte Organizar objetos no console do Amazon S3 usando pastas.

- A terceira coluna é o tamanho do objeto em bytes.

```
"DOC-EXAMPLE-BUCKET","example-folder/","0"
"DOC-EXAMPLE-BUCKET","example-folder/object1","2011267"
"DOC-EXAMPLE-BUCKET","example-folder/object2","1570024"
```

Para usar uma expressão SUM para calcular o tamanho total da pasta *example-folder*, execute a consulta SQL com o Amazon S3 Select.

```
SELECT SUM(CAST(_3 as INT)) FROM s3object s WHERE _2 LIKE 'example-folder/%' AND _2 !=
 'example-folder/';
```

Resultado da consulta:

```
3581291
```

Funções condicionais

> **Important**
>
> O Amazon S3 Select não está mais disponível para novos clientes. Os clientes existentes do Amazon S3 Select podem continuar usando o recurso normalmente. Saiba mais

O Amazon S3 Select é compatível com as seguintes funções condicionais.

Tópicos

- CASE
- COALESCE

- NULLIF

CASE

A expressão CASE é uma expressão condicional, semelhante às instruções `if/then/else` encontradas em outras linguagens. CASE é usado para especificar um resultado com várias condições. Há dois tipos de expressões CASE: simples e pesquisada.

Em expressões CASE simples, uma expressão é comparada a um valor. Quando uma correspondência é encontrada, a ação especificada na cláusula THEN é aplicada. Se nenhuma correspondência é encontrada, a ação especificada na cláusula ELSE é aplicada.

Em expressões CASE pesquisadas, cada CASE é avaliado com base em uma expressão booliana e a instrução CASE retorna o primeiro CASE correspondente. Se nenhuma correspondência de CASE for encontrada entre as cláusulas WHEN, a ação na cláusula ELSE será retornada.

Sintaxe

> **Note**
>
> Atualmente, o Amazon S3 Select não é compatível com `ORDER BY` ou consultas que contenham novas linhas. Use consultas sem quebras de linha.

A seguir está uma declaração CASE simples usada para corresponder às condições:

```
CASE expression WHEN value THEN result [WHEN...] [ELSE result] END
```

Veja a seguir uma declaração CASE pesquisada usada para avaliar cada condição:

```
CASE WHEN boolean condition THEN result [WHEN ...] [ELSE result] END
```

Exemplos

> **Note**
>
> Se você usar o console do Amazon S3 para executar os exemplos a seguir e o arquivo CSV tiver uma linha de cabeçalho, selecione Excluir a primeira linha de dados do CSV.

Exemplo 1: use uma expressão CASE simples para substituir `New York City` por `Big Apple` em uma consulta. Substitua todos os outros nomes de cidade por `other`.

```
SELECT venuecity, CASE venuecity WHEN 'New York City' THEN 'Big Apple' ELSE 'other' END
 FROM S3Object;
```

Resultado da consulta:

```
venuecity        |   case
-----------------+-----------
Los Angeles      | other
New York City    | Big Apple
San Francisco    | other
Baltimore        | other
...
```

Exemplo 2: use uma expressão CASE pesquisada para atribuir números de grupo com base no valor `pricepaid` para vendas individuais de ingresso:

```
SELECT pricepaid, CASE WHEN CAST(pricepaid as FLOAT) < 10000 THEN 'group 1' WHEN
 CAST(pricepaid as FLOAT) > 10000 THEN 'group 2' ELSE 'group 3' END FROM S3Object;
```

Resultado da consulta:

```
pricepaid |  case
-----------+---------
12624.00 | group 2
10000.00 | group 3
10000.00 | group 3
9996.00 | group 1
9988.00 | group 1
...
```

COALESCE

`COALESCE` avalia os argumentos na ordem e retorna o primeiro valor não desconhecido, ou seja, o primeiro valor que não for nulo ou ausente. Essa função não propaga valores nulos e ausentes.

Sintaxe

```
COALESCE ( expression, expression, ... )
```

Parâmetros

expression

A expressão de destino na qual a função opera.

Exemplos

```
COALESCE(1)                -- 1
COALESCE(null)             -- null
COALESCE(null, null)       -- null
COALESCE(missing)          -- null
COALESCE(missing, missing) -- null
COALESCE(1, null)          -- 1
COALESCE(null, null, 1)    -- 1
COALESCE(null, 'string')   -- 'string'
COALESCE(missing, 1)       -- 1
```

NULLIF

Dadas as duas expressões, `NULLIF` retorna `NULL` se as duas forem avaliadas para o mesmo valor. Caso contrário, `NULLIF` retorna o resultado da avaliação da primeira expressão.

Sintaxe

```
NULLIF ( expression1, expression2 )
```

Parâmetros

expression1, *expression2*

As expressões de destino nas quais a função opera.

Exemplos

```
NULLIF(1, 1)             -- null
NULLIF(1, 2)             -- 1
NULLIF(1.0, 1)           -- null
NULLIF(1, '1')           -- 1
NULLIF([1], [1])         -- null
NULLIF(1, NULL)          -- 1
```

```
NULLIF(NULL, 1)          -- null
NULLIF(null, null)       -- null
NULLIF(missing, null)    -- null
NULLIF(missing, missing) -- null
```

Funções de conversão

> **Important**
>
> O Amazon S3 Select não está mais disponível para novos clientes. Os clientes existentes do Amazon S3 Select podem continuar usando o recurso normalmente. Saiba mais

O Amazon S3 Select é compatível com a seguinte função de conversão.

Tópicos

- CAST

CAST

A função CAST converte uma entidade, como uma expressão que retorna um único valor, de um tipo em outro.

Sintaxe

```
CAST ( expression AS data_type )
```

Parâmetros

expression

Uma combinação de um ou mais valores, operadores e funções SQL que retornam um valor.

data_type

O tipo de dados de destino, como INT, no qual a expressão será convertida. Para obter uma lista dos tipos de dados compatíveis, consulte Tipos de dados.

Exemplos

```
CAST('2007-04-05T14:30Z' AS TIMESTAMP)
```

```
CAST(0.456 AS FLOAT)
```

Funções de data

> **Important**
>
> O Amazon S3 Select não está mais disponível para novos clientes. Os clientes existentes do Amazon S3 Select podem continuar usando o recurso normalmente. Saiba mais

O Amazon S3 Select é compatível com as seguintes funções de data.

Tópicos

- DATE_ADD
- DATE_DIFF
- EXTRACT
- TO_STRING
- TO_TIMESTAMP
- UTCNOW

DATE_ADD

Dada uma parte da data, uma quantidade e um carimbo de data/hora, `DATE_ADD` retorna um carimbo de data/hora atualizado, alterando a parte da data pela quantidade.

Sintaxe

```
DATE_ADD( date_part, quantity, timestamp )
```

Parâmetros

`date_part`

Especifica que parte da data deve ser modificada. Pode ser uma das partes a seguir:

- year
- mês

- dia
- hora
- minuto
- segundos

quantity

O valor a ser aplicado a um carimbo de data/hora atualizado. Os valores positivos para a *quantity* são adicionados à date_part do carimbo de data/hora e os valores negativos são subtraídos.

timestamp

O carimbo de data/hora de destino no qual a função opera.

Exemplos

```
DATE_ADD(year, 5, `2010-01-01T`)                -- 2015-01-01 (equivalent to
 2015-01-01T)
DATE_ADD(month, 1, `2010T`)                     -- 2010-02T (result will add precision
 as necessary)
DATE_ADD(month, 13, `2010T`)                    -- 2011-02T
DATE_ADD(day, -1, `2017-01-10T`)                -- 2017-01-09 (equivalent to
 2017-01-09T)
DATE_ADD(hour, 1, `2017T`)                      -- 2017-01-01T01:00-00:00
DATE_ADD(hour, 1, `2017-01-02T03:04Z`)          -- 2017-01-02T04:04Z
DATE_ADD(minute, 1, `2017-01-02T03:04:05.006Z`) -- 2017-01-02T03:05:05.006Z
DATE_ADD(second, 1, `2017-01-02T03:04:05.006Z`) -- 2017-01-02T03:04:06.006Z
```

DATE_DIFF

Dada uma parte da data e dois carimbos de data/hora válidos, DATE_DIFF retorna a diferença nas partes da data. O valor de retorno é um inteiro negativo quando o valor *date_part* do *timestamp1* for maior que o valor *date_part* do *timestamp2*. O valor de retorno é um inteiro positivo quando o valor *date_part* do *timestamp1* for menor que o valor *date_part* do *timestamp2*.

Sintaxe

```
DATE_DIFF( date_part, timestamp1, timestamp2 )
```

Parâmetros

date_part

Especifica que parte dos carimbos de data/hora deve ser comparada. Para a definição de `date_part`, consulte DATE_ADD.

timestamp1

O primeiro carimbo de data/hora a ser comparado.

timestamp2

O segundo carimbo de data/hora a ser comparado.

Exemplos

```
DATE_DIFF(year, `2010-01-01T`, `2011-01-01T`)            -- 1
DATE_DIFF(year, `2010T`, `2010-05T`)                     -- 4 (2010T is equivalent to
 2010-01-01T00:00:00.000Z)
DATE_DIFF(month, `2010T`, `2011T`)                       -- 12
DATE_DIFF(month, `2011T`, `2010T`)                       -- -12
DATE_DIFF(day, `2010-01-01T23:00`, `2010-01-02T01:00`) -- 0 (need to be at least 24h
 apart to be 1 day apart)
```

EXTRACT

Dada uma parte da data e um carimbo de data/hora, `EXTRACT` retorna o valor da parte da data do carimbo de data/hora.

Sintaxe

```
EXTRACT( date_part FROM timestamp )
```

Parâmetros

date_part

Especifica que parte dos carimbos de data/hora deve ser extraída. Pode ser uma das partes a seguir:

- `YEAR`
- `MONTH`

- DAY
- HOUR
- MINUTE
- SECOND
- TIMEZONE_HOUR
- TIMEZONE_MINUTE

timestamp

O carimbo de data/hora de destino no qual a função opera.

Exemplos

```
EXTRACT(YEAR FROM `2010-01-01T`)                              -- 2010
EXTRACT(MONTH FROM `2010T`)                                   -- 1 (equivalent to
 2010-01-01T00:00:00.000Z)
EXTRACT(MONTH FROM `2010-10T`)                                -- 10
EXTRACT(HOUR FROM `2017-01-02T03:04:05+07:08`)                -- 3
EXTRACT(MINUTE FROM `2017-01-02T03:04:05+07:08`)              -- 4
EXTRACT(TIMEZONE_HOUR FROM `2017-01-02T03:04:05+07:08`)       -- 7
EXTRACT(TIMEZONE_MINUTE FROM `2017-01-02T03:04:05+07:08`)     -- 8
```

TO_STRING

Dado um carimbo de data/hora e um padrão de formato, TO_STRING retorna uma representação de string do carimbo de data/hora no formato especificado.

Sintaxe

```
TO_STRING ( timestamp time_format_pattern )
```

Parâmetros

timestamp

O carimbo de data/hora de destino no qual a função opera.

time_format_pattern

Uma string que possui as seguintes interpretações de caracteres especiais:

Formato	Exemplo	Descrição
yy	69	Ano com dois dígitos
y	1969	Ano com quatro dígitos
yyyy	1969	Ano com 4 dígitos preenchido com zeros
M	1	Mês do ano
MM	01	Mês do ano preenchido com zeros
MMM	Jan	Nome do ano referente ao mês abreviado
MMMM	January	Nome completo do mês do ano
MMMMM	J	Primeira letra do mês do ano (NOTA: esse formato não é válido para uso com a função TO_TIMESTAMP .)
d	2	Dia do mês (1 a 31)

Formato	Exemplo	Descrição
dd	02	Dia do mês preenchido com zeros (01 a 31)
a	AM	H do dia
h	3	Hora do dia (1 a 12)
hh	03	Hora do dia preenchida com zeros (01 a 12)
H	3	Hora do dia (0 a 23)
HH	03	Hora do dia preenchida com zeros (00 a 23)
m	4	Minuto da hora (0 a 59)
mm	04	Minuto da hora preenchido com zeros (00 a 59)
s	5	Segundo do minuto (0 a 59)

Formato	Exemplo	Descrição
`ss`	`05`	Segundo do minuto preenchido com zeros (00 a 59)
`S`	`0`	Fração de um segundo (precisão: 0,1, intervalo: de 0,0 a 0,9)
`SS`	`6`	Fração de um segundo (precisão: 0,01, intervalo: de 0,0 a 0,99)
`SSS`	`60`	Fração de um segundo (precisão : 0,001, intervalo: de 0,0 a 0,999)
…	…	…
`SSSSSSSSS`	`60000000`	Fração de um segundo (precisão máxima: 1 nanossegundo, intervalo : de 0,0 a 0,999999999)

Formato	Exemplo	Descrição
n	60000000	Nano de um segundo
X	+07 ou Z	Deslocamento em horas ou Z se o deslocamento for 0
XX ou XXXX	+0700 ou Z	Deslocamento em horas e minutos ou Z se o deslocamento for 0
XXX ou XXXXX	+07:00 ou Z	Deslocamento em horas e minutos ou Z se o deslocamento for 0
x	7	Deslocamento em horas
xx ou xxxx	700	Deslocamento em horas e minutos
xxx ou xxxxx	+07:00	Deslocamento em horas e minutos

Exemplos

```
TO_STRING(`1969-07-20T20:18Z`,  'MMMM d, y')                    -- "July 20, 1969"
TO_STRING(`1969-07-20T20:18Z`, 'MMM d, yyyy')                   -- "Jul 20, 1969"
TO_STRING(`1969-07-20T20:18Z`, 'M-d-yy')                        -- "7-20-69"
TO_STRING(`1969-07-20T20:18Z`, 'MM-d-y')                        -- "07-20-1969"
TO_STRING(`1969-07-20T20:18Z`, 'MMMM d, y h:m a')               -- "July 20, 1969 8:18
 PM"
TO_STRING(`1969-07-20T20:18Z`, 'y-MM-dd''T''H:m:ssX')           --
 "1969-07-20T20:18:00Z"
TO_STRING(`1969-07-20T20:18+08:00Z`, 'y-MM-dd''T''H:m:ssX')     --
 "1969-07-20T20:18:00Z"
TO_STRING(`1969-07-20T20:18+08:00`, 'y-MM-dd''T''H:m:ssXXXX')   --
 "1969-07-20T20:18:00+0800"
TO_STRING(`1969-07-20T20:18+08:00`, 'y-MM-dd''T''H:m:ssXXXXX')  --
 "1969-07-20T20:18:00+08:00"
```

TO_TIMESTAMP

Dada uma string, `TO_TIMESTAMP` converte-se em um carimbo de data/hora. `TO_TIMESTAMP` é a operação inversa de `TO_STRING`.

Sintaxe

```
TO_TIMESTAMP ( string )
```

Parâmetros

`string`

A string de destino na qual a função opera.

Exemplos

```
TO_TIMESTAMP('2007T')                          -- `2007T`
TO_TIMESTAMP('2007-02-23T12:14:33.079-08:00') -- `2007-02-23T12:14:33.079-08:00`
```

UTCNOW

`UTCNOW` retorna o tempo atual em UTC como um carimbo de data/hora.

Sintaxe

```
UTCNOW()
```

Parâmetros

`UTCNOW` não aceita parâmetros.

Exemplos

```
UTCNOW() -- 2017-10-13T16:02:11.123Z
```

Funções de string

> **Important**
>
> O Amazon S3 Select não está mais disponível para novos clientes. Os clientes existentes do Amazon S3 Select podem continuar usando o recurso normalmente. Saiba mais

O Amazon S3 Select é compatível com as seguintes funções de string.

Tópicos

- CHAR_LENGTH, CHARACTER_LENGTH
- LOWER
- SUBSTRING
- TRIM
- UPPER

CHAR_LENGTH, CHARACTER_LENGTH

`CHAR_LENGTH` (ou `CHARACTER_LENGTH`) conta o número de caracteres na string especificada.

> **Note**
>
> `CHAR_LENGTH` e `CHARACTER_LENGTH` são sinônimos.

Sintaxe

```
CHAR_LENGTH ( string )
```

Parâmetros

string

A string de destino na qual a função opera.

Exemplos

```
CHAR_LENGTH('')          -- 0
CHAR_LENGTH('abcdefg')   -- 7
```

LOWER

Dada uma string, LOWER converte todos os caracteres maiúsculos em minúsculos. Todos os caracteres minúsculos permanecem inalterados.

Sintaxe

```
LOWER ( string )
```

Parâmetros

string

A string de destino na qual a função opera.

Exemplos

```
LOWER('AbCdEfG!@#$') -- 'abcdefg!@#$'
```

SUBSTRING

Dada uma string, um índice inicial e, opcionalmente, um tamanho, SUBSTRING retorna a substring do índice inicial até o final da string ou até o tamanho fornecido.

> **Note**
>
> O primeiro caractere da string de entrada tem uma posição de índice de 1.
>
> - Se `start` < 1, sem comprimento especificado, a posição do índice será definida como 1.
> - Se `start` for < 1, sem comprimento especificado, a posição do índice será definida como `start + length -1`.
> - Se `start + length -1` < 0, uma string vazia será retornada.
> - Se `start + length -1` > = 0, a substring começando na posição de índice 1 de comprimento `start + length - 1` será retornada.

Sintaxe

```
SUBSTRING( string FROM start [ FOR length ] )
```

Parâmetros

string

A string de destino na qual a função opera.

start

A posição inicial da string.

length

O tamanho da substring a ser retornada. Se não estiver presente, prossiga para o final da string.

Exemplos

```
SUBSTRING("123456789", 0)      -- "123456789"
SUBSTRING("123456789", 1)      -- "123456789"
SUBSTRING("123456789", 2)      -- "23456789"
SUBSTRING("123456789", -4)     -- "123456789"
SUBSTRING("123456789", 0, 999) -- "123456789"
SUBSTRING("123456789", 1, 5)   -- "12345"
```

TRIM

Corta os caracteres iniciais ou finais de uma string. O caractere padrão a ser removido é um espaço (' ').

Sintaxe

```
TRIM ( [[LEADING | TRAILING | BOTH remove_chars] FROM] string )
```

Parâmetros

string

A string de destino na qual a função opera.

LEADING | TRAILING | BOTH

Esse parâmetro indica se é necessário cortar os caracteres iniciais ou finais, ou ambos.

remove_chars

O conjunto de caracteres a ser removido. *remove_chars* pode ser uma string com tamanho > 1. Essa função retorna a string com qualquer caractere de *remove_chars* encontrado no início ou final da string que foi removida.

Exemplos

```
TRIM('       foobar         ')               -- 'foobar'
TRIM('      \tfoobar\t         ')            -- '\tfoobar\t'
TRIM(LEADING FROM '       foobar         ')  -- 'foobar         '
TRIM(TRAILING FROM '       foobar         ') -- '       foobar'
TRIM(BOTH FROM '       foobar         ')     -- 'foobar'
TRIM(BOTH '12' FROM '1112211foobar22211122') -- 'foobar'
```

UPPER

Dada uma string, UPPER converte todos os caracteres minúsculos em maiúsculos. Todos os caracteres maiúsculos permanecem inalterados.

Sintaxe

```
UPPER ( string )
```

Parâmetros

string

A string de destino na qual a função opera.

Exemplos

```
UPPER('AbCdEfG!@#$') -- 'ABCDEFG!@#$'
```

Trabalhar com buckets de diretório

Os buckets de diretório organizam os dados de forma hierárquica em diretórios, ao contrário da estrutura de armazenamento plana dos buckets de uso geral. Não há limites de prefixo para os buckets de diretório, e diretórios individuais podem ser escalados horizontalmente.

Você pode criar até cem buckets de diretório em cada uma de suas Contas da AWS, sem limite no número de objetos que podem ser armazenados em um bucket. A cota de buckets é aplicada a cada região na Conta da AWS. Se for preciso aumentar esse limite para a aplicação, entre em contato com o Suporte.

> **Important**
>
> Os buckets de diretório em zonas de disponibilidade que não tiverem nenhuma atividade de solicitação por um período de pelo noventa dias passarão para um estado inativo. Enquanto estiver inativo, um bucket de diretório ficará temporariamente inacessível para leituras e gravações. Os buckets inativos retêm todo o armazenamento, os metadados de objetos e os metadados de bucket. As cobranças de armazenamento existentes se aplicam aos buckets inativos. Se você fizer uma solicitação de acesso a um bucket inativo, o bucket passará para um estado ativo, normalmente em alguns minutos. Durante esse período de transição, as leituras e gravações retornarão um código de erro HTTP `503 (Service Unavailable)`. Isso não se aplica a buckets em zonas locais.

Há vários tipos de bucket do Amazon S3. Antes de criar um bucket, escolha o tipo de bucket que melhor se adapte aos requisitos de performance e da aplicação. Para obter mais informações sobre os vários tipos de bucket e os casos de uso apropriados para cada um, consulte Buckets.

Os tópicos a seguir fornecem informações sobre buckets de diretório. Para obter mais informações sobre os buckets de uso geral, consulte Visão geral dos buckets de uso geral.

Consulte mais informações sobre buckets de diretório nos tópicos a seguir.

- Nomes de bucket de diretório
- Diretórios
- Nomes de chave
- Gerenciamento de acesso

Nomes de bucket de diretório

Um nome de bucket de diretório consiste em um nome base que você fornece e um sufixo que contém o ID da zona (zona de disponibilidade ou zona local) em que o bucket está localizado. Os nomes de bucket de diretório devem usar o seguinte formato e seguir as regras de nomenclatura para buckets de diretório:

```
bucket-base-name--zone-id--x-s3
```

Por exemplo, o seguinte nome de bucket de diretório contém o ID da zona de disponibilidade `usw2-az1`:

```
bucket-base-name--usw2-az1--x-s3
```

Para obter mais informações, consulte Regras de nomenclatura de buckets de diretório.

Diretórios

Os buckets de diretório organizam os dados de forma hierárquica em diretórios, ao contrário da estrutura de organização plana dos buckets de uso geral.

Com um namespace hierárquico, o delimitador na chave de objeto é importante. O único delimitador compatível é a barra (`/`). Os diretórios são determinados pelos limites de delimitador. Por exemplo, a chave de objeto `dir1/dir2/file1.txt` resulta na criação automática dos diretórios `dir1/` e `dir2/`, além da adição do objeto `file1.txt` ao diretório `/dir2` no caminho `dir1/dir2/file1.txt`.

O modelo de indexação de buckets de diretório retorna resultados não organizados para a operação de API `ListObjectsV2`. Se precisar limitar os resultados a uma subseção do bucket, você poderá especificar um caminho de subdiretório no parâmetro `prefix`, como `prefix=dir1/`.

Nomes de chave

Para buckets de diretório, os subdiretórios que são comuns a várias chaves de objeto são criados com a primeira chave de objeto. As chaves de objeto adicionais para o mesmo subdiretório usam o subdiretório criado anteriormente. Esse modelo oferece flexibilidade na escolha de chaves de objeto mais adequadas à aplicação, com o mesmo suporte a diretórios esparsos e densos.

Gerenciamento de acesso

Os buckets de diretório têm todas as configurações da funcionalidade Bloqueio de Acesso Público do S3 habilitadas por padrão no nível do bucket. A Propriedade de Objetos do S3 está definida como Imposto pelo proprietário do bucket e as listas de controle de acesso (ACLs) estão desabilitadas. Essas configurações não podem ser modificadas.

Por padrão, os usuários não têm permissões para os buckets de diretório. Para conceder permissões de acesso a buckets de diretório, você pode usar o IAM para criar usuários ou perfis e anexar permissões a essas identidades. Para obter mais informações, consulte Autorizar operações de API de endpoint regional com o IAM.

Você também pode controlar o acesso aos buckets de diretório por meio de pontos de acesso. Os pontos de acesso simplificam o gerenciamento do acesso a dados em escala para conjuntos de dados compartilhados no Amazon S3. Pontos de acesso são nomes de host exclusivos que você cria para impor permissões e controles de rede distintos a todas as solicitações feitas por meio de um ponto de acesso. Para obter mais informações, consulte Gerenciar o acesso a conjuntos de dados compartilhados em buckets de diretório por meio de pontos de acesso.

Buckets de diretório

As cotas, também chamadas de limites, correspondem ao número máximo de recursos ou operações de serviço para uma Conta da AWS. A seguir são apresentadas as cotas dos buckets de diretório. Para ter mais informações sobre cotas no Amazon S3, consulte as cotas do Amazon S3.

Name	Padrão	Ajustável	Descrição
Buckets de diretório	Cada conta: 100	Sim	O número de buckets de diretório do Amazon S3 que você pode criar em uma conta.
TPS de leitura por bucket de diretório	Cada bucket de diretório: até 200 mil TPS de leitura	Para solicitar um aumento na cota, entre em contato com o Support.	O número de solicitações GET/HEAD por segundo por bucket de diretório.

Name	Padrão	Ajustável	Descrição
TPS de gravação por bucket de diretório	Cada bucket de diretório: até 100 mil TPS de gravação	Para solicitar um aumento na cota, entre em contato com o Support.	O número de solicitações PUT/DELETE por segundo por bucket de diretório.

Criar e usar buckets de diretório

Para obter mais informações sobre como trabalhar com buckets de diretório, consulte os tópicos a seguir.

- Usar casos para buckets de diretório
- Diferenças de buckets de diretório
- Rede para buckets de diretório
- Regras de nomenclatura de buckets de diretório
- Visualizar as propriedades de buckets de diretório
- Gerenciar políticas de bucket de diretório
- Esvaziar um bucket de diretório
- Excluir um bucket de diretório
- Listar buckets de diretório
- Determinar se você pode acessar um bucket de diretório
- Trabalhar com objetos em um bucket de diretório
- Segurança para buckets de diretório
- Gerenciar o acesso a conjuntos de dados compartilhados em buckets de diretório por meio de pontos de acesso
- Otimizar o desempenho do bucket de diretório
- Desenvolvimento com buckets de diretório
- Usar tags com buckets de diretório do S3

Usar casos para buckets de diretório

Os buckets de diretório permitem a criação de buckets nos seguintes tipos de localização de bucket: zona de disponibilidade ou zona local.

Para casos de uso de baixa latência, você pode criar um bucket de diretórios em uma única zona de disponibilidade para armazenar dados. Buckets de diretório em zonas de disponibilidade permitem a classe de armazenamento S3 Express One Zone. A classe de armazenamento S3 Express One Zone é recomendada se a aplicação é sensível ao desempenho e se beneficia de latências inferiores a dez milissegundos para `PUT` e `GET`. Consulte mais informações sobre como criar buckets de diretório em zonas de disponibilidade em Workloads de alto desempenho.

Para casos de uso de residência de dados, você pode criar um bucket de diretório em uma zona local dedicada da AWS (DLZ) única para armazenar dados. Os buckets de diretório em zonas locais são compatíveis com a classe de armazenamento S3 One Zone-Infrequent Access (S3 One Zone-IA; Z-IA). Para saber mais sobre como criar buckets de diretório em zonas locais, consulte Workloads de residência de dados.

Tópicos

- Workloads de alto desempenho
- Workloads de residência de dados

Workloads de alto desempenho

S3 Express One Zone

É possível usar a classe Amazon S3 Express One Zone para workloads de alto desempenho. S3 Express One Zone é a primeira classe de armazenamento do S3 em que é possível selecionar uma única zona de disponibilidade com a opção de manter o armazenamento de objetos e os recursos de computação na mesma localização, o que fornece a maior velocidade de acesso possível. Os objetos na classe S3 Express One Zone são armazenados em buckets de diretório localizados em zonas de disponibilidade. Para ter mais informações sobre os buckets de diretório, consulte Buckets de diretório.

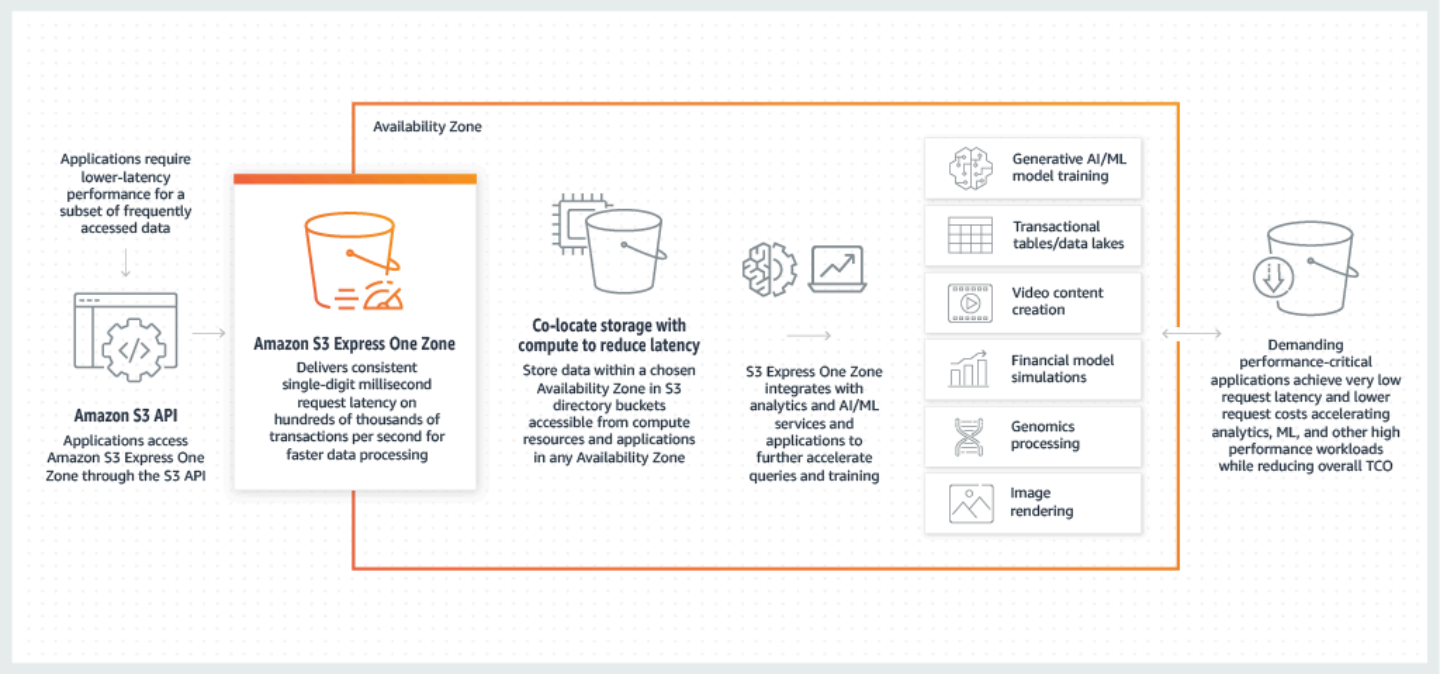
A classe Amazon S3 Express One Zone é uma classe de armazenamento de zona única e alto desempenho do Amazon S3 desenvolvida com o propósito específico de fornecer acesso consistente aos dados e com latência inferior a dez milissegundos para as aplicações mais sensíveis

à latência. A classe S3 Express One Zone é a classe de armazenamento de objetos em nuvem de menor latência disponível atualmente, com velocidades de acesso aos dados até dez vezes mais rápidas e custos de solicitação 50% mais baixos do que a classe S3 Standard. As aplicações podem se beneficiar imediatamente da conclusão de solicitações até uma ordem de magnitude mais rápida. A classe S3 Express One Zone oferece elasticidade de performance semelhante a outras classes de armazenamento do S3. A classe S3 Express One Zone é usada para workloads ou aplicações de desempenho crítico que requerem latência consistente inferior a dez milissegundos.

Assim como outras classes de armazenamento do Amazon S3, não é necessário planejar ou provisionar requisitos de capacidade ou throughput com antecedência. Você pode aumentar ou reduzir a escala do armazenamento verticalmente, de acordo com a necessidade, e acessar os dados por meio da API do Amazon S3.

A classe de armazenamento Amazon S3 Express One Zone foi projetada para oferecer disponibilidade de 99,95% em uma única zona de disponibilidade e tem o respaldo do Acordo de Serviço do Amazon S3. Com a classe S3 Express One Zone, os dados são armazenados de forma redundante em vários dispositivos dentro de uma única zona de disponibilidade. A classe S3 Express One Zone foi projetada para lidar com falhas simultâneas de dispositivos, detectando e reparando rapidamente qualquer redundância perdida. Se o dispositivo existente encontrar uma falha, a classe S3 Express One Zone transferirá automaticamente as solicitações para novos dispositivos dentro da mesma zona de disponibilidade. Essa redundância ajuda a garantir o acesso ininterrupto aos dados dentro de uma zona de disponibilidade.

A classe S3 Express One Zone é ideal para qualquer aplicação em que seja importante minimizar a latência necessária para acessar um objeto. Tais aplicações podem ser fluxos de trabalho com interatividade humana, como edição de vídeo, em que profissionais criativos precisam de acesso responsivo ao conteúdo por meio de suas interfaces de usuário. A classe S3 Express One Zone também beneficia workloads de análise e machine learning que têm requisitos de capacidade de resposta semelhantes dos dados, especialmente workloads com muitos acessos menores ou grandes quantidades de acessos aleatórios. A classe S3 Express One Zone pode ser usada com outros Serviços da AWS para oferecer suporte a workloads de analytics e de inteligência artificial/machine learning (IA/ML), como Amazon EMR, Amazon SageMaker AI e Amazon Athena.



Para buckets de diretório que usam a classe de armazenamento S3 Express One Zone, os dados são armazenados em vários dispositivos dentro de uma única zona de disponibilidade, mas não os armazena de forma redundante entre zonas de disponibilidade. Ao criar um bucket de diretório para usar a classe de armazenamento S3 Express One Zone, recomendamos que você especifique uma Região da AWS e uma zona de disponibilidade que seja local para suas instâncias de computação do Amazon EC2, do Amazon Elastic Kubernetes Service ou do Amazon Elastic Container Service (Amazon ECS) a fim de otimizar o desempenho.

Ao usar a classe S3 Express One Zone, você pode interagir com o bucket de diretório em uma nuvem privada virtual (VPC) usando um endpoint da VPC do gateway. Com um endpoint de gateway, é possível acessar buckets de diretório da classe S3 Express One Zone pela VPC sem precisar de um gateway da Internet ou um dispositivo NAT para a VPC, e tudo isso sem custos adicionais.

Você pode usar muitas das mesmas operações de API e recursos do Amazon S3 com buckets de diretório que já usa com buckets de uso geral e outras classes de armazenamento. Isso inclui o Mountpoint para Amazon S3, a criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3), a criptografia do lado do servidor com chaves do AWS Key Management Service (AWS KMS) (SSE-KMS) e os recursos Operações em Lote do S3 e Bloqueio de Acesso Público do S3. Você pode acessar a classe de armazenamento S3 Express One Zone pelo console do Amazon S3, pela AWS Command Line Interface (AWS CLI), pelos AWS SDKs e pela API REST do Amazon S3.

Para obter mais informações sobre a classe S3 Express One Zone, consulte os tópicos a seguir.

- Visão geral
- Recursos da classe S3 Express One Zone
- Serviços relacionados
- Próximas etapas

Visão geral

Para otimizar a performance e reduzir a latência, a classe S3 Express One Zone apresenta os novos conceitos a seguir.

Zonas de disponibilidade

A classe de armazenamento Amazon S3 Express One Zone foi projetada para oferecer disponibilidade de 99,95% em uma única zona de disponibilidade e tem o respaldo do Acordo de Serviço do Amazon S3. Com a classe S3 Express One Zone, os dados são armazenados de forma redundante em vários dispositivos dentro de uma única zona de disponibilidade. A classe S3 Express One Zone foi projetada para lidar com falhas simultâneas de dispositivos, detectando e reparando rapidamente qualquer redundância perdida. Se o dispositivo existente encontrar uma falha, a classe S3 Express One Zone transferirá automaticamente as solicitações para novos dispositivos dentro da mesma zona de disponibilidade. Essa redundância ajuda a garantir o acesso ininterrupto aos dados dentro de uma zona de disponibilidade.

Uma zona de disponibilidade é um ou mais datacenters discretos com energia, redes e conectividade redundantes em uma Região da AWS. Ao criar um bucket de diretório, escolha a zona de disponibilidade e a Região da AWS em que o bucket ficará localizado.

Zona de disponibilidade única

Ao criar um bucket de diretório, escolha a zona de disponibilidade e a Região da AWS.

Os buckets de diretório usam a classe de armazenamento S3 Express One Zone, desenvolvida para ser usada por aplicações sensíveis à performance. S3 Express One Zone é a primeira classe de armazenamento do S3 em que é possível selecionar uma única zona de disponibilidade com a opção de manter o armazenamento de objetos e os recursos de computação na mesma localização, o que fornece a maior velocidade de acesso possível.

Com a classe S3 Express One Zone, os dados são armazenados de forma redundante em vários dispositivos dentro de uma única zona de disponibilidade. A classe S3 Express One Zone foi

projetada para oferecer disponibilidade de 99,95% em uma única zona de disponibilidade e tem o respaldo do Acordo de Serviço do Amazon S3. Para obter mais informações, consulte Zonas de disponibilidade.

Endpoints e endpoints de VPC do gateway

As operações de API de gerenciamento para buckets de diretório estão disponíveis por meio de um endpoint regional e são chamadas de operações de API de endpoint regional. Exemplos de operações de API de endpoint regional são `CreateBucket` e `DeleteBucket`. Depois de criar um bucket de diretório, você pode usar operações de API de endpoint zonal para fazer upload e gerenciar os objetos no bucket de diretório. As operações de API de endpoint zonal estão disponíveis por meio de um endpoint zonal. Exemplos de operações de API de endpoint zonal são `PutObject` e `CopyObject`.

É possível acessar a classe S3 Express One Zone pela VPC usando endpoints de VPC do gateway. Depois de criar um endpoint de gateway, é possível adicioná-lo como um destino na tabela de rotas para o tráfego destinado da VPC à classe S3 Express One Zone. Assim como no Amazon S3, não há cobrança adicional pelo uso de endpoints de gateway. Para obter mais informações sobre como configurar endpoints de VPC do gateway, consulte Rede para buckets de diretório.

Autorização baseada em sessão

Com a classe S3 Express One Zone, é possível autenticar e autorizar solicitações por meio de um novo mecanismo baseado em sessão que é otimizado para fornecer a menor latência. Você pode usar `CreateSession` para solicitar credenciais temporárias que forneçam acesso de baixa latência ao bucket. Essas credenciais temporárias têm como escopo um bucket de diretório específico do S3. Os tokens de sessão são usados somente com operações zonais (nível de objeto) (com exceção de CopyObject). Para obter mais informações, consulte Autorizar operações de API de endpoint zonal com `CreateSession`.

Os AWS SDKs compatíveis com a classe S3 Express One Zone lidam com o estabelecimento e a atualização de sessões em seu nome. Para proteger as sessões, as credenciais de segurança temporárias expiram após 5 minutos. Depois de baixar e instalar os AWS SDKs e configurar as permissões necessárias do AWS Identity and Access Management (IAM), você pode começar imediatamente a usar as operações de API.

Recursos da classe S3 Express One Zone

Os recursos do S3 a seguir estão disponíveis para a classe S3 Express One Zone. Para obter uma lista completa de operações de APIs compatíveis e recursos não compatíveis, consulte Diferenças de buckets de diretório.

Gerenciamento de acesso e segurança

Você pode usar os recursos a seguir para auditar e gerenciar o acesso. Por padrão, os buckets de diretório são privados e só podem ser acessados por usuários que tenham recebido acesso explícito. Ao contrário dos buckets de uso geral que podem definir o limite de controle de acesso no nível do bucket, do prefixo ou da etiqueta de objeto, o limite do controle de acesso para buckets de diretório é definido somente no nível do bucket. Para obter mais informações, consulte Autorizar operações de API de endpoint regional com o IAM.

- Bloqueio de Acesso Público do S3: todas as configurações da funcionalidade Bloqueio de Acesso Público do S3 são habilitadas por padrão no nível do bucket. Essa configuração padrão não pode ser modificada.
- Propriedade de Objetos do S3 (padrão: Imposto pelo proprietário do bucket): as listas de controle de acesso (ACLs) não são compatíveis com buckets de diretório. Os buckets de diretório usam automaticamente a configuração Imposto pelo proprietário do bucket para a funcionalidade Propriedade de Objetos do S3. A opção Imposto pelo proprietário do bucket significa que as ACLs são desabilitadas e que o proprietário do bucket tem automaticamente a propriedade e o controle total sobre todos os objetos do bucket. Essa configuração padrão não pode ser modificada.
- AWS Identity and Access Management (IAM): o IAM ajuda você a controlar com segurança o acesso aos buckets de diretório. Você pode usar o IAM para conceder acesso às operações de API gerenciamento de buckets (regionais) e às operações de API de gerenciamento de objetos (zonais) por meio da ação `s3express:CreateSession`. Para obter mais informações, consulte Autorizar operações de API de endpoint regional com o IAM. Ao contrário das ações de gerenciamento de objetos, as ações de gerenciamento de buckets não podem ser executadas entre contas. Somente o proprietário do bucket pode realizar essas ações.
- Políticas de bucket: use a linguagem de política baseada no IAM para configurar permissões baseadas em recurso para os buckets de diretório. Você também pode usar o IAM para controlar o acesso à operação de API `CreateSession`, que permite usar as operações de API zonais ou de gerenciamento de objetos. Você pode conceder acesso entre contas ou na mesma conta para operações de API zonais. Para obter mais informações sobre as permissões e políticas da classe S3 Express One Zone, consulte Autorizar operações de API de endpoint regional com o IAM.

- IAM Access Analyzer para S3: avalie e monitore as políticas de acesso a fim de garantir que elas forneçam apenas o acesso pretendido aos recursos do S3.

Registro em log e monitoramento

A classe S3 Express One Zone usa as seguintes ferramentas de registro em log e monitoramento do S3, que você pode usar para monitorar e controlar como os recursos do estão sendo usados:

- Métricas do Amazon CloudWatch: monitore os recursos e as aplicações da AWS usando o CloudWatch para coletar e monitorar métricas. A classe S3 Express One Zone usa o mesmo namespace do CloudWatch que outras classes de armazenamento do Amazon S3 (`AWS/S3`) e oferece suporte a métricas de armazenamento diárias para buckets de diretório: `BucketSizeBytes` e `NumberOfObjects`. Para obter mais informações, consulte Monitoramento de métricas com o Amazon CloudWatch.
- Logs do AWS CloudTrail: o AWS CloudTrail é um AWS service (Serviço da AWS) que ajuda você a implementar a auditoria, a governança e a conformidade operacionais e de risco da sua Conta da AWS ao registrar as ações realizadas por um usuário, um perfil ou um AWS service (Serviço da AWS). Para a classe S3 Express One Zone, o CloudTrail captura operações de API de endpoint regional (por exemplo, `CreateBucket` e `PutBucketPolicy`) como eventos de gerenciamento e operações da API zonal (por exemplo, `GetObject` e `PutObject`) como eventos de dados. Esses eventos incluem ações realizadas no AWS Management Console, na AWS Command Line Interface (AWS CLI), em AWS SDKs e em operações de API da AWS. Para ter mais informações, consulte Logging with AWS CloudTrail for S3 Express One Zone.

> **Note**
>
> Os logs de acesso ao servidor do Amazon S3 não são compatíveis com a classe S3 Express One Zone.

Gerenciamento de objetos

Você pode gerenciar o armazenamento de objetos usando o console do Amazon S3, os AWS SDKs e a AWS CLI. Os seguintes recursos estão disponíveis para o gerenciamento de objetos com a classe S3 Express One Zone:

- Operações em Lote do S3: use a funcionalidade Operações em Lote para realizar operações em massa nos objetos em buckets de diretório, como Copiar e Invocar função do AWS Lambda. Por exemplo, você pode usar a funcionalidade Operações em Lote para copiar objetos entre buckets de diretório e buckets de uso geral. Com a funcionalidade Operações em Lote, você pode gerenciar bilhões de objetos em grande escala com uma única solicitação do S3 usando os AWS SDKs ou a AWS CLI ou com alguns cliques no console do Amazon S3.
- Importação: depois de criar um bucket de diretório, você poderá preenchê-lo com objetos usando o recurso de importação no console do Amazon S3. Importar é um método simplificado para criar trabalhos da funcionalidade Operações em Lote a fim de copiar objetos de buckets de uso geral para buckets de diretório.

AWS SDKs e bibliotecas de clientes

Você pode gerenciar o armazenamento de objetos usando os AWS SDKs e as bibliotecas de cliente.

- Mountpoint para Amazon S3: o Mountpoint para Amazon S3 é um cliente de arquivos de código aberto que oferece acesso de alto throughput, reduzindo os custos de computação para data lakes no Amazon S3. O Mountpoint para Amazon S3 converte chamadas de API do sistema de arquivos local em chamadas de API de objetos do S3, como `GET` e `LIST`. É ideal para workloads de data lake com muitas leituras que processam petabytes de dados e precisam do alto throughput elástico fornecido pelo Amazon S3 para aumentar e reduzir a escala verticalmente em milhares de instâncias.
- S3A: o S3A é uma interface compatível com Hadoop recomendada para acessar datastores no Amazon S3. O S3A substitui o cliente do sistema de arquivos S3N do Hadoop.
- PyTorch na AWS: o PyTorch na AWS é um framework de aprendizado profundo de código aberto que facilita o desenvolvimento de modelos de machine learning e a implantação deles na produção.
- AWS SDKs: você pode usar os AWS SDKs ao desenvolver aplicações com o Amazon S3. Os AWS SDKs simplificam suas tarefas de programação agrupando a API REST subjacente do Amazon S3. Para obter mais informações sobre como usar os AWS SDKs com a classe S3 Express One Zone, consulte the section called “SDKs da AWS”.

Criptografia e proteção de dados

Os objetos na classe S3 Express One Zone são criptografados automaticamente usando a criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3). O S3 Express

One Zone também é compatível com a criptografia no lado do servidor com chaves do AWS Key Management Service (AWS KMS) (SSE-KMS). A classe S3 Express One Zone não é compatível com a criptografia do lado do servidor com chaves de criptografia fornecidas pelo cliente (SSE-C) ou criptografia de camada dupla do lado do servidor com AWS KMS keys (DSSE-KMS). Para obter mais informações, consulte Proteção e criptografia de dados.

A classe S3 Express One Zone oferece a opção de escolher o algoritmo de soma de verificação usado para validar os dados durante o upload ou o download. Você pode selecionar um dos seguintes algoritmos de verificação de integridade de dados de hash seguro (SHA) ou de verificação de redundância cíclica (CRC): CRC32, CRC32C, SHA-1 e SHA-256. As somas de verificação baseadas em MD5 não são compatíveis com a classe de armazenamento S3 Express One Zone.

Para obter mais informações, consulte Práticas recomendadas adicionais de soma de verificação do S3.

Signature Version 4 (SigV4) da AWS

A classe S3 Express One Zone usa o Signature Version 4 (SigV4) da AWS. SigV4 é um protocolo de assinatura usado para autenticar solicitações ao Amazon S3 via HTTPS. A classe S3 Express One Zone assina solicitações usando o Sigv4 da AWS. Para obter mais informações, consulte Autenticação de solicitações (AWS Signature Version 4)) na Referência de APIs do Amazon Simple Storage Service.

Consistência forte

A classe S3 Express One Zone oferece uma sólida consistência de leitura após gravação para solicitações `PUT` e `DELETE` de objetos em buckets de diretório em todas as Regiões da AWS. Para obter mais informações, consulte Modelo de consistência de dados do Amazon S3.

Serviços relacionados

Você pode usar os seguintes Serviços da AWS com a classe de armazenamento S3 Express One Zone para oferecer suporte ao seu caso de uso específico de baixa latência.

- Amazon Elastic Compute Cloud (Amazon EC2): o Amazon EC2 oferece capacidade de computação segura e escalável na Nuvem AWS. O uso do Amazon EC2 reduz a necessidade de investimento antecipado em hardware. Por isso, você pode desenvolver e implantar aplicações com maior rapidez. É possível usar o Amazon EC2 para executar quantos servidores virtuais forem necessários, configurar a segurança e as redes e gerenciar o armazenamento.

- AWS Lambda: o Lambda é um serviço de computação que permite que você execute o código sem provisionar ou gerenciar servidores. Você define as configurações de notificação em um bucket e concede permissão ao Amazon S3 para invocar uma função na política de permissões baseada em recursos da função.
- Amazon Elastic Kubernetes Service (Amazon EKS): o Amazon EKS é um serviço gerenciado que elimina a necessidade de instalar, operar e manter o seu próprio ambiente de gerenciamento do Kubernetes na AWS. O Kubernetes é um sistema de código aberto que automatiza o gerenciamento, a escalação e a implantação de aplicações em contêineres.
- Amazon Elastic Container Service (Amazon ECS): o Amazon ECS é um serviço totalmente gerenciado de orquestração de contêineres que ajuda a implantar, gerenciar e dimensionar facilmente aplicações em contêineres.
- AWS Key Management Service (AWS KMS): o AWS Key Management Service (AWS KMS) é um serviço gerenciado que facilita a criação e o controle de chaves de criptografia usadas para criptografar seus dados. As chaves do AWS que você cria no AWS KMS são protegidas por módulos de segurança de hardware (HSM) com validação FIPS 140-2. Para usar ou gerenciar suas chaves do KMS, você interage com o AWS KMS.
- Amazon Athena: o Athena é um serviço de consultas interativas que facilita a análise de dados no Amazon S3 usando SQL padrão. Você também pode usar o Athena para executar análises de dados de maneira interativa usando o Apache Spark sem a necessidade de planejamento, configuração ou gerenciamento de recursos. Ao executar aplicações do Apache Spark no Athena, você envia o código Spark para processamento e recebe os resultados de forma direta.
- Treinamento do Amazon SageMaker: analise as opções de modelos de treinamento com o Amazon SageMaker, incluindo algoritmos integrados, algoritmos personalizados, bibliotecas e modelos do AWS Marketplace.
- AWS Glue: o AWS Glue é um serviço de integração de dados com tecnologia sem servidor que facilita aos usuários de análise a descoberta, preparação, transferência e integração de dados de várias fontes. Você pode usar o AWS Glue para análise, machine learning e desenvolvimento de aplicações. O AWS Glue também inclui outras ferramentas de produtividade e operações de dados para criação, execução de trabalhos e implementação de fluxos de trabalho de negócios.
- Amazon EMR: o Amazon EMR é uma plataforma de cluster gerenciada que simplifica a execução de frameworks de big data, como Apache Hadoop e Apache Spark, na AWS a fim de processar e analisar grandes volumes de dados.
- AWS CloudTrail: o AWS CloudTrail é um serviço da AWS que ajuda você a habilitar governança, conformidade e auditorias operacionais e de risco na sua conta da AWS. As ações realizadas por um usuário, uma função ou um serviço da AWS são registradas como eventos no CloudTrail. Os

eventos incluem ações realizadas no Console de Gerenciamento da AWS, na AWS Command Line Interface e nos AWS SDKs e APIs.

- AWS CloudFormation: é um serviço que ajuda você a modelar e configurar seus recursos da AWS para gastar menos tempo gerenciando esses recursos e mais tempo se concentrando nas aplicações executadas na AWS. Você cria um modelo que descreve todos os recursos da AWS desejados (como funções do Amazon EC2 e tabelas do Amazon RDS), e o CloudFormation cuida do provisionamento e da configuração desses recursos para você. Não é necessário criar e configurar individualmente os recursos da AWS e descobrir o que depende do que: o CloudFormation lida com tudo isso.

Próximas etapas

Para obter mais informações sobre como usar a classe de armazenamento S3 Express One Zone e os buckets de diretório, consulte os seguintes tópicos:

- Tutorial: Conceitos básicos da classe S3 Express One Zone
- Zonas de disponibilidade e regiões da classe S3 Express One Zone
- Rede para buckets de diretório em uma zona de disponibilidade
- Criar buckets de diretório em uma zona de disponibilidade
- Endpoints regionais e zonais para buckets de diretório em uma zona de disponibilidade
- Otimizar o desempenho da classe S3 Express One Zone

Tutorial: Conceitos básicos da classe S3 Express One Zone

A classe Amazon S3 Express One Zone é a primeira classe de armazenamento do S3 em que é possível selecionar uma única Zona de Disponibilidade com a opção de manter o armazenamento de objetos e os recursos de computação na mesma localização, o que oferece a maior velocidade de acesso possível. Os dados na classe S3 Express One Zone são armazenados em buckets de diretório localizados em zonas de disponibilidade. Para ter mais informações sobre os buckets de diretório, consulte Buckets de diretório.

A classe S3 Express One Zone é ideal para qualquer aplicação em que seja essencial minimizar a latência da solicitação. Tais aplicações podem ser fluxos de trabalho com interatividade humana, como edição de vídeo, em que profissionais criativos precisam de acesso responsivo ao conteúdo por meio de suas interfaces de usuário. A classe S3 Express One Zone também beneficia workloads de analytics e machine learning que têm requisitos de capacidade de resposta semelhantes dos

dados, especialmente workloads com muitos acessos menores ou grandes quantidades de acessos aleatórios. A classe S3 Express One Zone pode ser usada com outros serviços da AWS, como Amazon EMR, Amazon Athena, AWS Glue Data Catalog e o Treinamento de modelo do Amazon SageMaker para oferecer suporte a workloads de analytics, de inteligência artificial e de machine learning (IA/ML). É possível trabalhar com a classe de armazenamento S3 Express One Zone e os buckets de diretório usando o console do Amazon S3, os AWS SDKs, a AWS Command Line Interface (AWS CLI) e a API REST do Amazon S3. Para ter mais informações, consulte O que é a classe S3 Express One Zone? e O que diferencia a classe S3 Express One Zone?
Este é um diagrama do fluxo de trabalho da classe S3 Express One Zone.

Objetivo

Neste tutorial, você aprenderá como criar um endpoint de gateway, criar e anexar uma política do IAM, criar um bucket de diretório e, depois, usar a ação Import para preencher o bucket de diretório com objetos atualmente armazenados no bucket de uso geral. Como alternativa, é possível fazer upload manualmente de objetos no bucket de diretório.

Tópicos

- Pré-requisitos
- Etapa 1: configurar um endpoint da VPC de gateway para acessar buckets de diretório da classe S3 Express One Zone
- Etapa 2: criar um bucket de diretório da classe S3 Express One Zone
- Etapa 3: importar dados para um bucket de diretório da classe S3 Express One Zone
- Etapa 4: fazer upload manual de objetos no bucket de diretório da classe S3 Express One Zone
- Etapa 5: esvaziar um bucket de diretório da classe S3 Express One Zone
- Etapa 6: excluir um bucket de diretório da classe S3 Express One Zone
- Próximas etapas

Pré-requisitos

Antes de começar este tutorial, você deve ter uma Conta da AWS na qual possa fazer login como um usuário do AWS Identity and Access Management (IAM) com permissões corretas.

Subetapas

- Criar uma Conta da AWS
- Criar um usuário do IAM na Conta da AWS (console)

- Criar uma política do IAM e anexá-la a um usuário ou um perfil do IAM (console)

Criar uma Conta da AWS

Para concluir este tutorial, você precisa de uma Conta da AWS. Ao cadastrar-se na AWS, sua Conta da AWS é automaticamente cadastrada em todos os serviços da AWS incluindo o Amazon S3. A cobrança incorrerá apenas pelos serviços utilizados. Para ter mais informações sobre a definição de preço, consulte S3 pricing.

Criar um usuário do IAM na Conta da AWS (console)

O AWS Identity and Access Management (IAM) é um AWS service (Serviço da AWS) que ajuda os administradores a controlar o acesso aos recursos da AWS de forma segura. Os administradores do IAM controlam quem pode se autenticar (se conectar) e ter autorização (permissões) para acessar os objetos e usar os buckets de diretório na classe S3 Express One Zone. Você pode usar o IAM sem custo adicional.

Por padrão, os usuários não têm permissões para acessar os buckets de diretório e realizar as operações da classe S3 Express One Zone. Para conceder permissões de acesso a buckets de diretório e operações da classe S3 Express One Zone, você pode usar o IAM para criar usuários ou perfis e anexar permissões a essas identidades. Para obter mais informações sobre como criar um usuário do IAM, consulte Criar usuários do IAM (console) no Guia do usuário do IAM. Para ter mais informações sobre como criar um perfil do IAM, consulte Criação de uma função para delegar permissões a um usuário do IAM no Guia do usuário do IAM.

Para simplificar, este tutorial cria e usa um usuário do IAM. Depois de concluir este tutorial, lembre-se de Excluir o usuário do IAM. Para uso em produção, recomendamos que você siga as Práticas recomendadas de segurança no IAM no Guia do usuário do IAM. Uma das práticas recomendadas exige que os usuários humanos usem a federação com um provedor de identidades para acessar a AWS usando credenciais temporárias. Outra prática recomendada é exigir que as workloads usem credenciais temporárias com perfis do IAM para acessar a AWS. Para saber mais sobre como usar o AWS IAM Identity Center para criar usuários com credenciais temporárias, consulte Getting started no Guia do usuário do AWS IAM Identity Center.

> **Warning**
>
> Os usuários do IAM têm credenciais de longo prazo, o que representa um risco de segurança. Para ajudar a reduzir esse risco, recomendamos que você forneça a esses

usuários somente as permissões necessárias para realizar a tarefa e que você os remova quando não forem mais necessários.

Criar uma política do IAM e anexá-la a um usuário ou um perfil do IAM (console)

Por padrão, os usuários não têm permissões para os buckets de diretório e as operações da classe S3 Express One Zone. Para conceder permissões de acesso a buckets de diretório, você pode usar o IAM para criar usuários ou perfis e anexar permissões a essas identidades. Os buckets de diretório são o único recurso que você pode incluir nas políticas de bucket ou nas políticas de identidade do IAM para acesso à classe S3 Express One Zone.

Para usar as operações de API do endpoint regional (operações em nível de bucket ou ambiente de gerenciamento) com a classe S3 Express One Zone, use o modelo de autorização do IAM, que não envolve gerenciamento de sessões. As permissões são concedidas individualmente para as ações. Para usar as operações de API do endpoint zonal (operações em nível de objeto ou plano de dados), use `CreateSession` para criar e gerenciar sessões otimizadas para autorização de solicitações de dados com baixa latência. Para recuperar e usar um token de sessão, você deve permitir a ação `s3express:CreateSession` para o bucket de diretório em uma política baseada em identidade ou em uma política de bucket. Se você acessar a classe S3 Express One Zone pelo console do Amazon S3, pela AWS Command Line Interface (AWS CLI) ou usando os AWS SDKs, a classe S3 Express One Zone criará uma sessão em seu nome. Para ter mais informações, consulte `CreateSession` authorization e AWS Identity and Access Management (IAM) para a classe S3 Express One Zone.

Como criar uma política do IAM e anexá-la a um usuário do IAM (ou perfil)

1. Faça login no Console de Gerenciamento da AWS e abra o Console de Gerenciamento do IAM.
2. No painel de navegação, selecione Políticas.
3. Escolha Create Policy.
4. Selecione JSON.
5. Copie a política abaixo na janela do Editor de políticas. Para criar buckets de diretório ou usar a classe S3 Express One Zone, é necessário conceder as permissões necessárias ao perfil ou ao usuário do AWS Identity and Access Management (IAM). Esse exemplo de política permite acesso à operação de API `CreateSession` (para uso com as operações de API em nível de objeto ou zonais) e a todas as operações de API do endpoint regional (nível de bucket). Essa política permite que a operação de API `CreateSession` seja usada com todos os buckets de diretório, mas as operações de API de endpoint regional só são permitidas para uso com o

bucket de diretório especificado. Para usar esse exemplo de política, substitua os *user input placeholders* por suas próprias informações.

```
{
     "Version": "2012-10-17",
     "Statement": [
         {
             "Sid": "AllowAccessRegionalEndpointAPIs",
             "Effect": "Allow",
             "Action": [
                 "s3express:DeleteBucket",
                 "s3express:DeleteBucketPolicy",
                 "s3express:CreateBucket",
                 "s3express:PutBucketPolicy",
                 "s3express:GetBucketPolicy",
                 "s3express:ListAllMyDirectoryBuckets"
             ],

             "Resource": "arn:aws:s3express:region:account_id:bucket/bucket-base-name--zone-id--x-s3/*"
         },
         {
             "Sid": "AllowCreateSession",
             "Effect": "Allow",
             "Action": "s3express:CreateSession",
             "Resource": "*"
         }
     ]
 }
```

6. Escolha Próximo.
7. Atribua o nome à política.

> **Note**
>
> As tags de bucket não são compatíveis com a classe S3 Express One Zone.

8. Selecione Criar política.
9. Agora que você criou uma política do IAM, poderá anexá-la a um usuário do IAM. No painel de navegação, selecione Políticas.
10. Na caixa de pesquisa, insira o nome da política.

11. No menu Ações, selecione Anexar.
12. Em Filtrar por tipo de entidade, selecione Usuários do IAM ou Perfis.
13. No campo de pesquisa, digite o nome do usuário ou do perfil que você deseja usar.
14. Escolha Attach Policy.

Etapa 1: configurar um endpoint da VPC de gateway para acessar buckets de diretório da classe S3 Express One Zone

Você pode acessar operações de API zonais e regionais por meio de endpoints de nuvem privada virtual (VPC) de gateway. Os endpoints do gateway podem permitir que o tráfego chegue à classe S3 Express One Zone sem atravessar um gateway NAT. É altamente recomendável usar endpoints de gateway, pois eles fornecem o melhor caminho de rede ao trabalhar com a classe S3 Express One Zone. É possível acessar buckets de diretório da classe S3 Express One Zone pela VPC sem precisar de um gateway da Internet ou um dispositivo NAT para a VPC, e tudo isso sem custos adicionais. Use o procedimento a seguir para configurar um endpoint de gateway que se conecte aos objetos da classe de armazenamento S3 Express One Zone e aos buckets de diretório.

Para acessar a classe S3 Express One Zone, use endpoints regionais e zonais que são diferentes dos endpoints padrão do Amazon S3. Dependendo da operação de API do Amazon S3 usada, será necessário um endpoint regional ou zonal. Para ter uma lista completa das operações de API compatíveis por tipo de endpoint, consulte Operações de API compatíveis com a classe S3 Express One Zone. Você deve acessar endpoints zonais e regionais por meio de um endpoint de nuvem privada virtual (VPC) do gateway.

Use o procedimento a seguir para criar um endpoint de gateway que se conecte aos objetos da classe S3 Express One Zone e aos buckets de diretório.

Como configurar um endpoint da VPC do gateway

1. Abra o console do Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação lateral, em Nuvem privada virtual, escolha Endpoints.
3. Escolha Criar endpoint.
4. Crie um nome para o endpoint.
5. Em Service category (Categoria de serviço), escolha Serviços da AWS.
6. Em Serviços, pesquise usando o filtro Tipo=Gateway e escolha o botão de opções ao lado de com.amazonaws.***region***.s3express.

7. Em VPC, escolha a VPC na qual deseja criar o endpoint.
8. Em Route tables (Tabelas de rotas), selecione as tabelas de rotas a serem usadas pelo endpoint. O Amazon VPC adiciona automaticamente uma rota que aponta o tráfego destinado ao serviço para a interface de rede do endpoint.
9. Em Política, escolha Acesso total para permitir todas as operações de todas as entidades principais em todos os recursos no endpoint da VPC. Como alternativa, escolha Personalizado para anexar uma política de endpoint da VPC que controle as permissões das entidades principais para realizar ações em recursos pelo endpoint da VPC.
10. Escolha Criar endpoint.

Depois de criar um endpoint de gateway, você pode usar endpoints de API regionais e endpoints de API zonais para acessar objetos da classe de armazenamento Amazon S3 Express One Zone e buckets de diretório.

Etapa 2: criar um bucket de diretório da classe S3 Express One Zone

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Na barra de navegação na parte superior da página, escolha o nome da Região da AWS exibida no momento. Em seguida, escolha a região na qual você deseja criar um bucket.

   > **Note**
   >
   > Para reduzir a latência e os custos e atender aos requisitos regulatórios, selecione uma região perto de você. Os objetos armazenados em uma região nunca saem dessa região, a menos que você os transfira para outra região. Para obter uma lista de Regiões da AWS do Amazon S3, consulte Endpoints de AWS service (Serviço da AWS) no Referência geral da Amazon Web Services.

3. No painel de navegação à esquerda, escolha Buckets de diretórios.
4. Selecione Create bucket (Criar bucket). A página Create bucket (Criar bucket) é aberta.
5. Em Configuração geral, visualize a Região da AWS onde o bucket será criado.

   Em Tipo de bucket, escolha Diretório.

> **Note**
>
> - Se você escolher uma região que não oferece suporte a buckets de diretório, a opção Tipo de bucket desaparecerá e o tipo de bucket assumirá um bucket de uso geral como padrão. Para criar um bucket de diretório, escolha uma região compatível. Para obter uma lista de regiões que oferecem suporte a buckets de diretório e à classe de armazenamento Amazon S3 Express One Zone, consulte the section called “Zonas de disponibilidade e regiões da classe S3 Express One Zone”.
> - Depois de criar o bucket, não será possível alterar o tipo.

> **Note**
>
> A zona de disponibilidade não poderá ser alterada após a criação do bucket.

6. Em Zona de disponibilidade, escolha uma zona de disponibilidade que seja local para os seus serviços de computação. Para obter uma lista de zonas de disponibilidade que oferecem suporte a buckets de diretório e à classe de armazenamento S3 Express One Zone, consulte the section called “Zonas de disponibilidade e regiões da classe S3 Express One Zone”.

   Em Zona de disponibilidade, marque a caixa de seleção para indicar que, em caso de interrupção na zona de disponibilidade, seus dados poderão ficar indisponíveis ou ser perdidos.

   > **Important**
   >
   > Embora os buckets de diretório sejam armazenados em vários dispositivos dentro de uma única zona de disponibilidade, eles não armazenam dados de forma redundante entre zonas de disponibilidade.

7. Em Nome do bucket, insira um nome para o bucket de diretório.

   As regras de nomenclatura a seguir se aplicam a buckets de diretório.

   - O nome deve ser exclusivo na zona escolhida (zona de disponibilidade da AWS ou zona local da AWS).
   - O nome deve ter entre 3 (mín.) e 63 (máx.) caracteres, incluindo o sufixo.

- Consistir em letras minúsculas, números e hifens (-).
- Inicie e termine com uma letra ou um número.
- Deve incluir o seguinte sufixo: `--`*`zone-id`*`--x-s3`.
- O nome do bucket não deve iniciar com o prefixo `xn--`.
- O nome do bucket não deve iniciar com o prefixo `sthree-`.
- O nome do bucket não deve iniciar com o prefixo `sthree-configurator`.
- O nome do bucket não deve iniciar com o prefixo `amzn-s3-demo-`.
- Os nomes de bucket não podem terminar com o sufixo `-s3alias`. Esse sufixo se reserva a nomes de alias de ponto de acesso. Para obter mais informações, consulte Alias de ponto de acesso.
- Os nomes de bucket não podem terminar com o sufixo `--ol-s3`. Esse sufixo é reservado a nomes de alias de ponto de acesso de objeto do Lambda. Para obter mais informações, consulte Como usar um alias no estilo do bucket para o ponto de acesso do Object Lambda do bucket do S3.
- Os nomes de bucket não podem terminar com o sufixo `.mrap`. Esse sufixo é reservado para nomes de ponto de acesso de várias regiões. Para obter mais informações, consulte Regras para nomear pontos de acesso multirregionais do Amazon S3.

Um sufixo é adicionado automaticamente ao nome de base que você fornece ao criar um bucket de diretório usando o console. Esse sufixo inclui o ID da zona de disponibilidade que você escolheu.

Depois de criado o bucket, você não pode mudar seu nome. Para obter mais informações sobre como nomear buckets, consulte Regras de nomenclatura de buckets de uso geral.

> **Important**
>
> Não inclua informações confidenciais, como números de conta, no nome do bucket. O nome do bucket é visível nos URLs que apontam para os objetos no bucket.

8. Em Propriedade do objeto, a configuração Imposto pelo proprietário do bucket está habilitada automaticamente e todas as listas de controle de acesso (ACLs) estão desabilitadas. Para os buckets de diretório, não é possível habilitar ACLs.

Imposto pelo proprietário do bucket (padrão): as ACLs são desabilitadas e o proprietário do bucket automaticamente tem propriedade e controle total sobre todos os objetos do bucket de uso geral. As ACLs não afetam mais as permissões de acesso aos dados no bucket de uso geral do S3. O bucket usa políticas exclusivamente para definir o controle de acesso.

9. Em Configurações de bloqueio do acesso público deste bucket, todas as configurações da funcionalidade Bloqueio de Acesso Público para o bucket de diretório estão automaticamente habilitadas. Não é possível modificar essas configurações para buckets de diretório. Para obter mais informações sobre como bloquear o acesso público, consulte Bloquear o acesso público ao armazenamento do Amazon S3.
10. Para configurar a criptografia padrão, em Tipo de criptografia, selecione uma das seguintes opções:

    - Criptografia do lado do servidor com chave gerenciada pelo Amazon S3 (SSE-S3)
    - Criptografia do lado do servidor com chave do AWS Key Management Service (SSE-KMS)

    Para obter mais informações sobre como usar a criptografia no lado do servidor do Amazon S3 para criptografar seus dados, consulte Proteção e criptografia de dados.

    > **Important**
    >
    > Se você usar a opção SSE-KMS em sua configuração de criptografia padrão, estará sujeito à cota de solicitações por segundo (RPS) do AWS KMS. Para obter mais informações sobre as cotas do AWS KMS e como solicitar um aumento de cota, consulte Cotas no Guia do desenvolvedor do AWS Key Management Service.
    > Ao habilitar a criptografia padrão, poderá ser necessário atualizar a política de bucket. Para obter mais informações, consulte Usar criptografia SSE-KMS para operações entre contas.

11. Se você escolher Criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3), aparecerá Habilitado em Chave do bucket. As chaves de bucket do S3 são sempre habilitadas quando você configura o bucket de diretório para usar a criptografia padrão com SSE-S3. As chaves de bucket do S3 estão sempre habilitadas para operações `GET` e `PUT` em um bucket de diretório e não podem ser desabilitadas. Não são aceitas chaves de bucket do S3 quando você copia objetos criptografados por SSE-KMS de buckets de uso geral para buckets de diretório, de buckets de diretório para buckets de uso geral ou entre buckets de diretório, por meio de CopyObject, de UploadPartCopy, da operação Copy em Operações em Lote ou de

trabalhos de import. Nesse caso, o Amazon S3 faz uma chamada para o AWS KMS sempre que uma solicitação de cópia é feita para um objeto criptografado pelo KMS.

As chaves de bucket do S3 diminuem o custo de criptografia reduzindo o tráfego de solicitações do Amazon S3 para o AWS KMS. Para obter mais informações, consulte Redução do custo do SSE-KMS com chaves de bucket do Amazon S3.

12. Se você escolher Criptografia do lado do servidor com chave do AWS Key Management Service (SSE-KMS), em Chave do AWS KMS, especifique uma chave do AWS Key Management Service de uma das maneiras a seguir ou crie uma chave.

    - Para escolher uma chave do KMS na lista disponível, selecione Escolher entre suas AWS KMS keys e escolha sua Chave do KMS em AWS KMS keys disponíveis.

      Somente as suas chaves gerenciadas pelo cliente são exibidas nessa lista. Não é possível usar o Chave gerenciada pela AWS (`aws/s3`) em buckets de diretório. Para ter mais informações sobre chaves gerenciadas pelo cliente, consulte Chaves de clientes e chaves da AWS no Guia do desenvolvedor do AWS Key Management Service.
    - Para inserir o ARN ou o alias da chave do KMS, escolha Inserir ARN da AWS KMS key e insira o ARN ou o alias da chave do KMS em ARN da AWS KMS key.
    - Para criar uma chave gerenciada pelo cliente no console do AWS KMS, selecione Criar uma chave do KMS.

      Para ter mais informações sobre como criar uma AWS KMS key, consulte Criação de chaves no Guia do desenvolvedor do AWS Key Management Service.

    > **Important**
    >
    > - A configuração de SSE-KMS só comporta uma chave gerenciada pelo cliente por bucket de diretório durante a vida útil do bucket. Não há suporte para Chave gerenciada pela AWS (`aws/s3`). Além disso, depois que você especifica uma chave gerenciada pelo cliente para SSE-KMS, não é possível substituí-la pela configuração de SSE-KMS do bucket.
    >
    >   É possível identificar a chave gerenciada pelo cliente que você especificou para a configuração SSE-KMS do bucket, da seguinte forma:
    >
    >   - Faça uma solicitação de operação de API `HeadObject` para encontrar o valor de `x-amz-server-side-encryption-aws-kms-key-id` em sua resposta.

Para usar uma nova chave gerenciada pelo cliente em seus dados, recomendamos copiar os objetos existentes em um novo bucket de diretório com uma nova chave gerenciada pelo cliente.

- Você só pode usar chaves do KMS disponíveis na mesma Região da AWS que o bucket. O console do Amazon S3 lista somente as primeiras 100 chaves do KMS na mesma região que o bucket. Para usar uma chave do KMS que não esteja listada, você deve inserir o ARN da chave do KMS. Se quiser usar uma chave do KMS que seja de propriedade de outra conta, primeiro você deverá ter permissão para usar a chave e, depois, inserir o ARN da chave do KMS. Para obter mais informações sobre permissões entre contas para chaves do KMS, consulte Criar chaves do KMS que outras contas podem usar no Guia do desenvolvedor do AWS Key Management Service. Para obter mais informações sobre a SSE-KMS, consulte Especificar a criptografia do lado do servidor com o AWS KMS (SSE-KMS) para novos uploads de objetos em buckets de diretório.
- Ao usar uma AWS KMS key para criptografia do lado do servidor em buckets de diretório, você deve escolher uma chave de criptografia do KMS simétrica. O Amazon S3 só é compatível com chaves do KMS de criptografia simétrica, e não com chaves assimétricas do KMS. Para ter mais informações, consulte Identificar chaves do KMS simétricas e assimétricas no Guia do desenvolvedor do AWS Key Management Service.

Para obter mais informações sobre como usar o AWS KMS com o Amazon S3, consulte Usar a criptografia do lado do servidor com chaves do AWS KMS (SSE-KMS) em buckets de diretório.

13. Escolha Criar bucket. Depois de criar o bucket, você pode adicionar arquivos e pastas a ele. Para obter mais informações, consulte the section called “Trabalhar com objetos em um bucket de diretório”.

Etapa 3: importar dados para um bucket de diretório da classe S3 Express One Zone

Para concluir essa etapa, é necessário ter um bucket de uso geral que contenha objetos e esteja localizado na mesma Região da AWS que o bucket de diretório.

Depois de criar um bucket de diretório no Amazon S3, é possível preencher o novo bucket com dados usando a ação Importar no console do Amazon S3. A importação simplifica a cópia de dados em buckets de diretório, permitindo que você escolha um prefixo ou um bucket de uso geral para

importar dados sem precisar especificar todos os objetos a serem copiados individualmente. A importação usa o S3 Batch Operations, que copia os objetos no prefixo selecionado ou no bucket de uso geral. É possível monitorar o andamento do trabalho de importação de cópias por meio da página de detalhes do trabalho do S3 Batch Operations.

Como usar a ação Importar

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Na barra de navegação na parte superior da página, escolha o nome da Região da AWS exibida no momento. Depois, escolha a região associada à Zona de Disponibilidade na qual o bucket de diretório está localizado.
3. No painel de navegação à esquerda, escolha Buckets de diretórios.
4. Selecione o botão de opções ao lado do nome do bucket para o qual você deseja importar objetos.
5. Escolha Importar.
6. Em Origem, insira o bucket de uso geral (ou o caminho do bucket com o prefixo) que contém os objetos que você deseja importar. Para escolher um bucket de uso geral existente em uma lista, selecione Procurar no S3.
7. Na seção Permissões, é possível optar por gerar automaticamente um perfil do IAM. Como alternativa, é possível selecionar um perfil do IAM em uma lista ou inserir diretamente um ARN do perfil do IAM.

   - Para permitir que o Amazon S3 crie um perfil do IAM em seu nome, escolha Criar perfil do IAM.

     > **Note**
     >
     > Se os objetos da origem estiverem criptografados com criptografia do lado do servidor com chaves do AWS Key Management Service (AWS KMS) (SSE-KMS), não escolha a opção Criar perfil do IAM. Em vez disso, especifique um perfil do IAM existente que tenha a permissão `kms:Decrypt`.
     > O Amazon S3 usará essa permissão para descriptografar os objetos. Durante o processo de importação, o Amazon S3 recriptografará esses objetos usando criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3).

- Para escolher um perfil do IAM existente em uma lista, escolha Escolher entre perfis do IAM existentes.
- Para especificar um perfil do IAM existente inserindo o nome do recurso da Amazon (ARN), escolha Inserir ARN do perfil do IAM e insira o ARN no campo correspondente.

8. Revise as informações exibidas nas seções Destino e Configurações do objeto copiado. Se as informações na seção Destino estiverem corretas, escolha Importar para iniciar o trabalho de cópia.

   O console do Amazon S3 exibirá o status do novo trabalho na página Operações em lotes. Para obter mais informações sobre o trabalho, escolha o botão de opções ao lado do nome do trabalho e selecione Visualizar detalhes no menu Ações. Para abrir o bucket de diretório para o qual os objetos serão importados, escolha Exibir destino de importação.

Etapa 4: fazer upload manual de objetos no bucket de diretório da classe S3 Express One Zone

Também é possível fazer upload manual de objetos para o bucket de diretório.

Como fazer upload de objetos manualmente

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Na barra de navegação no canto superior direito da página, escolha o nome da Região da AWS exibida no momento. Depois, escolha a região associada à Zona de Disponibilidade na qual o bucket de diretório está localizado.
3. No painel de navegação à esquerda, escolha Buckets de diretórios.
4. Escolha o nome do bucket no qual você deseja fazer upload de pastas ou arquivos.

   > **Note**
   >
   > Se você escolher o mesmo bucket de diretório usado nas etapas anteriores deste tutorial, o bucket de diretório conterá os objetos que foram carregados da ferramenta de importação. Observe que esses objetos agora estão armazenados na classe de armazenamento S3 Express One Zone.

5. Na guia Objetos, escolha Fazer upload.
6. Na página Fazer upload, execute uma das seguintes ações:

- Arraste e solte arquivos e pastas para a área de upload tracejada.
- Escolha Adicionar arquivos ou Adicionar pasta, selecione os arquivos ou as pastas que deseja carregar e escolha Abrir ou Fazer upload.

7. Em Checksums, escolha a Função de soma de verificação que deseja usar.

> **Note**
>
> Recomendamos usar CRC32 e CRC32C para obter a melhor performance com a classe de armazenamento S3 Express One Zone. Para ter mais informações, consulte as Práticas recomendadas adicionais de checksum do S3.

(Opcional) Se você estiver fazendo upload de um único objeto com menos de 16 MB, também poderá especificar um valor de checksum pré-calculado. Ao fornecer um valor pré-calculado, o Amazon S3 compara esse valor com o valor calculado usando a função de checksum selecionada. Se os valores não corresponderem, o upload não será iniciado.

8. As opções nas seções Permissões e Propriedades são definidas automaticamente com as configurações padrão e não podem ser modificadas. A funcionalidade Bloqueio de Acesso Público é habilitada automaticamente, e as funcionalidades Versionamento do S3 e Bloqueio de Objetos do S3 não podem ser habilitadas para buckets de diretório.

   (Opcional) Se você quiser adicionar metadados em pares de chave e valor aos objetos, expanda a seção Propriedades e escolha Adicionar metadados na seção Metadados.

9. Para fazer upload das pastas e dos arquivos listados, escolha Fazer upload.

   O Amazon S3 faz o upload de seus objetos e pastas. Quando o upload for concluído, você verá uma mensagem de sucesso na página Upload: status.

   Você criou com êxito um bucket de diretório e fez upload de objetos para o bucket.

Etapa 5: esvaziar um bucket de diretório da classe S3 Express One Zone

É possível esvaziar um bucket de diretório do Amazon S3 usando o console do Amazon S3.

Como esvaziar um bucket de diretório

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Na barra de navegação no canto superior direito da página, escolha o nome da Região da AWS exibida no momento. Depois, escolha a região associada à Zona de Disponibilidade na qual o bucket de diretório está localizado.
3. No painel de navegação à esquerda, escolha Buckets de diretórios.
4. Escolha o botão de opções ao lado do nome do bucket que você deseja esvaziar, depois selecione Esvaziar.
5. Na página Empty bucket (Esvaziar bucket), confirme se deseja esvaziar o bucket inserindo **`permanently delete`** no campo de texto e depois escolha Empty (Esvaziar).
6. Monitore o andamento do processo de esvaziamento do bucket na página Bucket vazio: status.

Etapa 6: excluir um bucket de diretório da classe S3 Express One Zone

Depois de esvaziar o bucket de diretório e interromper todos os uploads multiparte em andamento, você poderá excluir o bucket usando o console do Amazon S3.

Como excluir um bucket de diretório

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Na barra de navegação no canto superior direito da página, escolha o nome da Região da AWS exibida no momento. Depois, escolha a região associada à Zona de Disponibilidade na qual o bucket de diretório está localizado.
3. No painel de navegação à esquerda, escolha Buckets de diretórios.
4. Na lista Buckets de diretório, escolha o botão de opções ao lado do bucket que você deseja excluir.
5. Escolha Excluir.
6. Na página Excluir bucket, insira o nome do bucket no campo de texto para confirmar a exclusão do bucket.

> **Important**
>
> Não é possível desfazer a exclusão de um bucket.

7. Para excluir um bucket de diretório, escolha Excluir bucket.

Próximas etapas

Neste tutorial, você aprendeu a criar um bucket de diretório e usar a classe de armazenamento S3 Express One Zone. Depois de concluir este tutorial, você poderá explorar os serviços da AWS relacionados a serem usados com a classe de armazenamento S3 Express One Zone.

Você pode usar os seguintes Serviços da AWS com a classe de armazenamento S3 Express One Zone para oferecer suporte ao seu caso de uso específico de baixa latência.

- Amazon Elastic Compute Cloud (Amazon EC2): o Amazon EC2 oferece capacidade de computação segura e escalável na Nuvem AWS. O uso do Amazon EC2 reduz a necessidade de investimento antecipado em hardware. Por isso, você pode desenvolver e implantar aplicações com maior rapidez. É possível usar o Amazon EC2 para executar quantos servidores virtuais forem necessários, configurar a segurança e as redes e gerenciar o armazenamento.
- AWS Lambda: o Lambda é um serviço de computação que permite que você execute o código sem provisionar ou gerenciar servidores. Você define as configurações de notificação em um bucket e concede permissão ao Amazon S3 para invocar uma função na política de permissões baseada em recursos da função.
- Amazon Elastic Kubernetes Service (Amazon EKS): o Amazon EKS é um serviço gerenciado que elimina a necessidade de instalar, operar e manter o seu próprio ambiente de gerenciamento do Kubernetes na AWS. O Kubernetes é um sistema de código aberto que automatiza o gerenciamento, a escalação e a implantação de aplicações conteinerizadas.
- Amazon Elastic Container Service (Amazon ECS): o Amazon ECS é um serviço totalmente gerenciado de orquestração de contêineres que ajuda a implantar, gerenciar e dimensionar facilmente aplicações em contêineres.
- Amazon EMR: o Amazon EMR é uma plataforma de cluster gerenciada que simplifica a execução de frameworks de big data, como Apache Hadoop e Apache Spark, na AWS a fim de processar e analisar grandes volumes de dados.
- Amazon Athena: o Athena é um serviço de consultas interativas que facilita a análise de dados no Amazon S3 usando SQL padrão. Você também pode usar o Athena para executar análises

de dados de maneira interativa usando o Apache Spark sem a necessidade de planejamento, configuração ou gerenciamento de recursos. Ao executar aplicações do Apache Spark no Athena, você envia o código Spark para processamento e recebe os resultados de forma direta.

- AWS Glue Data Catalog: o AWS Glue é um serviço de integração de dados sem servidor que facilita aos usuários de analytics a descoberta, a preparação, a transferência e a integração de dados de várias fontes. É possível usar o AWS Glue para analytics, machine learning e desenvolvimento de aplicações. AWS O Glue Data Catalog é um repositório centralizado que armazena metadados sobre os conjuntos de dados da sua organização. Ele funciona como um índice para métricas de localização, esquema e runtime das fontes de dados.
- Treinamento de modelos do Amazon SageMaker Runtime: o Amazon SageMaker Runtime é um serviço de machine learning totalmente gerenciado. Com o SageMaker Runtime, cientistas de dados e desenvolvedores podem criar e treinar modelos de machine learning com rapidez e facilidade, depois implantá-los diretamente em um ambiente hospedado pronto para produção.

Para ter mais informações sobre a classe S3 Express One Zone, consulte O que é a classe S3 Express One Zone? e O que diferencia a classe S3 Express One Zone?

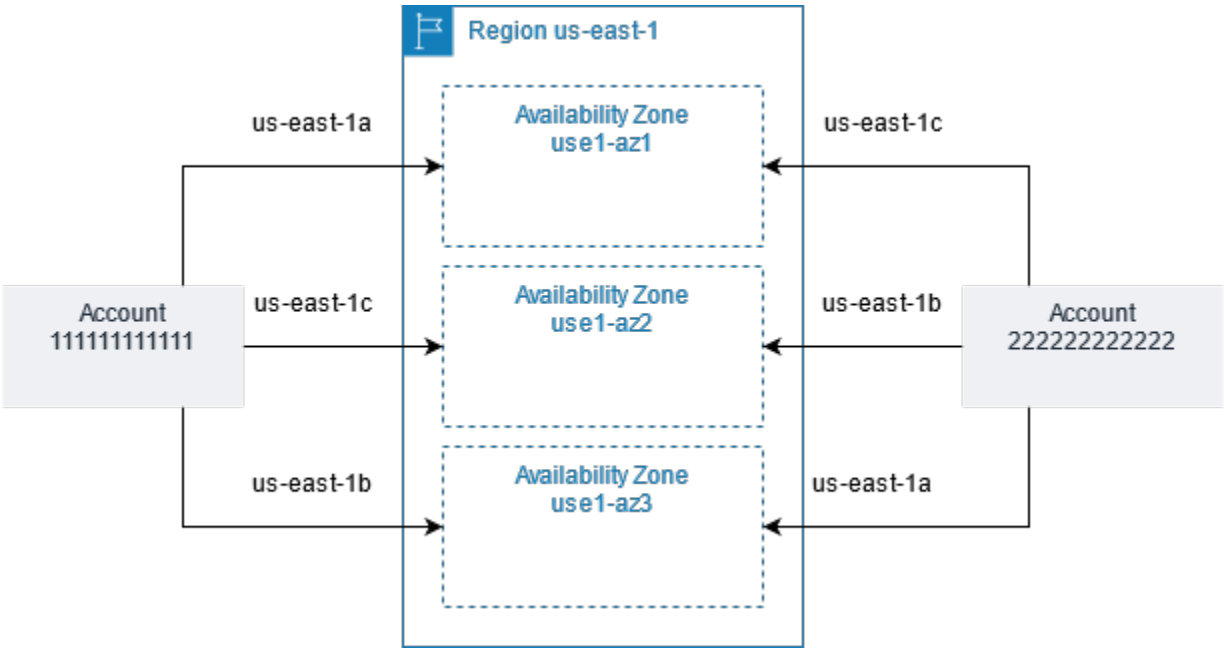
Zonas de disponibilidade e regiões da classe S3 Express One Zone

Uma zona de disponibilidade é um ou mais datacenters discretos com energia, redes e conectividade redundantes em uma Região da AWS. Para otimizar as recuperações de baixa latência, os objetos na classe de armazenamento Amazon S3 Express One Zone são armazenados de forma redundante em buckets de diretório do S3 em uma única zona de disponibilidade que seja local para sua workload computacional. Ao criar um bucket de diretório, escolha a zona de disponibilidade e a Região da AWS em que o bucket ficará localizado.

A AWS mapeia as zonas de disponibilidade físicas aleatoriamente em relação aos nomes das zonas de disponibilidade para cada Conta da AWS. Essa abordagem ajuda a distribuir recursos pelas zonas de disponibilidade em uma Região da AWS, em vez de os recursos provavelmente ficarem concentrados na primeira zona de disponibilidade de cada região. Como resultado, a zona de disponibilidade `us-east-1a` para sua Conta da AWS pode não representar a mesma localização física que `us-east-1a` para outra Conta da AWS. Para obter mais informações, consulte Regiões e Zonas de Disponibilidade no Guia do usuário do Amazon EC2.

Para coordenar as zonas de disponibilidade entre contas, use o ID da AZ que é um identificador exclusivo e consistente para uma zona de disponibilidade. Por exemplo, `use1-az1` é um ID de AZ para a região `us-east-1` e tem o mesmo local físico em cada Conta da AWS. A ilustração a seguir

mostra como os IDs da AZ são os mesmos para todas as contas, embora os nomes das zonas de disponibilidade possam ser mapeados de forma diferente para cada conta.



Com a classe S3 Express One Zone, os dados são armazenados de forma redundante em vários dispositivos dentro de uma única zona de disponibilidade. A classe S3 Express One Zone foi projetada para oferecer disponibilidade de 99,95% em uma única zona de disponibilidade e tem o respaldo do Acordo de Serviço do Amazon S3. Para obter mais informações, consulte Zonas de disponibilidade.

A tabela a seguir mostra as regiões e zonas de disponibilidade compatíveis com o S3 Express One Zone.

Nome da região	Código da região	ID da zona de disponibilidade				
Leste dos EUA (Norte da Virgínia)	`us-east-1`	`use1-az4`				
		`use1-az5`				
		`use1-az6`				
Leste dos EUA (Ohio)	`us-east-2`	`use2-az1`				
		`use2-az2`				

Nome da região	Código da região	ID da zona de disponibilidade				
Oeste dos EUA (Oregon)	us-west-2	usw2-az1				
		usw2-az3				
		usw2-az4				
Ásia-Pacífico (Mumbai)	ap-south-1	aps1-az1				
		aps1-az3				
Ásia-Pacífico (Tóquio)	ap-northeast-1	apne1-az1				
		apne1-az4				
Europa (Irlanda)	eu-west-1	euw1-az1				
		euw1-az3				
Europa (Estocolmo)	eu-north-1	eun1-az1				
		eun1-az2				
		eun1-az3				

Rede para buckets de diretório em uma zona de disponibilidade

Os tópicos a seguir descrevem os requisitos de rede para acessar a classe S3 Express One Zone usando um endpoint da VPC do gateway.

Tópicos

- Endpoints de buckets de diretório em zonas de disponibilidade
- Configurar endpoints de gateway da VPC

Endpoints de buckets de diretório em zonas de disponibilidade

A tabela a seguir mostra os endpoints de API regionais e zonais que estão disponíveis para cada região e zona de disponibilidade.

Configurar endpoints de gateway da VPC

Use o procedimento a seguir para criar um endpoint de gateway que se conecte aos objetos da classe de armazenamento Amazon S3 Express One Zone e aos buckets de diretório.

Como configurar um endpoint da VPC do gateway

1. Abra o console da Amazon VPC.
2. No painel de navegação, escolha Endpoints.
3. Escolha Criar endpoint.
4. Crie um nome para o endpoint.
5. Em Service category (Categoria de serviço), escolha Serviços da AWS.
6. Em Serviços, adicione o filtro Tipo=Gateway e escolha o botão de opções ao lado de com.amazonaws.***região***.s3express.
7. Em VPC, escolha a VPC na qual deseja criar o endpoint.
8. Em Route tables (Tabelas de rotas), selecione as tabelas de rotas a serem usadas pelo endpoint. O Amazon VPC adiciona automaticamente uma rota que aponta o tráfego destinado ao serviço para a interface de rede do endpoint.
9. Em Política, escolha Acesso total para permitir todas as operações de todas as entidades principais em todos os recursos no endpoint da VPC. Como alternativa, escolha Personalizado para anexar uma política de endpoint da VPC que controle as permissões das entidades principais para realizar ações em recursos pelo endpoint da VPC.
10. (Opcional) Para adicionar uma etiqueta, escolha Adicionar nova tag e insira a chave e o valor da etiqueta.
11. Escolha Criar endpoint.

Depois de criar um endpoint de gateway, você pode usar endpoints de API regionais e endpoints de API zonais para acessar objetos da classe de armazenamento Amazon S3 Express One Zone e buckets de diretório.

Criar buckets de diretório em uma zona de disponibilidade

Para começar a usar a classe de armazenamento Amazon S3 Express One Zone, crie um bucket de diretório. A classe de armazenamento S3 Express One Zone só pode ser usada com buckets de diretório. A classe de armazenamento S3 Express One Zone oferece suporte a casos de uso de baixa latência e fornece processamento de dados mais rápido em uma única zona de disponibilidade. Se sua aplicação é sensível à performance e se beneficia de latências inferiores a dez milissegundos para `PUT` e `GET`, recomendamos criar um bucket de diretório para que possa usar a classe de armazenamento S3 Express One Zone.

Há dois tipos de buckets do Amazon S3: buckets de uso geral e buckets de diretório. Você deve escolher o tipo de bucket que melhor se adapte aos requisitos de desempenho e da aplicação. Os buckets de uso geral são o tipo original de bucket do S3. Os buckets de uso geral são recomendados para a maioria dos casos de uso e padrões de acesso, permitindo que objetos sejam armazenados em todas as classes de armazenamento, exceto na classe S3 Express One Zone. Para obter mais informações sobre os buckets de uso geral, consulte Visão geral dos buckets de uso geral.

Os buckets de diretório usam a classe de armazenamento S3 Express One Zone, projetada para workloads ou aplicações de performance crítica que exigem latência consistente inferior a dez milissegundos. S3 Express One Zone é a primeira classe de armazenamento do S3 em que é possível selecionar uma única zona de disponibilidade com a opção de manter o armazenamento de objetos e os recursos de computação na mesma localização, o que fornece a maior velocidade de acesso possível. Ao criar um bucket de diretório, você tem a opção de especificar uma Região da AWS e uma zona de disponibilidade que seja local para suas instâncias computacionais do Amazon EC2, do Amazon Elastic Kubernetes Service ou do Amazon Elastic Container Service (Amazon ECS) a fim de otimizar a performance.

Com a classe S3 Express One Zone, os dados são armazenados de forma redundante em vários dispositivos dentro de uma única zona de disponibilidade. A classe S3 Express One Zone foi projetada para oferecer disponibilidade de 99,95% em uma única zona de disponibilidade e tem o respaldo do Acordo de Serviço do Amazon S3. Para obter mais informações, consulte Zonas de disponibilidade.

Os buckets de diretório organizam os dados de forma hierárquica em diretórios, ao contrário da estrutura de armazenamento plana dos buckets de uso geral. Não há limites de prefixo para os buckets de diretório, e diretórios individuais podem ser escalados horizontalmente.

Para obter mais informações sobre os buckets de diretório, consulte Trabalhar com buckets de diretório.

Nomes de bucket de diretório

Os nomes de bucket de diretório devem seguir o seguinte formato e estar em conformidade com as regras de nomenclatura para buckets de diretório:

```
bucket-base-name--zone-id--x-s3
```

Por exemplo, o seguinte nome de bucket de diretório contém o ID da zona de disponibilidade `usw2-az1`:

```
bucket-base-name--usw2-az1--x-s3
```

Para obter mais informações sobre as regras de nomenclatura para buckets de diretório, consulte Regras de nomenclatura de buckets de diretório.

Usar o console do S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Na barra de navegação na parte superior da página, escolha o nome da Região da AWS exibida no momento. Em seguida, escolha a região na qual você deseja criar um bucket.

   > **Note**
   >
   > Para reduzir a latência e os custos e atender aos requisitos regulatórios, selecione uma região perto de você. Os objetos armazenados em uma região nunca saem dessa região, a menos que você os transfira para outra região. Para obter uma lista de Regiões da AWS do Amazon S3, consulte Endpoints de AWS service (Serviço da AWS) no Referência geral da Amazon Web Services.

3. No painel de navegação à esquerda, escolha Buckets de diretórios.
4. Selecione Create bucket (Criar bucket). A página Create bucket (Criar bucket) é aberta.
5. Em Configuração geral, visualize a Região da AWS onde o bucket será criado.

   Em Tipo de bucket, escolha Diretório.

> **Note**
>
> - Se você escolher uma região que não oferece suporte a buckets de diretório, a opção Tipo de bucket desaparecerá e o tipo de bucket assumirá um bucket de uso geral como padrão. Para criar um bucket de diretório, escolha uma região compatível. Para obter uma lista de regiões que oferecem suporte a buckets de diretório e à classe de armazenamento Amazon S3 Express One Zone, consulte the section called “Zonas de disponibilidade e regiões da classe S3 Express One Zone”.
> - Depois de criar o bucket, não será possível alterar o tipo.

> **Note**
>
> A zona de disponibilidade não poderá ser alterada após a criação do bucket.

6. Em Zona de disponibilidade, escolha uma zona de disponibilidade que seja local para os seus serviços de computação. Para obter uma lista de zonas de disponibilidade que oferecem suporte a buckets de diretório e à classe de armazenamento S3 Express One Zone, consulte the section called “Zonas de disponibilidade e regiões da classe S3 Express One Zone”.

   Em Zona de disponibilidade, marque a caixa de seleção para indicar que, em caso de interrupção na zona de disponibilidade, seus dados poderão ficar indisponíveis ou ser perdidos.

   > **Important**
   >
   > Embora os buckets de diretório sejam armazenados em vários dispositivos dentro de uma única zona de disponibilidade, eles não armazenam dados de forma redundante entre zonas de disponibilidade.

7. Em Nome do bucket, insira um nome para o bucket de diretório.

   As regras de nomenclatura a seguir se aplicam a buckets de diretório.

   - O nome deve ser exclusivo na zona escolhida (zona de disponibilidade da AWS ou zona local da AWS).
   - O nome deve ter entre 3 (mín.) e 63 (máx.) caracteres, incluindo o sufixo.

- Consistir em letras minúsculas, números e hifens (-).
- Inicie e termine com uma letra ou um número.
- Deve incluir o seguinte sufixo: `--`*`zone-id`*`--x-s3`.
- O nome do bucket não deve iniciar com o prefixo `xn--`.
- O nome do bucket não deve iniciar com o prefixo `sthree-`.
- O nome do bucket não deve iniciar com o prefixo `sthree-configurator`.
- O nome do bucket não deve iniciar com o prefixo `amzn-s3-demo-`.
- Os nomes de bucket não podem terminar com o sufixo `-s3alias`. Esse sufixo se reserva a nomes de alias de ponto de acesso. Para obter mais informações, consulte Alias de ponto de acesso.
- Os nomes de bucket não podem terminar com o sufixo `--ol-s3`. Esse sufixo é reservado a nomes de alias de ponto de acesso de objeto do Lambda. Para obter mais informações, consulte Como usar um alias no estilo do bucket para o ponto de acesso do Object Lambda do bucket do S3.
- Os nomes de bucket não podem terminar com o sufixo `.mrap`. Esse sufixo é reservado para nomes de ponto de acesso de várias regiões. Para obter mais informações, consulte Regras para nomear pontos de acesso multirregionais do Amazon S3.

Um sufixo é adicionado automaticamente ao nome de base que você fornece ao criar um bucket de diretório usando o console. Esse sufixo inclui o ID da zona de disponibilidade que você escolheu.

Depois de criado o bucket, você não pode mudar seu nome. Para obter mais informações sobre como nomear buckets, consulte Regras de nomenclatura de buckets de uso geral.

> **Important**
>
> Não inclua informações confidenciais, como números de conta, no nome do bucket. O nome do bucket é visível nos URLs que apontam para os objetos no bucket.

8. Em Propriedade do objeto, a configuração Imposto pelo proprietário do bucket está habilitada automaticamente e todas as listas de controle de acesso (ACLs) estão desabilitadas. Para os buckets de diretório, não é possível habilitar ACLs.

Imposto pelo proprietário do bucket (padrão): as ACLs são desabilitadas e o proprietário do bucket automaticamente tem propriedade e controle total sobre todos os objetos do bucket de uso geral. As ACLs não afetam mais as permissões de acesso aos dados no bucket de uso geral do S3. O bucket usa políticas exclusivamente para definir o controle de acesso.

9. Em Configurações de bloqueio do acesso público deste bucket, todas as configurações da funcionalidade Bloqueio de Acesso Público para o bucket de diretório estão automaticamente habilitadas. Não é possível modificar essas configurações para buckets de diretório. Para obter mais informações sobre como bloquear o acesso público, consulte Bloquear o acesso público ao armazenamento do Amazon S3.
10. Para configurar a criptografia padrão, em Tipo de criptografia, selecione uma das seguintes opções:

    - Criptografia do lado do servidor com chave gerenciada pelo Amazon S3 (SSE-S3)
    - Criptografia do lado do servidor com chave do AWS Key Management Service (SSE-KMS)

    Para obter mais informações sobre como usar a criptografia no lado do servidor do Amazon S3 para criptografar seus dados, consulte Proteção e criptografia de dados.

    > **Important**
    >
    > Se você usar a opção SSE-KMS em sua configuração de criptografia padrão, estará sujeito à cota de solicitações por segundo (RPS) do AWS KMS. Para obter mais informações sobre as cotas do AWS KMS e como solicitar um aumento de cota, consulte Cotas no Guia do desenvolvedor do AWS Key Management Service.
    > Ao habilitar a criptografia padrão, poderá ser necessário atualizar a política de bucket. Para obter mais informações, consulte Usar criptografia SSE-KMS para operações entre contas.

11. Se você escolher Criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3), aparecerá Habilitado em Chave do bucket. As chaves de bucket do S3 são sempre habilitadas quando você configura o bucket de diretório para usar a criptografia padrão com SSE-S3. As chaves de bucket do S3 estão sempre habilitadas para operações `GET` e `PUT` em um bucket de diretório e não podem ser desabilitadas. Não são aceitas chaves de bucket do S3 quando você copia objetos criptografados por SSE-KMS de buckets de uso geral para buckets de diretório, de buckets de diretório para buckets de uso geral ou entre buckets de diretório, por meio de CopyObject, de UploadPartCopy, da operação Copy em Operações em Lote ou de

trabalhos de import. Nesse caso, o Amazon S3 faz uma chamada para o AWS KMS sempre que uma solicitação de cópia é feita para um objeto criptografado pelo KMS.

As chaves de bucket do S3 diminuem o custo de criptografia reduzindo o tráfego de solicitações do Amazon S3 para o AWS KMS. Para obter mais informações, consulte Redução do custo do SSE-KMS com chaves de bucket do Amazon S3.

12. Se você escolher Criptografia do lado do servidor com chave do AWS Key Management Service (SSE-KMS), em Chave do AWS KMS, especifique uma chave do AWS Key Management Service de uma das maneiras a seguir ou crie uma chave.

    - Para escolher uma chave do KMS na lista disponível, selecione Escolher entre suas AWS KMS keys e escolha sua Chave do KMS em AWS KMS keys disponíveis.

      Somente as suas chaves gerenciadas pelo cliente são exibidas nessa lista. Não é possível usar o Chave gerenciada pela AWS (`aws/s3`) em buckets de diretório. Para ter mais informações sobre chaves gerenciadas pelo cliente, consulte Chaves de clientes e chaves da AWS no Guia do desenvolvedor do AWS Key Management Service.
    - Para inserir o ARN ou o alias da chave do KMS, escolha Inserir ARN da AWS KMS key e insira o ARN ou o alias da chave do KMS em ARN da AWS KMS key.
    - Para criar uma chave gerenciada pelo cliente no console do AWS KMS, selecione Criar uma chave do KMS.

      Para ter mais informações sobre como criar uma AWS KMS key, consulte Criação de chaves no Guia do desenvolvedor do AWS Key Management Service.

    Important

    - A configuração de SSE-KMS só comporta uma chave gerenciada pelo cliente por bucket de diretório durante a vida útil do bucket. Não há suporte para Chave gerenciada pela AWS (`aws/s3`). Além disso, depois que você especifica uma chave gerenciada pelo cliente para SSE-KMS, não é possível substituí-la pela configuração de SSE-KMS do bucket.

      É possível identificar a chave gerenciada pelo cliente que você especificou para a configuração SSE-KMS do bucket, da seguinte forma:

      - Faça uma solicitação de operação de API `HeadObject` para encontrar o valor de `x-amz-server-side-encryption-aws-kms-key-id` em sua resposta.

Para usar uma nova chave gerenciada pelo cliente em seus dados, recomendamos copiar os objetos existentes em um novo bucket de diretório com uma nova chave gerenciada pelo cliente.

- Você só pode usar chaves do KMS disponíveis na mesma Região da AWS que o bucket. O console do Amazon S3 lista somente as primeiras 100 chaves do KMS na mesma região que o bucket. Para usar uma chave do KMS que não esteja listada, você deve inserir o ARN da chave do KMS. Se quiser usar uma chave do KMS que seja de propriedade de outra conta, primeiro você deverá ter permissão para usar a chave e, depois, inserir o ARN da chave do KMS. Para obter mais informações sobre permissões entre contas para chaves do KMS, consulte Criar chaves do KMS que outras contas podem usar no Guia do desenvolvedor do AWS Key Management Service. Para obter mais informações sobre a SSE-KMS, consulte Especificar a criptografia do lado do servidor com o AWS KMS (SSE-KMS) para novos uploads de objetos em buckets de diretório.
- Ao usar uma AWS KMS key para criptografia do lado do servidor em buckets de diretório, você deve escolher uma chave de criptografia do KMS simétrica. O Amazon S3 só é compatível com chaves do KMS de criptografia simétrica, e não com chaves assimétricas do KMS. Para ter mais informações, consulte Identificar chaves do KMS simétricas e assimétricas no Guia do desenvolvedor do AWS Key Management Service.

Para obter mais informações sobre como usar o AWS KMS com o Amazon S3, consulte Usar a criptografia do lado do servidor com chaves do AWS KMS (SSE-KMS) em buckets de diretório.

13. Escolha Criar bucket. Depois de criar o bucket, você pode adicionar arquivos e pastas a ele. Para obter mais informações, consulte the section called “Trabalhar com objetos em um bucket de diretório”.

Uso da SDKs AWS

SDK for Go

Este exemplo mostra como criar um bucket de diretório usando o AWS SDK para Go.

Example

```
var bucket = "..."

func runCreateBucket(c *s3.Client) {
    resp, err := c.CreateBucket(context.Background(), &s3.CreateBucketInput{
        Bucket: &bucket,
        CreateBucketConfiguration: &types.CreateBucketConfiguration{
            Location: &types.LocationInfo{
                Name: aws.String("usw2-az1"),
                Type: types.LocationTypeAvailabilityZone,
            },
            Bucket: &types.BucketInfo{
                DataRedundancy: types.DataRedundancySingleAvailabilityZone,
                Type:           types.BucketTypeDirectory,
            },
        },
    })
    var terr *types.BucketAlreadyOwnedByYou
    if errors.As(err, &terr) {
        fmt.Printf("BucketAlreadyOwnedByYou: %s\n", aws.ToString(terr.Message))
        fmt.Printf("noop...\n")
        return
    }
    if err != nil {
        log.Fatal(err)
    }

    fmt.Printf("bucket created at %s\n", aws.ToString(resp.Location))
}
```

SDK for Java 2.x

Este exemplo mostra como criar um bucket de diretório usando o AWS SDK for Java 2.x.

Example

```
public static void createBucket(S3Client s3Client, String bucketName) {

    //Bucket name format is {base-bucket-name}--{az-id}--x-s3
    //example: doc-example-bucket--usw2-az1--x-s3 is a valid name for a directory
 bucket created in
```

```
   //Region us-west-2, Availability Zone 2

   CreateBucketConfiguration bucketConfiguration =
CreateBucketConfiguration.builder()
            .location(LocationInfo.builder()
                    .type(LocationType.AVAILABILITY_ZONE)
                    .name("usw2-az1").build()) //this must match the Region and
Availability Zone in your bucket name
            .bucket(BucketInfo.builder()
                   .type(BucketType.DIRECTORY)
                   .dataRedundancy(DataRedundancy.SINGLE_AVAILABILITY_ZONE)
                   .build()).build();
   try {

            CreateBucketRequest bucketRequest =
CreateBucketRequest.builder().bucket(bucketName).createBucketConfiguration(bucketConfigurat
            CreateBucketResponse response = s3Client.createBucket(bucketRequest);
            System.out.println(response);
   }

   catch (S3Exception e) {
           System.err.println(e.awsErrorDetails().errorMessage());
           System.exit(1);
        }
   }
```

AWS SDK para JavaScript

Este exemplo mostra como criar um bucket de diretório usando o AWS SDK para JavaScript.

Example

```
// file.mjs, run with Node.js v16 or higher
// To use with the preview build, place this in a folder
// inside the preview build directory, such as /aws-sdk-js-v3/workspace/

import { S3 } from "@aws-sdk/client-s3";

const region = "us-east-1";
const zone = "use1-az4";
const suffix = `${zone}--x-s3`;
```

```
const s3 = new S3({ region });

const bucketName = `...--${suffix}`;

const createResponse = await s3.createBucket(
    { Bucket: bucketName,
      CreateBucketConfiguration: {Location: {Type: "AvailabilityZone", Name: zone},
      Bucket: { Type: "Directory", DataRedundancy: "SingleAvailabilityZone" }}
    }
   );
```

SDK para .NET

Este exemplo mostra como criar um bucket de diretório usando o SDK para .NET.

Example

```
using (var amazonS3Client = new AmazonS3Client())
{
    var putBucketResponse = await amazonS3Client.PutBucketAsync(new PutBucketRequest
    {

       BucketName = "DOC-EXAMPLE-BUCKET--usw2-az1--x-s3",
       PutBucketConfiguration = new PutBucketConfiguration
       {
         BucketInfo = new BucketInfo { DataRedundancy =
 DataRedundancy.SingleAvailabilityZone, Type = BucketType.Directory },
         Location = new LocationInfo { Name = "usw2-az1", Type =
 LocationType.AvailabilityZone }
       }
     }).ConfigureAwait(false);
}
```

SDK for PHP

Este exemplo mostra como criar um bucket de diretório usando o AWS SDK for PHP.

Example

```
require 'vendor/autoload.php';
```

```
$s3Client = new S3Client([

    'region'      => 'us-east-1',
]);


$result = $s3Client->createBucket([
    'Bucket' => 'doc-example-bucket--use1-az4--x-s3',
    'CreateBucketConfiguration' => [
        'Location' => ['Name'=> 'use1-az4', 'Type'=> 'AvailabilityZone'],
        'Bucket' => ["DataRedundancy" => "SingleAvailabilityZone" ,"Type" =>
 "Directory"]   ],
]);
```

SDK for Python

Este exemplo mostra como criar um bucket de diretório usando o AWS SDK para Python (Boto3).

Example

```
import logging
import boto3
from botocore.exceptions import ClientError

def create_bucket(s3_client, bucket_name, availability_zone):
    '''
    Create a directory bucket in a specified Availability Zone

    :param s3_client: boto3 S3 client
    :param bucket_name: Bucket to create; for example, 'doc-example-bucket--usw2-
az1--x-s3'
    :param availability_zone: String; Availability Zone ID to create the bucket in,
 for example, 'usw2-az1'
    :return: True if bucket is created, else False
    '''

    try:
        bucket_config = {
                'Location': {
                    'Type': 'AvailabilityZone',
                    'Name': availability_zone
                },
```

```
                'Bucket': {
                    'Type': 'Directory',
                    'DataRedundancy': 'SingleAvailabilityZone'
                }
            }
        s3_client.create_bucket(
            Bucket = bucket_name,
            CreateBucketConfiguration = bucket_config
        )
    except ClientError as e:
        logging.error(e)
        return False
    return True


if __name__ == '__main__':
    bucket_name = 'BUCKET_NAME'
    region = 'us-west-2'
    availability_zone = 'usw2-az1'
    s3_client = boto3.client('s3', region_name = region)
    create_bucket(s3_client, bucket_name, availability_zone)
```

SDK for Ruby

Este exemplo mostra como criar um bucket de diretório usando o AWS SDK para Ruby.

Example

```
s3 = Aws::S3::Client.new(region:'us-west-2')
s3.create_bucket(
  bucket: "bucket_base_name--az_id--x-s3",
  create_bucket_configuration: {
    location: { name: 'usw2-az1', type: 'AvailabilityZone' },
    bucket: { data_redundancy: 'SingleAvailabilityZone', type: 'Directory' }
  }
)
```

Como usar o AWS CLI

Este exemplo mostra como criar um bucket de diretório usando o AWS CLI. Para usar o comando, substitua os *espaços reservados para entrada do usuário* por suas próprias informações.

Ao criar um bucket de diretório, você deve fornecer detalhes de configuração e usar a seguinte convenção de nomenclatura: *bucket-base-name*--*zone-id*--x-s3.

```
aws s3api create-bucket
--bucket bucket-base-name--zone-id--x-s3
--create-bucket-configuration 'Location={Type=AvailabilityZone,Name=usw2-
az1},Bucket={DataRedundancy=SingleAvailabilityZone,Type=Directory}'
--region us-west-2
```

Para obter mais informações, consulte create-bucket na AWS Command Line Interface.

Endpoints regionais e zonais para buckets de diretório em uma zona de disponibilidade

Para acessar seus buckets de objetos e de diretório armazenados na classe de armazenamento S3 Express One Zone, use os endpoints da VPC de gateway. Os buckets de diretório usam endpoints de API regionais e zonais. Dependendo da operação de API do Amazon S3 usada, será necessário um endpoint regional ou zonal. Não há cobrança adicional pelo uso de endpoints do gateway.

As operações de API em nível de bucket (ou ambiente de gerenciamento) estão disponíveis por meio de endpoints regionais e são chamadas de operações de API do endpoint regional. Exemplos de operações de API de endpoint regional são `CreateBucket` e `DeleteBucket`.

Ao criar buckets de diretório armazenados na classe de armazenamento S3 Express One Zone, escolha a zona de disponibilidade em que o bucket ficará localizado. É possível usar operações de API de endpoint zonal para fazer upload e gerenciar os objetos no bucket de diretório.

As operações de API em nível de objeto (ou plano de dados) estão disponíveis por meio de endpoints zonais e são chamadas de operações de API do endpoint zonal. Exemplos de operações de API de endpoint zonal são `CreateSession` e `PutObject`.

Otimizar o desempenho da classe S3 Express One Zone

A classe Amazon S3 Express One Zone é uma classe de armazenamento de zona de disponibilidade (AZ) única e alta performance do S3 desenvolvida com o propósito específico de fornecer acesso consistente aos dados e com latência inferior a dez milissegundos para as aplicações mais sensíveis à latência. A classe S3 Express One Zone é a primeira classe de armazenamento do S3 que oferece a opção de manter o armazenamento de objetos de alto desempenho e os recursos de computação da AWS, como o Amazon Elastic Compute Cloud, o Amazon Elastic Kubernetes Service

e o Amazon Elastic Container Service, em uma única zona de disponibilidade. A manutenção dos recursos de armazenamento e computação na mesma localização otimiza a performance e os custos computacionais e acelera o processamento de dados.

A classe S3 Express One Zone oferece elasticidade de performance semelhante a outras classes de armazenamento do S3, mas com latências consistentes de solicitações de leitura e gravação do primeiro byte inferiores a dez milissegundos — até dez vezes mais rápidas do que a classe S3 Standard. A classe S3 Express One Zone foi projetada do zero para oferecer suporte a um throughput expansível até níveis agregados muito altos. A classe de armazenamento S3 Express One Zone usa uma arquitetura personalizada para otimizar a performance e oferecer latência de solicitações consistentemente baixa, armazenando dados em hardware de alta performance. O protocolo de objetos para a classe S3 Express One Zone foi aprimorado a fim de simplificar a autenticação e a sobrecarga de metadados.

Para reduzir ainda mais a latência e comportar até 2 milhões de leituras e até 200 mil gravações por segundo, a classe S3 One Zone armazena os dados em um bucket de diretório do Amazon S3. Por padrão, cada bucket de diretório comporta até 200 mil leituras e até 100 mil gravações por segundo. Se a workload exigir uma quantidade acima dos limites padrão de TPS, você poderá solicitar um aumento por meio do AWS Support.

A combinação de hardware e software de alta performance com propósito específico que oferece velocidade de acesso aos dados inferior a dez milissegundos e buckets de diretório escaláveis para um grande número de transações por segundo faz da classe S3 Express One Zone a melhor classe de armazenamento do Amazon S3 para operações com alto consumo de solicitações ou aplicações de performance crítica.

Os tópicos a seguir descrevem as diretrizes de práticas recomendadas e os padrões de design para otimizar a performance de aplicações que usam a classe de armazenamento S3 Express One Zone.

Tópicos

- Práticas recomendadas para otimizar a performance da classe S3 Express One Zone

Práticas recomendadas para otimizar a performance da classe S3 Express One Zone

Ao criar aplicações que fazem upload e recuperam objetos da classe Amazon S3 Express One Zone, siga as nossas diretrizes de práticas recomendadas para otimizar a performance. Para usar a classe de armazenamento S3 Express One Zone, é necessário criar um bucket de diretório do S3. A classe de armazenamento S3 Express One Zone não é compatível com buckets de uso geral do S3.

Para consultar as diretrizes de desempenho para todas as outras classes de armazenamento do Amazon S3 e para buckets de uso geral do S3, consulte Padrões de design de melhores práticas: otimização do desempenho do Amazon S3.

Para obter performance e escalabilidade ideais com a classe de armazenamento S3 Express One Zone e os buckets de diretório em workloads de alta escala, é importante entender em que sentido os buckets de diretório funcionam de forma diferente dos buckets de uso geral. Em seguida, fornecemos as práticas recomendadas para alinhar suas aplicações à forma como os buckets de diretório funcionam.

Como os buckets de diretório funcionam

A classe de armazenamento Amazon S3 Express One Zone pode comportar workloads com até 2 milhões de transações GET e até 200 mil transações PUT por segundo (TPS) por bucket de diretório. Com o S3 Express One Zone, os dados são armazenados em buckets de diretório do S3 em zonas de disponibilidade. Os objetos nos buckets de diretório podem ser acessados em um namespace hierárquico, de modo semelhante a um sistema de arquivos e diferentemente dos buckets de uso geral do S3, que têm um namespace simples. Ao contrário dos buckets de uso geral, os buckets de diretórios organizam as chaves hierarquicamente em diretórios em vez de prefixos. Um prefixo é uma string no início do nome da chave do objeto. Você pode usar prefixos para organizar os dados e gerenciar uma arquitetura de armazenamento de objetos simples em buckets de uso geral. Para obter mais informações, consulte Organizar objetos usando prefixos.

Nos buckets de diretório, os objetos são organizados em um namespace hierárquico usando a barra (`/`) como o único delimitador compatível. Quando você carrega um objeto com uma chave, como `dir1/dir2/file1.txt`, os diretórios `dir1/` e `dir2/` são automaticamente criados e gerenciados pelo Amazon S3. Os diretórios são criados durante as operações `CreateMultiPartUpload` ou `PutObject` e removidos automaticamente quando ficam vazios após após operações `DeleteObject` ou `AbortMultiPartUpload`. Não há limite máximo para o número de objetos e subdiretórios em um diretório.

Os diretórios criados quando os objetos são carregados em buckets de diretório podem ser escalados instantaneamente para reduzir a chance de erros HTTP `503 (Slow Down)`. Esse ajuste de escala automático permite que as aplicações emparelhem as solicitações de leitura e gravação dentro de um diretório e entre diretórios, conforme necessário. Para o S3 Express One Zone, os diretórios individuais são projetados para atender à taxa máxima de solicitações de um bucket de diretório. Não há necessidade de randomizar prefixos de chave para obter a performance ideal, pois o sistema distribui automaticamente os objetos para uma distribuição uniforme da carga, mas,

como resultado, as chaves não são armazenadas lexicograficamente em buckets de diretório. Isso ocorre de maneira diferente nos buckets de uso geral do S3, nos quais as chaves que estão lexicograficamente mais próximas têm maior probabilidade de serem colocadas no mesmo servidor.

Para ter mais informações sobre exemplos de operações de bucket de diretório e interações de diretório, consulte Exemplos de operação de bucket de diretório e interação de diretórios.

Práticas recomendadas

Siga as práticas recomendadas para otimizar a performance do bucket de diretório e ajudar a escalar suas workloads ao longo do tempo.

Usar diretórios que contenham várias entradas (objetos ou subdiretórios)

Os buckets de diretório oferecem alta performance por padrão para todas as workloads. Para otimizar ainda mais a performance com determinadas operações, a consolidação de mais entradas (que são objetos ou subdiretórios) nos diretórios diminuirá a latência e aumentará a taxa de solicitações:

- Operações de API mutantes, como `PutObject`, `DeleteObject`, `CreateMultiPartUpload` e `AbortMultiPartUpload`, alcançam uma performance ideal quando implementadas com uma quantidade menor de diretórios mais densos que contenham milhares de entradas, em vez de com um grande número de diretórios menores.
- As operações `ListObjectsV2` funcionam melhor quando menos diretórios precisam ser percorridos para preencher uma página de resultados.

Não usar entropia em prefixos

Nas operações do Amazon S3, a entropia se refere à aleatoriedade na nomenclatura de prefixos que ajuda a distribuir workloads uniformemente entre as partições de armazenamento. No entanto, como os buckets de diretório gerenciam internamente a distribuição de carga, não é recomendável usar entropia em prefixos para obter a melhor performance. Isso ocorre porque, em buckets diretório, a entropia pode fazer com que as solicitações fiquem mais lentas por não reutilizar os diretórios que já foram criados.

Um padrão de chave como `$HASH/directory/object` pode acabar criando muitos diretórios intermediários. No exemplo a seguir, todos os trabalhos `job-1` são diretórios diferentes, pois os principais são diferentes. Os diretórios serão esparsos e as solicitações de mutação e lista serão mais lentas. Neste exemplo, há 12 diretórios intermediários, todos com uma única entrada.

```
s3://my-bucket/0cc175b9c0f1b6a831c399e269772661/job-1/file1

s3://my-bucket/92eb5ffee6ae2fec3ad71c777531578f/job-1/file2

s3://my-bucket/4a8a08f09d37b73795649038408b5f33/job-1/file3

s3://my-bucket/8277e0910d750195b448797616e091ad/job-1/file4

s3://my-bucket/e1671797c52e15f763380b45e841ec32/job-1/file5

s3://my-bucket/8fa14cdd754f91cc6554c9e71929cce7/job-1/file6
```

Em vez disso, para melhorar a performance, podemos remover o componente `$HASH` e permitir que `job-1` se torne um único diretório, melhorando a densidade de um diretório. No exemplo a seguir, o único diretório intermediário que tem seis entradas pode aumentar a performance, em comparação com o exemplo anterior.

```
s3://my-bucket/job-1/file1

s3://my-bucket/job-1/file2

s3://my-bucket/job-1/file3

s3://my-bucket/job-1/file4

s3://my-bucket/job-1/file5

s3://my-bucket/job-1/file6
```

Essa vantagem de performance ocorre porque, quando uma chave de objeto é criada e seu nome inclui um diretório, o diretório é criado automaticamente para o objeto. Os uploads subsequentes de objetos para o mesmo diretório não exigirão que o diretório seja criado, o que reduzirá a latência dos uploads de objetos nos diretórios existentes.

Usar um separador diferente do delimitador / para separar partes da chave se não for necessário agrupar objetos logicamente durante as chamadas **`ListObjectsV2`**

Como o delimitador `/` é tratado especialmente para buckets de diretório, ele deve ser usado com propósito. Embora os buckets de diretório não ordenem objetos lexicograficamente, os objetos dentro de um diretório ainda assim são agrupados nas saídas de `ListObjectsV2`. Se você não precisar

dessa funcionalidade, poderá substituir / por outro caractere como separador para não provocar a criação de diretórios intermediários.

Por exemplo, suponha que as seguintes chaves estejam em um padrão de prefixo YYYY/MM/DD/HH/:

```
s3://my-bucket/2024/04/00/01/file1

s3://my-bucket/2024/04/00/02/file2

s3://my-bucket/2024/04/00/03/file3

s3://my-bucket/2024/04/01/01/file4

s3://my-bucket/2024/04/01/02/file5

s3://my-bucket/2024/04/01/03/file6
```

Se você não precisar agrupar objetos por hora ou dia nos resultados de `ListObjectsV2`, mas precisar agrupar objetos por mês, o padrão de chave YYYY/MM/DD-HH- a seguir gerará um número significativamente menor de diretórios e melhorará a performance para a operação `ListObjectsV2`.

```
s3://my-bucket/2024/04/00-01-file1

s3://my-bucket/2024/04/00-01-file2

s3://my-bucket/2024/04/00-01-file3

s3://my-bucket/2024/04/01-02-file4

s3://my-bucket/2024/04/01-02-file5

s3://my-bucket/2024/04/01-02-file6
```

Usar operações de lista delimitada sempre que possível

Uma solicitação `ListObjectsV2` sem um `delimiter` executa uma travessia recursiva no modo primeiro em profundidade em todos os diretórios. Uma solicitação `ListObjectsV2` com um `delimiter` recupera somente entradas no diretório especificado pelo parâmetro `prefix`, reduzindo a latência da solicitação e aumentando as chaves agregadas por segundo. Para buckets de diretório,

use operações de lista delimitada sempre que possível. As listas delimitadas fazem com que os diretórios sejam visitados menos vezes, o que aumenta a quantidade de chaves por segundo e diminui a latência das solicitações.

Por exemplo, para os seguintes diretórios e objetos em seu bucket de diretório:

```
s3://my-bucket/2024/04/12-01-file1

s3://my-bucket/2024/04/12-01-file2

...

s3://my-bucket/2024/05/12-01-file1

s3://my-bucket/2024/05/12-01-file2

...

s3://my-bucket/2024/06/12-01-file1

s3://my-bucket/2024/06/12-01-file2

...

s3://my-bucket/2024/07/12-01-file1

s3://my-bucket/2024/07/12-01-file2

...
```

Para melhorar a performance de `ListObjectsV2`, use uma lista delimitada para listar seus subdiretórios e objetos, se a lógica da aplicação permitir. Por exemplo, você pode executar o seguinte comando para a operação de lista delimitada:

```
aws s3api list-objects-v2 --bucket my-bucket --prefix '2024/' --delimiter '/'
```

A saída é a lista de subdiretórios.

```
{
    "CommonPrefixes": [
        {
```

```
            "Prefix": "2024/04/"
        },
        {
            "Prefix": "2024/05/"
        },
        {
            "Prefix": "2024/06/"
        },
        {
            "Prefix": "2024/07/"
        }
    ]
}
```

Para listar cada subdiretório com melhor performance, execute um comando como o mostrada no seguinte exemplo:

Comando:

```
aws s3api list-objects-v2 --bucket my-bucket --prefix '2024/04' --delimiter '/'
```

Saída:

```
{
    "Contents": [
        {
            "Key": "2024/04/12-01-file1"
        },
        {
            "Key": "2024/04/12-01-file2"
        }
    ]
}
```

Implantar o armazenamento da classe S3 Express One Zone na mesma localização dos recursos de computação

Com o S3 Express One Zone, cada bucket de diretório fica localizado em uma única zona de disponibilidade que você seleciona ao criar o bucket. Primeiro você pode criar um bucket de diretório em uma zona de disponibilidade local para workloads ou recursos de computação. Depois, você pode iniciar imediatamente leituras e gravações de latência muito baixa. Os buckets de diretório são

um tipo de bucket do S3 em que você pode escolher a zona de disponibilidade em uma Região da AWS para reduzir a latência entre computação e armazenamento.

Se você acessar buckets de diretório entre zonas de disponibilidade, poderá experimentar um pequeno aumento na latência. Para otimizar a performance, recomendamos que você acesse um bucket de diretório por instâncias do Amazon Elastic Container Service, do Amazon Elastic Kubernetes Service e do Amazon Elastic Compute Cloud que estejam localizadas na mesma zona de disponibilidade, sempre que possível.

Usar conexões simultâneas para obter alto throughput com objetos acima de 1 MB

O melhor desempenho pode ser atingido com a emissão de várias solicitações simultâneas para buckets de diretório a fim de distribuir as solicitações em conexões separadas e maximizar a largura de banda acessível. Como os buckets de uso geral, a classe S3 Express One Zone não tem nenhum limite para o número de conexões feitas com o bucket de diretório. Diretórios individuais podem escalar a performance horizontal e automaticamente quando ocorre um grande número de gravações simultâneas no mesmo diretório.

As conexões TCP individuais com buckets de diretório têm um limite superior fixo no número de bytes que podem ser carregados ou baixados por segundo. Quando os objetos ficam maiores, o tempo de solicitação é controlado pelo streaming de bytes, e não pelo processamento de transações. Para usar várias conexões para paralelizar o upload ou o download de objetos maiores, você pode reduzir a latência de ponta a ponta. Se estiver usando o SDK da `Java 2.x`, considere usar o Gerenciador de transferências do S3, que aproveitará as melhorias de performance, como as operações de API de multipart upload e as consultas em escala de bytes, para acessar os dados em paralelo.

Endpoints da VPC de gateway

Os endpoints de gateway oferecem uma conexão direta entre a VPC e os buckets de diretório, sem a necessidade de um gateway da internet ou de um dispositivo NAT para a VPC. Para reduzir o tempo que seus pacotes permanecem na rede, você deve configurar a VPC com um endpoint da VPC de gateway para buckets de diretório. Para obter mais informações, consulte Rede para buckets de diretório.

Usar a autenticação de sessão e reutilizar os tokens de sessão enquanto estiverem válidos

Os buckets de diretório oferecem um mecanismo de autenticação de token de sessão para reduzir a latência em operações de API sensíveis à performance. Você pode fazer uma única chamada

`CreateSession` para obter um token de sessão válido para todas as solicitações nos próximos 5 minutos. Para obter a menor latência em suas chamadas de API, adquira um token de sessão e reutilize-o durante toda a vida útil desse token antes de atualizá-lo.

Se você usar SDKs da AWS, as atualizações de token de sessão serão feitas automaticamente pelo SDK para evitar interrupções no serviço quando uma sessão expirar. Recomendamos que você use os SDKs da AWS para iniciar e gerenciar solicitações para a operação de API `CreateSession`.

Para obter mais informações sobre o `CreateSession`, consulte Autorizar operações de API de endpoint zonal com `CreateSession`.

Usar um cliente baseado em CRT

O AWS Common Runtime (CRT) é um conjunto de bibliotecas modulares e eficientes escritas em C e destinadas a atuar como base dos SDKs da AWS. O CRT oferece throughput aprimorado, melhor gerenciamento de conexão e tempos de inicialização mais rápidos. Ele está disponível em todos os SDKs da AWS, exceto no Go.

Para ter mais informações sobre como configurar o CRT para o SDK que você usa, consulte AWS Common Runtime (CRT) libraries, Accelerate Amazon S3 throughput with the AWS Common Runtime, Introducing CRT-based S3 client and the S3 Transfer Manager in the AWS SDK for Java 2.x, Using S3CrtClient for Amazon S3 operations e Configure AWS CRT-based HTTP clients.

Usar a versão mais recente dos SDKs da AWS

Os AWS SDKs fornecem suporte integrado a muitas da diretrizes recomendadas para otimizar a performance do Amazon S3. Os SDKs oferecem uma API mais simples para aproveitar o Amazon S3 em uma aplicação e são atualizados regularmente para seguir as práticas recomendadas mais recentes. Por exemplo, os SDKs repetem automaticamente as solicitações após erros HTTP `503` e lidam com respostas de conexões lentas.

Se estiver usando o SDK da `Java 2.x`, considere usar o Gerenciador de transferências do S3, que escala horizontalmente as conexões de maneira automática para atingir milhares de solicitações por segundo usando solicitações em escala de bytes quando apropriado. As solicitações em escala de bytes podem melhorar a performance porque você pode usar conexões simultâneas com o S3 para consultar escalas de bytes diferentes no mesmo objeto. Isso ajuda a atingir um throughput agregado maior em comparação com uma única solicitação de objeto inteiro. É importante usar a última versão dos SDKs da AWS para obter os recursos mais recentes de otimização de performance.

Solução de problemas de performance

Você está definindo as solicitações de nova tentativa para aplicações sensíveis à latência?

A classe S3 Express One Zone foi desenvolvida com o propósito específico de oferecer níveis consistentes de alta performance sem ajustes adicionais. No entanto, definir valores agressivos de tempo limite e novas tentativas pode ajudar ainda mais a impulsionar níveis consistentes de latência e desempenho. Os AWS SDKs têm valores configuráveis de tempo limite e repetição que podem ser ajustados de acordo com as tolerâncias da aplicação específica.

Você está usando bibliotecas do AWS Common Runtime (CRT) e tipos ideais de instância do Amazon EC2?

As aplicações que executam um grande número de operações de leitura e gravação provavelmente precisam de mais memória ou capacidade de computação do que as aplicações que não o fazem. Ao inicializar as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) para uma workload que exige muita performance, escolha tipos de instância com a quantidade desses recursos que a aplicação precisa. O armazenamento de alta performance da classe S3 Express One Zone apresenta combinação ideal com tipos de instância maiores e mais novos, com quantidades maiores de memória do sistema e CPUs e GPUs mais poderosas que podem aproveitar o armazenamento de alta performance. Também recomendamos usar as versões mais recentes dos AWS SDKs habilitados para CRT, que podem acelerar ainda mais as solicitações de leitura e gravação em paralelo.

Você está usando SDKs da AWS para autenticação baseada em sessão?

Com o Amazon S3, você também pode otimizar a performance ao usar solicitações da API REST HTTP seguindo as mesmas práticas recomendadas que fazem parte dos AWS SDKs. No entanto, com o mecanismo de autorização e autenticação baseado em sessão usado pela classe S3 Express One Zone, é altamente recomendável que você use os AWS SDKs para gerenciar `CreateSession` e o respectivo token de sessão gerenciada. Os AWS SDKs criam e atualizam tokens automaticamente em seu nome usando a operação de API `CreateSession`. O uso de `CreateSession` gera economia na latência de ida e volta por solicitação para que o AWS Identity and Access Management (IAM) autorize cada solicitação.

Exemplos de operação de bucket de diretório e interação de diretórios

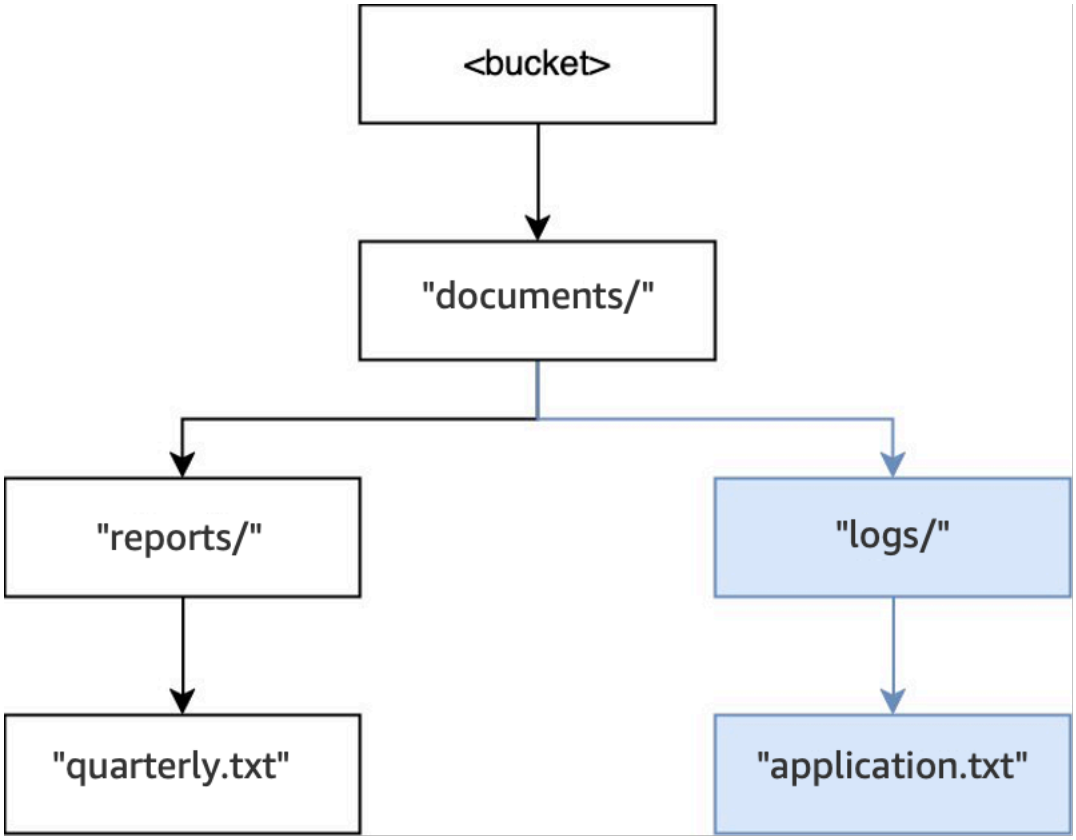
Veja a seguir três exemplos sobre como os buckets de diretório funcionam.

Exemplo 1: como as solicitações **`PutObject`** do S3 para um bucket de diretório interagem com os diretórios

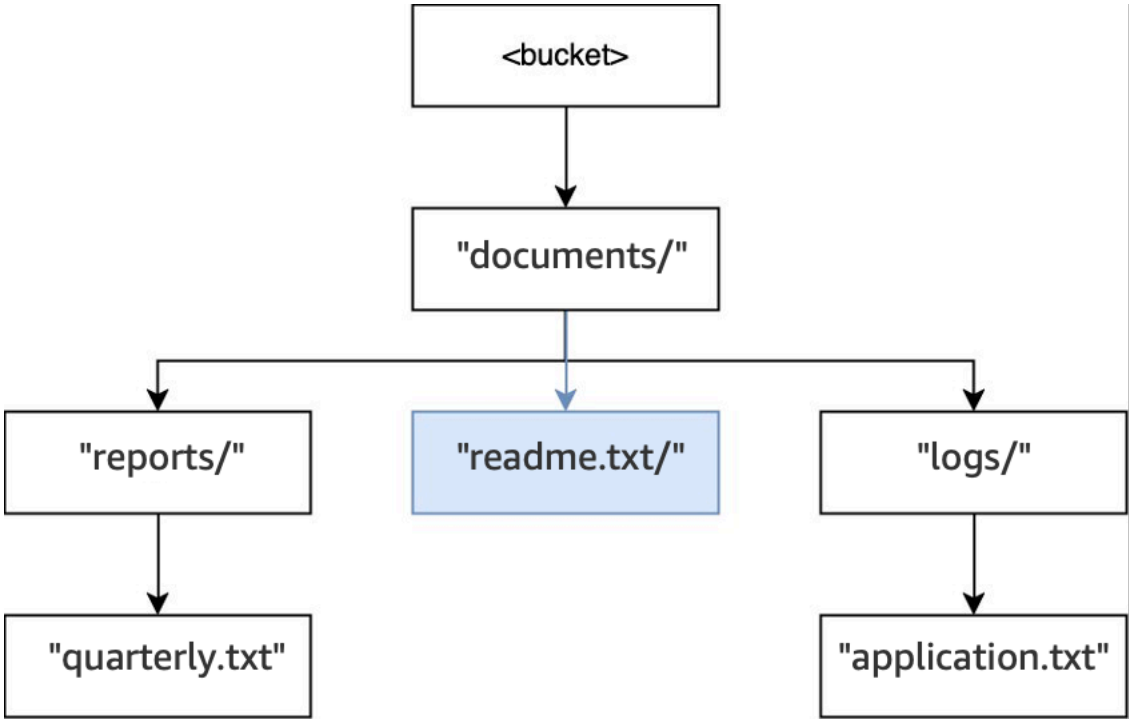
1. Quando a operação `PUT(<bucket>, "documents/reports/quarterly.txt")` é executada em um bucket vazio, o diretório `documents/` na raiz do bucket é criado, o diretório `reports/` em `documents/` é criado e o objeto `quarterly.txt` em `reports/` é criado. Para essa operação, além do objeto, foram criados dois diretórios.



2. Portanto, quando outra operação `PUT(<bucket>, "documents/logs/application.txt")` é executada, o diretório `documents/` já existe, o diretório `logs/` em `documents/` não existe e é criado e o objeto `application.txt` em `logs/` é criado. Para essa operação, além do objeto, foram criados dois diretórios.



3. Por fim, quando uma operação `PUT(<bucket>, "documents/readme.txt")` é executada, o diretório `documents/` na raiz já existe e o objeto `readme.txt` é criado. Para essa operação, nenhum diretório é criado.



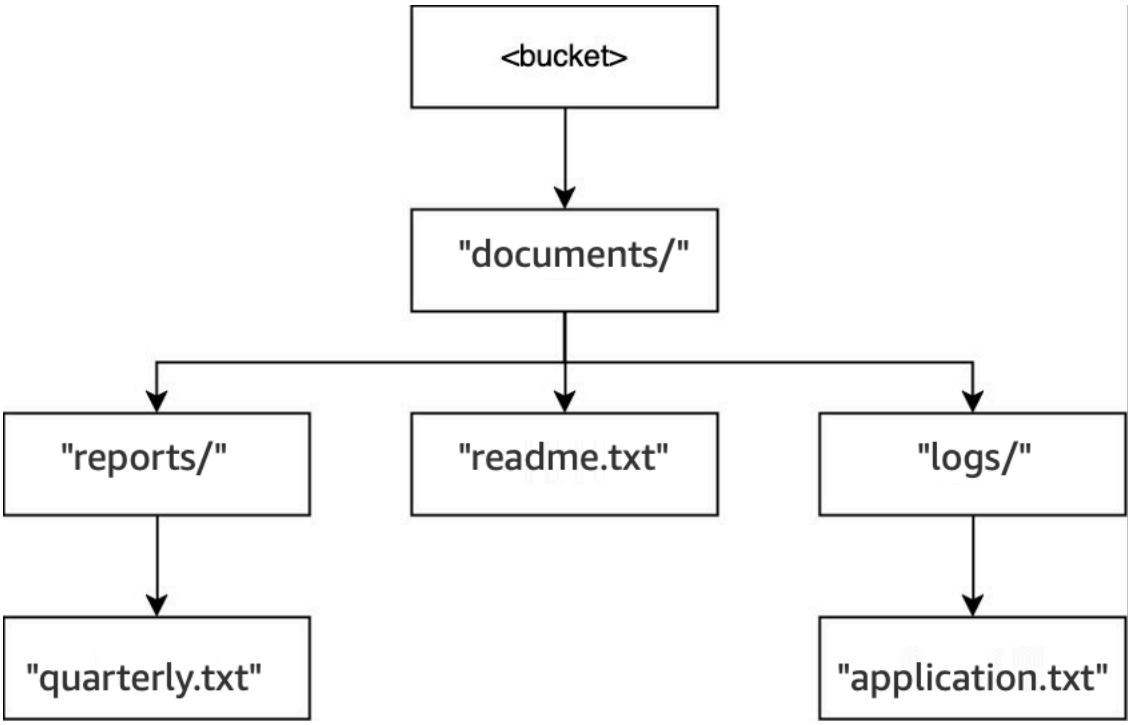
Exemplo 2: como as solicitações **ListObjectsV2** do S3 para um bucket de diretório interagem com os diretórios

Para as solicitações `ListObjectsV2` do S3 sem a especificação de um delimitador, o bucket é percorrido de acordo com o modo primeiro em profundidade. As saídas são retornadas em uma ordem consistente. No entanto, embora essa ordem permaneça a mesma entre as solicitações, ela não é lexicográfica. Para o bucket e os diretórios criados no exemplo anterior:

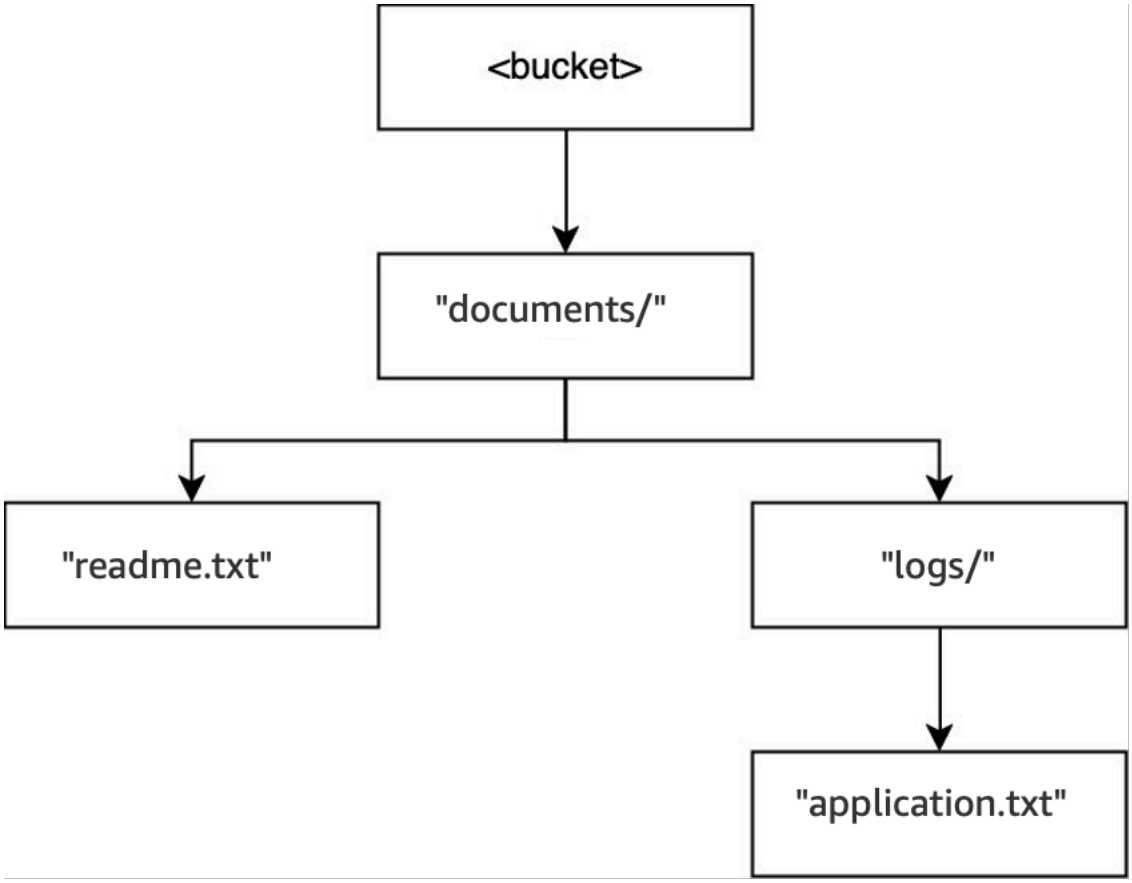
1. Quando `LIST(<bucket>)` é executada, o diretório `documents/` é inserido e a travessia começa.
2. O subdiretório `logs/` é inserido e a travessia começa.
3. O objeto `application.txt` é encontrado em `logs/`.
4. Não existem mais entradas em `logs/`. A operação List sai de `logs/` e entra em `documents/` novamente.
5. O diretório `documents/` continua sendo percorrido e o objeto `readme.txt` é encontrado.
6. O diretório `documents/` continua sendo percorrido, o subdiretório `reports/` é inserido e a travessia começa.
7. O objeto `quarterly.txt` é encontrado em `reports/`.
8. Não existem mais entradas em `reports/`. List sai de `reports/` e entra em `documents/` novamente.
9. Não existem mais entradas em `documents/` e a operação List retorna.

Neste exemplo, `logs/` é colocado antes de `readme.txt` e `readme.txt` é colocado antes de `reports/`.

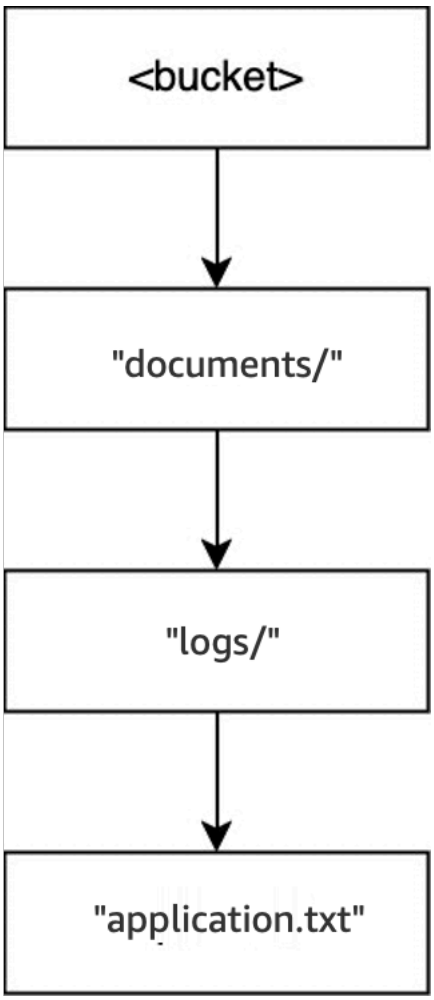
Exemplo 3: como as solicitações **`DeleteObject`** do S3 para um bucket de diretório interagem com os diretórios



1. Nesse mesmo bucket, quando a operação `DELETE(<bucket>, "documents/reports/quarterly.txt")` é executada, o objeto `quarterly.txt` é excluído, deixando o diretório `reports/` vazio e fazendo com que ele seja excluído imediatamente. O diretório `documents/` não está vazio porque tem o diretório `logs/` e o objeto `readme.txt` dentro dele; portanto, não é excluído. Nessa operação, somente um objeto e um diretório foram excluídos.



2. Quando a operação `DELETE(<bucket>, "documents/readme.txt")` é executada, o objeto `readme.txt` é excluído. `documents/` ainda não está vazio porque contém o diretório `logs/`; portanto, não foi excluído. Nessa operação, nenhum diretório é excluído e somente o objeto é excluído.



3. Por fim, quando a operação `DELETE(<bucket>, "documents/logs/application.txt")` é executada, `application.txt` é excluído, deixando `logs/` vazio e fazendo com que ele seja excluído imediatamente. Isso então deixa `documents/` vazio e faz com que ele também seja excluído imediatamente. Nessa operação, dois diretórios e um objeto são excluídos. O bucket agora está vazio.



Workloads de residência de dados

As zonas locais dedicadas da AWS são um tipo de infraestrutura da AWS totalmente gerenciada pela AWS, criada para uso exclusivo por você ou pela sua comunidade e colocada em um local ou data center especificado por você para ajudar a cumprir os requisitos regulatórios. As zonas locais

dedicadas são um tipo de oferta de zonas locais da AWS. Para ter mais informações, consulte Zonas locais dedicadas da AWS.

Nas zonas locais dedicadas, você pode criar buckets de diretório do S3 para armazenar dados em um perímetro de dados específico, o que ajuda a oferecer suporte a casos de uso de isolamento e residência de dados. Os buckets de diretório em zonas locais dedicadas podem comportar classes de armazenamento S3 Express One Zone e S3 One Zone-Infrequent Access (S3 One Zone-IA; Z-IA). Os buckets de diretório ainda não estão disponíveis em outras Localizações de zonas locais da AWS.

Você pode usar o AWS Management Console, a API REST, a AWS Command Line Interface (AWS CLI) e os AWS SDKs nas zonas locais dedicadas.

Para ter mais informações sobre como trabalhar com buckets de diretório em zonas locais, consulte os seguintes tópicos:

Tópicos

- Conceitos para buckets de diretório em zonas locais
- Habilitar contas para zonas locais
- Conectividade privada de uma VPC
- Criar um bucket de diretório em uma zona local
- Autenticação e autorização para buckets de diretório em zonas locais

Conceitos para buckets de diretório em zonas locais

Antes de criar um bucket de diretório em uma zona local, você deve saber o ID da zona local onde você deseja criar um bucket. Você pode encontrar informações sobre todas as zonas locais usando a operação de API DescribeAvailabilityZones. Essa operação de API fornece informações sobre as zonas locais, incluindo os IDs de zona local, nomes de região principal, grupos de borda de rede e status de adesão. Assim que você tiver o ID da zona local e tiver aderido, poderá criar um bucket de diretório na zona local. Um nome de bucket de diretório consiste em um nome base que você fornece e um sufixo que contém o ID da zona em que o bucket está localizado, seguido de `--x-s3`.

Uma zona local é conectada à região principal usando a rede privada redundante e de banda altamente larga da Amazon. Isso concede às aplicações em execução na zona local acesso rápido, seguro e contínuo aos demais Serviços da AWS na região principal. O ID da zona principal é o ID da zona que lida com as operações do ambiente de gerenciamento da zona Local. O grupo de

fronteira da rede é um grupo exclusivo do qual a AWS anuncia endereços IP públicos. Para ter mais informações sobre as zonas locais, a região principal e o ID da zona principal, consulte AWS Local Zones concepts no AWS Local Zones User Guide.

Todos os buckets de diretório usam o namespace `s3express`, que é separado do namespace `s3` para buckets de uso geral. Para buckets de diretório, as solicitações são roteadas para um endpoint regional ou um endpoint zonal. O roteamento é feito automaticamente para você se usar o AWS Management Console, a AWS CLI ou os AWS SDKs.

A maioria da operações de API em nível de bucket (como `CreateBucket` e `DeleteBucket`) é roteada para endpoints regionais e são chamadas de operações de API de endpoint regional. Os endpoints regionais estão no formato `s3express-control.ParentRegionCode.amazonaws.com`. Todas as operações de API ao nível do objeto (como `PutObject`) e duas operações de API ao nível do bucket (`CreateSession` e `HeadBucket`) são roteadas para endpoints zonais e são chamadas de operações de API de endpoint zonal. Os endpoints zonais estão no formato `s3express-LocalZoneID.ParentRegionCode.amazonaws.com`. Para conferir uma lista completa das operações de API por tipo de endpoint, consulte Operações de API de bucket de diretório.

O S3 está disponível na zona local de Pequim:

ID da zona local: `cnn1-pkx1-az1`

- Nome da região principal: `China (Beijing)`
- Código da região principal: `cn-north-1`
- IDs de zona principal: `cnn1-az1`
- Nome da zona Local: `China (Beijing)`
- Código de zona local: `cnn1-pkx1-az1`
- Grupo de borda de rede: `cn-north-1-pkx-1`
- Exemplo de ARN de bucket: `arn:aws-cn:s3express:cn-north-1:`*`123456789012`*`:bucket/`*`amzn-s3-demo-bucket`*`--cnn1-pkx1-az1--x-s3`
- Endpoint regional: `s3express-control.cn-north-1.amazonaws.com.cn`
- Endpoint zonal: `s3express-cnn1-pkx1-az1.cn-north-1.amazonaws.com.cn`

Categoria de armazenamento: `S3 One Zone-Infrequent Access (S3 One Zone-IA; Z-IA)`

Para acessar os buckets de diretório em zonas locais por meio de uma nuvem privada virtual (VPC), você pode usar os endpoints da VPC de gateway. Não há cobrança adicional pelo uso de endpoints do gateway. Para configurar endpoints da VPC de gateway para acessar buckets de diretório e objetos em zonas locais, consulte Conectividade privada de uma VPC.

Habilitar contas para zonas locais

O tópico a seguir descreve como as contas são habilitadas para zonas locais dedicadas.

Para todos os serviços em zonas locais dedicadas da AWS, incluindo o Amazon S3, seu administrador deve habilitar sua Conta da AWS antes que você possa criar ou acessar qualquer recurso na zona local dedicada. Você pode usar a operação de API DescribeAvailabilityZones para confirmar o acesso do ID da sua conta a uma zona local.

Para proteger ainda mais os dados no Amazon S3, por padrão, você só tem acesso aos recursos do S3 que você cria. Os buckets em zonas locais têm todas as configurações da funcionalidade Bloqueio de Acesso Público do S3 habilitadas por padrão e a funcionalidade Propriedade do Objetos do S3 está definida como Imposto pelo proprietário do bucket. Essas configurações não podem ser modificadas. Opcionalmente, para restringir o acesso a apenas os grupos de fronteira da rede da zona local, você pode usar a chave de condição `s3express:AllAccessRestrictedToLocalZoneGroup` nas políticas do IAM. Para obter mais informações, consulte Autenticação e autorização para buckets de diretório em zonas locais.

Conectividade privada de uma VPC

É possível usar um endpoint de gateway para acessar buckets de diretório em zonas locais da AWS por meio de uma nuvem privada virtual (VPC), sem precisar de um gateway da internet ou de um dispositivo NAT para a VPC, e sem nenhum custo adicional. O tópico a seguir descreve a configuração de endpoints da VPC de gateway entre uma VPC e buckets de diretório em zonas locais.

Como configurar um endpoint da VPC do gateway

1. Abra o console da Amazon VPC.
2. No painel de navegação, escolha Endpoints.
3. Escolha Criar endpoint.

4. Crie um nome para o endpoint.
5. Em Service category (Categoria de serviço), escolha Serviços da AWS.
6. Em Serviços, adicione o filtro Tipo=Gateway e escolha o botão de opções ao lado de com.amazonaws.***região***.s3express.
7. Em VPC, escolha a VPC na qual deseja criar o endpoint.
8. Em Tabelas de rotas, selecione a tabela de rotas a ser usada pelo endpoint na zona local. Depois que o endpoint for criado, um registro de rota será adicionado à tabela de rotas selecionada nesta etapa.
9. Em Política, escolha Acesso total para permitir todas as operações de todas as entidades principais em todos os recursos no endpoint da VPC. Como alternativa, escolha Personalizado para anexar uma política de endpoint da VPC que controle as permissões das entidades principais para realizar ações em recursos pelo endpoint da VPC.
10. (Opcional) Para adicionar uma etiqueta, escolha Adicionar nova tag e insira a chave e o valor da etiqueta.
11. Escolha Criar endpoint.

Para saber mais sobre endpoints da VPC de gateway, consulte Gateway endpoints no Guia do usuário do AWS PrivateLink. Para os casos de uso de residência de dados, recomendamos habilitar o acesso aos buckets somente por meio da VPC usando os endpoints da VPC de gateway. Quando o acesso é restrito a uma VPC ou a um endpoint da VPC, você pode acessar os objetos por meio do AWS Management Console, da API REST, da AWS CLI e dos AWS SDKs.

> **Note**
>
> Para restringir o acesso a uma VPC ou a um endpoint da VPC usando o AWS Management Console, você deve usar o acesso privado do AWS Management Console. Para ter mais informações, consulte AWS Management Console Private Access no Guia do AWS Management Console.

Criar um bucket de diretório em uma zona local

Em zonas locais dedicadas, você pode criar buckets de diretório para armazenar e recuperar objetos em um perímetro de dados específico a fim de ajudar a atender aos casos de uso de isolamento e residência de dados. Os buckets de diretório do S3 são o único tipo de bucket compatível em zonas locais e contêm um tipo de localização de bucket chamada `LocalZone`. Um nome de bucket de

diretório consiste em um nome base que você fornece e um sufixo que contém o ID da zona em que o bucket está localizado e `--x-s3`. Você pode obter uma lista dos IDs de zonas locais usando a operação de API DescribeAvailabilityZones. Para obter mais informações, consulte Regras de nomenclatura de buckets de diretório.

> **Note**
>
> - Para todos os serviços em zonas locais dedicadas da AWS, incluindo o S3, seu administrador deve habilitar sua Conta da AWS antes que você possa criar ou acessar qualquer recurso na zona local dedicada. Para obter mais informações, consulte Habilitar contas para zonas locais.
> - Para os requisitos de residência de dados, recomendamos habilitar o acesso aos buckets somente por meio dos endpoints da VPC de gateway. Para obter mais informações, consulte Conectividade privada de uma VPC.
> - Para restringir o acesso a apenas os grupos de fronteira da rede da zona local, você pode usar a chave de condição `s3express:AllAccessRestrictedToLocalZoneGroup` nas políticas do IAM. Para obter mais informações, consulte Autenticação e autorização para buckets de diretório em zonas locais.

Veja a seguir maneiras de criar um bucket de diretório em uma única zona local com o AWS Management Console, a AWS CLI e os AWS SDKs.

Usar o console do S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Na barra de navegação na parte superior da página, escolha o nome da Região da AWS exibida no momento. Depois, escolha a região principal de uma zona local na qual você deseja criar um bucket de diretório.

   > **Note**
   >
   > Para ter mais informações sobre as regiões principais, consulte Conceitos para buckets de diretório em zonas locais.

3. No painel de navegação à esquerda, escolha Buckets.

4. Selecione Create bucket (Criar bucket).

   A página Create bucket (Criar bucket) é aberta.

5. Em Configuração geral, visualize a Região da AWS onde o bucket será criado.

6. Em Tipo de bucket, escolha Diretório.

   > **Note**
   >
   > - Se você escolher uma região que não oferece suporte a buckets de diretório, o tipo de bucket assumirá um bucket de uso geral como padrão. Para criar um bucket de diretório, escolha uma região compatível. Para conferir uma lista de regiões compatíveis com buckets de diretório, consulte the section called “Endpoints regionais e zonais para buckets de diretório”.
   > - Depois de criar o bucket, não será possível alterar o tipo.

7. Em Localização do bucket, escolha uma zona local que você deseja usar.

   > **Note**
   >
   > A zona local não poderá ser alterada após a criação do bucket.

8. Em Localização do bucket, marque a caixa de seleção para confirmar que, no caso de uma interrupção da zona local, seus dados poderão ficar indisponíveis ou serem perdidos.

   > **Important**
   >
   > Embora os buckets de diretório sejam armazenados em vários dispositivos dentro de uma única zona local, eles não armazenam dados de forma redundante entre zonas locais.

9. Em Nome do bucket, insira um nome para o bucket de diretório.

   Para ter mais informações sobre as regras de nomenclatura para buckets de diretório, consulte Regras de nomenclatura de buckets de uso geral. Um sufixo é adicionado automaticamente ao nome de base que você fornece ao criar um bucket de diretório usando o console. Esse sufixo inclui o ID da zona local que você escolheu.

   Depois de criado o bucket, você não pode mudar seu nome.

> **Important**
>
> Não inclua informações confidenciais, como números de conta, no nome do bucket. O nome do bucket é visível nos URLs que apontam para os objetos no bucket.

10. Em Propriedade do objeto, a configuração Imposto pelo proprietário do bucket está habilitada automaticamente e todas as listas de controle de acesso (ACLs) estão desabilitadas. Para os buckets de diretório, as ACLs estão desabilitadas e não é possível habilitá-las.

    Com a configuração Imposto pelo proprietário do bucket habilitada, o proprietário do bucket automaticamente tem a propriedade e o controle total sobre todos os objetos do bucket. As ACLs não afetam mais as permissões de acesso aos dados no bucket do S3. O bucket usa políticas exclusivamente para definir o controle de acesso. A maioria dos casos de uso modernos no Amazon S3 não exige mais o uso de ACLs. Para obter mais informações, consulte Controlar a propriedade de objetos e desabilitar ACLs para seu bucket.
11. Em Configurações de bloqueio do acesso público deste bucket, todas as configurações da funcionalidade Bloqueio de Acesso Público para o bucket de diretório estão automaticamente habilitadas. Não é possível modificar essas configurações para buckets de diretório. Para obter mais informações sobre como bloquear o acesso público, consulte Bloquear o acesso público ao armazenamento do Amazon S3.
12. Em Criptografia padrão, os buckets de diretório usam a Criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3) para criptografar os dados por padrão. Você também tem a opção de criptografar dados em buckets de diretório com a Criptografia do lado do servidor com chaves do AWS Key Management Service (SSE-KMS).
13. Escolha Criar bucket.

    Depois de criar o bucket, você pode adicionar arquivos e pastas a ele. Para obter mais informações, consulte the section called “Trabalhar com objetos em um bucket de diretório”.

Usar a AWS CLI

Este exemplo mostra como criar um bucket de diretório em uma zona local usando a AWS CLI. Para usar o comando, substitua os *espaços reservados para entrada do usuário* por suas próprias informações.

Ao criar um bucket de diretório, você deve fornecer detalhes de configuração e usar a seguinte convenção de nomenclatura: *bucket-base-name*`--`*zone-id*`--x-s3`.

```
aws s3api create-bucket
--bucket bucket-base-name--zone-id--x-s3
--create-bucket-configuration 'Location={Type=LocalZone,Name=local-zone-
id},Bucket={DataRedundancy=SingleLocalZone,Type=Directory}'
--region parent-region-code
```

Para ter mais informações sobre o ID da zona local e o código da região principal, consulte Conceitos para buckets de diretório em zonas locais. Para ter mais informações sobre o comando da AWS CLI, consulte create-bucket na AWS CLI Command Reference.

Uso dos SDKs da AWS

SDK for Go

Este exemplo mostra como criar um bucket de diretório em uma zona local usando o AWS SDK para Go.

Example

```
var bucket = "bucket-base-name--zone-id--x-s3" // The full directory bucket name

func runCreateBucket(c *s3.Client) {
    resp, err := c.CreateBucket(context.Background(), &s3.CreateBucketInput{
        Bucket: &bucket,
        CreateBucketConfiguration: &types.CreateBucketConfiguration{
            Location: &types.LocationInfo{
                Name: aws.String("local-zone-id"),
                Type: types.LocationTypeLocalZone,
            },
            Bucket: &types.BucketInfo{
                DataRedundancy: types.DataRedundancySingleLocalZone,
                Type:           types.BucketTypeDirectory,
            },
        },
    })
    var terr *types.BucketAlreadyOwnedByYou
    if errors.As(err, &terr) {
        fmt.Printf("BucketAlreadyOwnedByYou: %s\n", aws.ToString(terr.Message))
        fmt.Printf("noop...\n") // No operation performed, just printing a message
        return
    }
    if err != nil {
        log.Fatal(err)
```

```
    }

    fmt.Printf("bucket created at %s\n", aws.ToString(resp.Location))
}
```

SDK for Java 2.x

Este exemplo mostra como criar um bucket de diretório em uma zona local usando o AWS SDK for Java 2.x.

Example

```
public static void createBucket(S3Client s3Client, String bucketName) {

    //Bucket name format is {base-bucket-name}--{local-zone-id}--x-s3
    //example: doc-example-bucket--local-zone-id--x-s3 is a valid name for a
 directory bucket created in a Local Zone.

    CreateBucketConfiguration bucketConfiguration =
 CreateBucketConfiguration.builder()
             .location(LocationInfo.builder()
                     .type(LocationType.LOCAL_ZONE)
                     .name("local-zone-id").build()) //this must match the Local
 Zone ID in your bucket name
             .bucket(BucketInfo.builder()
                    .type(BucketType.DIRECTORY)
                    .dataRedundancy(DataRedundancy.SINGLE_LOCAL_ZONE)
                    .build()).build();
    try {

             CreateBucketRequest bucketRequest =
 CreateBucketRequest.builder().bucket(bucketName).createBucketConfiguration(bucketConfigurat
             CreateBucketResponse response = s3Client.createBucket(bucketRequest);
             System.out.println(response);
    }

    catch (S3Exception e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
         }
    }
```

AWS SDK para JavaScript

Este exemplo mostra como criar um bucket de diretório em uma zona local usando o AWS SDK para JavaScript.

Example

```
// file.mjs, run with Node.js v16 or higher
// To use with the preview build, place this in a folder
// inside the preview build directory, such as /aws-sdk-js-v3/workspace/

import { S3 } from "@aws-sdk/client-s3";

const region = "parent-region-code";
const zone = "local-zone-id";
const suffix = `${zone}--x-s3`;

const s3 = new S3({ region });

const bucketName = `bucket-base-name--${suffix}`; // Full directory bucket name

const createResponse = await s3.createBucket(
    { Bucket: bucketName,
      CreateBucketConfiguration: {Location: {Type: "LocalZone", Name: "local-zone-
id"},
      Bucket: { Type: "Directory", DataRedundancy: "SingleLocalZone" }}
    }
   );
```

SDK para .NET

Este exemplo mostra como criar um bucket de diretório em uma zona local usando o SDK para .NET.

Example

```
using (var amazonS3Client = new AmazonS3Client())
{
    var putBucketResponse = await amazonS3Client.PutBucketAsync(new PutBucketRequest
    {

       BucketName = "bucket-base-name--local-zone-id--x-s3",
       PutBucketConfiguration = new PutBucketConfiguration
```

```
        {
          BucketInfo = new BucketInfo { DataRedundancy =
 DataRedundancy.SingleLocalZone, Type = BucketType.Directory },
          Location = new LocationInfo { Name = "local-zone-id", Type =
 LocationType.LocalZone }
        }
      }).ConfigureAwait(false);
}
```

SDK for PHP

Este exemplo mostra como criar um bucket de diretório em uma zona local usando o AWS SDK for PHP.

Example

```
require 'vendor/autoload.php';

$s3Client = new S3Client([

    'region'      => 'parent-region-code',
]);


$result = $s3Client->createBucket([
    'Bucket' => 'bucket-base-name--local-zone-id--x-s3',
    'CreateBucketConfiguration' => [
        'Location' => ['Name'=> 'local-zone-id', 'Type'=> 'LocalZone'],
        'Bucket' => ["DataRedundancy" => "SingleLocalZone" ,"Type" => "Directory"]
  ],
]);
```

SDK for Python

Este exemplo mostra como criar um bucket de diretório em uma zona local usando o AWS SDK para Python (Boto3).

Example

```
import logging
import boto3
from botocore.exceptions import ClientError
```

```
def create_bucket(s3_client, bucket_name, local_zone):
    '''
    Create a directory bucket in a specified Local Zone

    :param s3_client: boto3 S3 client
    :param bucket_name: Bucket to create; for example, 'bucket-base-name--local-
zone-id--x-s3'
    :param local_zone: String; Local Zone ID to create the bucket in
    :return: True if bucket is created, else False
    '''

    try:
        bucket_config = {
                'Location': {
                    'Type': 'LocalZone',
                    'Name': local_zone
                },
                'Bucket': {
                    'Type': 'Directory',
                    'DataRedundancy': 'SingleLocalZone'
                }
            }
        s3_client.create_bucket(
            Bucket = bucket_name,
            CreateBucketConfiguration = bucket_config
        )
    except ClientError as e:
        logging.error(e)
        return False
    return True


if __name__ == '__main__':
    bucket_name = 'BUCKET_NAME'
    region = 'parent-region-code'
    local_zone = 'local-zone-id'
    s3_client = boto3.client('s3', region_name = region)
    create_bucket(s3_client, bucket_name, local_zone)
```

SDK for Ruby

Este exemplo mostra como criar um bucket de diretório em uma zona local usando o AWS SDK para Ruby.

Example

```
s3 = Aws::S3::Client.new(region:'parent-region-code')
s3.create_bucket(
  bucket: "bucket-base-name--local-zone-id--x-s3",
  create_bucket_configuration: {
    location: { name: 'local-zone-id', type: 'LocalZone' },
    bucket: { data_redundancy: 'SingleLocalZone', type: 'Directory' }
  }
)
```

Autenticação e autorização para buckets de diretório em zonas locais

Os buckets de diretório em zonas locais oferecem suporte à autorização do AWS Identity and Access Management (IAM) e à autorização baseada em sessão. Para ter mais informações sobre autenticação e autorização para buckets de diretório, consulte Autenticar e autorizar solicitações.

Recursos

Os nomes de recurso da Amazon (ARNs) para buckets de diretório contêm o namespace `s3express`, a região principal da AWS, o ID da Conta da AWS e o nome do bucket de diretório, que inclui o ID da zona. Para acessar e executar ações no bucket de diretório, você deve usar o seguinte formato de ARN:

```
arn:aws:s3express:region-code:account-id:bucket/bucket-base-name--ZoneID--x-s3
```

Para buckets de diretório em uma zona local, o ID da zona é o ID da zona local. Para ter mais informações sobre os buckets de diretório em zonas locais, consulte Conceitos para buckets de diretório em zonas locais. Para obter mais informações sobre ARNs, consulte Nome do recurso da Amazon (ARN) no Guia do usuário do IAM. Para ter mais informações sobre recursos, consulte Elementos de política JSON do IAM: Resource no Guia do usuário do IAM.

Chaves de condição para buckets de diretório em zonas locais

Em zonas locais, você pode usar todas essas chaves de condição nas políticas do IAM. Além disso, para criar um perímetro de dados em torno dos grupos de fronteira da rede da zona local, você pode usar a chave de condição `s3express:AllAccessRestrictedToLocalZoneGroup` para negar todas as solicitações de fora dos grupos.

A chave de condição a seguir pode ser usada para refinar ainda mais as condições sob as quais a instrução de política do IAM se aplica. Para conferir uma lista completa de operações de API, ações de política e chaves de condição compatíveis com buckets de diretório, consulte Ações de política para buckets de diretório.

> **Note**
>
> A chave de condição a seguir se aplica somente às zonas locais e não é compatível com zonas de disponibilidade e Regiões da AWS.

Operações de API	Ações de políticas	Descrição	Chave de condição	Descrição	Tipo
Operações de API de endpoint zonal	`s3expres: :CreateSession`	Concede permissão para criar um token de sessão, que é usado para conceder acesso a todas as operações de API de endpoint zonal, como `CreateSession` , `HeadBucket` , `CopyObject` , `PutObject` e `GetObject` .	`s3expres: :AllAcces sRestrict edToLocal ZoneGroup`	Filtra todo o acesso ao bucket, a menos que a solicitação seja originada dos grupos de fronteira da rede da zona local da AWS fornecidos nessa chave de condição. Valores: valor do grupo de borda da rede da zona local.	`String`

Exemplo de política

Para restringir o acesso a objetos às solicitações de dentro de um limite de residência de dados definido por você (especificamente, um grupo de zonas locais, que é um conjunto de zonas locais associadas à mesma Região da AWS), você pode definir uma das seguintes políticas:

- A política de controle de serviços (SCP). Para ter mais informações sobre as SCPs, consulte Service control policies (SCPs) no Guia do usuário do AWS Organizations.
- A política baseada em identidade do IAM para o perfil do IAM.

- A política de endpoint da VPC. Para ter mais informações sobre as políticas de endpoint da VPC, consulte Control access to VPC endpoints using endpoint policies no Guia do AWS PrivateLink.
- A política de bucket do S3.

> **Note**
>
> A chave de condição `s3express:AllAccessRestrictedToLocalZoneGroup` não oferece suporte ao acesso por meio de um ambiente on-premises. Para oferecer suporte ao acesso por meio de um ambiente on-premises, é necessário adicionar o IP de origem às políticas. Para ter mais informações, consulte aws:SourceIp no Guia do usuário do IAM.

Example – Política SCP

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Access-to-specific-LocalZones-only",
            "Effect": "Deny",
            "Action": [
                "s3express:*",
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEqualsIfExists": {
                    "s3express:AllAccessRestrictedToLocalZoneGroup": [
                        "local-zone-network-border-group-value"
                    ]
                }
            }
        }
    ]
}
```

Example – Política baseada em identidade do IAM (anexada ao perfil do IAM)

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Deny",
        "Action": "s3express:CreateSession",
        "Resource": "*",
        "Condition": {
            "StringNotEqualsIfExists": {
                "s3express:AllAccessRestrictedToLocalZoneGroup": [
                    "local-zone-network-border-group-value"
                ]
            }
        }
    }
}
```

Example Política de endpoint da VPC

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Access-to-specific-LocalZones-only",
            "Principal": "*",
            "Action": "s3express:CreateSession",
            "Effect": "Deny",
            "Resource": "*",
            "Condition": {
                 "StringNotEqualsIfExists": {
                     "s3express:AllAccessRestrictedToLocalZoneGroup": [
                         "local-zone-network-border-group-value"
                     ]
                 }
            }
        }
    ]
}
```

Example – Política de bucket

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Access-to-specific-LocalZones-only",
            "Principal": "*",
            "Action": "s3express:CreateSession",
            "Effect": "Deny",
            "Resource": "*",
            "Condition": {
                 "StringNotEqualsIfExists": {
                     "s3express:AllAccessRestrictedToLocalZoneGroup": [
                         "local-zone-network-border-group-value"
                     ]
                 }
            }
        }
    ]
}
```

Diferenças de buckets de diretório

Ao usar o Amazon S3, escolha o tipo de bucket que melhor se adapta aos seus requisitos de desempenho e da aplicação. Um bucket de diretório é um tipo de bucket ideal para casos de uso de baixa latência e de residência de dados. Para saber mais sobre os buckets de diretório, consulte Trabalhar com buckets de diretório.

Consulte mais informações sobre a diferença de buckets de diretório nos tópicos a seguir.

Tópicos

- Diferenças de buckets de diretório
- Operações de API compatíveis com buckets de diretório
- Recursos do Amazon S3 não compatíveis com buckets de diretório

Diferenças de buckets de diretório

- Nomes de bucket de diretório
  - Um nome de bucket de diretório consiste em um nome base que você fornece e em um sufixo que contém o ID da zona da AWS (uma zona de disponibilidade ou zona local) em que o bucket está localizado, seguido de `--x-s`. Consulte uma lista de regras e exemplos de nomes de bucket de diretório em Regras de nomenclatura de buckets de diretório.
- Comportamento de **`ListObjectsV2`**
  - Para buckets de diretório, `ListObjectsV2` não retorna objetos na ordem lexicográfica (alfabética). Além disso, os prefixos devem terminar com um delimitador e somente “/” pode ser especificado como delimitador.
  - Para buckets de diretório, a resposta de `ListObjectsV2` inclui os prefixos relacionados somente aos carregamentos fracionados em andamento.
- Comportamento de exclusão: quando você exclui um objeto de um bucket de diretório, o Amazon S3 exclui recursivamente todos os diretórios vazios no caminho do objeto. Por exemplo, se você excluir a chave de objeto `dir1/dir2/file1.txt`, o Amazon S3 excluirá `file1.txtt`. Se os diretórios `dir1/` e `dir2/` estiverem vazios e não contiverem outros objetos, o Amazon S3 também excluirá esses diretórios.
- ETags e somas de verificação: as tags de entidade (ETags) para buckets de diretório são strings alfanuméricas aleatórias, exclusivas para cada objeto, e não somas de verificação MD5. Para ter mais informações sobre como usar somas de verificação adicionais com buckets de diretório, consulte Práticas recomendadas adicionais de soma de verificação do S3.
- Chaves de objeto em solicitações **`DeleteObjects`**
  - As chaves de objeto em solicitações `DeleteObjects` devem conter pelo menos um caractere diferente de um espaço em branco. Strings compostas somente por caracteres de espaço em branco não são compatíveis com solicitações `DeleteObjects`.
  - As chaves de objeto em solicitações `DeleteObjects` não podem conter caracteres de controle Unicode, exceto nova linha (`\t`), tabulação (`\n`) e avanço de linha (`\r`).
- Endpoints regionais e zonais: as operações de API de gerenciamento para buckets de diretório estão disponíveis por meio de um endpoint regional e são chamadas de operações de API de endpoint regional. Exemplos de operações de API de endpoint regional são CreateBucket e DeleteBucket. Depois de criar um bucket de diretório, você pode usar operações de API de endpoint zonal para fazer upload e gerenciar os objetos no bucket de diretório. As operações de API de endpoint zonal estão disponíveis por meio de um endpoint zonal. Exemplos de operações

de API de endpoint zonal são `PutObject` e `CopyObject`. Ao usar buckets de diretório, você deve especificar a região em todas as solicitações. Para endpoints regionais, especifique a região, como `s3express-control.us-west-2.amazonaws.com`. Para endpoints zonais, especifique a região e a zona de disponibilidade, como `s3express-usw2-az1.us-west-2.amazonaws.com`. Para obter mais informações, consulte Endpoints regionais e zonais para buckets de diretório.

- Carregamentos fracionados: você pode fazer upload e copiar objetos grandes armazenados em buckets de diretório usando o processo de carregamento fracionado. No entanto, veja a seguir algumas diferenças ao usar o processo de carregamento fracionado com objetos armazenados em buckets de diretório. Para obter mais informações, consulte the section called “Usar uploads multiparte com buckets de diretório”.
  - A data de criação do objeto é a data de conclusão do multipart upload.
  - Os números das partes de um carregamento multiparte devem ser consecutivos. Se você tentar concluir uma solicitação de multipart upload com números de parte não consecutivos, o Amazon S3 gerará um erro HTTP `400 (Bad Request)`.
  - O iniciador de um carregamento multiparte só poderá anular a solicitação de carregamento multiparte se tiver recebido acesso explícito a `AbortMultipartUpload` por meio da permissão `s3express:CreateSession`. Para obter mais informações, consulte Autorizar operações de API de endpoint regional com o IAM.
- Esvaziar um bucket de diretório: o comando `s3 rm` por meio da AWS Command Line Interface (CLI), a operação `delete` por meio do Mountpoint e o botão de opção Esvaziar bucket por meio do AWS Management Console não conseguem excluir carregamentos fracionados em andamento em um bucket de diretório. Para excluir esses carregamentos fracionados em andamento, use a operação `ListMultipartUploads` para listá-los no bucket e a operação `AbortMultipartUpload` para anular todos eles.
- Zonas locais da AWS: as zonas locais são compatíveis somente com buckets de diretório, não com buckets de uso geral.
  - A anexação de dados a objetos existentes não é compatível com buckets de diretório que residem em zonas locais. Você só pode anexar dados a objetos existentes em buckets de diretório que residem em zonas de disponibilidade.
  - A funcionalidade Ciclo de Vida do S3 não é compatível com buckets de diretório em zonas locais.

Operações de API compatíveis com buckets de diretório

Os buckets de diretório oferecem suporte às operações de API de endpoint regional (nível do bucket ou ambiente de gerenciamento) e zonal (nível do objeto ou plano de dados). Para obter mais informações, consulte Rede para buckets de diretório e Endpoints e endpoints de VPC do gateway. Para ver uma lista das operações de API permitidas, consulte Operações de API de bucket de diretório.

Recursos do Amazon S3 não compatíveis com buckets de diretório

Os seguintes recursos do Amazon S3 não são compatíveis com buckets de diretório:

- Políticas gerenciadas AWS
- AWS PrivateLink para S3
- Somas de verificação MD5
- Exclusão de autenticação multifator (MFA)
- Bloqueio de objetos do S3
- Requester Pays (Pagamento pelo solicitante)
- Concessões de Acesso do S3
- Métricas de solicitação do Amazon CloudWatch
- Notificações de eventos do S3
- Ações de transição da funcionalidade Ciclo de Vida do S3
- Pontos de Acesso Multirregionais do S3
- Pontos de Acesso do S3 Object Lambda
- Versionamento do S3
- Inventário S3
- Replicação do S3
- Tags de objeto
- S3 Select
- Logs de acesso ao servidor
- Hospedagem de site estático
- Lente de Armazenamento do S3

- Grupos da Lente de Armazenamento do S3
- Aceleração de Transferências do S3
- Criptografia de camada dupla do lado do servidor com chaves do AWS Key Management Service (AWS KMS) (DSSE-KMS)
- Criptografia do lado do servidor com chaves fornecidas pelo cliente (SSE-C)
- A opção de copiar as configurações de um bucket existente ao criar um bucket no console do Amazon S3
- Mensagens de erro aprimoradas de acesso negado (HTTP `403 Forbidden`)

Rede para buckets de diretório

Para acessar buckets de diretório e os objetos dentro, use endpoints de API regional e zonal diferentes dos endpoints padrão do Amazon S3. Dependendo da operação de API do S3 usada, será necessário um endpoint regional ou zonal. Para obter uma lista completa das operações de API por tipo de endpoint, consulte Diferenças de buckets de diretório.

Você pode acessar operações de API zonais e regionais por meio de endpoints de nuvem privada virtual (VPC) de gateway.

Os tópicos a seguir descrevem os requisitos de rede para acessar a classe S3 Express One Zone usando um endpoint da VPC do gateway.

Tópicos

- Endpoints
- Configurar endpoints de gateway da VPC

Endpoints

É possível acessar buckets de diretório e objetos dentro pela VPC usando endpoints da VPC de gateway. Os buckets de diretório usam endpoints de API regionais e zonais. Dependendo da operação de API do Amazon S3 usada, será necessário um endpoint regional ou zonal. Não há cobrança adicional pelo uso de endpoints do gateway.

As operações de API em nível de bucket (ou ambiente de gerenciamento) estão disponíveis por meio de endpoints regionais e são chamadas de operações de API do endpoint regional. Exemplos de operações de API de endpoint regional são `CreateBucket` e `DeleteBucket`. Ao criar um bucket

de diretório, escolha uma única zona (zona de disponibilidade ou zona local) em que o bucket de diretório será criado. Depois de criar um bucket de diretório, você pode usar operações de API de endpoint zonal para fazer upload e gerenciar os objetos no bucket de diretório.

As operações de API em nível de objeto (ou plano de dados) estão disponíveis por meio de endpoints zonais e são chamadas de operações de API do endpoint zonal. Exemplos de operações de API de endpoint zonal são `CreateSession` e `PutObject`.

Consulte mais informações sobre endpoints e locais compatíveis com buckets de diretório em zonas de disponibilidade em Endpoints de buckets de diretório em zonas de disponibilidade.

Para ter mais informações sobre os endpoints e os locais compatíveis com buckets de diretório em zonas locais, consulte Habilitar contas para zonas locais.

Configurar endpoints de gateway da VPC

Para configurar endpoints da VPC de gateway para buckets de diretório de acesso em zonas de disponibilidade, consulte the section called “Configurar endpoints de gateway da VPC”.

Para configurar endpoints da VPC de gateway para acesso a buckets de diretório em zonas locais, consulte Conectividade privada de uma VPC.

Regras de nomenclatura de buckets de diretório

Ao criar um bucket de diretório no Amazon S3, as regras de nomenclatura de buckets a seguir se aplicam. Para conferir as regras de nomenclatura para buckets de uso geral, consulte Regras de nomenclatura de buckets de uso geral.

Um nome de bucket de diretório consiste em um nome base que você fornece e um sufixo que contém o ID da zona da AWS (uma zona de disponibilidade ou zona local) em que o bucket está localizado e `--x-s3`. O *`zone-id`* pode ser o ID de uma zona de disponibilidade ou zona local.

```
base-name--zoneid--x-s3
```

Por exemplo, o seguinte nome de bucket de diretório contém o ID da zona de disponibilidade `usw2-az1`:

```
bucket-base-name--usw2-az1--x-s3
```

> **Note**
>
> Quando você cria um bucket de diretório usando o console, um sufixo é adicionado automaticamente ao nome base fornecido. Esse sufixo inclui o ID da zona (zona de disponibilidade ou zona local) que você escolheu.
> Ao criar um bucket de diretório usando uma API, é necessário fornecer o sufixo completo, incluindo o ID da zona de disponibilidade, na solicitação. Consulte uma lista dos IDs de zona em Endpoints.

As regras de nomenclatura a seguir se aplicam a buckets de diretório.

- O nome deve ser exclusivo na zona escolhida (zona de disponibilidade da AWS ou zona local da AWS).
- O nome deve ter entre 3 (mín.) e 63 (máx.) caracteres, incluindo o sufixo.
- Consistir em letras minúsculas, números e hifens (-).
- Inicie e termine com uma letra ou um número.
- Deve incluir o seguinte sufixo: `--`*`zone-id`*`--x-s3`.
- O nome do bucket não deve iniciar com o prefixo `xn--`.
- O nome do bucket não deve iniciar com o prefixo `sthree-`.
- O nome do bucket não deve iniciar com o prefixo `sthree-configurator`.
- O nome do bucket não deve iniciar com o prefixo `amzn-s3-demo-`.
- Os nomes de bucket não podem terminar com o sufixo `-s3alias`. Esse sufixo se reserva a nomes de alias de ponto de acesso. Para obter mais informações, consulte Alias de ponto de acesso.
- Os nomes de bucket não podem terminar com o sufixo `--ol-s3`. Esse sufixo é reservado a nomes de alias de ponto de acesso de objeto do Lambda. Para obter mais informações, consulte Como usar um alias no estilo do bucket para o ponto de acesso do Object Lambda do bucket do S3.
- Os nomes de bucket não podem terminar com o sufixo `.mrap`. Esse sufixo é reservado para nomes de ponto de acesso de várias regiões. Para obter mais informações, consulte Regras para nomear pontos de acesso multirregionais do Amazon S3.

Visualizar as propriedades de buckets de diretório

Você pode visualizar e configurar as propriedades de um bucket de diretório do Amazon S3 usando o console do Amazon S3. Para obter mais informações, consulte Trabalhar com buckets de diretório.

Usar o console do S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets de diretórios.
3. Na lista Buckets de diretórios, escolha o nome do bucket cujas propriedades deseja visualizar.
4. Escolha a guia Properties (Propriedades).
5. Na guia Propriedades, você pode visualizar as seguintes propriedades do bucket:

    - Visão geral do bucket de diretório: você pode ver a Região da AWS, a zona (zona de disponibilidade ou zona local), o nome do recurso da Amazon (ARN) e a data de criação do bucket.
    - Configurações de criptografia do lado do servidor: o Amazon S3 aplica a criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3) como o nível básico de criptografia para todos os buckets do S3. O Amazon S3 criptografa um objeto antes de salvá-lo em um disco e descriptografa o objeto ao baixá-lo. Para obter mais informações, consulte Definir e monitorar a criptografia padrão para buckets de diretório.

      Para obter mais informações sobre os recursos compatíveis com buckets de diretório, consulte Criar e usar buckets de diretório.

Gerenciar políticas de bucket de diretório

É possível adicionar, excluir, atualizar e visualizar políticas de bucket para buckets de diretório do Amazon S3 usando o console do Amazon S3, os SDKs da AWS e a AWS CLI. Para obter mais informações, consulte os tópicos a seguir. Consulte mais informações sobre ações do AWS Identity and Access Management (IAM) compatíveis em Autorizar operações de API de endpoint regional com o IAM. Para conferir exemplos de políticas para buckets de diretório, consulte Exemplos de políticas para buckets de diretório.

Tópicos

- Adicionar uma política de bucket
- Visualizar uma política de bucket
- Excluir uma política de bucket

Adicionar uma política de bucket

Para adicionar uma política de bucket a um bucket de diretório, você pode usar o console do Amazon S3, os SDKs da AWS ou a AWS CLI.

Usar o console do S3

Para criar ou editar uma política de bucket

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets de diretórios.
3. Na lista Buckets de diretórios, escolha o nome do bucket para o qual você deseja adicionar uma política.
4. Escolha a aba Permissões.
5. Em Bucket policy (Política de bucket), escolha Edit (Editar). A página Edit bucket policy (Editar política de bucket) é exibida.
6. Para gerar uma política automaticamente, escolha Gerador de políticas.

   Se você escolher Policy generator (Gerador de políticas), o Gerador de Políticas da AWS será aberto em uma nova janela.

   Se você não quiser usar o gerador de políticas da AWS, poderá adicionar ou editar instruções JSON na seção Política.

   a. Na página Gerador de Políticas da AWS, em Selecionar tipo de política, escolha Política de bucket do S3.

   b. Adicione uma instrução inserindo as informações nos campos fornecidos e escolha Add Statement (Adicionar instrução). Repita esta etapa para todas as instruções que quiser adicionar. Para ter mais informações sobre esses campos, consulte a Referência de elementos de política JSON do IAM no Guia do usuário do IAM.

> **Note**
>
> Por conveniência, a página Editar política de bucket exibe o ARN do bucket (nome do recurso da Amazon) do bucket atual acima do campo de texto Política. Você pode copiar este ARN para usá-lo nas instruções da página do AWS Policy Generator.

c. Depois de terminar de adicionar as instruções, escolha Generate Policy (Gerar política).

d. Copie o texto da política gerada, escolha Close (Fechar) e retorne à página Edit bucket policy (Editar política de bucket) no console do Amazon S3.

7. Na caixa Policy (Política), edite a política existente ou cole a política de bucket do Gerador de Políticas da AWS. Solucione avisos de segurança, erros, avisos gerais e sugestões antes de salvar a política.

> **Note**
>
> As políticas de bucket são limitadas a 20 KB.

8. Escolha Save changes (Salvar alterações), o que levará você de volta à guia Permissions (Permissões).

Uso dos SDKs da AWS

SDK for Java 2.x

Example

`PutBucketPolicy` AWS SDK for Java 2.x

```
public static void setBucketPolicy(S3Client s3Client, String bucketName, String
 policyText) {

      //sample policy text
      /**
       * policy_statement = {
       *         'Version': '2012-10-17',
       *         'Statement': [
       *             {
       *                 'Sid': 'AdminPolicy',
```

```
        *                 'Effect': 'Allow',
        *                 'Principal': {
        *                     "AWS": "111122223333"
        *                 },
        *                 'Action': 's3express:*',
        *                 'Resource':
'arn:aws:s3express:region:111122223333:bucket/bucket-base-name--zone-id--x-s3'
        *             }
        *         ]
        *     }
        */
        System.out.println("Setting policy:");
        System.out.println("----");
        System.out.println(policyText);
        System.out.println("----");
        System.out.format("On Amazon S3 bucket: \"%s\"\n", bucketName);

        try {
            PutBucketPolicyRequest policyReq = PutBucketPolicyRequest.builder()
                    .bucket(bucketName)
                    .policy(policyText)
                    .build();
            s3Client.putBucketPolicy(policyReq);
            System.out.println("Done!");
        }

        catch (S3Exception e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }
    }
```

Como usar o AWS CLI

Este exemplo mostra como adicionar uma política de bucket a um bucket de diretório usando a AWS CLI. Para usar o comando, substitua os *espaços reservados para entrada do usuário* por suas próprias informações.

```
aws s3api put-bucket-policy --bucket bucket-base-name--zone-id--x-s3 --policy file://
bucket_policy.json
```

bucket_policy.json:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AdminPolicy",
            "Effect": "Allow",
            "Principal": {
                "AWS": "111122223333"
            },
            "Action": "s3express*",
            "Resource": "arn:aws:s3express:us-west-2:111122223333:bucket/amzn-s3-demo-bucket--usw2-az1--x-s3"
        }
    ]
}
```

Para obter mais informações, consulte put-bucket-policy na AWS Command Line Interface.

Visualizar uma política de bucket

Para visualizar uma política de um bucket de diretório, use os exemplos a seguir.

Como usar o AWS CLI

Este exemplo mostra como visualizar a política de bucket anexada a um bucket de diretório usando a AWS CLI. Para usar o comando, substitua os *espaços reservados para entrada do usuário* por suas próprias informações.

```
aws s3api get-bucket-policy --bucket bucket-base-name--zone-id--x-s3
```

Para obter mais informações, consulte get-bucket-policy na AWS Command Line Interface.

Excluir uma política de bucket

Para excluir uma política de um bucket de diretório, use os exemplos a seguir.

Uso dos SDKs da AWS

SDK for Java 2.x

Example

`DeleteBucketPolicy` AWS SDK for Java 2.x

```
public static void deleteBucketPolicy(S3Client s3Client, String bucketName) {
      try {
          DeleteBucketPolicyRequest deleteBucketPolicyRequest =
 DeleteBucketPolicyRequest
                  .builder()
                  .bucket(bucketName)
                  .build()
          s3Client.deleteBucketPolicy(deleteBucketPolicyRequest);
          System.out.println("Successfully deleted bucket policy");
      }

      catch (S3Exception e) {
          System.err.println(e.awsErrorDetails().errorMessage());
          System.exit(1);
      }
```

Como usar o AWS CLI

Este exemplo mostra como excluir uma política de bucket de um bucket de diretório usando a AWS CLI. Para usar o comando, substitua os *espaços reservados para entrada do usuário* por suas próprias informações.

```
aws s3api delete-bucket-policy --bucket bucket-base-name--zone-id--x-s3
```

Para obter mais informações, consulte delete-bucket-policy na AWS Command Line Interface.

Esvaziar um bucket de diretório

Você pode esvaziar um bucket de diretório do Amazon S3 usando o console do Amazon S3. Para obter mais informações sobre os buckets de diretório, consulte Trabalhar com buckets de diretório.

Antes de esvaziar um bucket de diretório, observe o seguinte:

- Ao esvaziar um bucket de diretório, você exclui todos os objetos, mas mantém o bucket.
- Não é possível desfazer a ação de esvaziar um bucket de diretório.
- Os objetos que forem adicionados ao bucket de diretório enquanto a ação de esvaziar estiver em andamento também poderão ser excluídos.

Se você também quiser excluir o bucket, observe o seguinte:

- Todas os objetos no bucket de diretório devem ser excluídos antes que o bucket em si possa ser excluído.
- Os multipart uploads em andamento no bucket de diretório devem ser anulados antes que o bucket em si possa ser excluído.

> **Note**
>
> O comando `s3 rm` por meio da AWS Command Line Interface (CLI), a operação `delete` por meio do Mountpoint e o botão de opção Esvaziar bucket por meio do AWS Management Console não conseguem excluir carregamentos fracionados em andamento em um bucket de diretório. Para excluir esses carregamentos fracionados em andamento, use a operação `ListMultipartUploads` para listá-los no bucket e a operação `AbortMultipartUpload` para anular todos eles.

Para excluir um bucket de diretório, consulte Excluir um bucket de diretório. Para anular um upload multiparte em andamento, consulte the section called “Abortar um multipart upload”.

Para esvaziar um bucket de uso geral, consulte Esvaziar um bucket de uso geral.

Usar o console do S3

Como esvaziar um bucket de diretório

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets de diretórios.
3. Escolha o botão de opções ao lado do nome do bucket que você deseja esvaziar, depois selecione Esvaziar.

4. Na página Empty bucket (Esvaziar bucket), confirme se deseja esvaziar o bucket inserindo **`permanently delete`** no campo de texto e depois escolha Empty (Esvaziar).
5. Monitore o andamento do processo de esvaziamento do bucket na página Bucket vazio: status.

Excluir um bucket de diretório

Só é possível excluir buckets de diretório vazios do Amazon S3. Antes de excluir um bucket de diretório, é necessário excluir todos os objetos do bucket e anular todos os uploads multiparte em andamento.

Se o bucket do diretório estiver conectado a um ponto de acesso, primeiro será necessário excluir o ponto de acesso. Para obter mais informações, consulte Excluir o ponto de acesso para buckets de diretório.

Para esvaziar um bucket de diretório, consulte Esvaziar um bucket de diretório. Para anular um upload multiparte em andamento, consulte the section called “Abortar um multipart upload”.

Para excluir um bucket de uso geral, consulte Excluir um bucket de uso geral.

Usar o console do S3

Depois de esvaziar o bucket de diretório e anular todos os uploads multiparte em andamento, você poderá excluir o bucket.

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets de diretórios.
3. Na lista Buckets de diretório, escolha o botão de opções ao lado do bucket que você deseja excluir.
4. Escolha Excluir.
5. Na página Excluir bucket, insira o nome do bucket no campo de texto para confirmar a exclusão do bucket.

> **Important**
>
> Não é possível desfazer a exclusão de um bucket.

6. Para excluir um bucket de diretório, escolha Excluir bucket.

Uso dos SDKs da AWS

Os exemplos a seguir excluem um bucket de diretório usando o AWS SDK for Java 2.x e o AWS SDK para Python (Boto3).

SDK for Java 2.x

Example

```
public static void deleteBucket(S3Client s3Client, String bucketName) {

    try {
        DeleteBucketRequest del = DeleteBucketRequest.builder()
                .bucket(bucketName)
                .build();
        s3Client.deleteBucket(del);
        System.out.println("Bucket " + bucketName + " has been deleted");
    }
    catch (S3Exception e) {
        System.err.println(e.awsErrorDetails().errorMessage());
        System.exit(1);
    }
}
```

SDK for Python

Example

```
import logging
import boto3
from botocore.exceptions import ClientError

def delete_bucket(s3_client, bucket_name):
    '''
    Delete a directory bucket in a specified Region

    :param s3_client: boto3 S3 client
    :param bucket_name: Bucket to delete; for example, 'doc-example-bucket--usw2-
az1--x-s3'
    :return: True if bucket is deleted, else False
```

```
    '''

    try:
        s3_client.delete_bucket(Bucket = bucket_name)
    except ClientError as e:
        logging.error(e)
        return False
    return True

if __name__ == '__main__':
    bucket_name = 'BUCKET_NAME'
    region = 'us-west-2'
    s3_client = boto3.client('s3', region_name = region)
```

Como usar o AWS CLI

Este exemplo mostra como excluir um bucket de diretório usando a AWS CLI. Para usar o comando, substitua os *espaços reservados para entrada do usuário* por suas próprias informações.

```
aws s3api delete-bucket --bucket bucket-base-name--zone-id--x-s3 --region us-west-2
```

Para obter mais informações, consulte delete-bucket na AWS Command Line Interface.

Listar buckets de diretório

Os exemplos a seguir mostram como listar buckets de diretório usando o AWS Management Console, SDKS da AWS e a AWS CLI.

Usar o console do S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Na barra de navegação na parte superior da página, escolha o nome da Região da AWS exibida no momento. Em seguida, escolha a região na qual você deseja visualizar uma lista dos seus buckets de diretório.
3. No painel de navegação à esquerda, escolha Buckets de diretórios. Uma lista de bucket de diretório é exibida. Para visualizar os objetos no bucket, as propriedades do bucket, as permissões do bucket, as métricas e os pontos de acesso associados ao bucket ou para gerenciar o bucket, escolha o nome do bucket.

Uso dos SDKs da AWS

SDK for Java 2.x

Example

O exemplo a seguir lista os buckets de diretório usando o AWS SDK for Java 2.x.

```
public static void listBuckets(S3Client s3Client) {
       try {
           ListDirectoryBucketsRequest listDirectoryBucketsRequest =
ListDirectoryBucketsRequest.builder().build();
           ListDirectoryBucketsResponse response =
s3Client.listDirectoryBuckets(listDirectoryBucketsRequest);
           if (response.hasBuckets()) {
               for (Bucket bucket: response.buckets()) {
                   System.out.println(bucket.name());
                   System.out.println(bucket.creationDate());
               }
           }
       }

       catch (S3Exception e) {
           System.err.println(e.awsErrorDetails().errorMessage());
           System.exit(1);
       }
   }
```

SDK for Python

Example

O exemplo a seguir lista os buckets de diretório usando o AWS SDK para Python (Boto3).

```
import logging
import boto3
from botocore.exceptions import ClientError

def list_directory_buckets(s3_client):
'''
Prints a list of all directory buckets in a Region
```

```
:param s3_client: boto3 S3 client
:return: True if there are buckets in the Region, else False
'''
try:
    response = s3_client.list_directory_buckets()
    for bucket in response['Buckets']:
        print (bucket['Name'])
except ClientError as e:
    logging.error(e)
    return False
return True


if __name__ == '__main__':
    region = 'us-east-1'
    s3_client = boto3.client('s3', region_name = region)
    list_directory_buckets(s3_client)
```

SDK para .NET

Example

O exemplo a seguir lista os buckets de diretório usando o AWS SDK para .NET.

```
var listDirectoryBuckets = await amazonS3Client.ListDirectoryBucketsAsync(new
 ListDirectoryBucketsRequest
{
  MaxDirectoryBuckets = 10
  }).ConfigureAwait(false);
```

SDK for PHP

Example

O exemplo a seguir lista os buckets de diretório usando o AWS SDK para PHP.

```
require 'vendor/autoload.php';

$s3Client = new S3Client([
    'region'      => 'us-east-1',
```

```
]);
$result = $s3Client->listDirectoryBuckets();
```

SDK for Ruby

Example

O exemplo a seguir lista os buckets de diretório usando o AWS SDK para Ruby.

```
s3 = Aws::S3::Client.new(region:'us-west-1')
s3.list_directory_buckets
```

Como usar o AWS CLI

O exemplo de comando `list-directory-buckets` a seguir mostra como você pode usar a AWS CLI para listar seus buckets de diretório na região *`us-east-1`*. Para executar esse comando, substitua os *`user input placeholders`* por suas próprias informações.

```
aws s3api list-directory-buckets --region us-east-1
```

Para obter mais informações, consulte list-directory-buckets na Referência de comandos da AWS CLI.

Determinar se você pode acessar um bucket de diretório

Os exemplos de AWS SDK a seguir mostram como usar a operação de API `HeadBucket` para determinar se existe um bucket de diretório do Amazon S3 e se você tem permissão para acessá-lo.

Uso dos SDKs da AWS

O exemplo a seguir para AWS SDK for Java 2.x mostra como determinar se um bucket existe e se você tem permissão para acessá-lo.

SDK for Java 2.x

Example

AWS SDK for Java 2.x

```
public static void headBucket(S3Client s3Client, String bucketName) {
   try {
        HeadBucketRequest headBucketRequest = HeadBucketRequest
                .builder()
                .bucket(bucketName)
                .build();
        s3Client.headBucket(headBucketRequest);
        System.out.format("Amazon S3 bucket: \"%s\" found.", bucketName);
   }

   catch (S3Exception e) {
       System.err.println(e.awsErrorDetails().errorMessage());
       System.exit(1);
   }
}
```

Como usar o AWS CLI

O exemplo de comando `head-bucket` a seguir mostra como é possível usar a AWS CLI para determinar se um bucket de diretório existe e se você tem permissão para acessá-lo. Para executar esse comando, substitua os espaços reservados de entrada por suas próprias informações.

```
aws s3api head-bucket --bucket bucket-base-name--zone-id--x-s3
```

Para obter mais informações, consulte head-bucket na Referência de comandos da AWS CLI.

Trabalhar com objetos em um bucket de diretório

Depois de criar um bucket de diretório do Amazon S3, você pode trabalhar com objetos usando o console do Amazon S3, a AWS Command Line Interface (AWS CLI) e os AWS SDKs.

Consulte mais informações sobre como realizar em massa operações, importação, upload, cópia, exclusão e download de objetos em buckets de diretório nos tópicos a seguir.

Tópicos

- Importar objetos em um bucket de diretório
- Trabalhar com o S3 Lifecycle para buckets de diretório

- Usar a funcionalidade Operações em Lote com buckets de diretório
- Anexar dados a objetos em buckets de diretórios
- Renomear objetos em buckets de diretório
- Fazer upload de objetos em um bucket de diretório
- Copiar objetos de ou para um bucket de diretório
- Excluir objetos de um bucket de diretório
- Baixar um objeto de um bucket de diretório
- Gerar URLs pré-assinados para compartilhar objetos de bucket de diretório
- Recuperar metadados de objeto dos buckets de diretório
- Listar objetos de um bucket de diretório

Importar objetos em um bucket de diretório

Depois de criar um bucket de diretório no Amazon S3, você pode preencher o novo bucket com dados usando a ação de importação. A importação é um método simplificado para criar trabalhos da funcionalidade Operações em Lote do S3 a fim de copiar objetos de buckets de uso geral para buckets de diretório.

> **Note**
>
> As seguintes limitações se aplicam aos trabalhos de importação:
>
> - O bucket de origem e o bucket de destino devem estar nas mesmas conta e Região da AWS.
> - O bucket de origem não pode ser um bucket de diretório.
> - Objetos maiores que 5 GB não são compatíveis e serão omitidos da operação de cópia.
> - Os objetos nas classes de armazenamento Glacier Flexible Retrieval, Glacier Deep Archive, Intelligent-Tiering Archive Access e Intelligent-Tiering Deep Archive devem ser restaurados antes que possam ser importados.
> - Os objetos importados com algoritmos de soma de verificação MD5 são convertidos para usar somas de verificação CRC32.
> - Os objetos importados usam a classe de armazenamento Express One Zone, que tem uma estrutura de preços diferente das classes de armazenamento usadas por buckets de uso geral. Considere essa diferença de custo ao importar um grande número de objetos.

Ao configurar um trabalho de importação, especifique o bucket ou prefixo de origem de onde os objetos existentes serão copiados. Forneça também um perfil do AWS Identity and Access Management (IAM) com permissões para acessar os objetos de origem. Depois, o Amazon S3 inicia um trabalho da funcionalidade Operações em Lote que copia os objetos e aplica automaticamente as configurações apropriadas de classe de armazenamento e soma de verificação.

Para configurar trabalhos de importação, use o console do Amazon S3.

Usar o console do Amazon S3

Como importar objetos em um bucket de diretório

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação esquerdo, escolha Buckets e selecione a guia Buckets de diretórios. Selecione o botão de opções ao lado do bucket de diretório para o qual você deseja importar objetos.
3. Escolha Importar.
4. Em Origem, insira o bucket de uso geral (ou o caminho do bucket com o prefixo) que contém os objetos que você deseja importar. Para escolher um bucket de uso geral existente em uma lista, selecione Procurar no S3.
5. Em Permissão para acessar e copiar objetos de origem, execute uma das seguintes ações para especificar um perfil do IAM com as permissões necessárias para importar os objetos da origem:
   - Para permitir que o Amazon S3 crie um perfil do IAM em seu nome, escolha Criar perfil do IAM.
   - Para escolher um perfil do IAM existente em uma lista, escolha Escolher entre perfis do IAM existentes.
   - Para especificar um perfil do IAM existente inserindo o nome do recurso da Amazon (ARN), escolha Inserir ARN do perfil do IAM e insira o ARN no campo correspondente.
6. Revise as informações exibidas nas seções Destino e Configurações do objeto copiado. Se as informações na seção Destino estiverem corretas, escolha Importar para iniciar o trabalho de cópia.

   O console do Amazon S3 exibirá o status do novo trabalho na página Operações em lotes. Para obter mais informações sobre o trabalho, escolha o botão de opções ao lado do nome do

trabalho e selecione Visualizar detalhes no menu Ações. Para abrir o bucket de diretório para o qual os objetos serão importados, escolha Exibir destino de importação.

Trabalhar com o S3 Lifecycle para buckets de diretório

O S3 Lifecycle ajuda você a armazenar objetos na classe S3 Express One Zone em buckets de diretório de forma econômica ao excluir objetos expirados em seu nome. Para gerenciar o ciclo de vida de objetos, crie uma configuração do S3 Lifecycle para o bucket de diretório. Uma configuração do Amazon S3 Lifecycle é um conjunto de regras que define as ações aplicadas pelo Amazon S3 a um grupo de objetos. Você pode definir uma configuração do Amazon S3 Lifecycle em um bucket de diretório usando a AWS Command Line Interface (AWS CLI), os AWS SDKs, a API REST do Amazon S3 e o AWS CloudFormation.

Na configuração do ciclo de vida, você usa regras para definir ações que você deseja que o Amazon S3 realize em objetos. Para objetos armazenados em buckets de diretório, você pode criar regras de ciclo de vida para expirar objetos à medida que envelhecem. Você também pode criar regras de ciclo de vida para excluir carregamentos fracionados em buckets de diretório com frequência diária.

Quando você adiciona uma configuração do ciclo de vida a um bucket, as regras de configuração se aplicam aos objetos existentes e aos objetos que serão adicionados no futuro. Por exemplo, se você adicionar uma regra de configuração de ciclo de vida hoje com uma ação de expiração que faz com que os objetos com um prefixo específico expirem 30 dias após sua criação, o S3 organizará para exclusão todos os objetos existentes com mais de 30 dias e com o prefixo especificado.

Como o S3 Lifecycle para buckets de diretório é diferente

Para objetos em buckets de diretório, é possível criar regras de ciclo de vida para expirar objetos e excluir carregamentos fracionados incompletos. No entanto, o S3 Lifecycle para buckets de diretório não permite ações de transição entre classes de armazenamento.

CreateSession

O Lifecycle usa operações de API `DeleteObject` e `DeleteObjects` públicas para expirar objetos em buckets de diretório. Para usar essas operações de API, o S3 Lifecycle usará a API `CreateSession` para estabelecer credenciais de segurança temporárias a fim de acessar os objetos nos buckets de diretório. Consulte mais informações em `CreateSession` na Referência da API do Amazon S3.

Se você tiver uma política ativa que nega permissões de exclusões, à entidade principal de ciclo de vida, isso impedirá que você permita que o S3 Lifecycle exclua objetos em seu nome.

Usar uma política de bucket para conceder permissões à entidade principal do serviço S3 Lifecycle

A política de bucket a seguir concede permissão para permitir chamadas de CreateSession com a sessão `ReadWrite` padrão e permite a entidade principal do serviço de ciclo de vida.

Example : política de bucket para permitir chamadas de **`CreateSession`** com a sessão padrão **`ReadWrite`**

```
 {
   "Version":"2008-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal": {
            "Service":"lifecycle.s3.amazonaws.com"
          },
          "Action":"s3express:CreateSession",
          "Condition": {
             "StringEquals": {
                "s3express:SessionMode": "ReadWrite"
              }
           },
           "Resource":"arn:aws:s3express:us-east-2:412345678921:bucket/amzn-s3-demo-
bucket--use2-az2--x-s3"
       }
   ]
}
```

Monitorar regras de ciclo de vida

Para objetos armazenados em buckets de diretório, o S3 Lifecycle gera logs de eventos de dados e gerenciamento do AWS CloudTrail. Consulte mais informações em Exemplos de arquivos de log de eventos de dados do CloudTrail para a classe Amazon S3 Express One Zone.

Consulte mais informações sobre como criar configurações de ciclo de vida e solucionar problemas relacionados ao S3 Lifecycle nos seguintes tópicos:

Tópicos

- Criar e gerenciar uma configuração de ciclo de vida para o bucket de diretório
- Solução de problemas do S3 Lifecycle para buckets de diretório

Criar e gerenciar uma configuração de ciclo de vida para o bucket de diretório

É possível criar uma configuração de ciclo de vida para buckets de diretório usando a AWS Command Line Interface (AWS CLI), os AWS SDKs e as APIs REST.

Usar a CLI do AWS

Use os comandos da AWS CLI a seguir para gerenciar as configurações do S3 Lifecycle:

- `put-bucket-lifecycle-configuration`
- `get-bucket-lifecycle-configuration`
- `delete-bucket-lifecycle`

Consulte instruções sobre como configurar a AWS CLI em Developing with Amazon S3 using the AWS CLI na Referência de API do Amazon S3.

A configuração do ciclo de vida do Amazon S3 é um arquivo XML. Porém, ao usar a AWS CLI, você não pode especificar o formado XML. Em vez disso, você deve especificar o formato JSON. Veja a seguir exemplos de configurações de ciclo de vida em XML e as configurações JSON equivalentes que podem ser especificadas em um comando da AWS CLI.

O exemplo a seguir da AWS CLI coloca uma política de configuração de ciclo de vida em um bucket de diretório. Essa política especifica que todos os objetos que têm o prefixo sinalizado (myprefix) e têm o tamanho de objeto definido expiram após sete dias. Para usar esse exemplo, substitua cada *espaço reservado para entrada do usuário* por suas próprias informações.

Salve a política da configuração do ciclo de vida em um arquivo JSON. Neste exemplo, o arquivo é chamado lifecycle1.json.

Example

JSON

```
{
    "Rules": [
        {
        "Expiration": {
```

```
            "Days": 7
        },
        "ID": "Lifecycle expiration rule",
        "Filter": {
            "And": {
                "Prefix": "myprefix/",
                "ObjectSizeGreaterThan": 500,
                "ObjectSizeLessThan": 64000
            }
        },
        "Status": "Enabled"
    }
    ]
}
```

Envie o arquivo JSON como parte do comando `put-bucket-lifecycle-configuration` da CLI. Para usar esse comando, substitua *cada espaço reservado para entrada do usuário* por suas próprias informações.

```
aws s3api put-bucket-lifecycle-configuration --region us-west-2 --profile default
 --bucket amzn-s3-demo-bucket--usw2-az1--x-s3 --lifecycle-configuration file://lc-
policy.json --checksum-algorithm crc32c
```

Example

XML

```
<LifecycleConfiguration>
    <Rule>
        <ID>Lifecycle expiration rule</ID>
        <Filter>
            <And>
                <Prefix>myprefix/</Prefix>
                <ObjectSizeGreaterThan>500</ObjectSizeGreaterThan>
                <ObjectSizeLessThan>64000</ObjectSizeLessThan>
            </And>
        </Filter>
        <Status>Enabled</Status>
        <Expiration>
             <Days>7</Days>
        </Expiration>
    </Rule>
```

```
</LifecycleConfiguration>
```

Uso dos SDKs da AWS

SDK for Java

Example

```
import
 software.amazon.awssdk.services.s3.model.PutBucketLifecycleConfigurationRequest;
import
 software.amazon.awssdk.services.s3.model.PutBucketLifecycleConfigurationResponse;
import software.amazon.awssdk.services.s3.model.ChecksumAlgorithm;
import software.amazon.awssdk.services.s3.model.BucketLifecycleConfiguration;
import software.amazon.awssdk.services.s3.model.LifecycleRule;
import software.amazon.awssdk.services.s3.model.LifecycleRuleFilter;
import software.amazon.awssdk.services.s3.model.LifecycleExpiration;
import software.amazon.awssdk.services.s3.model.LifecycleRuleAndOperator;
import
 software.amazon.awssdk.services.s3.model.GetBucketLifecycleConfigurationResponse;
import
 software.amazon.awssdk.services.s3.model.GetBucketLifecycleConfigurationRequest;
import software.amazon.awssdk.services.s3.model.DeleteBucketLifecycleRequest;
import software.amazon.awssdk.services.s3.model.DeleteBucketLifecycleResponse;
import software.amazon.awssdk.services.s3.model.AbortIncompleteMultipartUpload;

// PUT a Lifecycle policy
LifecycleRuleFilter objectExpirationFilter =
 LifecycleRuleFilter.builder().and(LifecycleRuleAndOperator.builder().prefix("dir1/").object
LifecycleRuleFilter mpuExpirationFilter =
 LifecycleRuleFilter.builder().prefix("dir2/").build();

LifecycleRule objectExpirationRule =
 LifecycleRule.builder().id("lc").filter(objectExpirationFilter).status("Enabled").expiratio
                    .days(10)
                    .build())
                .build();
LifecycleRule mpuExpirationRule = LifecycleRule.builder().id("lc-
mpu").filter(mpuExpirationFilter).status("Enabled").abortIncompleteMultipartUpload(AbortInco
                        .daysAfterInitiation(10)
                        .build())
                .build();
```

```
PutBucketLifecycleConfigurationRequest putLifecycleRequest =
 PutBucketLifecycleConfigurationRequest.builder()
                .bucket("amzn-s3-demo-bucket--usw2-az1--x-s3")
                .checksumAlgorithm(ChecksumAlgorithm.CRC32)
                .lifecycleConfiguration(
                        BucketLifecycleConfiguration.builder()
                                .rules(objectExpirationRule, mpuExpirationRule)
                                .build()
                ).build();

PutBucketLifecycleConfigurationResponse resp =
 client.putBucketLifecycleConfiguration(putLifecycleRequest);

// GET the Lifecycle policy
GetBucketLifecycleConfigurationResponse getResp =
 client.getBucketLifecycleConfiguration(GetBucketLifecycleConfigurationRequest.builder().buc
s3-demo-bucket--usw2-az1--x-s3").build());

// DELETE the Lifecycle policy
DeleteBucketLifecycleResponse delResp =
 client.deleteBucketLifecycle(DeleteBucketLifecycleRequest.builder().bucket("amzn-
s3-demo-bucket--usw2-az1--x-s3").build());
```

SDK for Go

Example

```
package main

import (
    "context"
    "log"

    "github.com/aws/aws-sdk-go-v2/aws"
    "github.com/aws/aws-sdk-go-v2/config"
    "github.com/aws/aws-sdk-go-v2/service/s3"
    "github.com/aws/aws-sdk-go-v2/service/s3/types"
)
// PUT a Lifecycle policy
func putBucketLifecycleConfiguration(client *s3.Client, bucketName string ) error {
    lifecycleConfig := &s3.PutBucketLifecycleConfigurationInput{
        Bucket: aws.String(bucketName),
        LifecycleConfiguration: &types.BucketLifecycleConfiguration{
            Rules: []types.LifecycleRule{
```

```
                {
                    ID:     aws.String("lc"),
                    Filter: &types.LifecycleRuleFilter{
                        And: &types.LifecycleRuleAndOperator{
                            Prefix: aws.String("foo/"),
                            ObjectSizeGreaterThan: aws.Int64(1000000),
                            ObjectSizeLessThan:    aws.Int64(100000000),
                            },
                        },

                    Status: types.ExpirationStatusEnabled,
                    Expiration: &types.LifecycleExpiration{
                        Days: aws.Int32(int32(1)),
                    },
                },
                {
                    ID:     aws.String("abortmpu"),
                    Filter: &types.LifecycleRuleFilter{
                        Prefix: aws.String("bar/"),
                    },
                    Status: types.ExpirationStatusEnabled,
                    AbortIncompleteMultipartUpload:
 &types.AbortIncompleteMultipartUpload{
                        DaysAfterInitiation: aws.Int32(int32(5)),
                    },
                },
            },
        },
    }
    _, err := client.PutBucketLifecycleConfiguration(context.Background(),
 lifecycleConfig)
    return err
}
// Get the Lifecycle policy
func getBucketLifecycleConfiguration(client *s3.Client, bucketName string) error {
    getLifecycleConfig := &s3.GetBucketLifecycleConfigurationInput{
        Bucket: aws.String(bucketName),
    }

    resp, err := client.GetBucketLifecycleConfiguration(context.Background(),
 getLifecycleConfig)
    if err != nil {
        return err
    }
```

```
    return nil
}
// Delete the Lifecycle policy
func deleteBucketLifecycleConfiguration(client *s3.Client, bucketName string) error
 {
    deleteLifecycleConfig := &s3.DeleteBucketLifecycleInput{
        Bucket: aws.String(bucketName),
    }
    _, err := client.DeleteBucketLifecycle(context.Background(),
 deleteLifecycleConfig)
    return err
}
func main() {
    cfg, err := config.LoadDefaultConfig(context.Background(),
 config.WithRegion("us-west-2")) // Specify your region here
    if err != nil {
        log.Fatalf("unable to load SDK config, %v", err)
    }
    s3Client := s3.NewFromConfig(cfg)
    bucketName := "amzn-s3-demo-bucket--usw2-az1--x-s3"
    putBucketLifecycleConfiguration(s3Client, bucketName)
    getBucketLifecycleConfiguration(s3Client, bucketName)
    deleteBucketLifecycleConfiguration(s3Client, bucketName)
    getBucketLifecycleConfiguration(s3Client, bucketName)
}
```

SDK for .NET

Example

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Collections.Generic;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class LifecycleTest
    {
        private const string bucketName = "amzn-s3-demo-bucket--usw2-az1--x-s3";
        // Specify your bucket region (an example region is shown).
```

```
        private static readonly RegionEndpoint bucketRegion =
RegionEndpoint.USWest2;
        private static IAmazonS3 client;
        public static void Main()
        {
            client = new AmazonS3Client(bucketRegion);
            AddUpdateDeleteLifecycleConfigAsync().Wait();
        }

        private static async Task AddUpdateDeleteLifecycleConfigAsync()
        {
            try
            {
                var lifeCycleConfiguration = new LifecycleConfiguration()
                {
                    Rules = new List <LifecycleRule>
                        {
                            new LifecycleRule
                            {
                                 Id = "delete rule",
                                  Filter = new LifecycleFilter()
                                 {
                                     LifecycleFilterPredicate = new
LifecyclePrefixPredicate()
                                     {
                                         Prefix = "projectdocs/"
                                     }
                                 },
                                 Status = LifecycleRuleStatus.Enabled,
                                 Expiration = new LifecycleRuleExpiration()
                                 {
                                       Days = 10
                                 }
                            }
                        }
                };

                // Add the configuration to the bucket.
                await AddExampleLifecycleConfigAsync(client,
lifeCycleConfiguration);

                // Retrieve an existing configuration.
                lifeCycleConfiguration = await RetrieveLifecycleConfigAsync(client);
```

```
                // Add a new rule.
                lifeCycleConfiguration.Rules.Add(new LifecycleRule
                {
                    Id = "mpu abort rule",
                    Filter = new LifecycleFilter()
                    {
                        LifecycleFilterPredicate = new LifecyclePrefixPredicate()
                        {
                            Prefix = "YearlyDocuments/"
                        }
                    },
                    Expiration = new LifecycleRuleExpiration()
                    {
                        Days = 10
                    },
                    AbortIncompleteMultipartUpload = new
LifecycleRuleAbortIncompleteMultipartUpload()
                    {
                        DaysAfterInitiation = 10
                    }
                });

                // Add the configuration to the bucket.
                await AddExampleLifecycleConfigAsync(client,
lifeCycleConfiguration);

                // Verify that there are now two rules.
                lifeCycleConfiguration = await RetrieveLifecycleConfigAsync(client);
                Console.WriteLine("Expected # of rulest=2; found:{0}",
lifeCycleConfiguration.Rules.Count);

                // Delete the configuration.
                await RemoveLifecycleConfigAsync(client);

                // Retrieve a nonexistent configuration.
                lifeCycleConfiguration = await RetrieveLifecycleConfigAsync(client);

            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered ***. Message:'{0}' when writing
an object", e.Message);
            }
            catch (Exception e)
```

```
            {
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
 writing an object", e.Message);
            }
        }

        static async Task AddExampleLifecycleConfigAsync(IAmazonS3 client,
 LifecycleConfiguration configuration)
        {

            PutLifecycleConfigurationRequest request = new
 PutLifecycleConfigurationRequest
            {
                BucketName = bucketName,
                Configuration = configuration
            };
            var response = await client.PutLifecycleConfigurationAsync(request);
        }

        static async Task <LifecycleConfiguration>
 RetrieveLifecycleConfigAsync(IAmazonS3 client)
        {
            GetLifecycleConfigurationRequest request = new
 GetLifecycleConfigurationRequest
            {
                BucketName = bucketName
            };
            var response = await client.GetLifecycleConfigurationAsync(request);
            var configuration = response.Configuration;
            return configuration;
        }

        static async Task RemoveLifecycleConfigAsync(IAmazonS3 client)
        {
            DeleteLifecycleConfigurationRequest request = new
 DeleteLifecycleConfigurationRequest
            {
                BucketName = bucketName
            };
            await client.DeleteLifecycleConfigurationAsync(request);
        }
    }
}
```

SDK for Python

Example

```
import boto3

client = boto3.client("s3", region_name="us-west-2")
bucket_name = 'amzn-s3-demo-bucket--usw2-az1--x-s3'

client.put_bucket_lifecycle_configuration(
    Bucket=bucket_name,
    ChecksumAlgorithm='CRC32',
    LifecycleConfiguration={
        'Rules': [
            {
                'ID': 'lc',
                'Filter': {
                    'And': {
                        'Prefix': 'foo/',
                        'ObjectSizeGreaterThan': 1000000,
                        'ObjectSizeLessThan': 100000000,
                    }
                },
                'Status': 'Enabled',
                'Expiration': {
                    'Days': 1
                }
            },
            {
                'ID': 'abortmpu',
                'Filter': {
                    'Prefix': 'bar/'
                },
                'Status': 'Enabled',
                'AbortIncompleteMultipartUpload': {
                    'DaysAfterInitiation': 5
                }
            }
        ]
    }
)

result = client.get_bucket_lifecycle_configuration(
    Bucket=bucket_name
```

```
)

client.delete_bucket_lifecycle(
    Bucket=bucket_name
)
```

Solução de problemas do S3 Lifecycle para buckets de diretório

Tópicos

- Eu defini minha configuração de ciclo de vida, mas os objetos no meu bucket de diretório não estão expirando
- Como monitorar as ações realizadas pelas minhas regras de ciclo de vida?

Eu defini minha configuração de ciclo de vida, mas os objetos no meu bucket de diretório não estão expirando

O S3 Lifecycle para buckets de diretório utiliza APIs públicas para excluir objetos na classe S3 Express One Zone. Para usar APIs públicas no nível do objeto, você deve conceder permissão para `CreateSession` e permitir que o S3 Lifecycle exclua seus objetos. Se você tiver uma política ativa que nega exclusões, isso impedirá que você permita que o S3 Lifecycle exclua objetos em seu nome.

É importante configurar as políticas de bucket corretamente para garantir que os objetos que você deseja excluir sejam elegíveis para expiração. Você pode verificar seus logs do AWS CloudTrail para trilhas `AccessDenied` de invocações da API `CreateSession` no CloudTrail para verificar se o acesso foi negado. A verificação dos logs do CloudTrail pode ajudar a solucionar problemas de acesso e identificar a causa raiz dos erros de acesso negado. Depois, você pode corrigir seus controles de acesso incorretos atualizando as políticas relevantes.

Se você confirmar que as políticas de bucket estão definidas corretamente e ainda está enfrentando problemas, recomendamos revisar as regras do ciclo de vida para garantir que elas sejam aplicadas ao subconjunto correto de objetos.

Como monitorar as ações realizadas pelas minhas regras de ciclo de vida?

Você pode usar os logs de eventos de dados do AWS CloudTrail para monitorar as ações realizadas pelo S3 Lifecycle em buckets de diretório. Consulte mais informações em CloudTrail log file examples.

Usar a funcionalidade Operações em Lote com buckets de diretório

Você pode usar a funcionalidade Operações em Lote do Amazon S3 para executar operações em lote de grande escala em objetos armazenados em buckets do S3. Para saber mais sobre a funcionalidade Operações em Lote do S3, consulte Executar operações em lote de grande escala em objetos do Amazon S3.

Os tópicos a seguir discutem a execução de operações em lote em objetos armazenados em buckets de diretório na classe de armazenamento S3 Express One Zone.

Tópicos

- Usar a funcionalidade Operações em Lote com buckets de diretório
- Principais diferenças

Usar a funcionalidade Operações em Lote com buckets de diretório

Você pode realizar a operação Copiar e as operações Invocar função do AWS Lambda em objetos armazenados em buckets de diretório. Com Copiar, é possível copiar objetos entre buckets do mesmo tipo (por exemplo, de um bucket de diretório para outro bucket de diretório). Você também pode copiar entre buckets de uso geral e buckets de diretório. Com Invocar função do AWS Lambda, você pode usar uma função do Lambda para realizar ações em objetos no seu bucket de diretório com código definido por você.

Cópia de objetos

Você pode copiar entre o mesmo tipo de bucket ou entre buckets de diretório e buckets de uso geral. Ao copiar para um bucket de diretório, você deve usar o formato de nome do recurso da Amazon (ARN) correto para esse tipo de bucket. O formato de ARN para um bucket de diretório é `arn:aws:s3express:`*`region`*`:`*`account-id`*`:bucket/`*`bucket-base-name`*`--x-s3`.

> **Note**
>
> Não há suporte à cópia de objetos entre diferentes Regiões da AWS quando o bucket de origem ou de destino está em uma zona local da AWS. Os buckets de origem e de destino devem ter a mesma Região da AWS principal. Os buckets de origem e de destino podem ser de diferentes tipos de localização de bucket (zona de disponibilidade ou zona local).

Você também pode preencher o bucket de diretório com dados usando a ação Importar no console do S3. Importar é um método simplificado para criar trabalhos da funcionalidade Operações em Lote a fim de copiar objetos de buckets de uso geral para buckets de diretório. Para trabalhos de cópia com Importar de buckets de uso geral para buckets de diretório, o S3 gera um manifesto automaticamente. Para obter mais informações, consulte Importar objetos em um bucket de diretório e Specifying a manifest.

Invocar funções do Lambda (**`LambdaInvoke`**)

Há requisitos especiais para usar a funcionalidade Operações em Lote para invocar funções do Lambda que atuam em buckets de diretório. Por exemplo, você deve estruturar a solicitação do Lambda usando um esquema de invocação JSON v2 e especificar InvocationSchemaVersion 2.0 ao criar o trabalho. Para obter mais informações, consulte Invocar função do AWS Lambda.

Principais diferenças

Veja a seguir uma lista das principais diferenças ao usar a funcionalidade Operações em Lote para realizar operações em massa para objetos armazenados em buckets de diretório com a classe de armazenamento S3 Express One Zone:

- Em relação a buckets de diretório, são aceitas a SSE-S3 e a criptografia do lado do servidor com chaves do AWS Key Management Service (AWS KMS) (SSE-KMS). Se você fizer uma solicitação `CopyObject` que especifique a criptografia do lado do servidor com chaves fornecidas pelo cliente (SSE-C) em um bucket de diretório (origem ou destino), a resposta exibirá um erro HTTP `400 (Bad Request)`.

  Recomendamos que a criptografia padrão do bucket use a configuração desejada e que você não a substitua em suas solicitações `CreateSession` ou de objetos PUT. Desse modo, os novos objetos são criptografados automaticamente com as configurações de criptografia desejadas. Para ter mais informações sobre os comportamentos de substituição de criptografia em buckets de diretório e como criptografar novas cópias de objetos em um bucket de diretório com SSE-KMS, consulte Especificar a criptografia do lado do servidor com o AWS KMS (SSE-KMS) para novos uploads de objetos em buckets de diretório.

  As chaves de bucket do S3 não são aceitas quando você copia objetos criptografados por SSE-KMS de buckets de uso geral para buckets de diretório, de buckets de diretório para buckets de uso geral ou entre buckets de diretório, por meio da operação Copy em Operações em Lote. Nesse caso, o Amazon S3 faz uma chamada para o AWS KMS sempre que uma solicitação de cópia é feita para um objeto criptografado pelo KMS. Para ter mais informações sobre como usar a

SSE-KMS em buckets de diretório, consulte Definir e monitorar a criptografia padrão para buckets de diretório e Usar a criptografia do lado do servidor com chaves do AWS KMS (SSE-KMS) em buckets de diretório.

- Não é possível marcar objetos em buckets de diretório. Você só pode especificar um conjunto vazio de etiquetas. Por padrão, a funcionalidade Operações em Lote copia as etiquetas. Se você copiar um objeto que tenha etiquetas entre buckets de uso geral e buckets de diretório, receberá uma resposta `501 (Not Implemented)`.
- A classe S3 Express One Zone oferece a opção de escolher o algoritmo de soma de verificação usado para validar os dados durante uploads ou downloads. Você pode selecionar um dos seguintes algoritmos de verificação de integridade de dados de hash seguro (SHA) ou de verificação de redundância cíclica (CRC): CRC32, CRC32, SHA-1 e SHA-256. As somas de verificação baseadas em MD5 não são compatíveis com a classe de armazenamento S3 Express One Zone.
- Por padrão, todos os buckets do Amazon S3 definem a configuração Propriedade do objeto do S3 como Imposto pelo proprietário do bucket e as listas de controle de acesso (ACLs) estão desabilitadas. Para buckets de diretório, essa configuração não pode ser modificada. Você pode copiar um objeto de buckets de uso geral para buckets de diretório. No entanto, não é possível sobrescrever a ACL padrão ao copiar de ou para um bucket de diretório.
- Independentemente de como você especifica o manifesto, a lista em si deve ser armazenada em um bucket de uso geral. A funcionalidade Operações em Lote não pode importar manifestos existentes de buckets de diretório (nem salvar manifestos gerados neles). No entanto, os objetos descritos no manifesto podem ser armazenados em buckets de diretório.
- A funcionalidade Operações em Lote não consegue especificar um bucket de diretório como um local em um relatório da funcionalidade Inventário S3. Os relatórios da funcionalidade Inventário não são compatíveis com buckets de diretório. Você pode criar um arquivo de manifesto para objetos em um bucket de diretório usando a operação de API `ListObjectsV2` para listar os objetos. Depois, você pode inserir a lista em um arquivo CSV.

Como conceder acesso ao

Para realizar trabalhos de cópia, você deve ter as seguintes permissões:

- Para copiar objetos de um bucket de diretório para outro bucket de diretório, você precisa ter a permissão `s3express:CreateSession`.

- Para copiar objetos de buckets de diretório para buckets de uso geral, você precisa ter a permissão `s3express:CreateSession` e a permissão `s3:PutObject` para gravar a cópia do objeto no bucket de destino.
- Para copiar objetos de buckets de uso geral para buckets de diretório, você precisa ter a permissão `s3express:CreateSession` e a permissão `s3:GetObject` para ler o objeto de origem que está sendo copiado.

  Para obter mais informações, consulte CopyObject na Referência da API do Amazon Simple Storage Service.
- Para invocar uma função do Lambda, você deve conceder permissões ao recurso com base na função do Lambda. Para determinar quais permissões são necessárias, verifique as operações de API correspondentes.

Anexar dados a objetos em buckets de diretórios

É possível adicionar dados ao final de objetos existentes armazenados na classe de armazenamento S3 Express One Zone em buckets de diretório. Recomendamos que você use a capacidade de anexar dados a um objeto se os dados forem gravados continuamente por um período de tempo ou se você precisar ler o objeto enquanto estiver gravando nele. Anexar dados a objetos é comum em casos de uso como adição de novas entradas de log a arquivos de log ou adição de novos segmentos de vídeo a arquivos de vídeo à medida que são transcodificados e transmitidos. Ao anexar dados aos objetos, você pode simplificar aplicações que anteriormente combinavam dados no armazenamento local antes de copiar o objeto final no Amazon S3.

Não há exigência de tamanho mínimo para os dados que você pode anexar a um objeto. No entanto, o tamanho máximo dos dados que você pode anexar a um objeto em uma única solicitação é de 5 GB. Esse é o mesmo limite do maior tamanho de solicitação ao carregar dados usando qualquer API do Amazon S3.

Com cada operação de anexação bem-sucedida, você cria uma parte do objeto e cada objeto pode ter até dez mil partes. Isso significa que você pode anexar dados a um objeto até dez mil vezes. Se um objeto for criado usando o carregamento fracionado do S3, cada parte carregada será contabilizada no máximo total de dez mil partes. Por exemplo, você pode anexar até novo mil vezes a um objeto criado pelo carregamento fracionado composto por mil partes.

> **Note**
>
> Se você atingir o limite de peças, receberá um erro TooManyParts. Você pode usar a API `CopyObject` para redefinir a contagem.

Se você quiser fazer um carregamento fracionado para um objeto em paralelo e não precisar ler as partes enquanto elas estão sendo carregadas, recomendamos usar o carregamento fracionado do Amazon S3. Consulte mais informações em Usar uploads multiparte.

Anexar dados a objetos só é permitido para objetos em buckets de diretório armazenados na classe de armazenamento S3 Express One Zone. Consulte mais informações sobre a classe S3 Express One Zone em Conceitos básicos da classe S3 Express One Zone.

Para começar a anexar dados a objetos em buckets de diretório, você pode usar os AWS SDKs, a AWS CLI e a API `PutObject`. Ao fazer uma solicitação `PutObject`, você define o cabeçalho `x-amz-write-offset-bytes` com o tamanho do objeto ao qual está anexando. Para usar a operação de API `PutObject`, você deve usar a API `CreateSession` para estabelecer credenciais de segurança temporárias a fim de acessar os objetos nos buckets de diretório. Para ter mais informações, consulte `PutObject` e `CreateSession` na Referência de API do Amazon S3.

Cada operação de anexação bem-sucedida é cobrada como uma solicitação `PutObject`. Para saber mais sobre o preço, consulte `Amazon S3 pricing`.

> **Note**
>
> A partir da versão 1.12, o Mountpoint para Amazon S3 é compatível com a anexação de dados a objetos armazenados na classe S3 Express One Zone. Para começar, é necessário definir o indicador `--incremental-upload` para ativação. Consulte mais informações sobre o Mountpoint em Working with Mountpoint.

Se você usar um algoritmo CRC (verificação de redundância cíclica) ao fazer upload dos dados anexados, poderá recuperar somas de verificação completas baseadas em CRC do objeto usando a solicitação `HeadObject` ou `GetObject`. Se você usar o algoritmo SHA-1 ou SHA-256 ao fazer upload dos dados anexados, poderá recuperar uma soma de verificação das partes anexadas e verificar sua integridade usando as somas de verificação SHA retornadas nas respostas anteriores de PutObject. Para ter mais informações, consulte Proteção de dados e criptografia.

Anexar dados a objetos usando a AWS CLI, os AWS SDKs e a API REST

Você pode anexar dados a objetos usando a AWS Command Line Interface (AWS CLI), os AWS SDKs e a API REST.

Usar a CLI do AWS

O exemplo de comando `put-object` a seguir mostra como você pode usar a AWS CLI para anexar dados a um objeto. Para executar esse comando, substitua os *espaços reservados de entrada do usuário* por suas próprias informações

```
aws s3api put-object --bucket amzn-s3-demo-bucket--azid--x-s3 --key sampleinput/
file001.bin --body bucket-seed/file001.bin --write-offset-bytes size-of-sampleinput/
file001.bin
```

Uso dos SDKs da AWS

SDK for Java

Você pode usar o AWS SDK para Java para anexar dados a objetos.

```
var putObjectRequestBuilder = PutObjectRequest.builder()
                                              .key(key)
                                              .bucket(bucketName)
                                              .writeOffsetBytes(9);
var response = s3Client.putObject(putObjectRequestBuilder.build());
```

SDK for Python

```
s3.put_object(Bucket='amzn-s3-demo-bucket--use2-az2--x-s3', Key='2024-11-05-sdk-
test', Body=b'123456789', WriteOffsetBytes=9)
```

Uso da API REST

Você pode enviar solicitações REST para anexar um objeto. Para obter mais informações, consulte `PutObject`.

Renomear objetos em buckets de diretório

Usando a operação `RenameObject`, você pode renomear atomicamente um objeto existente em um bucket de diretório que usa a classe de armazenamento S3 Express One Zone, sem nenhuma

movimentação de dados. Você pode renomear um objeto especificando o nome do objeto existente como origem e o novo nome como destino no mesmo bucket de diretório. A operação de API `RenameObject` não terá êxito em objetos que terminam com o caractere delimitador de barra (`/`). Para ter mais informações, consulte Nomear objetos do Amazon S3.

A operação `RenameObject` geralmente é concluída em milissegundos, independentemente do tamanho do objeto. Esse recurso acelera determinadas aplicações, como gerenciamento de arquivos de log, processamento de mídia e data analytics. Além disso, `RenameObject` preserva todas as propriedades de metadados do objeto, como classe de armazenamento, tipo de criptografia, data de criação, data da última modificação e soma de verificação.

> **Note**
>
> Só é possível usar `RenameObject` com objetos armazenados na classe de armazenamento S3 Express One Zone.

Para conceder acesso à operação `RenameObject`, recomendamos usar a operação `CreateSession` para autorização baseada em sessão. Mais especificamente, você concede a permissão `s3express:CreateSession` ao bucket de diretório em uma política de bucket ou em uma política baseada em identidade. Em seguida, você faz a chamada de API `CreateSession` no bucket do diretório para obter um token de sessão. Com o token de sessão no cabeçalho da solicitação, você pode fazer solicitações de API para essa operação. Depois que o token da sessão expirar, você faz outra chamada de API `CreateSession` para gerar um novo token de sessão e usá-lo. A AWS CLI e os SDKs da AWS vão criar e gerenciar sua sessão, até mesmo atualizar automaticamente o respectivo token para evitar interrupções no serviço quando uma sessão expira. Para ter mais informações sobre autorização, consulte `CreateSession` na Referência de API do Amazon S3. Para saber mais sobre as operações de API de endpoint zonal, consulte Autorizar operações de API de endpoint zonal com `CreateSession`.

Se você não quiser substituir um objeto existente, adicione o cabeçalho condicional `If-None-Match` com o valor `'*'` na solicitação `RenameObject`. O Amazon S3 retornará o erro `412 Precondition Failed` se o nome do objeto já existir. Para obter mais informações, consulte `RenameObject` na Referência da API do Amazon S3.

`RenameObject` é uma operação de API de endpoint zonal (operação em nível de objeto ou de plano de dados) que é registrada em log em AWS CloudTrail. Você pode usar o CloudTrail para coletar informações sobre a operação `RenameObject` realizada em seus objetos em buckets de diretório.

Para ter mais informações, consulte Registro em log com o AWS CloudTrail para buckets de diretório e Exemplos de arquivos de log do CloudTrail para buckets de diretório.

O S3 Express One Zone é a única classe de armazenamento que permite a operação `RenameObject`, que tem o mesmo preço das solicitações `PUT`, `COPY`, `POST` e `LIST` (por mil solicitações) no S3 Express One Zone. Para obter mais informações, consulte Preço do Amazon S3.

Renomear um objeto

Para renomear um objeto em um bucket de diretório, você pode usar o console do Amazon S3, a AWS CLI, SDKs da AWS, a API REST ou o Mountpoint para Amazon S3 (versão 1.19.0 ou posterior).

Usar o console do S3

Como renomear um objeto em um bucket de diretório

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets e selecione a guia Buckets de diretório. Navegue até o bucket de diretório do Amazon S3 que contém o objeto que você deseja renomear.
3. Marque a caixa de seleção referente ao objeto que você quer renomear.
4. No menu Ações, selecione Renomear objeto.
5. Na caixa Nome do novo objeto, insira o novo nome do objeto.

> **Note**
>
> Se você especificar um nome de objeto que seja igual ao de um objeto existente, a operação não terá êxito e o Amazon S3 retornará o erro `412 Precondition Failed`. O comprimento do nome da chave do objeto não pode exceder 1.024 bytes. Os prefixos incluídos no nome do objeto entram na contagem do comprimento total.

6. Escolha Renomear objeto. O Amazon S3 renomeia o objeto.

Usar a CLI do AWS

Os exemplos de `rename-object` mostram como você pode usar a AWS CLI para renomear um objeto. Para executar esse comando, substitua os *espaços reservados para entrada do usuário* por suas próprias informações.

O exemplo a seguir mostra como renomear um objeto com uma verificação condicional na ETag do objeto de origem.

```
aws s3api rename-object \
    --bucket amzn-s3-demo-bucket--usw2-az1--x-s3 \
    --key new-file.txt \
    --rename-source amzn-s3-demo-bucket--usw2-az1--x-s3/original-file.txt \
    --source-if-match "\"a1b7c3d2e5f6\""
```

Esse comando faz o seguinte:

- Muda o nome de um objeto de *original-file.txt* para *new-file.txt* no bucket de diretório *amzn-s3-demo-bucket--usw2-az1--x-s3*.
- Só renomeia se a ETag do objeto de origem corresponder a "*a1b7c3d4e5f6*".

Se a ETag não corresponder, a operação não terá êxito e exibirá um erro `412 Precondition Failed`.

O exemplo a seguir mostra como renomear um objeto com uma verificação condicional no novo nome de objeto especificado.

```
aws s3api rename-object \
    --bucket amzn-s3-demo-bucket--usw2-az1--x-s3 \
    --key new-file.txt \
    --rename-source amzn-s3-demo-bucket--usw2-az1--x-s3/original-file.txt \
    --destination-if-none-match "\"e5f3g7h8i9j0\""
```

Esse comando faz o seguinte:

- Muda o nome de um objeto de *original-file.txt* para *new-file.txt* no bucket de diretório *amzn-s3-demo-bucket--usw2-az1--x-s3*.
- Só executa a operação de renomeação se o objeto existir e a respectiva ETag não corresponder a "*e5f3g7h8i9j0*".

Se já existir um objeto com o novo nome especificado e a ETag correspondente, a operação não terá êxito e exibirá o erro `412 Precondition Failed`.

Uso dos SDKs da AWS

SDK for Java

Você pode usar o AWS SDK para Java para renomear objetos. Para usar esses exemplos, substitua os *espaços reservados para entrada do usuário* por suas próprias informações.

O exemplo a seguir demonstra como criar um `RenameObjectRequest` usando o AWS SDK para Java.

```
String key = "key";
String newKey = "new-key";
String expectedETag = "e5f3g7h8i9j0";
RenameObjectRequest renameRequest = RenameObjectRequest.builder()
    .bucket(amzn-s3-demo-bucket--usw2-az1--x-s3)
    .key(newKey)
    .renameSource(key)
    .destinationIfMatch(e5f3g7h8i9j0)
    .build();
```

Esse código faz o seguinte:

- Crie uma solicitação para renomear um objeto de "*key*" para "*new-key*" no bucket de diretório *amzn-s3-demo-bucket--usw2-az1--x-s3*.
- Inclui a condição de que a renomeação só ocorrerá se a ETag do objeto corresponder a "*e5f3g7h8i9j0*".
- Se a ETag não corresponder ou o objeto não existir, a operação não terá êxito.

O exemplo a seguir mostra como criar uma `RenameObjectRequest` com uma condição de não correspondência usando o AWS SDK para Java.

```
String key = "key";
String newKey = "new-key";
String noneMatchETag = "e5f3g7h8i9j0";
RenameObjectRequest renameRequest = RenameObjectRequest.builder()
    .bucket(amzn-s3-demo-bucket--usw2-az1--x-s3)
```

```
    .key(newKey)
    .renameSource(key)
    .destinationIfNoneMatch(noneMatchETag)
    .build();
```

Esse código faz o seguinte:

- Cria uma solicitação para renomear um objeto de "*key*" para "*new-key*" no bucket de diretório *amzn-s3-demo-bucket--usw2-az1--x-s3*.
- Inclui uma condição usando `.destinationIfNoneMatch(noneMatchETag)`, que garante que a renomeação só ocorrerá se a ETag do objeto de destino corresponder a "*e5f3g7h8i9j0*".

A operação não terá êxito e exibirá o erro `412 Precondition Failed` se um objeto com o novo nome especificado existir e tiver a ETag especificada.

SDK for Python

Você pode usar o SDK para Python para renomear objetos. Para usar esses exemplos, substitua os *espaços reservados para entrada do usuário* por suas próprias informações.

O exemplo a seguir demonstra como renomear um objeto usando o AWS SDK para Python (Boto3).

```
def basic_rename(bucket, source_key, destination_key):
    try:
        s3.rename_object(
            Bucket=amzn-s3-demo-bucket--usw2-az1--x-s3,
            Key=destination_key,
            RenameSource=f"{amzn-s3-demo-bucket--usw2-az1--x-s3}/{source_key}"
        )
        print(f"Successfully renamed {source_key} to {destination_key}")
    except ClientError as e:
        print(f"Error renaming object: {e}")
```

Esse código faz o seguinte:

- Muda o nome de um objeto de *source_key* para *destination_key* no bucket de diretório *amzn-s3-demo-bucket--usw2-az1--x-s3*.
- Imprime uma mensagem de êxito se a renomeação do objeto for bem-sucedida ou uma mensagem de erro se ela não tiver êxito.

O exemplo a seguir demonstra como renomear um objeto com as condições `SourceIfMatch` e `DestinationIfNoneMatch` usando o AWS SDK para Python (Boto3).

```
def rename_with_conditions(bucket, source_key, destination_key, source_etag,
 dest_etag):
    try:
        s3.rename_object(
            Bucket=amzn-s3-demo-bucket--usw2-az1--x-s3,
            Key=destination_key,
            RenameSource=f"{amzn-s3-demo-bucket--usw2-az1--x-s3}/{source_key}",
            SourceIfMatch=source_ETag,
            DestinationIfNoneMatch=dest_ETag
        )
        print(f"Successfully renamed {source_key} to {destination_key} with
 conditions")
    except ClientError as e:
        print(f"Error renaming object: {e}")
```

Esse código faz o seguinte:

- Executa uma operação de renomeação condicional e aplica duas condições, `SourceIfMatch` e `DestinationIfNoneMatch`. A combinação dessas condições confere se o objeto não foi modificado e se ainda não existe um objeto com o novo nome especificado.
- Muda o nome de um objeto de *source_key* para *destination_key* no bucket de diretório *amzn-s3-demo-bucket--usw2-az1--x-s3*.
- Imprime uma mensagem de êxito se a renomeação do objeto for bem-sucedida ou uma mensagem de erro se as condições não forem atendidas.

SDK for Rust

Você pode usar o SDK para Rust para renomear objetos. Para usar esses exemplos, substitua os *espaços reservados para entrada do usuário* por suas próprias informações.

O exemplo a seguir demonstra como renomear um objeto no bucket de diretório *amzn-s3-demo-bucket--usw2-az1--x-s3* usando o SDK para Rust.

```
async fn basic_rename_example(client: &Client) -> Result<(), Box<dyn Error>> {
    let response = client
        .rename_object()
        .bucket(" amzn-s3-demo-bucket--usw2-az1--x-s3")
```

```
        .key("new-name.txt")  // New name/path for the object
        .rename_source("old-name.txt")  // Original object name/path
        .send()
        .await?;
    Ok(())
}
```

Esse código faz o seguinte:

- Cria uma solicitação para mudar o nome de um objeto de "*old-name.tx*" para "*new-name.txt*" no bucket de diretório *amzn-s3-demo-bucket--usw2-az1--x-s3*.
- Retorna um tipo `Result` para lidar com possíveis erros.

Uso da API REST

Você pode enviar solicitações REST para renomear um objeto. Para obter mais informações, consulte `RenameObject` na Referência da API do Amazon S3.

Usar o Mountpoint para Amazon S3

A partir da versão 1.19.0 ou posterior, o Mountpoint para Amazon S3 permite a renomeação de objetos no S3 Express One Zone. Consulte mais informações sobre o Mountpoint em Working with Mountpoint.

Fazer upload de objetos em um bucket de diretório

Depois de criar um bucket de diretório do Amazon S3, você pode fazer upload de objetos nele. Os exemplos a seguir mostram como fazer upload de um objeto em um bucket de diretório usando o console do S3 e os AWS SDKs. Para obter informações sobre as operações de upload de objetos em massa com a classe S3 Express One Zone, consulte Gerenciamento de objetos.

Usar o console do S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets de diretórios.
3. Escolha o nome do bucket no qual você deseja fazer upload de pastas ou arquivos.
4. Na guia Objetos, escolha Fazer upload.
5. Na página Fazer upload, execute uma das seguintes ações:

- Arraste e solte arquivos e pastas para a área de upload tracejada.
- Escolha Adicionar arquivos ou Adicionar pasta, selecione os arquivos ou as pastas que deseja carregar e escolha Abrir ou Fazer upload.

6. Em Checksums, escolha a Função de soma de verificação que deseja usar.

   (Opcional) Se você estiver fazendo upload de um único objeto com menos de 16 MB, também poderá especificar um valor de soma de verificação pré-calculado. Quando você fornece um valor pré-calculado, o Amazon S3 compara esse valor com o valor calculado usando a função de soma de verificação selecionada. Se os valores não corresponderem, o upload não será iniciado.

7. As opções nas seções Permissões e Propriedades são definidas automaticamente com as configurações padrão e não podem ser modificadas. A funcionalidade Bloqueio de Acesso Público é habilitada automaticamente, e as funcionalidades Versionamento do S3 e Bloqueio de Objetos do S3 não podem ser habilitadas para buckets de diretório.

   (Opcional) Se você quiser adicionar metadados em pares de chave e valor aos objetos, expanda a seção Propriedades e escolha Adicionar metadados na seção Metadados.

8. Para fazer upload das pastas e dos arquivos listados, escolha Fazer upload.

   O Amazon S3 faz o upload de seus objetos e pastas. Quando o upload for concluído, você verá uma mensagem de sucesso na página Upload: status.

Uso dos SDKs da AWS

SDK for Java 2.x

Example

```
public static void putObject(S3Client s3Client, String bucketName, String objectKey,
 Path filePath) {
       //Using File Path to avoid loading the whole file into memory
       try {
           PutObjectRequest putObj = PutObjectRequest.builder()
                   .bucket(bucketName)
                   .key(objectKey)
                   //.metadata(metadata)
                   .build();
           s3Client.putObject(putObj, filePath);
```

```
            System.out.println("Successfully placed " + objectKey +" into bucket
 "+bucketName);

        }

        catch (S3Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
}
```

SDK for Python

Example

```
import boto3
import botocore
from botocore.exceptions import ClientError


def put_object(s3_client, bucket_name, key_name, object_bytes):
    """
    Upload data to a directory bucket.
    :param s3_client: The boto3 S3 client
    :param bucket_name: The bucket that will contain the object
    :param key_name: The key of the object to be uploaded
    :param object_bytes: The data to upload
    """
    try:
        response = s3_client.put_object(Bucket=bucket_name, Key=key_name,
                            Body=object_bytes)
        print(f"Upload object '{key_name}' to bucket '{bucket_name}'.")
        return response
    except ClientError:
        print(f"Couldn't upload object '{key_name}' to bucket '{bucket_name}'.")
        raise

def main():
    # Share the client session with functions and objects to benefit from S3 Express
 One Zone auth key
    s3_client = boto3.client('s3')
    # Directory bucket name must end with --zone-id--x-s3
    resp = put_object(s3_client, 'doc-bucket-example--use1-az5--x-s3', 'sample.txt',
 b'Hello, World!')
```

```
    print(resp)

if __name__ == "__main__":
    main()
```

Como usar o AWS CLI

O exemplo de comando `put-object` a seguir mostra como você pode usar a AWS CLI para carregar um objeto do Amazon S3. Para executar esse comando, substitua os *`user input placeholders`* por suas próprias informações.

```
aws s3api put-object --bucket bucket-base-name--zone-id--x-s3 --key sampleinut/
file001.bin --body bucket-seed/file001.bin
```

Para obter mais informações, consulte put-object na Referência de comandos da AWS CLI.

Tópicos

- Usar uploads multiparte com buckets de diretório

Usar uploads multiparte com buckets de diretório

Você pode usar o processo de upload multiparte para fazer upload de um único objeto como um conjunto de partes. Cada parte é uma parte contígua de dados do objeto. O upload dessas partes de objetos pode ser feito de maneira independente e em qualquer ordem. Se a transmissão de alguma parte falhar, você poderá retransmitir essa parte sem afetar outras partes. Depois que todas as partes do objeto forem carregadas, o Amazon S3 montará essas partes e criará o objeto. Geralmente, quando seu objeto alcança 100 MB de tamanho, você deve considerar o uso de multipart uploads em vez de fazer upload do objeto em uma única operação.

Usar o multipart upload fornece as seguintes vantagens:

- Improved throughput (Throughput aprimorada): você pode carregar as partes em paralelo para melhorar o throughput.
- Rápida recuperação de qualquer problema de rede: o tamanho menor das partes minimiza o impacto de reiniciar um upload que falhou devido a um erro de rede.
- Pause and resume object uploads (Pausar e retomar carregamentos de objetos): você pode carregar as partes do objeto ao longo do tempo. Um upload multiparte iniciado não tem data de expiração. Você deve concluir ou anular explicitamente o upload multiparte.

- Begin an upload before you know the final object size (Começar um carregamento antes de saber o tamanho final do objeto): você pode carregar um objeto à medida que ele é criado.

Recomendamos que você use uploads multiparte das seguintes maneiras:

- Se você estiver fazendo upload de objetos grandes em uma rede de banda larga estável, use os uploads multiparte para maximizar o uso da banda larga disponível, fazendo upload das partes do objeto em paralelo para performance com vários threads.
- Se você estiver fazendo upload em uma rede lenta, use os uploads multiparte para aumentar a resiliência dos erros de rede, evitando reinícios de upload. Ao usar os uploads multiparte, tente fazer upload novamente apenas das partes que foram interrompidas durante o upload. Você não precisa reiniciar o upload do seu objeto do começo.

Quando você usa uploads multiparte para fazer upload de objetos para a classe de armazenamento Amazon S3 Express One Zone em buckets de diretório, o processo de upload multiparte é semelhante ao processo de uso de um upload multiparte para fazer upload de objetos em buckets de uso geral. No entanto, há algumas diferenças importantes.

Para obter mais informações sobre como usar uploads multiparte para fazer upload de objetos na classe S3 Express One Zone, consulte os tópicos a seguir.

Tópicos

- O processo de upload multiparte
- Somas de verificação com operações de carregamento fracionado
- Operações simultâneas de carregamento fracionado
- Uploads multiparte e preços
- Operações de API de upload multiparte e permissões
- Exemplos

O processo de upload multiparte

Um upload multiparte é um processo de três etapas:

- Você inicia o upload.
- Você faz upload das partes do objeto.

- Depois de fazer upload de todas as partes, você conclui o upload multiparte.

Ao receber a solicitação de conclusão do upload multiparte, o Amazon S3 cria o objeto com base nas partes carregadas, e você poderá acessar o objeto como qualquer outro objeto no bucket.

Iniciação do multipart upload

Quando você envia uma solicitação para iniciar um multipart upload, o Amazon S3 retorna uma resposta com um ID de upload, que é um identificador exclusivo do seu multipart upload. Você deve incluir esse ID de upload sempre que fizer upload de partes, listar as partes, concluir um upload ou anular um upload.

Carregamento de partes

Ao fazer upload de uma parte, além do ID de upload, você deve especificar um número de parte. Ao usar um upload multiparte com a classe S3 Express One Zone, os números do upload multiparte devem ser consecutivos. Se você tentar concluir uma solicitação de upload multiparte com números de parte não consecutivos, será gerado um erro `HTTP 400 Bad Request` (ordem das partes inválida).

Um número de parte identifica de maneira única uma parte e sua posição no objeto que está sendo carregado. Se você fizer upload de uma nova parte usando o mesmo número da parte anteriormente carregada, a parte anteriormente carregada será substituída.

Sempre que você carregar uma parte, o Amazon S3 retornará um cabeçalho entity tag (ETag) etiqueta de entidade (ETag) na resposta. Para cada upload de parte, você deve registrar o número de parte e o valor de ETag. Os valores de ETag para todos os uploads de partes do objeto permanecerá o mesmo, mas cada parte receberá um número de parte diferente. Você tem que incluir esses valores na solicitação subsequente para concluir o multipart upload.

O Amazon S3 criptografa automaticamente todos os novos objetos que são carregados em um bucket do S3. Ao realizar um carregamento multiparte, se você não especificar informações de criptografia na solicitação, a configuração de criptografia das partes carregadas será definida como a configuração de criptografia padrão do bucket de destino. A configuração de criptografia padrão de um bucket do Amazon S3 está sempre habilitada e, no mínimo, definida como criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3). Em relação a buckets de diretório, são aceitas a SSE-S3 e a criptografia do lado do servidor com chaves do AWS KMS (SSE-KMS). Para obter mais informações, consulte Proteção e criptografia de dados.

Conclusão de carregamento fracionado

Quando você concluir um upload multiparte, o Amazon S3 criará o objeto concatenando as partes em ordem crescente com base no número da parte. Depois de uma solicitação de conclusão bem-sucedida, as partes não existem mais.

Sua solicitação concluir upload multiparte deve incluir o ID de upload e uma lista dos números das partes e dos valores de ETag correspondentes. A resposta do Amazon S3 inclui um ETag que identifica exclusivamente os dados do objeto combinados. Esse ETag não é um hash MD5 dos dados do objeto.

Listagens de carregamento fracionado

Você pode listar as partes de um multipart upload específico ou de todos os multipart uploads em andamento. A operação de listagem de partes retorna as informações das partes que você fez upload em um multipart upload específico. Para cada solicitação de listagem de partes, o Amazon S3 retorna informações das partes do multipart upload especificado, até no máximo 1.000 partes. Se houver mais de 1.000 partes no carregamento multiparte, você deverá usar a paginação para recuperar todas as partes.

A lista de partes retornada não inclui aquelas cujo upload não foi concluído. Usando a operação list multipart uploads (listar carregamentos fracionados), você pode obter uma lista daqueles que estão em andamento.

Um multipart upload em andamento é um upload que você iniciou, mas que ainda não concluiu ou anulou. Cada solicitação retorna no máximo 1.000 multipart uploads. Se houver mais de 1.000 carregamento fracionados em andamento, você precisará enviar solicitações adicionais para recuperar os carregamento fracionados restantes. Use a listagem retornada apenas para verificação. Não use o resultado dessa listagem ao enviar uma solicitação complete multipart upload (concluir carregamento fracionado). Em vez disso, mantenha sua própria lista de números de parte que você especificou ao carregar as partes e os valores correspondentes de ETag que o Amazon S3 retorna.

Para obter mais informações sobre listagens de upload multiparte, consulte ListParts na Referência da API do Amazon Simple Storage Service.

Somas de verificação com operações de carregamento fracionado

Ao fazer upload de um objeto, você pode especificar um algoritmo de soma de verificação para verificar a integridade dele. O MD5 não é compatível com buckets de diretório. Você pode especificar

um dos seguintes algoritmos de verificação de integridade de dados de hash seguro (SHA) ou de verificação de redundância cíclica (CRC):

- CRC32
- CRC32C
- SHA-1
- SHA-256

Você pode usar a API REST do Amazon S3 ou os AWS SDKs para recuperar o valor da soma de verificação para partes específicas usando `GetObject` ou `HeadObject`. Se você quiser recuperar os valores da soma de verificação para partes individuais de carregamentos fracionados ainda em andamento, você pode usar `ListParts`.

> **Important**
>
> Ao usar os algoritmos de soma de verificação anteriores, os números de parte do upload multiparte devem ser consecutivos. Se você tentar concluir uma solicitação de upload multiparte com números de parte não consecutivos, o Amazon S3 gerará um erro `HTTP 400 Bad Request` (ordem das partes inválida).

Consulte mais informações sobre como as somas de verificação funcionam com objetos de carregamento fracionado em Verificar a integridade do objeto no Amazon S3.

Operações simultâneas de carregamento fracionado

Em um ambiente de desenvolvimento distribuído, a aplicação pode iniciar várias atualizações no mesmo objeto ao mesmo tempo. Por exemplo, a aplicação pode iniciar vários uploads multiparte usando a mesma chave de objeto. Para cada um desses uploads, sua aplicação pode fazer upload das partes e enviar uma solicitação de conclusão de upload ao Amazon S3 para criar o objeto. Para a classe S3 Express One Zone, a hora de criação do objeto é a data de conclusão do carregamento multiparte.

> **Important**
>
> O versionamento não é compatível com objetos armazenados em buckets de diretório.

Uploads multiparte e preços

Depois que você iniciar um carregamento multiparte, o Amazon S3 reterá todas as partes até você concluir ou anular o upload. Durante todo o ciclo de vida, você será cobrado por armazenamento, largura de banda e solicitações desse multipart upload e das partes associadas. Se você anular o upload multiparte, o Amazon S3 excluirá os artefatos de upload e todas as partes carregadas, o que significa que não serão mais cobrados de você. Não há cobrança de exclusão antecipada pela exclusão de uploads multiparte incompletos, independentemente da classe de armazenamento especificada. Para obter mais informações sobre a definição de preços, consulte Definição de preços do Amazon S3.

> **Important**
>
> Se a solicitação de conclusão do carregamento fracionado não for enviada com êxito, as partes do objeto não serão montadas e o objeto não será criado. Você é cobrado por todo o armazenamento associado a partes enviadas por upload. É importante que você conclua o upload multiparte para que o objeto seja criado ou anule o upload multiparte para remover todas as partes carregadas.
>
> Antes de excluir um bucket de diretório, é necessário concluir ou anular todos os uploads multiparte em andamento. Os buckets de diretório não oferecem suporte às configurações da funcionalidade Ciclo de Vida do S3. Se necessário, você pode listar os uploads multiparte ativos, depois anulá-los e excluir o bucket.

Operações de API de upload multiparte e permissões

Para permitir o acesso às operações de API de gerenciamento de objetos em um bucket de diretório, conceda a permissão `s3express:CreateSession` em uma política de bucket ou em uma política baseada em identidade do AWS Identity and Access Management (IAM).

Você deve ter as permissões necessárias para usar as operações do multipart upload. Você pode usar políticas de bucket ou políticas baseadas em identidade do IAM para conceder permissões a entidades principais do IAM para realizar essas operações. A tabela a seguir lista as permissões necessárias para diversas operações de carregamento multiparte.

Você pode identificar o iniciador de um upload multiparte por meio do elemento `Initiator`. Se o iniciador for uma Conta da AWS, esse elemento fornecerá as mesmas informações que o elemento `0wner`. Se o iniciador for um usuário do IAM, esse elemento fornecerá o ARN e o nome da exibição do usuário.

Ação	Permissões obrigatórias
Criar um carregamento fracionado	Para criar um upload multiparte, você deve ter permissão para realizar a ação `s3express:CreateSession` em um bucket de diretório.
Iniciar um upload multiparte	Para iniciar o upload multiparte, você deve ter permissão para realizar a ação `s3express:CreateSession` no bucket de diretório.
Fazer upload de uma parte	Para fazer upload de uma parte, você deve ter permissão para realizar a ação `s3express:CreateSession` em um bucket de diretório. Para que o iniciador possa fazer upload de uma parte, o proprietário do bucket deve permitir que o iniciador realize a ação `s3express:CreateSession` em um bucket de diretório.
Fazer upload de uma parte (cópia)	Para fazer upload de uma parte, você deve ter permissão para realizar a ação `s3express:CreateSession` em um bucket de diretório. Para iniciador fazer upload de uma parte para um objeto, o proprietário do bucket deve permitir que o iniciador realize a ação `s3express:CreateSession` no objeto.
Concluir um carregamento fracionado	Para concluir um upload multiparte, você deve ter permissão para realizar a ação `s3express:CreateSession` no bucket de diretório. Para que o iniciador possa concluir um upload multiparte, o proprietário do bucket deve permitir que o iniciador realize a ação `s3express:CreateSession` no objeto.
Anular um multipart upload	Para anular um upload multiparte, você deve ter permissão para realizar a ação `s3express:CreateSession` . Para que o iniciador anule um upload multiparte, ele deve receber permissão explícita para realizar a ação `s3express:CreateSession` .
Listar partes	Para listar as partes de um upload multiparte, você deve ter permissão para realizar a ação `s3express:CreateSession` no bucket de diretório.

Ação	Permissões obrigatórias
Listar carregamentos fracionados em andamento	Para listar os uploads multiparte em andamento em um bucket, você deve ter permissão para realizar a ação `s3:ListBucketMultipartUploads` nesse bucket.

Suporte às operações de API para uploads multiparte

As seções a seguir na Referência da API do Amazon Simple Storage Service descrevem a API REST do Amazon S3 para uploads multiparte.

- CreateMultipartUpload
- UploadPart
- UploadPartCopy
- CompleteMultipartUpload
- AbortMultipartUpload
- ListParts
- ListMultipartUploads

Exemplos

Para usar um upload multiparte a fim de fazer upload de um objeto na classe S3 Express One Zone em um bucket de diretório, consulte os exemplos a seguir.

Tópicos

- Criar um carregamento multiparte
- Fazer upload das partes de um upload multiparte
- Concluir um carregamento multiparte
- Abortar um multipart upload
- Criar uma operação de cópia de carregamento multiparte
- Listar os uploads multiparte em andamento

- Listar as partes de um upload multiparte

Criar um carregamento multiparte

> **Note**
>
> Em relação a buckets de diretório, quando você realiza uma operação `CreateMultipartUpload` e `UploadPartCopy`, a criptografia padrão do bucket deve usar a configuração de criptografia desejada, e os cabeçalhos fornecidos na solicitação `CreateMultipartUpload` devem corresponder à configuração de criptografia padrão do bucket de destino.

Os exemplos a seguir mostram como criar um carregamento fracionado.

Uso dos SDKs da AWS

SDK for Java 2.x

Example

```
/**
 * This method creates a multipart upload request that generates a unique upload ID
 that is used to track
 * all the upload parts
 *
 * @param s3
 * @param bucketName - for example, 'doc-example-bucket--use1-az4--x-s3'
 * @param key
 * @return
 */
 private static String createMultipartUpload(S3Client s3, String bucketName, String
 key) {

     CreateMultipartUploadRequest createMultipartUploadRequest =
 CreateMultipartUploadRequest.builder()
             .bucket(bucketName)
             .key(key)
             .build();

     String uploadId = null;
```

```
    try {
        CreateMultipartUploadResponse response =
 s3.createMultipartUpload(createMultipartUploadRequest);
        uploadId = response.uploadId();
    }
    catch (S3Exception e) {
        System.err.println(e.awsErrorDetails().errorMessage());
        System.exit(1);
    }
    return uploadId;
```

SDK for Python

Example

```
def create_multipart_upload(s3_client, bucket_name, key_name):
    '''
   Create a multipart upload to a directory bucket

   :param s3_client: boto3 S3 client
   :param bucket_name: The destination bucket for the multipart upload
   :param key_name: The key name for the object to be uploaded
   :return: The UploadId for the multipart upload if created successfully, else None
   '''

   try:
        mpu = s3_client.create_multipart_upload(Bucket = bucket_name, Key =
 key_name)
        return mpu['UploadId']
    except ClientError as e:
        logging.error(e)
        return None
```

Como usar o AWS CLI

Este exemplo mostra como criar um carregamento fracionado em um bucket de diretório usando a AWS CLI. Esse comando inicia um carregamento fracionado no bucket de diretório *bucket-base-name*--*zone-id*--x-s3 para o objeto *KEY_NAME*. Para usar o comando, substitua os *espaços reservados para entrada do usuário* por suas próprias informações.

```
aws s3api create-multipart-upload --bucket bucket-base-name--zone-id--x-s3 --
key KEY_NAME
```

Para obter mais informações, consulte create-multipart-upload na AWS Command Line Interface.

Fazer upload das partes de um upload multiparte

Os exemplos a seguir mostram como carregar partes de um carregamento fracionado.

Uso dos SDKs da AWS

SDK for Java 2.x

O exemplo a seguir mostra como dividir um único objeto em partes e carregá-las em um bucket de diretório usando o SDK para Java 2.x.

Example

```
/**
 * This method creates part requests and uploads individual parts to S3 and then
 returns all the completed parts
 *
 * @param s3
 * @param bucketName
 * @param key
 * @param uploadId
 * @throws IOException
 */
 private static ListCompletedPartmultipartUpload(S3Client s3, String bucketName,
 String key, String uploadId, String filePath) throws IOException {

        int partNumber = 1;
        ListCompletedPart completedParts = new ArrayList<>();
        ByteBuffer bb = ByteBuffer.allocate(1024 * 1024 * 5); // 5 MB byte buffer

        // read the local file, breakdown into chunks and process
        try (RandomAccessFile file = new RandomAccessFile(filePath, "r")) {
            long fileSize = file.length();
            int position = 0;
            while (position < fileSize) {
                file.seek(position);
                int read = file.getChannel().read(bb);
```

```
                bb.flip(); // Swap position and limit before reading from the
 buffer.
                UploadPartRequest uploadPartRequest = UploadPartRequest.builder()
                        .bucket(bucketName)
                        .key(key)
                        .uploadId(uploadId)
                        .partNumber(partNumber)
                        .build();

                UploadPartResponse partResponse = s3.uploadPart(
                        uploadPartRequest,
                        RequestBody.fromByteBuffer(bb));

                CompletedPart part = CompletedPart.builder()
                        .partNumber(partNumber)
                        .eTag(partResponse.eTag())
                        .build();
                completedParts.add(part);

                bb.clear();
                position += read;
                partNumber++;
            }
        }

        catch (IOException e) {
            throw e;
        }
        return completedParts;
    }
```

SDK for Python

O exemplo a seguir mostra como dividir um único objeto em partes e carregá-las em um bucket de diretório usando o SDK para Python.

Example

```
def multipart_upload(s3_client, bucket_name, key_name, mpu_id, part_size):
    '''
    Break up a file into multiple parts and upload those parts to a directory bucket

    :param s3_client: boto3 S3 client
    :param bucket_name: Destination bucket for the multipart upload
```

```
    :param key_name: Key name for object to be uploaded and for the local file
that's being uploaded
    :param mpu_id: The UploadId returned from the create_multipart_upload call
    :param part_size: The size parts that the object will be broken into, in bytes.
                      Minimum 5 MiB, Maximum 5 GiB. There is no minimum size for the
last part of your multipart upload.
    :return: part_list for the multipart upload if all parts are uploaded
successfully, else None
    '''

    part_list = []
    try:
        with open(key_name, 'rb') as file:
            part_counter = 1
            while True:
                file_part = file.read(part_size)
                if not len(file_part):
                    break
                upload_part = s3_client.upload_part(
                    Bucket = bucket_name,
                    Key = key_name,
                    UploadId = mpu_id,
                    Body = file_part,
                    PartNumber = part_counter
                )
                part_list.append({'PartNumber': part_counter, 'ETag':
upload_part['ETag']})
                part_counter += 1
    except ClientError as e:
        logging.error(e)
        return None
    return part_list
```

Como usar o AWS CLI

O exemplo a seguir mostra como dividir um único objeto em partes e carregá-las em um bucket de diretório usando a AWS CLI. Para usar o comando, substitua os *espaços reservados para entrada do usuário* por suas próprias informações.

```
aws s3api upload-part --bucket bucket-base-name--zone-id--x-s3 --
key KEY_NAME --part-number 1 --body LOCAL_FILE_NAME --upload-id
 "AS_mgt9RaQE9GEaifATue15dAAAAAAAAAAEMAAAAAAAAADQwNzI4MDU0MjUyMBYAAAAAAAAAAA0AAAAAAAAAAH2AfYAA
```

Para obter mais informações, consulte upload-part na AWS Command Line Interface.

Concluir um carregamento multiparte

Os exemplos a seguir mostram como concluir um carregamento fracionado.

Uso dos SDKs da AWS

SDK for Java 2.x

Os exemplos a seguir mostram como concluir um carregamento fracionado usando o SDK para Java 2.x.

Example

```
/**
 * This method completes the multipart upload request by collating all the upload
 parts
 * @param s3
 * @param bucketName - for example, 'doc-example-bucket--usw2-az1--x-s3'
 * @param key
 * @param uploadId
 * @param uploadParts
 */
 private static void completeMultipartUpload(S3Client s3, String bucketName, String
 key, String uploadId, ListCompletedPart uploadParts) {
        CompletedMultipartUpload completedMultipartUpload =
 CompletedMultipartUpload.builder()
                .parts(uploadParts)
                .build();

        CompleteMultipartUploadRequest completeMultipartUploadRequest =
                CompleteMultipartUploadRequest.builder()
                        .bucket(bucketName)
                        .key(key)
                        .uploadId(uploadId)
                        .multipartUpload(completedMultipartUpload)
                        .build();

        s3.completeMultipartUpload(completeMultipartUploadRequest);
    }

    public static void multipartUploadTest(S3Client s3, String bucketName, String
 key, String localFilePath)  {
```

```
        System.out.println("Starting multipart upload for: " + key);
        try {
            String uploadId = createMultipartUpload(s3, bucketName, key);
            System.out.println(uploadId);
            ListCompletedPart parts = multipartUpload(s3, bucketName, key, uploadId,
 localFilePath);
            completeMultipartUpload(s3, bucketName, key, uploadId, parts);
            System.out.println("Multipart upload completed for: " + key);
        }

        catch (Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
```

SDK for Python

Os exemplos a seguir mostram como concluir um carregamento fracionado usando o SDK para Python.

Example

```
def complete_multipart_upload(s3_client, bucket_name, key_name, mpu_id, part_list):
    '''
    Completes a multipart upload to a directory bucket

    :param s3_client: boto3 S3 client
    :param bucket_name: The destination bucket for the multipart upload
    :param key_name: The key name for the object to be uploaded
    :param mpu_id: The UploadId returned from the create_multipart_upload call
    :param part_list: The list of uploaded part numbers with their associated ETags
    :return: True if the multipart upload was completed successfully, else False
    '''

    try:
        s3_client.complete_multipart_upload(
            Bucket = bucket_name,
            Key = key_name,
            UploadId = mpu_id,
            MultipartUpload = {
                'Parts': part_list
            }
        )
```

```
    except ClientError as e:
        logging.error(e)
        return False
    return True

if __name__ == '__main__':
    MB = 1024 ** 2
    region = 'us-west-2'
    bucket_name = 'BUCKET_NAME'
    key_name = 'OBJECT_NAME'
    part_size = 10 * MB
    s3_client = boto3.client('s3', region_name = region)
    mpu_id = create_multipart_upload(s3_client, bucket_name, key_name)
    if mpu_id is not None:
        part_list = multipart_upload(s3_client, bucket_name, key_name, mpu_id,
 part_size)
        if part_list is not None:
            if complete_multipart_upload(s3_client, bucket_name, key_name, mpu_id,
 part_list):
                print (f'{key_name} successfully uploaded through a ultipart upload
 to {bucket_name}')
            else:
                print (f'Could not upload {key_name} hrough a multipart upload to
 {bucket_name}')
```

Como usar o AWS CLI

Este exemplo mostra como concluir um carregamento fracionado em um bucket de diretório usando a AWS CLI. Para usar o comando, substitua os *espaços reservados para entrada do usuário* por suas próprias informações.

```
aws s3api complete-multipart-upload --bucket bucket-base-name--zone-id--x-s3 --
key KEY_NAME --upload-id
 "AS_mgt9RaQE9GEaifATue15dAAAAAAAAAAEMAAAAAAAAADQwNzI4MDU0MjUyMBYAAAAAAAAAAA0AAAAAAAAAAH2AfYAA
 --multipart-upload file://parts.json
```

Este exemplo usa uma estrutura JSON que descreve quais partes do carregamento fracionado devem ser reagrupadas no arquivo completo. Neste exemplo, o prefixo `file://` é usado para carregar a estrutura JSON de um arquivo na pasta local chamada `parts`.

parts.json:

```
parts.json
{
  "Parts": [
    {
      "ETag": "6b78c4a64dd641a58dac8d9258b88147",
      "PartNumber": 1
    }
  ]
}
```

Para obter mais informações, consulte complete-multipart-upload na AWS Command Line Interface.

Abortar um multipart upload

Os exemplos a seguir mostram como interromper um carregamento fracionado.

Uso dos SDKs da AWS

SDK for Java 2.x

O exemplo a seguir mostra como interromper um carregamento fracionado usando o SDK para Java 2.x.

Example

```
public static void abortMultiPartUploads( S3Client s3, String bucketName ) {

        try {
            ListMultipartUploadsRequest listMultipartUploadsRequest =
 ListMultipartUploadsRequest.builder()
                    .bucket(bucketName)
                    .build();

            ListMultipartUploadsResponse response =
 s3.listMultipartUploads(listMultipartUploadsRequest);
            ListMultipartUpload uploads = response.uploads();

            AbortMultipartUploadRequest abortMultipartUploadRequest;
            for (MultipartUpload upload: uploads) {
                abortMultipartUploadRequest = AbortMultipartUploadRequest.builder()
                        .bucket(bucketName)
                        .key(upload.key())
                        .uploadId(upload.uploadId())
```

```
                        .build();

                s3.abortMultipartUpload(abortMultipartUploadRequest);
            }

        }

        catch (S3Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
```

SDK for Python

O exemplo a seguir mostra como interromper um carregamento fracionado usando o SDK para Python.

Example

```
import logging
import boto3
from botocore.exceptions import ClientError


def abort_multipart_upload(s3_client, bucket_name, key_name, upload_id):
    '''
    Aborts a partial multipart upload in a directory bucket.

    :param s3_client: boto3 S3 client
    :param bucket_name: Bucket where the multipart upload was initiated - for
 example, 'doc-example-bucket--usw2-az1--x-s3'
    :param key_name: Name of the object for which the multipart upload needs to be
 aborted
    :param upload_id: Multipart upload ID for the multipart upload to be aborted
    :return: True if the multipart upload was successfully aborted, False if not
    '''
    try:
        s3_client.abort_multipart_upload(
            Bucket = bucket_name,
            Key = key_name,
            UploadId = upload_id
        )
    except ClientError as e:
```

```
        logging.error(e)
        return False
    return True


if __name__ == '__main__':
    region = 'us-west-2'
    bucket_name = 'BUCKET_NAME'
    key_name = 'KEY_NAME'
        upload_id = 'UPLOAD_ID'
    s3_client = boto3.client('s3', region_name = region)
    if abort_multipart_upload(s3_client, bucket_name, key_name, upload_id):
        print (f'Multipart upload for object {key_name} in {bucket_name} bucket has
 been aborted')
    else:
        print (f'Unable to abort multipart upload for object {key_name} in
 {bucket_name} bucket')
```

Como usar o AWS CLI

O exemplo a seguir mostra como interromper um carregamento fracionado usando a AWS CLI. Para usar o comando, substitua os *espaços reservados para entrada do usuário* por suas próprias informações.

```
aws s3api abort-multipart-upload --bucket bucket-base-name--zone-id--x-s3 --
key KEY_NAME --upload-id
 "AS_mgt9RaQE9GEaifATue15dAAAAAAAAAAEMAAAAAAAAADQwNzI4MDU0MjUyMBYAAAAAAAAAAA0AAAAAAAAAAH2AfYAA
MAQAAAAB0OxUFeA7LTbWWFS8WYwhrxDxTIDN-pdEEq_agIHqsbg"
```

Para obter mais informações, consulte abort-multipart-upload na AWS Command Line Interface.

Criar uma operação de cópia de carregamento multiparte

> **Note**
>
> - Para criptografar novas cópias de partes de objetos em um bucket de diretório com SSE-KMS, é necessário especificar SSE-KMS como a configuração de criptografia padrão do bucket de diretório com uma chave do KMS (especificamente, uma chave gerenciada pelo cliente). Não há suporte para Chave gerenciada pela AWS (`aws/s3`). A configuração de SSE-KMS só comporta uma chave gerenciada pelo cliente por bucket de diretório durante

a vida útil do bucket. Depois que você especifica uma chave gerenciada pelo cliente para SSE-KMS, não é possível substituí-la pela configuração de SSE-KMS do bucket. Não é possível especificar as configurações de criptografia do lado do servidor para novas cópias de partes do objeto com SSE-KMS nos cabeçalhos da solicitação UploadPartCopy. Além disso, os cabeçalhos fornecidos na solicitação `CreateMultipartUpload` devem corresponder à configuração de criptografia padrão do bucket de destino.

- As chaves de bucket do S3 não são aceitas quando você copia objetos criptografados por SSE-KMS de buckets de uso geral para buckets de diretório, de buckets de diretório para buckets de uso geral ou entre buckets de diretório, por meio de UploadPartCopy. Nesse caso, o Amazon S3 faz uma chamada para o AWS KMS sempre que uma solicitação de cópia é feita para um objeto criptografado pelo KMS.

Os exemplos a seguir mostram como copiar objetos de um bucket em outro usando um carregamento fracionado.

Uso dos SDKs da AWS

SDK for Java 2.x

O exemplo a seguir mostra como usar um carregamento fracionado para copiar um objeto de um bucket para outro de forma programática usando o SDK para Java 2.x.

Example

```
/**
 * This method creates a multipart upload request that generates a unique upload ID
 that is used to track
 * all the upload parts.
 *
 * @param s3
 * @param bucketName
 * @param key
 * @return
 */
 private static String createMultipartUpload(S3Client s3, String bucketName, String
 key) {
        CreateMultipartUploadRequest createMultipartUploadRequest =
 CreateMultipartUploadRequest.builder()
                .bucket(bucketName)
                .key(key)
```

```
                .build();
        String uploadId = null;
        try {
            CreateMultipartUploadResponse response =
s3.createMultipartUpload(createMultipartUploadRequest);
            uploadId = response.uploadId();
        } catch (S3Exception e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }
        return uploadId;
 }

 /**
  * Creates copy parts based on source object size and copies over individual parts
  *
  * @param s3
  * @param sourceBucket
  * @param sourceKey
  * @param destnBucket
  * @param destnKey
  * @param uploadId
  * @return
  * @throws IOException
  */
   public static ListCompletedPart multipartUploadCopy(S3Client s3, String
sourceBucket, String sourceKey, String destnBucket, String destnKey, String
uploadId) throws IOException {

        // Get the object size to track the end of the copy operation.
        HeadObjectRequest headObjectRequest = HeadObjectRequest
                .builder()
                .bucket(sourceBucket)
                .key(sourceKey)
                .build();
        HeadObjectResponse response = s3.headObject(headObjectRequest);
        Long objectSize = response.contentLength();

        System.out.println("Source Object size: " + objectSize);

        // Copy the object using 20 MB parts.
        long partSize = 20 * 1024 * 1024;
        long bytePosition = 0;
        int partNum = 1;
```

```
        List<CompletedPart> completedParts = new ArrayList<>();
        while (bytePosition < objectSize) {
            // The last part might be smaller than partSize, so check to make sure
            // that lastByte isn't beyond the end of the object.
            long lastByte = Math.min(bytePosition + partSize - 1, objectSize - 1);

            System.out.println("part no: " + partNum + ", bytePosition: " +
bytePosition + ", lastByte: " + lastByte);

            // Copy this part.
            UploadPartCopyRequest req = UploadPartCopyRequest.builder()
                    .uploadId(uploadId)
                    .sourceBucket(sourceBucket)
                    .sourceKey(sourceKey)
                    .destinationBucket(destnBucket)
                    .destinationKey(destnKey)
                    .copySourceRange("bytes="+bytePosition+"-"+lastByte)
                    .partNumber(partNum)
                    .build();
            UploadPartCopyResponse res = s3.uploadPartCopy(req);
            CompletedPart part = CompletedPart.builder()
                    .partNumber(partNum)
                    .eTag(res.copyPartResult().eTag())
                    .build();
            completedParts.add(part);
            partNum++;
            bytePosition += partSize;
        }
        return completedParts;
    }


    public static void multipartCopyUploadTest(S3Client s3, String srcBucket, String
srcKey, String destnBucket, String destnKey)  {
        System.out.println("Starting multipart copy for: " + srcKey);
        try {
            String uploadId = createMultipartUpload(s3, destnBucket, destnKey);
            System.out.println(uploadId);
            List<CompletedPart> parts = multipartUploadCopy(s3, srcBucket,
srcKey,destnBucket,  destnKey, uploadId);
            completeMultipartUpload(s3, destnBucket, destnKey, uploadId, parts);
            System.out.println("Multipart copy completed for: " + srcKey);
        } catch (Exception e) {
            System.err.println(e.getMessage());
```

```
            System.exit(1);
        }
    }
```

SDK for Python

O exemplo a seguir mostra como usar um carregamento fracionado para copiar um objeto de um bucket para outro de forma programática usando o SDK para Python.

Example

```
import logging
import boto3
from botocore.exceptions import ClientError

def head_object(s3_client, bucket_name, key_name):
    '''
    Returns metadata for an object in a directory bucket

    :param s3_client: boto3 S3 client
    :param bucket_name: Bucket that contains the object to query for metadata
    :param key_name: Key name to query for metadata
    :return: Metadata for the specified object if successful, else None
    '''

    try:
        response = s3_client.head_object(
            Bucket = bucket_name,
            Key = key_name
        )
        return response
    except ClientError as e:
        logging.error(e)
        return None

def create_multipart_upload(s3_client, bucket_name, key_name):
    '''
    Create a multipart upload to a directory bucket

    :param s3_client: boto3 S3 client
    :param bucket_name: Destination bucket for the multipart upload
    :param key_name: Key name of the object to be uploaded
    :return: UploadId for the multipart upload if created successfully, else None
    '''
```

```
    try:
        mpu = s3_client.create_multipart_upload(Bucket = bucket_name, Key =
 key_name)
        return mpu['UploadId']
    except ClientError as e:
        logging.error(e)
        return None

def multipart_copy_upload(s3_client, source_bucket_name, key_name,
 target_bucket_name, mpu_id, part_size):
    '''
    Copy an object in a directory bucket to another bucket in multiple parts of a
 specified size

    :param s3_client: boto3 S3 client
    :param source_bucket_name: Bucket where the source object exists
    :param key_name: Key name of the object to be copied
    :param target_bucket_name: Destination bucket for copied object
    :param mpu_id: The UploadId returned from the create_multipart_upload call
    :param part_size: The size parts that the object will be broken into, in bytes.
                      Minimum 5 MiB, Maximum 5 GiB. There is no minimum size for the
 last part of your multipart upload.
    :return: part_list for the multipart copy if all parts are copied successfully,
 else None
    '''

    part_list = []
    copy_source = {
        'Bucket': source_bucket_name,
        'Key': key_name
    }
    try:
        part_counter = 1
        object_size = head_object(s3_client, source_bucket_name, key_name)
        if object_size is not None:
            object_size = object_size['ContentLength']
        while (part_counter - 1) * part_size <object_size:
            bytes_start = (part_counter - 1) * part_size
            bytes_end = (part_counter * part_size) - 1
            upload_copy_part = s3_client.upload_part_copy (
                Bucket = target_bucket_name,
                CopySource = copy_source,
                CopySourceRange = f'bytes={bytes_start}-{bytes_end}',
```

```
                Key = key_name,
                PartNumber = part_counter,
                UploadId = mpu_id
            )
            part_list.append({'PartNumber': part_counter, 'ETag':
 upload_copy_part['CopyPartResult']['ETag']})
            part_counter += 1
    except ClientError as e:
        logging.error(e)
        return None
    return part_list

def complete_multipart_upload(s3_client, bucket_name, key_name, mpu_id, part_list):
    '''
    Completes a multipart upload to a directory bucket

    :param s3_client: boto3 S3 client
    :param bucket_name: Destination bucket for the multipart upload
    :param key_name: Key name of the object to be uploaded
    :param mpu_id: The UploadId returned from the create_multipart_upload call
    :param part_list: List of uploaded part numbers with associated ETags
    :return: True if the multipart upload was completed successfully, else False
    '''

    try:
        s3_client.complete_multipart_upload(
            Bucket = bucket_name,
            Key = key_name,
            UploadId = mpu_id,
            MultipartUpload = {
                'Parts': part_list
            }
        )
    except ClientError as e:
        logging.error(e)
        return False
    return True

if __name__ == '__main__':
    MB = 1024 ** 2
    region = 'us-west-2'
    source_bucket_name = 'SOURCE_BUCKET_NAME'
    target_bucket_name = 'TARGET_BUCKET_NAME'
    key_name = 'KEY_NAME'
```

```
    part_size = 10 * MB
    s3_client = boto3.client('s3', region_name = region)
    mpu_id = create_multipart_upload(s3_client, target_bucket_name, key_name)
    if mpu_id is not None:
        part_list = multipart_copy_upload(s3_client, source_bucket_name, key_name,
target_bucket_name, mpu_id, part_size)
        if part_list is not None:
            if complete_multipart_upload(s3_client, target_bucket_name, key_name,
mpu_id, part_list):
                print (f'{key_name} successfully copied through multipart copy from
{source_bucket_name} to {target_bucket_name}')
            else:
                print (f'Could not copy {key_name} through multipart copy from
{source_bucket_name} to {target_bucket_name}')
```

Como usar o AWS CLI

O exemplo a seguir mostra como usar um carregamento fracionado para copiar um objeto de um bucket para outro de forma programática usando a AWS CLI. Para usar o comando, substitua os *espaços reservados para entrada do usuário* por suas próprias informações.

```
aws s3api upload-part-copy --bucket bucket-base-name--zone-id--x-s3 --
key TARGET_KEY_NAME --copy-source SOURCE_BUCKET_NAME/SOURCE_KEY_NAME --part-number 1 --
upload-id
 "AS_mgt9RaQE9GEaifATue15dAAAAAAAAAAEMAAAAAAAAADQwNzI4MDU0MjUyMBYAAAAAAAAAAA0AAAAAAAAAAH2AfYAA
```

Para obter mais informações, consulte upload-part-copy na AWS Command Line Interface.

Listar os uploads multiparte em andamento

Para listar carregamentos fracionados em andamento em um bucket de diretório, é possível usar os SDKs da AWS ou a AWS CLI.

Uso dos SDKs da AWS

SDK for Java 2.x

Os exemplos a seguir mostram como listar carregamentos fracionados em andamento (incompletos) usando o SDK para Java 2.x.

Example

```
public static void listMultiPartUploads( S3Client s3, String bucketName) {
       try {
           ListMultipartUploadsRequest listMultipartUploadsRequest =
ListMultipartUploadsRequest.builder()
               .bucket(bucketName)
               .build();

           ListMultipartUploadsResponse response =
s3.listMultipartUploads(listMultipartUploadsRequest);
           List MultipartUpload uploads = response.uploads();
           for (MultipartUpload upload: uploads) {
               System.out.println("Upload in progress: Key = \"" + upload.key() +
"\", id = " + upload.uploadId());
           }
     }
     catch (S3Exception e) {
           System.err.println(e.getMessage());
           System.exit(1);
     }
 }
```

SDK for Python

Os exemplos a seguir mostram como listar carregamentos fracionados em andamento (incompletos) usando o SDK para Python.

Example

```
import logging
import boto3
from botocore.exceptions import ClientError

def list_multipart_uploads(s3_client, bucket_name):
    '''
    List any incomplete multipart uploads in a directory bucket in e specified gion

    :param s3_client: boto3 S3 client
    :param bucket_name: Bucket to check for incomplete multipart uploads
    :return: List of incomplete multipart uploads if there are any, None if not
    '''
```

```
    try:
        response = s3_client.list_multipart_uploads(Bucket = bucket_name)
        if 'Uploads' in response.keys():
            return response['Uploads']
        else:
            return None
    except ClientError as e:
        logging.error(e)

if __name__ == '__main__':
    bucket_name = 'BUCKET_NAME'
    region = 'us-west-2'
    s3_client = boto3.client('s3', region_name = region)
    multipart_uploads = list_multipart_uploads(s3_client, bucket_name)
    if multipart_uploads is not None:
        print (f'There are {len(multipart_uploads)} ncomplete multipart uploads for
 {bucket_name}')
    else:
        print (f'There are no incomplete multipart uploads for {bucket_name}')
```

Como usar o AWS CLI

Os exemplos a seguir mostram como listar carregamentos fracionados em andamento (incompletos) usando a AWS CLI. Para usar o comando, substitua os *espaços reservados para entrada do usuário* por suas próprias informações.

```
aws s3api list-multipart-uploads --bucket bucket-base-name--zone-id--x-s3
```

Para obter mais informações, consulte list-multipart-uploads na AWS Command Line Interface.

Listar as partes de um upload multiparte

Os exemplos a seguir mostram como listar partes de um carregamento fracionado em um bucket de diretório.

Uso dos SDKs da AWS

SDK for Java 2.x

Os exemplos a seguir mostram como listar partes de um carregamento fracionado em um bucket de diretório usando o SDK para Java 2.x.

```
public static void listMultiPartUploadsParts( S3Client s3, String bucketName, String
 objKey, String uploadID) {

        try {
            ListPartsRequest listPartsRequest = ListPartsRequest.builder()
                .bucket(bucketName)
                .uploadId(uploadID)
                .key(objKey)
                .build();

            ListPartsResponse response = s3.listParts(listPartsRequest);
            ListPart parts = response.parts();
            for (Part part: parts) {
                System.out.println("Upload in progress: Part number = \"" +
 part.partNumber() + "\", etag = " + part.eTag());
            }

        }

        catch (S3Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }


    }
```

SDK for Python

Os exemplos a seguir mostram como listar partes de um carregamento fracionado em um bucket de diretório usando o SDK para Python.

```
import logging
import boto3
from botocore.exceptions import ClientError

def list_parts(s3_client, bucket_name, key_name, upload_id):
    '''
    Lists the parts that have been uploaded for a specific multipart upload to a
 directory bucket.

    :param s3_client: boto3 S3 client
    :param bucket_name: Bucket that multipart uploads parts have been uploaded to
```

```
    :param key_name: Name of the object that has parts uploaded
    :param upload_id: Multipart upload ID that the parts are associated with
    :return: List of parts associated with the specified multipart upload, None if
 there are no parts
    '''
    parts_list = []
    next_part_marker = ''
    continuation_flag = True
    try:
        while continuation_flag:
            if next_part_marker == '':
                response = s3_client.list_parts(
                    Bucket = bucket_name,
                    Key = key_name,
                    UploadId = upload_id
                )
            else:
                response = s3_client.list_parts(
                    Bucket = bucket_name,
                    Key = key_name,
                    UploadId = upload_id,
                    NextPartMarker = next_part_marker
                )
            if 'Parts' in response:
                for part in response['Parts']:
                    parts_list.append(part)
                if response['IsTruncated']:
                    next_part_marker = response['NextPartNumberMarker']
                else:
                    continuation_flag = False
            else:
                continuation_flag = False
        return parts_list
    except ClientError as e:
        logging.error(e)
        return None

if __name__ == '__main__':
    region = 'us-west-2'
    bucket_name = 'BUCKET_NAME'
    key_name = 'KEY_NAME'
    upload_id = 'UPLOAD_ID'
    s3_client = boto3.client('s3', region_name = region)
    parts_list = list_parts(s3_client, bucket_name, key_name, upload_id)
```

```
    if parts_list is not None:
        print (f'{key_name} has {len(parts_list)} parts uploaded to {bucket_name}')
    else:
        print (f'There are no multipart uploads with that upload ID for
{bucket_name} bucket')
```

Como usar o AWS CLI

Os exemplos a seguir mostram como listar partes de um carregamento fracionado em um bucket de diretório usando a AWS CLI. Para usar o comando, substitua os *espaços reservados para entrada do usuário* por suas próprias informações.

```
aws s3api list-parts --bucket bucket-base-name--zone-id--x-s3 --key KEY_NAME --upload-
id
 "AS_mgt9RaQE9GEaifATue15dAAAAAAAAAAEMAAAAAAAAADQwNzI4MDU0MjUyMBYAAAAAAAAAAA0AAAAAAAAAAH2AfYAA
```

Para obter mais informações, consulte list-parts na AWS Command Line Interface.

Copiar objetos de ou para um bucket de diretório

A operação de cópia cria uma cópia de um objeto que já está armazenado no Amazon S3. Você pode copiar objetos entre buckets de diretório e buckets de uso geral. Você também pode copiar objetos dentro de um bucket e entre buckets do mesmo tipo, por exemplo, de um bucket de diretório para outro bucket de diretório.

> **Note**
>
> Não há suporte à cópia de objetos entre diferentes Regiões da AWS quando o bucket de origem ou de destino está em uma zona local da AWS. Os buckets de origem e de destino devem ter a mesma Região da AWS principal. Os buckets de origem e de destino podem ser de diferentes tipos de localização de bucket (zona de disponibilidade ou zona local).

Você pode criar uma cópia do objeto de até 5 GB em uma única operação atômica. Contudo, para copiar um objeto maior do que 5 GB, você deve usar as operações de API de upload multiparte. Para obter mais informações, consulte Usar uploads multiparte com buckets de diretório.

Permissões

Para copiar objetos, você deve ter as seguintes permissões:

- Para copiar objetos de um bucket de diretório para outro bucket de diretório, você precisa ter a permissão `s3express:CreateSession`.
- Para copiar objetos de buckets de diretório para buckets de uso geral, você precisa ter a permissão `s3express:CreateSession` e a permissão `s3:PutObject` para gravar a cópia do objeto no bucket de destino.
- Para copiar objetos de buckets de uso geral para buckets de diretório, você precisa ter a permissão `s3express:CreateSession` e a permissão `s3:GetObject` para ler o objeto de origem que está sendo copiado.

  Para obter mais informações, consulte CopyObject na Referência da API do Amazon Simple Storage Service.

Criptografia

O Amazon S3 criptografa automaticamente todos os novos objetos que são carregados em um bucket do S3. A configuração de criptografia padrão de um bucket do S3 está sempre habilitada e, no mínimo, definida como criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3).

Em relação a buckets de diretório, são aceitas a SSE-S3 e a criptografia do lado do servidor com chaves do AWS Key Management Service (AWS KMS) (SSE-KMS). Quando o bucket de destino é um bucket de diretório, recomendamos que a criptografia padrão do bucket de destino use a configuração de criptografia desejada e você não substitua a criptografia padrão do bucket. Desse modo, os novos objetos são criptografados automaticamente com as configurações de criptografia desejadas. Além disso, não são aceitas chaves de bucket do S3 quando você copia objetos criptografados por SSE-KMS de buckets de uso geral para buckets de diretório, de buckets de diretório para buckets de uso geral ou entre buckets de diretório, por meio de CopyObject. Nesse caso, o Amazon S3 faz uma chamada para o AWS KMS sempre que uma solicitação de cópia é feita para um objeto criptografado pelo KMS. Para ter mais informações sobre os comportamentos de substituição de criptografia em buckets de diretório, consulte Specifying server-side encryption with AWS KMS for new object uploads.

Para buckets de uso geral, você pode usar SSE-S3 (padrão), criptografia do lado do servidor com chaves do AWS Key Management Service (AWS KMS) (SSE-KMS), criptografia de camada dupla do lado do servidor com chaves do AWS KMS (DSSE-KMS) ou criptografia do lado do servidor com chaves fornecidas pelo cliente (SSE-C).

Se você fizer uma solicitação de cópia que especifique o uso da DSSE-KMS ou da SSE-C para um bucket de diretório (o bucket de origem ou de destino), a resposta exibirá um erro.

Tags

Os buckets de diretório não oferecem suporte a etiquetas. Se você copiar um objeto que tenha etiquetas de um bucket de uso geral para um bucket de diretório, receberá uma resposta HTTP `501 (Not Implemented)`. Para obter mais informações, consulte CopyObject na Referência da API do Amazon Simple Storage Service.

ETags

As etiquetas de entidade (ETags) para a classe S3 Express One Zone são strings alfanuméricas aleatórias e não somas de verificação MD5. Para ajudar a garantir a integridade do objeto, use somas de verificação adicionais.

Somas de verificação adicionais

A classe S3 Express One Zone oferece a opção de escolher o algoritmo de soma de verificação usado para validar os dados durante o upload ou o download. Você pode selecionar um dos seguintes algoritmos de verificação de integridade de dados de hash seguro (SHA) ou de verificação de redundância cíclica (CRC): CRC32, CRC32C, SHA-1 e SHA-256. As somas de verificação baseadas em MD5 não são compatíveis com a classe de armazenamento S3 Express One Zone.

Para obter mais informações, consulte Práticas recomendadas adicionais de soma de verificação do S3.

Recursos compatíveis

Para obter mais informações sobre quais recursos do Amazon S3 são compatíveis com a classe S3 Express One Zone, consulte Diferenças de buckets de diretório.

Usar o console do S3 (copiar para um bucket de diretório)

> **Note**
>
> As restrições e limitações ao copiar um objeto em um bucket de diretório com o console são as seguintes:
>
> - A ação `Copy` se aplica a todos os objetos nas pastas especificadas (prefixos). Os objetos adicionados a essas pastas enquanto a ação estiver em andamento também poderão ser afetados.

- Objetos criptografados com chaves de criptografia fornecidas pelo cliente (SSE-C) não podem ser copiados usando o console do S3. Para copiar objetos criptografados com SSE-C, use a AWS CLI, o SDK da AWS ou a API REST do Amazon S3.
- Os objetos copiados não manterão as configurações do Bloqueio de Objetos dos objetos originais.
- Se o bucket do qual você está copiando os objetos usar a configuração aplicada pelo proprietário do bucket em Propriedade de objetos do S3, as ACLs de objeto não serão copiadas para o destino especificado.
- Se você quiser copiar objetos para um bucket que usa a configuração aplicada pelo proprietário do bucket em Propriedade de objetos do S3, o bucket de origem também deve usar a configuração aplicada pelo proprietário do bucket ou você deve remover qualquer objeto concedido pela ACL a outras contas e grupos da AWS.
- Os objetos copiados de um bucket de uso geral para um bucket de diretório não reterão tags de objeto, ACLs ou valores de Etag. Os valores da soma de verificação podem ser copiados, mas não são equivalentes a uma Etag. O valor da soma de verificação pode mudar em comparação com quando foi adicionado.
- Todos os objetos copiados para um bucket de diretório estarão com a configuração aplicada pelo proprietário do bucket para Propriedade de Objetos do S3.

Como copiar um objeto de um bucket de uso geral ou de diretório para um bucket de diretório

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, o tipo de bucket do qual você deseja copiar objetos:
   - Para copiar de um bucket de uso geral, escolha a guia Buckets de uso geral.
   - Para copiar de um bucket de diretório, escolha a guia Buckets de diretórios.
3. Escolha o bucket de uso geral ou de diretório que contém os objetos que você deseja copiar.
4. Escolha a guia Objetos. Na página Objetos, marque a caixa de seleção à esquerda dos nomes dos objetos que você deseja copiar.
5. No menu Actions (Ações), escolha Copy (Copiar).

   A página Copiar é exibida.

6. Em Destino, escolha Bucket de diretório como tipo de destino. Para especificar o caminho de destino, escolha Procurar no S3, navegue até o destino e selecione o botão de opções à esquerda do destino. Escolha Choose destination (Escolher destino) no canto inferior direito.

   Outra alternativa é inserir o caminho de destino.

7. Em Configurações adicionais de cópia, escolha se você quer Copiar configurações de origem, Não especificar configurações ou Especificar configurações. Copiar configurações de origem é a opção padrão. Se você quiser copiar o objeto somente sem os atributos das configurações de origem, escolha Não especificar configurações. Escolha Especificar configurações para especificar configurações para criptografia do lado do servidor, somas de verificação e metadados.
8. Escolha Copy (Copiar) no canto inferior direito. O Amazon S3 copia o objeto no destino.

Usar o console do S3 (copiar para um bucket de uso geral)

> **Note**
>
> As restrições e limitações ao copiar um objeto para um bucket de uso geral com o console são as seguintes:
>
> - A ação `Copy` se aplica a todos os objetos nas pastas especificadas (prefixos). Os objetos adicionados a essas pastas enquanto a ação estiver em andamento também poderão ser afetados.
> - Objetos criptografados com chaves de criptografia fornecidas pelo cliente (SSE-C) não podem ser copiados usando o console do S3. Para copiar objetos criptografados com SSE-C, use a AWS CLI, o SDK da AWS ou a API REST do Amazon S3.
> - Os objetos copiados não manterão as configurações do Bloqueio de Objetos dos objetos originais.
> - Se o bucket do qual você está copiando os objetos usar a configuração aplicada pelo proprietário do bucket em Propriedade de objetos do S3, as ACLs de objeto não serão copiadas para o destino especificado.
> - Se você quiser copiar objetos para um bucket que usa a configuração aplicada pelo proprietário do bucket em Propriedade de objetos do S3, o bucket de origem também deve usar a configuração aplicada pelo proprietário do bucket ou você deve remover qualquer objeto concedido pela ACL a outras contas e grupos da AWS.

Como copiar um objeto de um bucket de diretório para um bucket de uso geral

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets.
3. Escolha a guia Buckets de diretórios.
4. Selecione o bucket de diretório que contém os objetos que você deseja copiar.
5. Escolha a guia Objetos. Na página Objetos, marque a caixa de seleção à esquerda dos nomes dos objetos que você deseja copiar.
6. No menu Actions (Ações), escolha Copy (Copiar).
7. Em Destino, escolha Bucket de uso geral como tipo de destino. Para especificar o caminho de destino, escolha Procurar no S3, navegue até o destino e selecione o botão de opções à esquerda do destino. Escolha Choose destination (Escolher destino) no canto inferior direito.

   Outra alternativa é inserir o caminho de destino.
8. Em Configurações adicionais de cópia, escolha se você quer Copiar configurações de origem, Não especificar configurações ou Especificar configurações. Copiar configurações de origem é a opção padrão. Se você quiser copiar o objeto somente sem os atributos das configurações de origem, escolha Não especificar configurações. Escolha Especificar configurações para especificar configurações referentes a classes de armazenamento, ACLs, tags de objeto, metadados, criptografia do lado do servidor e somas de verificação adicionais.
9. Escolha Copy (Copiar) no canto inferior direito. O Amazon S3 copia o objeto no destino.

Uso dos SDKs da AWS

SDK for Java 2.x

Example

```
public static void copyBucketObject (S3Client s3, String sourceBucket, String
objectKey, String targetBucket) {
     CopyObjectRequest copyReq = CopyObjectRequest.builder()
         .sourceBucket(sourceBucket)
         .sourceKey(objectKey)
         .destinationBucket(targetBucket)
         .destinationKey(objectKey)
         .build();
```

```
        String temp = "";

        try {
            CopyObjectResponse copyRes = s3.copyObject(copyReq);
            System.out.println("Successfully copied " + objectKey +" from bucket " +
sourceBucket +" into bucket "+targetBucket);
        }

        catch (S3Exception e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }
}
```

Como usar o AWS CLI

O exemplo de comando `copy-object` a seguir mostra como é possível usar a AWS CLI para copiar um objeto de um bucket para outro. Você pode copiar objetos entre tipos de bucket. Para executar esse comando, substitua os espaços reservados de entrada por suas próprias informações.

```
aws s3api copy-object --copy-source SOURCE_BUCKET/SOURCE_KEY_NAME --key TARGET_KEY_NAME
 --bucket TARGET_BUCKET_NAME
```

Para obter mais informações, consulte copy-object na Referência de comandos da AWS CLI.

Excluir objetos de um bucket de diretório

Você pode excluir objetos de um bucket de diretório do Amazon S3 usando o console do Amazon S3, a AWS Command Line Interface (AWS CLI) ou os AWS SDKs. Para obter mais informações, consulte Trabalhar com buckets de diretório e S3 Express One Zone.

> **Warning**
>
> - Não é possível desfazer a exclusão de um objeto.
> - Essa ação exclui todos os objetos especificados. Ao excluir pastas, aguarde a conclusão da ação de exclusão antes de adicionar objetos novos à pasta. Caso contrário, os objetos novos também podem ser excluídos.

> **Note**
>
> Ao excluir vários objetos de um bucket de diretório de forma programática, observe o seguinte:
>
> - As chaves de objeto em solicitações `DeleteObjects` devem conter pelo menos um caractere diferente de um espaço em branco. As strings que têm somente espaços em branco não são compatíveis.
> - As chaves de objeto em solicitações `DeleteObjects` não podem conter caracteres de controle Unicode, exceto nova linha (`\t`), tabulação (`\n`) e avanço de linha (`\r`).

Usar o console do S3

Para excluir objetos

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets de diretórios.
3. Selecione o bucket de diretório que contém os objetos que você deseja excluir.
4. Escolha a guia Objetos. Na lista Objetos, marque as caixas de seleção à esquerda dos objetos que você deseja excluir.
5. Escolha Excluir.
6. Na página Excluir objetos, insira **`permanently delete`** na caixa de texto.
7. Escolha Delete objects (Excluir objetos).

Uso dos SDKs da AWS

SDK for Java 2.x

Example

O exemplo a seguir exclui objetos de um bucket de diretório usando o AWS SDK for Java 2.x.

```
static void deleteObject(S3Client s3Client, String bucketName, String objectKey) {
```

```
        try {

            DeleteObjectRequest del = DeleteObjectRequest.builder()
                    .bucket(bucketName)
                    .key(objectKey)
                    .build();

            s3Client.deleteObject(del);

            System.out.println("Object " + objectKey + " has been deleted");


        } catch (S3Exception e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }

    }
```

SDK for Python

Example

O exemplo a seguir exclui objetos de um bucket de diretório usando o AWS SDK para Python (Boto3).

```
import logging
import boto3
from botocore.exceptions import ClientError

def delete_objects(s3_client, bucket_name, objects):
    '''
    Delete a list of objects in a directory bucket

    :param s3_client: boto3 S3 client
    :param bucket_name: Bucket that contains objects to be deleted; for example,
 'doc-example-bucket--usw2-az1--x-s3'
    :param objects: List of dictionaries that specify the key names to delete
    :return: Response output, else False
    '''

    try:
```

```
        response = s3_client.delete_objects(
            Bucket = bucket_name,
            Delete = {
                'Objects': objects
            }
        )
        return response
    except ClientError as e:
        logging.error(e)
        return False


if __name__ == '__main__':
    region = 'us-west-2'
    bucket_name = 'BUCKET_NAME'
    objects = [
        {
            'Key': '0.txt'
        },
        {
            'Key': '1.txt'
        },
        {
            'Key': '2.txt'
        },
        {
            'Key': '3.txt'
        },
        {
            'Key': '4.txt'
        }
    ]

    s3_client = boto3.client('s3', region_name = region)
    results = delete_objects(s3_client, bucket_name, objects)
    if results is not None:
        if 'Deleted' in results:
            print (f'Deleted {len(results["Deleted"])} objects from {bucket_name}')
        if 'Errors' in results:
            print (f'Failed to delete {len(results["Errors"])} objects from
 {bucket_name}')
```

Como usar o AWS CLI

O exemplo de comando `delete-object` a seguir mostra como você pode usar a AWS CLI para excluir um objeto de um bucket. Para executar esse comando, substitua os *`user input placeholders`* por suas próprias informações.

```
aws s3api delete-object --bucket bucket-base-name--zone-id--x-s3 --key KEY_NAME
```

Para obter mais informações, consulte delete-object na Referência de comandos da AWS CLI.

O exemplo de comando `delete-objects` a seguir mostra como você pode usar a AWS CLI para excluir um objeto de um bucket. Para executar esse comando, substitua os *`user input placeholders`* por suas próprias informações.

O arquivo `delete.json` é o seguinte:

```
{
    "Objects": [
        {
            "Key": "0.txt"
        },
        {
            "Key": "1.txt"
        },
        {
            "Key": "2.txt"
        },
        {
            "Key": "3.txt"
        }
    ]
}
```

O exemplo de comando `delete-objects` é o seguinte:

```
aws s3api delete-objects --bucket bucket-base-name--zone-id--x-s3 --delete
 file://delete.json
```

Para obter mais informações, consulte delete-objects na Referência de comandos da AWS CLI.

Baixar um objeto de um bucket de diretório

Os exemplos de código a seguir mostram como ler dados de um objeto (download) em um bucket de diretório do Amazon S3 usando a operação de API `GetObject`.

Uso dos SDKs da AWS

SDK for Java 2.x

Example

O exemplo de código a seguir mostra como ler dados de um objeto em um bucket de diretório usando o AWS SDK for Java 2.x.

```
public static void getObject(S3Client s3Client, String bucketName, String objectKey)
 {
     try {
         GetObjectRequest objectRequest = GetObjectRequest
            .builder()
            .key(objectKey)
            .bucket(bucketName)
            .build();

         ResponseBytes GetObjectResponse objectBytes =
 s3Client.getObjectAsBytes(objectRequest);
         byte[] data = objectBytes.asByteArray();

         //Print object contents to console
         String s = new String(data, StandardCharsets.UTF_8);
         System.out.println(s);
    }

    catch (S3Exception e) {
        System.err.println(e.awsErrorDetails().errorMessage());
        System.exit(1);
    }
}
```

SDK for Python

Example

O exemplo de código a seguir mostra como ler dados de um objeto em um bucket de diretório usando o AWS SDK para Python (Boto3).

```
import boto3
from botocore.exceptions import ClientError
from botocore.response import StreamingBody

def get_object(s3_client: boto3.client, bucket_name: str, key_name: str) ->
 StreamingBody:
    """
    Gets the object.
    :param s3_client:
    :param bucket_name: The bucket that contains the object.
    :param key_name: The key of the object to be downloaded.
    :return: The object data in bytes.
    """
    try:
        response = s3_client.get_object(Bucket=bucket_name, Key=key_name)
        body = response['Body'].read()
        print(f"Got object '{key_name}' from bucket '{bucket_name}'.")
    except ClientError:
        print(f"Couldn't get object '{key_name}' from bucket '{bucket_name}'.")
        raise
    else:
        return body

def main():
    s3_client = boto3.client('s3')
    resp = get_object(s3_client, 'doc-example-bucket--use1-az4--x-s3', 'sample.txt')
    print(resp)

if __name__ == "__main__":
     main()
```

Como usar o AWS CLI

O exemplo de `get-object` a seguir mostra como você pode usar a AWS CLI para baixar um objeto do Amazon S3. Esse comando obtém o objeto *KEY_NAME* do bucket de diretório *bucket-base-*

name--*zone-id*--x-s3. O objeto será baixado em um arquivo chamado *LOCAL_FILE_NAME*. Para executar esse comando, substitua os *user input placeholders* por suas próprias informações.

```
aws s3api get-object --bucket bucket-base-name--zone-id--x-s3 --
key KEY_NAME LOCAL_FILE_NAME
```

Para obter mais informações, consulte get-object na Referência de comandos da AWS CLI.

Gerar URLs pré-assinados para compartilhar objetos de bucket de diretório

Os exemplos de código a seguir mostram como gerar URLs pré-assinados para compartilhar objetos de um bucket de diretório do Amazon S3.

Como usar o AWS CLI

O exemplo de comando a seguir mostra como você pode usar a AWS CLI para gerar um URL pré-assinado para um objeto do Amazon S3. Esse comando gera um URL pré-assinado para um objeto *KEY_NAME* do bucket de diretório *bucket-base-name*--*zone-id*--x-s3. Para executar esse comando, substitua os *user input placeholders* por suas próprias informações.

```
aws s3 presign s3://bucket-base-name--zone-id--x-s3/KEY_NAME --expires-in 7200
```

Para obter mais informações, consulte presign na Referência de comandos da AWS CLI.

Recuperar metadados de objeto dos buckets de diretório

Os exemplos a seguir de AWS SDK e da AWS CLI mostram como usar as operações de API `HeadObject` e `GetObjectAttributes` para recuperar metadados de um objeto em um bucket de diretório do Amazon S3 sem retornar o objeto em si.

Uso dos SDKs da AWS

SDK for Java 2.x

Example

```
public static void headObject(S3Client s3Client, String bucketName, String
 objectKey) {
     try {
         HeadObjectRequest headObjectRequest = HeadObjectRequest
                 .builder()
```

```
                .bucket(bucketName)
                .key(objectKey)
                .build();
        HeadObjectResponse response = s3Client.headObject(headObjectRequest);
        System.out.format("Amazon S3 object: \"%s\" found in bucket: \"%s\" with
ETag: \"%s\"", objectKey, bucketName, response.eTag());
    }
    catch (S3Exception e) {
        System.err.println(e.awsErrorDetails().errorMessage());
```

Como usar o AWS CLI

O exemplo de comando `head-object` a seguir mostra como você pode usar a AWS CLI para recuperar metadados de um objeto. Para executar esse comando, substitua os *`user input placeholders`* por suas próprias informações.

```
aws s3api head-object --bucket bucket-base-name--zone-id--x-s3 --key KEY_NAME
```

Para obter mais informações, consulte head-object na Referência de comandos da AWS CLI.

O exemplo de comando `get-object-attributes` a seguir mostra como você pode usar a AWS CLI para recuperar metadados de um objeto. Para executar esse comando, substitua os *`user input placeholders`* por suas próprias informações.

```
aws s3api get-object-attributes --bucket bucket-base-name--zone-id--x-s3 --key KEY_NAME
 --object-attributes "StorageClass" "ETag" "ObjectSize"
```

Para obter mais informações, consulte get-object-attributes na Referência de comandos da AWS CLI.

Listar objetos de um bucket de diretório

Os exemplos de código a seguir mostram como listar os objetos de um bucket de diretório do Amazon S3 usando a operação de API `ListObjectsV2`.

Como usar o AWS CLI

O exemplo de comando `list-objects-v2` a seguir mostra como você pode usar a AWS CLI para listar objetos do Amazon S3. Esse comando lista os objetos do bucket de diretório *`bucket-base-name--zone-id--x-s3`*. Para executar esse comando, substitua os *`user input placeholders`* por suas próprias informações.

```
aws s3api list-objects-v2 --bucket bucket-base-name--zone-id--x-s3
```

Para obter mais informações, consulte list-objects-v2 na Referência de comandos da AWS CLI.

Segurança para buckets de diretório

A segurança na nuvem na AWS é a nossa maior prioridade. Como cliente da AWS, você se beneficiará de data centers e arquiteturas de rede criados para atender aos requisitos das empresas com as maiores exigências de segurança. A segurança é uma responsabilidade compartilhada entre a AWS e você. O modelo de responsabilidade compartilhada descreve isto como segurança da nuvem e segurança na nuvem:

- Segurança da nuvem: a AWS é responsável pela proteção da infraestrutura que executa os Serviços da AWS na Nuvem AWS. A AWS também fornece serviços que você pode usar com segurança. Auditores de terceiros testam e verificam regularmente a eficácia da nossa segurança como parte dos AWS Compliance Programs.

  Para saber mais sobre os programas de conformidade, consulte Serviços da AWS in Scope by Compliance Program.
- Segurança na nuvem: sua responsabilidade é determinada pelo AWS service (Serviço da AWS) que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade dos dados, os requisitos da empresa e as leis e regulamentos aplicáveis.

Esta documentação ajudará você a entender como aplicar o modelo de responsabilidade compartilhada ao usar buckets de diretório. Os tópicos a seguir mostram como configurar buckets de diretório para atender aos seus objetivos de segurança e conformidade. Você também aprenderá como usar outros Serviços da AWS que podem ajudar a monitorar e proteger seus objetos em buckets de diretório.

Proteção e criptografia de dados

Consulte mais informações sobre como configurar a criptografia de buckets de diretório nos tópicos a seguir.

Tópicos

- Criptografia do lado do servidor
- Definir e monitorar a criptografia padrão para buckets de diretório

- Usar a criptografia do lado do servidor com chaves do AWS KMS (SSE-KMS) em buckets de diretório
- Criptografia em trânsito
- Exclusão de dados

Criptografia do lado do servidor

Todos os buckets de diretório têm criptografia configurada por padrão, e todos os novos objetos carregados em buckets de diretório são automaticamente criptografados em repouso. A criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3) é a configuração de criptografia padrão para todos os buckets de diretório. Se quiser especificar um tipo de criptografia diferente, você poderá usar a criptografia do lado do servidor com chaves do AWS Key Management Service (AWS KMS) (SSE-KMS), definindo a configuração de criptografia padrão do bucket. Para ter mais informações sobre SSE-KMS em buckets de diretório, consulte Usar a criptografia do lado do servidor com chaves do AWS KMS (SSE-KMS) em buckets de diretório.

Recomendamos que a criptografia padrão do bucket use a configuração desejada e que você não a substitua em suas solicitações `CreateSession` ou de objetos `PUT`. Desse modo, os novos objetos são criptografados automaticamente com as configurações de criptografia desejadas. Para ter mais informações sobre os comportamentos de substituição de criptografia em buckets de diretório, consulte Specifying server-side encryption with AWS KMS for new object uploads.

A SSE-KMS com buckets de diretório difere da SSE-KMS em buckets de uso geral nos aspectos a seguir.

- A configuração de SSE-KMS só comporta uma chave gerenciada pelo cliente por bucket de diretório durante a vida útil do bucket. Não há suporte para Chave gerenciada pela AWS (`aws/s3`). Além disso, depois que você especifica uma chave gerenciada pelo cliente para SSE-KMS, não é possível substituí-la pela configuração de SSE-KMS do bucket.

  É possível identificar a chave gerenciada pelo cliente que você especificou para a configuração SSE-KMS do bucket, da seguinte forma:

  - Faça uma solicitação de operação de API `HeadObject` para encontrar o valor de `x-amz-server-side-encryption-aws-kms-key-id` em sua resposta.

  Para usar uma nova chave gerenciada pelo cliente em seus dados, recomendamos copiar os objetos existentes em um novo bucket de diretório com uma nova chave gerenciada pelo cliente.

- Em operações de API de endpoint de zona (nível de objeto), com exceção de CopyObject e UploadPartCopy, você autentica e autoriza solicitações por meio de CreateSession para ter baixa latência. Recomendamos que a criptografia padrão do bucket use a configuração desejada e que você não a substitua em suas solicitações `CreateSession` ou de objetos PUT. Desse modo, os novos objetos são criptografados automaticamente com as configurações de criptografia desejadas. Para criptografar novos objetos em um bucket de diretório com SSE-KMS, é necessário especificar SSE-KMS como a configuração de criptografia padrão do bucket de diretório com uma chave do KMS (especificamente, uma chave gerenciada pelo cliente). Dessa forma, quando uma sessão é criada para operações de API de endpoint de zona, novos objetos são automaticamente criptografados e descriptografados com chaves de SSE-KMS e de bucket do S3 durante a sessão. Para ter mais informações sobre os comportamentos de substituição de criptografia em buckets de diretório, consulte Specifying server-side encryption with AWS KMS for new object uploads.

  Nas chamadas de API de endpoint de zona (exceto CopyObject e UploadPartCopy), não é possível substituir os valores de configuração de criptografia (`x-amz-server-side-encryption`, `x-amz-server-side-encryption-aws-kms-key-id`, `x-amz-server-side-encryption-context` e `x-amz-server-side-encryption-bucket-key-enabled`) da solicitação `CreateSession`. Não é necessário especificar explicitamente esses valores de configuração de criptografia em chamadas de API de endpoint de zona. O Amazon S3 usará os valores das configurações de criptografia da solicitação `CreateSession` para proteger novos objetos no bucket de diretório.

  > **Note**
  >
  > Quando você usa a AWS CLI ou os SDKs da AWS, para `CreateSession`, o token da sessão é atualizado automaticamente para evitar interrupções no serviço quando uma sessão expira. A AWS CLI ou os SDKs da AWS usam a configuração de criptografia padrão do bucket para a solicitação `CreateSession`. A substituição dos valores de configuração de criptografia não é aceita na solicitação `CreateSession`. Além disso, nas chamadas de API de endpoint de zona (exceto CopyObject e UploadPartCopy), não é possível substituir os valores de configuração de criptografia da solicitação `CreateSession`.

- Com relação a CopyObject, para criptografar novas cópias de objetos em um bucket de diretório com SSE-KMS, é necessário especificar SSE-KMS como a configuração de criptografia padrão do bucket de diretório com uma chave do KMS (especificamente, uma chave gerenciada pelo cliente). Depois, ao especificar as configurações de criptografia do lado do servidor para novas cópias de

objetos com SSE-KMS, é necessário garantir que a chave de criptografia seja a mesma chave gerenciada pelo cliente que você especificou para a configuração de criptografia padrão do bucket de diretório. Quanto a UploadPartCopy, para criptografar novas cópias de partes de objetos em um bucket de diretório com SSE-KMS, é necessário especificar SSE-KMS como a configuração de criptografia padrão do bucket de diretório com uma chave do KMS (especificamente, uma chave gerenciada pelo cliente). Não é possível especificar as configurações de criptografia do lado do servidor para novas cópias de partes do objeto com SSE-KMS nos cabeçalhos da solicitação UploadPartCopy. Além disso, as configurações de criptografia fornecidas na solicitação CreateMultipartUpload devem corresponder à configuração de criptografia padrão do bucket de destino.

- As chaves de bucket do S3 estão sempre habilitadas para operações `GET` e `PUT` em um bucket de diretório e não podem ser desabilitadas. Não são aceitas chaves de bucket do S3 quando você copia objetos criptografados por SSE-KMS de buckets de uso geral para buckets de diretório, de buckets de diretório para buckets de uso geral ou entre buckets de diretório, por meio de CopyObject, de UploadPartCopy, da operação Copy em Operações em Lote ou de trabalhos de import. Nesse caso, o Amazon S3 faz uma chamada para o AWS KMS sempre que uma solicitação de cópia é feita para um objeto criptografado pelo KMS.
- Ao especificar uma chave do AWS KMS gerenciada pelo cliente para criptografia no bucket de diretório, use somente o ID ou o ARN da chave. O formato de alias da chave do KMS não é aceito.

Os buckets de diretório não são compatíveis com criptografia de camada dupla do lado do servidor com chaves do AWS Key Management Service (AWS KMS) (DSSE-KMS) ou com criptografia do lado do servidor com chaves fornecidas pelo cliente (SSE-C).

Definir e monitorar a criptografia padrão para buckets de diretório

Os buckets do Amazon S3 têm a criptografia configurada por padrão, e os novos objetos são automaticamente criptografados usando criptografia do lado do servidor, com chaves gerenciadas do Amazon S3 (SSE-S3). Essa criptografia se aplica a todos os novos objetos em seus buckets do Amazon S3 e não tem nenhum custo para você.

Se você precisar de maior controle sobre suas chaves de criptografia, como gerenciar a alternância de chaves e as concessões de política de acesso, poderá optar por usar a criptografia do lado do servidor com chaves do AWS Key Management Service (AWS KMS) (SSE-KMS).

Note

- Recomendamos que a criptografia padrão do bucket use a configuração desejada e que você não a substitua em suas solicitações `CreateSession` ou de objetos `PUT`. Desse modo, os novos objetos são criptografados automaticamente com as configurações de criptografia desejadas. Para ter mais informações sobre os comportamentos de substituição de criptografia em buckets de diretório, consulte Specifying server-side encryption with AWS KMS for new object uploads.
- Para criptografar novos objetos em um bucket de diretório com SSE-KMS, é necessário especificar SSE-KMS como a configuração de criptografia padrão do bucket de diretório com uma chave do KMS (especificamente, uma chave gerenciada pelo cliente). Dessa forma, quando uma sessão é criada para operações de API de endpoint de zona, novos objetos são automaticamente criptografados e descriptografados com chaves de SSE-KMS e de bucket do S3 durante a sessão.
- Quando você define a criptografia de bucket padrão como SSE-KMS, as chaves de bucket do S3 permanecem habilitadas para operações `GET` e `PUT` em um bucket de diretório e não podem ser desabilitadas. Não são aceitas chaves de bucket do S3 quando você copia objetos criptografados por SSE-KMS de buckets de uso geral para buckets de diretório, de buckets de diretório para buckets de uso geral ou entre buckets de diretório, por meio de CopyObject, de UploadPartCopy, da operação Copy em Operações em Lote ou de trabalhos de import. Nesse caso, o Amazon S3 faz uma chamada para o AWS KMS sempre que uma solicitação de cópia é feita para um objeto criptografado pelo KMS. Para ter mais informações sobre como as chaves de bucket do S3 reduzem os custos de solicitação do AWS KMS, consulte Redução do custo do SSE-KMS com chaves de bucket do Amazon S3.
- Ao especificar uma chave do AWS KMS gerenciada pelo cliente para criptografia no bucket de diretório, use somente o ID ou o ARN da chave. O formato de alias da chave do KMS não é aceito.
- A criptografia de camada dupla do lado do servidor com chaves do AWS KMS (DSSE-KMS) e a criptografia do lado do servidor com chaves fornecidas pelo cliente (SSE-C) não são compatíveis com a criptografia padrão em buckets de diretório.

Para ter mais informações sobre como configurar a criptografia padrão, consulte Configurar a criptografia padrão.

Para ter mais informações sobre permissões necessárias para criptografia padrão, consulte PutBucketEncryption na Referência da API do Amazon Simple Storage Service.

Você pode configurar a criptografia padrão do Amazon S3 para um bucket do S3 usando o console do Amazon S3, os AWS SDKs, a API REST do Amazon S3 e a AWS Command Line Interface (AWS CLI).

Usar o console do S3

Como configurar a criptografia padrão em um bucket do Amazon S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets.
3. Na lista de Buckets, escolha o nome do bucket desejado.
4. Escolha a guia Properties (Propriedades).
5. Em Configurações de criptografia no lado do servidor, os buckets de diretório usam a criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3).
6. Escolha Salvar alterações.

Como usar o AWS CLI

Esses exemplos mostram como configurar a criptografia padrão usando SSE-S3 ou usando a SSE-KMS com uma chave de bucket do S3.

Para obter mais informações sobre criptografia padrão, consulte Definir o comportamento padrão da criptografia para os buckets do Amazon S3. Para obter mais informações sobre o uso da AWS CLI para configurar a criptografia padrão, consulte put-bucket-encryption.

Example – Criptografia padrão com SSE-S3

Esse exemplo configura a criptografia de bucket padrão com chaves gerenciadas pelo Amazon S3. Para usar o comando, substitua os *espaços reservados para entrada do usuário* por suas próprias informações.

```
aws s3api put-bucket-encryption --bucket bucket-base-name--zone-id--x-s3 --server-side-encryption-configuration '{
    "Rules": [
        {
```

```
            "ApplyServerSideEncryptionByDefault": {
                "SSEAlgorithm": "AES256"
            }
        }
    ]
}'
```

Example – Criptografia padrão com SSE-KMS usando uma chave de bucket do S3

Esse exemplo configura a criptografia de bucket padrão com o SSE-KMS usando uma chave de bucket do S3. Para usar o comando, substitua os *espaços reservados para entrada do usuário* por suas próprias informações.

```
aws s3api put-bucket-encryption --bucket bucket-base-name--zone-id--x-s3 --server-side-
encryption-configuration '{
    "Rules": [
            {
                "ApplyServerSideEncryptionByDefault": {
                    "SSEAlgorithm": "aws:kms",
                    "KMSMasterKeyID": "KMS-Key-ARN"
                },
                "BucketKeyEnabled": true
            }
        ]
    }'
```

Uso da API REST

Use a operação `PutBucketEncryption` da API REST para definir a criptografia padrão com o tipo de criptografia do lado do servidor a ser utilizado, ou seja, SSE-S3 ou SSE-KMS.

Para obter mais informações, consulte PutBucketEncryption na Referência da API do Amazon Simple Storage Service.

Uso dos SDKs da AWS

Ao usar AWS SDKs, é possível solicitar que o Amazon S3 use AWS KMS keys para criptografia do lado do servidor. Os exemplos de SDKs da AWS para Java e .NET a seguir definem a configuração de criptografia padrão para um bucket de diretório com SSE-KMS e uma chave de bucket do S3. Para obter informações sobre outros SDKs, consulte Código de exemplo e bibliotecas no Centro do desenvolvedor da AWS.

> **Important**
>
> Ao usar uma AWS KMS key para criptografia no lado do servidor no Amazon S3, você deve escolher uma chave de criptografia do KMS simétrica. O Amazon S3 só é compatível com chaves do KMS de criptografia simétrica. Para obter mais informações sobre essas chaves, consulte Chaves do KMS de criptografia simétrica no Guia do desenvolvedor do AWS Key Management Service.

Java

Com o AWS SDK for Java 2.x, é possível solicitar que o Amazon S3 use uma AWS KMS key utilizando o método `applyServerSideEncryptionByDefault` para especificar a configuração de criptografia padrão do bucket de diretório para criptografia de dados com a SSE-KMS. É possível criar uma chave de criptografia simétrica do KMS e especificar isso na solicitação.

```
import software.amazon.awssdk.services.s3.S3Client;
import software.amazon.awssdk.services.s3.model.PutBucketEncryptionRequest;
import software.amazon.awssdk.services.s3.model.ServerSideEncryption;
import software.amazon.awssdk.services.s3.model.ServerSideEncryptionByDefault;
import software.amazon.awssdk.services.s3.model.ServerSideEncryptionConfiguration;
import software.amazon.awssdk.services.s3.model.ServerSideEncryptionRule;

public class Main {
    public static void main(String[] args) {
        S3Client s3 = S3Client.create();
        String bucketName = "bucket-base-name--zoneid--x-s3";
        String kmsKeyId = "your-kms-customer-managed-key-id";

        // AWS managed KMS keys aren't supported. Only customer-managed keys are
 supported.
        ServerSideEncryptionByDefault serverSideEncryptionByDefault =
 ServerSideEncryptionByDefault.builder()
                .sseAlgorithm(ServerSideEncryption.AWS_KMS)
                .kmsMasterKeyID(kmsKeyId)
                .build();

        // The bucketKeyEnabled field is enforced to be true.
        ServerSideEncryptionRule rule = ServerSideEncryptionRule.builder()
```

```
                .bucketKeyEnabled(true)
                .applyServerSideEncryptionByDefault(serverSideEncryptionByDefault)
                .build();

        ServerSideEncryptionConfiguration serverSideEncryptionConfiguration =
 ServerSideEncryptionConfiguration.builder()
                .rules(rule)
                .build();

        PutBucketEncryptionRequest putRequest = PutBucketEncryptionRequest.builder()
                .bucket(bucketName)

 .serverSideEncryptionConfiguration(serverSideEncryptionConfiguration)
                .build();

        s3.putBucketEncryption(putRequest);

    }
}
```

Para obter mais informações sobre como criar chaves gerenciadas pelo cliente, consulte Programação da API do AWS KMS no Guia do desenvolvedor do AWS Key Management Service.

Para ver exemplos de código funcionais de upload de um objeto, consulte os seguintes tópicos. Para usar esses exemplos, é necessário atualizar os exemplos de código e fornecer informações de criptografia, conforme exibido no fragmento de código anterior.

- Para fazer upload de um objeto em uma única operação, consulte Fazer upload de objetos em um bucket de diretório.
- Em relação a operações de API de carregamento fracionado, consulte Usar uploads multiparte com buckets de diretório.

.NET

Com o AWS SDK para .NET, é possível solicitar que o Amazon S3 use uma AWS KMS key utilizando o método `ServerSideEncryptionByDefault` para especificar a configuração de criptografia padrão do bucket de diretório para criptografia de dados com a SSE-KMS. Você deve criar uma chave de criptografia simétrica gerenciada pelo cliente e especificar isso na solicitação.

```
    // Set the bucket server side encryption to use AWSKMS with a customer-managed
 key id.
    // bucketName: Name of the directory bucket. "bucket-base-name--zonsid--x-s3"
    // kmsKeyId: The Id of the customer managed KMS Key. "your-kms-customer-managed-
key-id"
    // Returns True if successful.
    public static async Task<bool> SetBucketServerSideEncryption(string bucketName,
 string kmsKeyId)
    {
        var serverSideEncryptionByDefault = new ServerSideEncryptionConfiguration
        {
            ServerSideEncryptionRules = new List<ServerSideEncryptionRule>
            {
                new ServerSideEncryptionRule
                {
                    ServerSideEncryptionByDefault = new
 ServerSideEncryptionByDefault
                    {
                        ServerSideEncryptionAlgorithm =
 ServerSideEncryptionMethod.AWSKMS,
                        ServerSideEncryptionKeyManagementServiceKeyId = kmsKeyId
                    }
                }
            }
        };
        try
        {
            var encryptionResponse =await _s3Client.PutBucketEncryptionAsync(new
 PutBucketEncryptionRequest
            {
                BucketName = bucketName,
                ServerSideEncryptionConfiguration = serverSideEncryptionByDefault,
            });

            return encryptionResponse.HttpStatusCode == HttpStatusCode.OK;
        }
        catch (AmazonS3Exception ex)
        {
            Console.WriteLine(ex.ErrorCode == "AccessDenied"
                ? $"This account does not have permission to set encryption on
 {bucketName}, please try again."
```

```
                : $"Unable to set bucket encryption for bucket {bucketName},
{ex.Message}");
        }
        return false;
    }
```

Para obter mais informações sobre como criar chaves gerenciadas pelo cliente, consulte Programação da API do AWS KMS no Guia do desenvolvedor do AWS Key Management Service.

Para ver exemplos de código funcionais de upload de um objeto, consulte os seguintes tópicos. Para usar esses exemplos, é necessário atualizar os exemplos de código e fornecer informações de criptografia, conforme exibido no fragmento de código anterior.

- Para fazer upload de um objeto em uma única operação, consulte Fazer upload de objetos em um bucket de diretório.
- Em relação a operações de API de carregamento fracionado, consulte Usar uploads multiparte com buckets de diretório.

Monitorar a criptografia padrão para buckets de diretório com o AWS CloudTrail

É possível acompanhar solicitações de configuração de criptografia padrão para buckets de diretório do Amazon S3 usando eventos do AWS CloudTrail. Os seguintes nomes de eventos de API são usados nos logs do CloudTrail:

- `PutBucketEncryption`
- `GetBucketEncryption`
- `DeleteBucketEncryption`

> **Note**
>
> - Não é possível usar o EventBridge em buckets de diretório.

- A criptografia de camada dupla do lado do servidor com chaves do AWS Key Management Service (AWS KMS) (DSSE-KMS) ou a criptografia do lado do servidor com chaves fornecidas pelo cliente (SSE-C) não são aceitas em buckets de diretório.

Para ter mais informações sobre como monitorar a criptografia padrão com o AWS CloudTrail, consulte Monitorar a criptografia padrão com o AWS CloudTrail e o Amazon EventBridge.

Usar a criptografia do lado do servidor com chaves do AWS KMS (SSE-KMS) em buckets de diretório

Os controles de segurança do AWS KMS podem ajudá-lo a satisfazer os requisitos de conformidade relacionados à criptografia. É possível optar por configurar buckets de diretório para usar a criptografia do lado do servidor com chaves do AWS Key Management Service (AWS KMS) (SSE-KMS) e usar essas chaves do KMS para proteger os dados em buckets de diretório do Amazon S3. Para obter mais informações sobre SSE-KMS, consulte Usar criptografia do lado do servidor com o AWS KMS (SSE-KMS).

Permissões

Para fazer upload ou baixar um objeto criptografado com uma AWS KMS key de ou para o Amazon S3, você precisa das permissões `kms:GenerateDataKey` e `kms:Decrypt` na chave. Para ter mais informações, consulte Permitir que os usuários da chave usem uma chave do KMS para operações criptográficas no Guia do desenvolvedor do AWS Key Management Service. Para obter informações sobre permissões do AWS KMS necessárias para uploads de várias partes, consulte API de multipart upload e permissões.

Para ter mais informações sobre chaves do KMS, consulte Especificando criptografia no lado do servidor com o AWS KMS (SSE-KMS).

Tópicos

- AWS KMS keys
- Usar SSE-KMS para operações entre contas
- Amazon S3 Bucket Keys
- Como exigir SSE-KMS
- Contexto de criptografia
- Enviar solicitações para objetos criptografados do AWS KMS

- Realizar auditoria da criptografia SSE-KMS em buckets de diretório
- Especificar a criptografia do lado do servidor com o AWS KMS (SSE-KMS) para novos uploads de objetos em buckets de diretório

AWS KMS keys

A configuração de SSE-KMS só comporta uma chave gerenciada pelo cliente por bucket de diretório durante a vida útil do bucket. Não há suporte para Chave gerenciada pela AWS (`aws/s3`). Além disso, depois que você especifica uma chave gerenciada pelo cliente para SSE-KMS, não é possível substituí-la pela configuração de SSE-KMS do bucket.

É possível identificar a chave gerenciada pelo cliente que você especificou para a configuração SSE-KMS do bucket, da seguinte forma:

- Faça uma solicitação de operação de API `HeadObject` para encontrar o valor de `x-amz-server-side-encryption-aws-kms-key-id` em sua resposta.

Para usar uma nova chave gerenciada pelo cliente em seus dados, recomendamos copiar os objetos existentes em um novo bucket de diretório com uma nova chave gerenciada pelo cliente.

Ao especificar uma chave do AWS KMS gerenciada pelo cliente para criptografia no bucket de diretório, use somente o ID ou o ARN da chave. O formato de alias da chave do KMS não é aceito.

Para ter mais informações sobre chaves do KMS, consulte AWS KMS keys.

Usar SSE-KMS para operações entre contas

Ao utilizar a criptografia para operações entre contas em buckets de diretório, lembre-se do seguinte:

- Se você quiser conceder acesso entre contas aos objetos do S3, configure uma política de chave gerenciada pelo cliente para permitir o acesso de outra conta.
- Para especificar uma chave gerenciada pelo cliente, é necessário usar um ARN de chave do KMS totalmente qualificado.

Amazon S3 Bucket Keys

As chaves de bucket do S3 estão sempre habilitadas para operações `GET` e `PUT` em um bucket de diretório e não podem ser desabilitadas. Não são aceitas chaves de bucket do S3 quando você copia objetos criptografados por SSE-KMS de buckets de uso geral para buckets de diretório, de buckets

de diretório para buckets de uso geral ou entre buckets de diretório, por meio de CopyObject, de UploadPartCopy, da operação Copy em Operações em Lote ou de trabalhos de import. Nesse caso, o Amazon S3 faz uma chamada para o AWS KMS sempre que uma solicitação de cópia é feita para um objeto criptografado pelo KMS.

Em operações de API de endpoint de zona (nível de objeto), com exceção de CopyObject e UploadPartCopy, você autentica e autoriza solicitações por meio de CreateSession para ter baixa latência. Recomendamos que a criptografia padrão do bucket use a configuração desejada e que você não a substitua em suas solicitações `CreateSession` ou de objetos PUT. Desse modo, os novos objetos são criptografados automaticamente com as configurações de criptografia desejadas. Para criptografar novos objetos em um bucket de diretório com SSE-KMS, é necessário especificar SSE-KMS como a configuração de criptografia padrão do bucket de diretório com uma chave do KMS (especificamente, uma chave gerenciada pelo cliente). Dessa forma, quando uma sessão é criada para operações de API de endpoint de zona, novos objetos são automaticamente criptografados e descriptografados com chaves de SSE-KMS e de bucket do S3 durante a sessão. Para ter mais informações sobre os comportamentos de substituição de criptografia em buckets de diretório, consulte Specifying server-side encryption with AWS KMS for new object uploads.

As chaves de bucket do S3 são usadas por um período limitado no Amazon S3, o que reduz ainda mais a necessidade de o Amazon S3 fazer solicitações ao AWS KMS para concluir operações de criptografia. Para ter mais informações sobre como usar chaves de bucket do S3, consulte Amazon S3 Bucket Keys e Redução do custo do SSE-KMS com chaves de bucket do Amazon S3.

Como exigir SSE-KMS

Para exigir SSE-KMS de todos os objetos em um bucket de diretório específico, use uma política de bucket. Por exemplo, ao usar a operação de API `CreateSession` para conceder permissão para fazer upload de um novo objeto (`PutObject`, `CopyObject` e `CreateMultipartUpload`), a política de bucket a seguir negará a permissão de upload de objeto (`s3express:CreateSession`) a todos se a solicitação `CreateSession` não incluir um cabeçalho `x-amz-server-side-encryption-aws-kms-key-id` que solicite SSE-KMS.

```
{
   "Version":"2012-10-17",
   "Id":"UploadObjectPolicy",
   "Statement":[{
         "Sid":"DenyObjectsThatAreNotSSEKMS",
         "Effect":"Deny",
         "Principal":"*",
```

```
         "Action":"s3express:CreateSession",
         "Resource":"arn:aws:s3express:region:account-id:bucket/bucket-base-name--zone-
id--x-s3/*",
         "Condition":{
            "Null":{
               "s3express:x-amz-server-side-encryption-aws-kms-key-id":"true"
            }
         }
      }
   ]
}
```

Para exigir que uma AWS KMS key específica seja usada para criptografar os objetos em um bucket, use a chave de condição `s3express:x-amz-server-side-encryption-aws-kms-key-id`. Para especificar a chave do KMS, é necessário usar um nome do recurso da Amazon (ARN) da chave no formato `arn:aws:kms:region:acct-id:key/key-id`. O AWS Identity and Access Management não validará se a string para `s3express:x-amz-server-side-encryption-aws-kms-key-id` existe. o ID de chave do AWS KMS que o Amazon S3 usa para a criptografia de objetos deve corresponder ao ID de chave do AWS KMS na política. Caso contrário, o Amazon S3 negará a solicitação.

Para ter mais informações sobre como usar a SSE-KMS para uploads de novos objetos, consulte Especificar a criptografia do lado do servidor com o AWS KMS (SSE-KMS) para novos uploads de objetos em buckets de diretório.

Para ter uma lista completa de chaves de condição específicas de buckets de diretório, consulte Autorizar operações de API de endpoint regional com o IAM.

Contexto de criptografia

No caso de buckets de diretório, contexto de criptografia é um conjunto de pares de chave-valor que contêm informações contextuais sobre os dados. Não é possível fornecer um valor de contexto de criptografia adicional. Para obter mais informações sobre o contexto de criptografia, consulte Contexto de criptografia.

Por padrão, se você usar a SSE-KMS em um bucket de diretório, o Amazon S3 usará o nome do recurso da Amazon (ARN) do bucket como o par de contexto de criptografia:

```
arn:aws:s3express:region:account-id:bucket/bucket-base-name--zone-id--x-s3
```

As políticas do IAM ou as políticas de chave do AWS KMS devem usar o ARN do bucket como contexto de criptografia.

Também é possível fornecer um par de contexto de criptografia explícito usando o cabeçalho `x-amz-server-side-encryption-context` em uma solicitação de API de endpoint de zona, como CreateSession. O valor desse cabeçalho é uma string codificada em base64 de um JSON codificado em UTF-8, que apresenta o contexto de criptografia como pares de chave-valor. Para buckets de diretório, o contexto de criptografia deve corresponder ao contexto de criptografia padrão: o nome do recurso da Amazon (ARN) do bucket. Além disso, como o contexto de criptografia não é criptografado, ele não deve incluir informações sigilosas.

É possível usar o contexto de criptografia para identificar e categorizar suas operações de criptografia. Também é possível usar o valor do ARN do contexto de criptografia padrão para monitorar solicitações relevantes no AWS CloudTrail visualizando qual ARN do bucket de diretório foi usado com qual chave de criptografia.

No campo `requestParameters` de um arquivo de log do CloudTrail, se você usar a SSE-KMS em um bucket de diretório, o valor do contexto de criptografia será o ARN do bucket.

```
"encryptionContext": {
    "aws:s3express:arn": "arn:aws:s3:::arn:aws:s3express:region:account-
id:bucket/bucket-base-name--zone-id--x-s3"
}
```

Além disso, para criptografia de objetos com SSE-KMS em um bucket de diretório, seus eventos do AWS KMS CloudTrail registram o ARN do bucket em vez do ARN do objeto.

Enviar solicitações para objetos criptografados do AWS KMS

Os buckets de diretório só podem ser acessados por meio de HTTPS (TLS). Além disso, os buckets de diretório assinam solicitações usando o AWS Signature Version 4 (SigV4). Para ter mais informações sobre o envio de solicitações de objetos criptografados do AWS KMS, consulte Enviar solicitações para objetos criptografados do AWS KMS.

Se o objeto usar SSE-KMS, não envie cabeçalhos de solicitação de criptografia para solicitações `GET` e solicitações `HEAD`. Caso contrário, você receberá um erro HTTP 400 Solicitação Inválida.

Realizar auditoria da criptografia SSE-KMS em buckets de diretório

Para auditar o uso das chaves do AWS KMS para seus dados criptografados por SSE-KMS, você pode usar logs do AWS CloudTrail. Você pode obter informações sobre suas operações

criptográficas, como GenerateDataKey e Decrypt. O CloudTrail oferece suporte a vários valores de atributos para filtrar a pesquisa, como nome do evento, nome de usuário e origem do evento.

Tópicos

- Especificar a criptografia do lado do servidor com o AWS KMS (SSE-KMS) para novos uploads de objetos em buckets de diretório

Especificar a criptografia do lado do servidor com o AWS KMS (SSE-KMS) para novos uploads de objetos em buckets de diretório

Em buckets de diretório, para criptografar dados, é possível usar a criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3) (padrão) ou com chaves do AWS Key Management Service (AWS KMS) (SSE-KMS). Recomendamos que a criptografia padrão do bucket use a configuração desejada e que você não a substitua em suas solicitações `CreateSession` ou de objetos PUT. Desse modo, os novos objetos são criptografados automaticamente com as configurações de criptografia desejadas. Para ter mais informações sobre os comportamentos de substituição de criptografia em buckets de diretório, consulte Specifying server-side encryption with AWS KMS for new object uploads.

Todos os buckets do Amazon S3 têm criptografia configurada por padrão e todos os novos objetos que são carregados em um bucket do S3 são automaticamente criptografados em repouso. A criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3) é a configuração de criptografia padrão para todos os buckets no Amazon S3. Se você quiser especificar um tipo de criptografia diferente para um bucket de diretório, é possível usar a criptografia do lado do servidor com chaves do AWS Key Management Service (AWS KMS) (SSE-KMS). Para criptografar novos objetos em um bucket de diretório com SSE-KMS, é necessário especificar SSE-KMS como a configuração de criptografia padrão do bucket de diretório com uma chave do KMS (especificamente, uma chave gerenciada pelo cliente). Não há suporte para Chave gerenciada pela AWS (`aws/s3`). A configuração de SSE-KMS só comporta uma chave gerenciada pelo cliente por bucket de diretório durante a vida útil do bucket. Depois que você especifica uma chave gerenciada pelo cliente para SSE-KMS, não é possível substituí-la pela configuração de SSE-KMS do bucket. Depois, ao especificar as configurações de criptografia do lado do servidor para novos objetos com SSE-KMS, é necessário garantir que a chave de criptografia seja a mesma chave gerenciada pelo cliente que você especificou para a configuração de criptografia padrão do bucket de diretório. Para usar uma nova chave gerenciada pelo cliente em seus dados, recomendamos copiar os objetos existentes em um novo bucket de diretório com uma nova chave gerenciada pelo cliente.

É possível aplicar criptografia durante o upload de um novo objeto ou ao copiar um objeto existente. Se você alterar a criptografia de um objeto, um novo objeto será criado para substituir o antigo.

É possível especificar a SSE-KMS utilizando as operações da API REST, SDKs da AWS e a AWS Command Line Interface (AWS CLI).

> **Note**
>
> - Para buckets de diretório, os comportamentos de substituição de criptografia são os seguintes:
>   - Ao usar CreateSession com a API REST para autenticar e autorizar solicitações de API de endpoint de zona, exceto CopyObject e UploadPartCopy, será possível substituir as configurações de criptografia para SSE-S3 ou SSE-KMS somente se você tiver especificado a criptografia padrão do bucket com SSE-KMS anteriormente.
>   - Ao usar CreateSession com a AWS CLI ou com os SDKs da AWS para autenticar e autorizar solicitações de API de endpoint de zona, exceto CopyObject e UploadPartCopy, não é possível substituir as configurações de criptografia de forma alguma.
>   - Ao fazer solicitações CopyObject, será possível substituir as configurações de criptografia como SSE-S3 ou SSE-KMS somente se você tiver especificado a criptografia padrão do bucket com SSE-KMS anteriormente. Ao fazer solicitações UploadPartCopy, não é possível substituir as configurações de criptografia.
> - Você pode usar uma AWS KMS keys de várias regiões no Amazon S3. No entanto, o Amazon S3 trata no momento as chaves de várias regiões como se fossem chaves de região única e não usa os recursos de várias regiões da chave. Para obter mais informações, consulte Usar chaves de várias regiões no Guia do desenvolvedor doAWS Key Management Service.
> - Se quiser usar uma chave do KMS que seja de propriedade de outra conta, você deverá ter permissão para usar a chave. Para obter mais informações sobre permissões entre contas para chaves do KMS, consulte Criar chaves do KMS que outras contas podem usar no Guia do desenvolvedor do AWS Key Management Service.

Uso da API REST

> **Note**
>
> Somente uma chave gerenciada pelo cliente é aceita por bucket de diretório durante o ciclo de vida do bucket. Não há suporte para Chave gerenciada pela AWS (`aws/s3`). Depois que você especificar a SSE-KMS como a configuração de criptografia padrão do bucket com uma chave gerenciada pelo cliente, não será possível alterar a chave gerenciada pelo cliente para a configuração SSE-KMS do bucket.

Em operações de API de endpoint de zona (nível de objeto), com exceção de CopyObject e UploadPartCopy, você autentica e autoriza solicitações por meio de CreateSession para ter baixa latência. Recomendamos que a criptografia padrão do bucket use as configurações desejadas e que você não a substitua em suas solicitações `CreateSession` ou de objetos PUT. Desse modo, os novos objetos são criptografados automaticamente com as configurações de criptografia desejadas. Para criptografar novos objetos em um bucket de diretório com SSE-KMS, é necessário especificar SSE-KMS como a configuração de criptografia padrão do bucket de diretório com uma chave do KMS (especificamente, uma chave gerenciada pelo cliente). Dessa forma, quando uma sessão é criada para operações de API de endpoint de zona, novos objetos são automaticamente criptografados e descriptografados com chaves de SSE-KMS e de bucket do S3 durante a sessão. Para ter mais informações sobre os comportamentos de substituição de criptografia em buckets de diretório, consulte Specifying server-side encryption with AWS KMS for new object uploads.

Nas chamadas de API de endpoint de zona (exceto CopyObject e UploadPartCopy) utilizando a API REST, não é possível substituir os valores das configurações de criptografia (`x-amz-server-side-encryption`, `x-amz-server-side-encryption-aws-kms-key-id`, `x-amz-server-side-encryption-context` e `x-amz-server-side-encryption-bucket-key-enabled`) da solicitação `CreateSession`. Não é necessário especificar explicitamente esses valores de configuração de criptografia em chamadas de API de endpoint de zona. O Amazon S3 usará os valores das configurações de criptografia da solicitação `CreateSession` para proteger novos objetos no bucket de diretório.

> **Note**
>
> Quando você usa a AWS CLI ou os SDKs da AWS, para `CreateSession`, o token da sessão é atualizado automaticamente para evitar interrupções no serviço quando uma sessão expira. A AWS CLI ou os SDKs da AWS usam a configuração de criptografia padrão

do bucket para a solicitação `CreateSession`. A substituição dos valores de configuração de criptografia não é aceita na solicitação `CreateSession`. Além disso, nas chamadas de API de endpoint de zona (exceto CopyObject e UploadPartCopy), não é possível substituir os valores de configuração de criptografia da solicitação `CreateSession`.

Com relação a CopyObject, para criptografar novas cópias de objetos em um bucket de diretório com SSE-KMS, é necessário especificar SSE-KMS como a configuração de criptografia padrão do bucket de diretório com uma chave do KMS (especificamente, uma chave gerenciada pelo cliente). Depois, ao especificar as configurações de criptografia do lado do servidor para novas cópias de objetos com SSE-KMS, é necessário garantir que a chave de criptografia seja a mesma chave gerenciada pelo cliente que você especificou para a configuração de criptografia padrão do bucket de diretório. Quanto a UploadPartCopy, para criptografar novas cópias de partes de objetos em um bucket de diretório com SSE-KMS, é necessário especificar SSE-KMS como a configuração de criptografia padrão do bucket de diretório com uma chave do KMS (especificamente, uma chave gerenciada pelo cliente). Não é possível especificar as configurações de criptografia do lado do servidor para novas cópias de partes do objeto com SSE-KMS nos cabeçalhos da solicitação UploadPartCopy. Além disso, as configurações de criptografia fornecidas na solicitação CreateMultipartUpload devem corresponder à configuração de criptografia padrão do bucket de destino.

Tópicos

- Operações da API REST do Amazon S3 compatíveis com SSE-KMS
- Contexto de criptografia (x-amz-server-side-encryption-context)
- ID da chave do AWS KMS (x-amz-server-side-encryption-aws-kms-key-id)
- Chaves de bucket do S3 (x-amz-server-side-encryption-aws-bucket-key-enabled)

Operações da API REST do Amazon S3 compatíveis com SSE-KMS

As operações da API REST em nível de objeto nos buckets de diretório a seguir aceitam os cabeçalhos de solicitação `x-amz-server-side-encryption`, `x-amz-server-side-encryption-aws-kms-key-id` e `x-amz-server-side-encryption-context`.

- CreateSession: ao usar operações de API de endpoint de zona (em nível de objeto) (exceto CopyObject e UploadPartCopy), é possível especificar esses cabeçalhos de solicitação.
- PutObject: ao carregar dados usando a operação de APIPUT, é possível especificar esses cabeçalhos de solicitação.

- CopyObject: quando você copia um objeto, há um objeto de origem e um objeto de destino. Ao transmitir cabeçalhos de SSE-KMS com a operação `CopyObject`, eles são aplicados somente ao objeto de destino.
- CreateMultipartUpload: ao fazer upload de objetos grandes usando a operação de API de upload multiparte, você pode especificar esses cabeçalhos. Esses cabeçalhos são especificados na solicitação `CreateMultipartUpload`.

Os cabeçalhos de resposta das operações de API REST a seguir retornam o cabeçalho `x-amz-server-side-encryption` quando um objeto é armazenado usando criptografia de servidor.

- CreateSession
- PutObject
- CopyObject
- POST Object
- CreateMultipartUpload
- UploadPart
- UploadPartCopy
- CompleteMultipartUpload
- GetObject
- HeadObject

> **Important**
>
> - Todas as solicitações `GET` e `PUT` para um objeto protegido pelo AWS KMS falharão se elas não forem feitas usando Transport Layer Security (TLS) ou Signature Version 4.
> - Se o objeto usar SSE-KMS, os cabeçalhos de solicitação de criptografia não deverão ser enviados para solicitações `GET` e solicitações `HEAD`,ou um erro HTTP 400 BadRequest será exibido.

Contexto de criptografia (**`x-amz-server-side-encryption-context`**)

Caso você especifique `x-amz-server-side-encryption:aws:kms`, a API do Amazon S3 permite que você forneça, opcionalmente, um contexto de criptografia explícito com o cabeçalho `x-`

`amz-server-side-encryption-context`. Para buckets de diretório, contexto de criptografia é um conjunto de pares de chave-valor que contêm informações contextuais sobre os dados. O valor deve corresponder ao contexto de criptografia padrão: o nome do recurso da Amazon (ARN) do bucket. Não é possível fornecer um valor de contexto de criptografia adicional.

Para ter informações sobre o contexto de criptografia nos buckets de diretório, consulte Contexto de criptografia. Para obter informações gerais sobre o contexto de criptografia, consulte Conceitos do AWS Key Management Service: contexto de criptografia no Guia do desenvolvedor do AWS Key Management Service.

ID da chave do AWS KMS (**`x-amz-server-side-encryption-aws-kms-key-id`**)

Você pode usar o cabeçalho `x-amz-server-side-encryption-aws-kms-key-id` para especificar o ID da chave gerenciada pelo cliente usada para proteger os dados.

A configuração de SSE-KMS só comporta uma chave gerenciada pelo cliente por bucket de diretório durante a vida útil do bucket. Não há suporte para Chave gerenciada pela AWS (`aws/s3`). Além disso, depois que você especifica uma chave gerenciada pelo cliente para SSE-KMS, não é possível substituí-la pela configuração de SSE-KMS do bucket.

É possível identificar a chave gerenciada pelo cliente que você especificou para a configuração SSE-KMS do bucket, da seguinte forma:

- Faça uma solicitação de operação de API `HeadObject` para encontrar o valor de `x-amz-server-side-encryption-aws-kms-key-id` em sua resposta.

Para usar uma nova chave gerenciada pelo cliente em seus dados, recomendamos copiar os objetos existentes em um novo bucket de diretório com uma nova chave gerenciada pelo cliente.

Para ter informações sobre o contexto de criptografia nos buckets de diretório, consulte AWS KMS keys.

Chaves de bucket do S3 (**`x-amz-server-side-encryption-aws-bucket-key-enabled`**)

As chaves de bucket do S3 estão sempre habilitadas para operações `GET` e `PUT` em um bucket de diretório e não podem ser desabilitadas. Não são aceitas chaves de bucket do S3 quando você copia objetos criptografados por SSE-KMS de buckets de uso geral para buckets de diretório, de buckets de diretório para buckets de uso geral ou entre buckets de diretório, por meio de CopyObject, de UploadPartCopy, da operação Copy em Operações em Lote ou de trabalhos de import. Nesse caso,

o Amazon S3 faz uma chamada para o AWS KMS sempre que uma solicitação de cópia é feita para um objeto criptografado pelo KMS. Para ter informações sobre as chaves de bucket do S3 em buckets de diretório, consulte Contexto de criptografia.

Como usar o AWS CLI

> **Note**
>
> Ao usar a AWS CLI, para `CreateSession`, o token da sessão é atualizado automaticamente para evitar interrupções no serviço quando uma sessão expira. A substituição dos valores de configuração de criptografia não é aceita para a solicitação `CreateSession`. Além disso, nas chamadas de API de endpoint de zona (exceto CopyObject e UploadPartCopy), não é possível substituir os valores de configuração de criptografia da solicitação `CreateSession`.
> Para criptografar novos objetos em um bucket de diretório com SSE-KMS, é necessário especificar SSE-KMS como a configuração de criptografia padrão do bucket de diretório com uma chave do KMS (especificamente, uma chave gerenciada pelo cliente). Dessa forma, quando uma sessão é criada para operações de API de endpoint de zona, novos objetos são automaticamente criptografados e descriptografados com chaves de SSE-KMS e de bucket do S3 durante a sessão.

Para usar os exemplos de comandos da AWS CLI a seguir, substitua os *`user input placeholders`* por suas próprias informações.

Ao fazer upload de um novo objeto ou copiar um objeto existente, ou seja, você pode especificar a utilização de criptografia do lado do servidor com chaves do AWS KMS para criptografar seus dados. Para fazer isso, use o comando `put-bucket-encryption` para definir a configuração de criptografia padrão do bucket de diretório como SSE-KMS (`aws:kms`). Especificamente, adicione o cabeçalho `--server-side-encryption aws:kms` à solicitação. Use `--ssekms-key-id` *`example-key-id`* para adicionar a chave do AWS KMS gerenciada pelo cliente que você criou. Se você especificar `--server-side-encryption aws:kms`, deverá fornecer um ID da chave do AWS KMS gerenciada pelo cliente. Os buckets de diretório não usam uma chave gerenciada pela AWS. Para obter um exemplo de comando, consulte Como usar o AWS CLI.

Desse modo, quando você faz upload de um novo objeto com o comando a seguir, o Amazon S3 usa as configurações do bucket para criptografia padrão para criptografar o objeto por padrão.

```
aws s3api put-object --bucket bucket-base-name--zone-id--x-s3 --key example-object-key
 --body filepath
```

Não é necessário adicionar `-\-bucket-key-enabled` explicitamente em comandos de operações de API de endpoint de zona. As chaves de bucket do S3 estão sempre habilitadas para operações `GET` e `PUT` em um bucket de diretório e não podem ser desabilitadas. Não são aceitas chaves de bucket do S3 quando você copia objetos criptografados por SSE-KMS de buckets de uso geral para buckets de diretório, de buckets de diretório para buckets de uso geral ou entre buckets de diretório, por meio de CopyObject, de UploadPartCopy, da operação Copy em Operações em Lote ou de trabalhos de import. Nesse caso, o Amazon S3 faz uma chamada para o AWS KMS sempre que uma solicitação de cópia é feita para um objeto criptografado pelo KMS.

É possível copiar um objeto de um bucket de origem (por exemplo, um bucket de uso geral) em um novo bucket (por exemplo, um bucket de diretório) e usar a criptografia SSE-KMS para os objetos de destino. Para isso, use o comando `put-bucket-encryption` para definir a configuração de criptografia padrão do bucket de destino (por exemplo, um bucket de diretório) como SSE-KMS (`aws:kms`). Para obter um exemplo de comando, consulte Como usar o AWS CLI. Desse modo, quando você copia um objeto com o comando a seguir, o Amazon S3 usa as configurações do bucket para criptografia padrão para criptografar o objeto por padrão.

```
aws s3api copy-object --copy-source amzn-s3-demo-bucket/example-object-key --
bucket bucket-base-name--zone-id--x-s3 --key example-object-key
```

Uso dos SDKs da AWS

Ao usar AWS SDKs, é possível solicitar que o Amazon S3 use AWS KMS keys para criptografia do lado do servidor. Os exemplos a seguir mostram como usar a SSE-KMS com os AWS SDKs para Java e .NET. Para obter informações sobre outros SDKs, consulte Código de exemplo e bibliotecas no Centro do desenvolvedor da AWS.

> **Note**
>
> Ao usar os SDKs da AWS para `CreateSession`, o token da sessão é atualizado automaticamente para evitar interrupções no serviço quando uma sessão expira. A substituição dos valores de configuração de criptografia não é aceita para a solicitação `CreateSession`. Além disso, nas chamadas de API de endpoint de zona (exceto CopyObject e UploadPartCopy), não é possível substituir os valores de configuração de criptografia da solicitação `CreateSession`.

Para criptografar novos objetos em um bucket de diretório com SSE-KMS, é necessário especificar SSE-KMS como a configuração de criptografia padrão do bucket de diretório com uma chave do KMS (especificamente, uma chave gerenciada pelo cliente). Dessa forma, quando uma sessão é criada para operações de API de endpoint de zona, novos objetos são automaticamente criptografados e descriptografados com chaves de SSE-KMS e de bucket do S3 durante a sessão.
Para ter mais informações sobre o uso de SDKs da AWS para definir a configuração de criptografia padrão de um bucket de diretório como SSE-KMS, consulte Uso dos SDKs da AWS.

Important

Ao usar uma AWS KMS key para criptografia no lado do servidor no Amazon S3, você deve escolher uma chave de criptografia do KMS simétrica. O Amazon S3 só é compatível com chaves do KMS de criptografia simétrica. Para obter mais informações sobre essas chaves, consulte Chaves do KMS de criptografia simétrica no Guia do desenvolvedor do AWS Key Management Service.

Para obter mais informações sobre como criar chaves gerenciadas pelo cliente, consulte Programação da API do AWS KMS no Guia do desenvolvedor do AWS Key Management Service.

Criptografia em trânsito

Os buckets de diretório usam endpoints de API regionais e zonais. Dependendo da operação de API do Amazon S3 usada, será necessário um endpoint regional ou zonal. Você pode acessar endpoints zonais e regionais por meio de um endpoint de nuvem privada virtual (VPC) do gateway. Não há cobrança adicional pelo uso de endpoints do gateway. Para saber mais sobre os endpoints de API regionais e zonais, consulte Rede para buckets de diretório.

Exclusão de dados

Você pode excluir um ou mais objetos diretamente dos buckets de diretório usando o console do Amazon S3, os AWS SDKs, a AWS Command Line Interface (AWS CLI) ou a API REST do Amazon S3. Como todos os objetos nos buckets de diretório incorrem em custos de armazenamento, recomendamos que você exclua os objetos de que não precisa mais.

A exclusão de um objeto armazenado em um bucket de diretório também exclui recursivamente todos os diretórios pai, desde que esses diretórios pai não contenham nenhum objeto além do objeto que está sendo excluído.

> **Note**
>
> A exclusão de autenticação multifator (MFA) e a funcionalidade Versionamento do S3 não são compatíveis com a classe S3 Express One Zone.

Autenticar e autorizar solicitações

Por padrão, os buckets de diretório são privados e só podem ser acessados por usuários que tenham recebido acesso explícito. O limite de controle de acesso para buckets de diretório é definido somente no nível do bucket. Por outro lado, o limite de controle de acesso para buckets de uso geral pode ser definido no nível do bucket, do prefixo ou da etiqueta de objeto. Essa diferença significa que os buckets de diretório são o único recurso que você pode incluir nas políticas de bucket ou nas políticas de identidade do IAM para acesso à classe S3 Express One Zone.

A classe Amazon S3 Express One Zone oferece suporte à autorização do AWS Identity and Access Management (AWS IAM) e à autorização baseada em sessão:

- Para usar as operações de API do endpoint regional (operações em nível de bucket ou ambiente de gerenciamento) com a classe S3 Express One Zone, use o modelo de autorização do IAM, que não envolve gerenciamento de sessões. As permissões são concedidas individualmente para as ações. Para obter mais informações, consulte Autorizar operações de API de endpoint regional com o IAM.
- Para usar as operações da API do endpoint zonal (operações em nível de objeto ou plano de dados), exceto `CopyObject` e `HeadBucket`, é possível usar a operação de API `CreateSession` para criar e gerenciar sessões otimizadas para autorização de solicitações de dados com baixa latência. Para recuperar e usar um token de sessão, você deve permitir a ação `s3express:CreateSession` para o bucket de diretório em uma política baseada em identidade ou em uma política de bucket. Para obter mais informações, consulte Autorizar operações de API de endpoint regional com o IAM. Se você acessar a classe S3 Express One Zone pelo console do Amazon S3, pela AWS Command Line Interface (AWS CLI) ou usando os AWS SDKs, a classe S3 Express One Zone criará uma sessão em seu nome.

Com a operação de API `CreateSession`, é possível autenticar e autorizar solicitações por meio de um novo mecanismo com base em sessão. Você pode usar `CreateSession` para solicitar credenciais temporárias que forneçam acesso de baixa latência ao bucket. Essas credenciais temporárias têm como escopo um bucket de diretório específico.

Para trabalhar com `CreateSession`, recomendamos usar a versão mais recente dos AWS SDKs ou usar a AWS Command Line Interface (AWS CLI). Os AWS SDKs compatíveis e a AWS CLI lidam com o estabelecimento, a atualização e o encerramento de sessões em seu nome.

Use tokens de sessão somente com operações zonais (nível de objeto) (exceto para `CopyObject` e `HeadBucket`) para distribuir a latência associada à autorização em várias solicitações em uma sessão. Para as operações de API do endpoint regional (operações em nível de bucket), use a autorização do IAM, que não envolve o gerenciamento de uma sessão. Para obter mais informações, consulte Autorizar operações de API de endpoint regional com o IAM e Autorizar operações de API de endpoint zonal com `CreateSession`.

Como as operações de API são autenticadas e autorizadas

A tabela a seguir lista as informações de autenticação e autorização para operações de API do bucket de diretório. Para cada operação de API, a tabela mostra o nome da operação de API, a ação da política do IAM, o tipo de endpoint (regional ou zonal) e o mecanismo de autorização (IAM ou baseada em sessão). Essa tabela também indica se o acesso entre contas é compatível. O acesso às ações no nível do bucket só pode ser concedido em políticas baseadas em identidade do IAM (usuário ou perfil), não em políticas de bucket.

API	Tipo de endpoint	Ação do IAM	Acesso entre contas
`CreateBucket`	Regional	`s3express:CreateBucket`	Não
`DeleteBucket`	Regional	`s3express:DeleteBucket`	Não
`ListDirectoryBuckets`	Regional	`s3express:ListAllMyDirectoryBuckets`	Não
`PutBucketPolicy`	Regional	`s3express:PutBucketPolicy`	Não

API	Tipo de endpoint	Ação do IAM	Acesso entre contas
GetBucketPolicy	Regional	s3express:GetBucketPolicy	Não
DeleteBucketPolicy	Regional	s3express:DeleteBucketPolicy	Não
CreateSession	Zonal	s3express:CreateSession	Sim
CopyObject	Zonal	s3express:CreateSession	Sim
DeleteObject	Zonal	s3express:CreateSession	Sim
DeleteObjects	Zonal	s3express:CreateSession	Sim
HeadObject	Zonal	s3express:CreateSession	Sim
PutObject	Zonal	s3express:CreateSession	Sim
RenameObject	Zonal	s3express:CreateSession	Não
GetObjectAttributes	Zonal	s3express:CreateSession	Sim
ListObjectsV2	Zonal	s3express:CreateSession	Sim
HeadBucket	Zonal	s3express:CreateSession	Sim
CreateMultipartUpload	Zonal	s3express:CreateSession	Sim
UploadPart	Zonal	s3express:CreateSession	Sim
UploadPartCopy	Zonal	s3express:CreateSession	Sim

API	Tipo de endpoint	Ação do IAM	Acesso entre contas
CompleteMultipartUpload	Zonal	s3express:CreateSession	Sim
AbortMultipartUpload	Zonal	s3express:CreateSession	Sim
ListParts	Zonal	s3express:CreateSession	Sim
ListMultipartUploads	Zonal	s3express:CreateSession	Sim
ListAccessPointsForDirectoryBuckets	Zonal	s3express:ListAccessPointsForDirectoryBuckets	Sim
GetAccessPointScope	Zonal	s3express:GetAccessPointScope	Sim
PutAccessPointScope	Zonal	s3express:PutAccessPointScope	Sim
DeleteAccessPointScope	Zonal	s3express:DeleteAccessPointScope	Sim

Tópicos

- Autorizar operações de API de endpoint regional com o IAM
- Autorizar operações de API de endpoint zonal com CreateSession

Autorizar operações de API de endpoint regional com o IAM

O AWS Identity and Access Management (IAM) é um AWS service (Serviço da AWS) que ajuda os administradores a controlar o acesso aos recursos da AWS de forma segura. Os administradores do IAM controlam quem pode se autenticar (se conectar) e ter autorização (permissões) para utilizar os recursos em buckets de diretório e operações do S3 Express One Zone. Você pode usar o IAM sem custo adicional.

Por padrão, os usuários não têm permissões para os buckets de diretório. Para conceder permissões de acesso a buckets de diretório, você pode usar o IAM para criar usuários ou perfis e anexar permissões a essas identidades. Para obter mais informações sobre o IAM, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.

Para fornecer acesso, você pode adicionar permissões aos usuários, grupos ou perfis das seguintes formas:

- Usuários e grupos no AWS IAM Identity Center: crie um conjunto de permissões. Siga as instruções em Criação de um conjunto de permissões no Guia do usuário do AWS IAM Identity Center.
- Usuários gerenciados no IAM por meio de um provedor de identidades: crie um perfil para federação de identidades. Siga as instruções em Criando um perfil para um provedor de identidades de terceiros (federação) no Guia do Usuário do IAM.
- Perfis e usuários do IAM: crie um perfil que o usuário possa assumir. Siga as instruções em Criação de uma função para delegar permissões a um usuário do IAM no Guia do usuário do IAM.

Para obter mais informações sobre o IAM para a classe S3 Express One Zone, consulte os tópicos a seguir.

Tópicos

- Entidades principais
- Recursos
- Ações para buckets de diretório
- Políticas baseadas em identidade do IAM para buckets de diretório
- Exemplos de políticas para buckets de diretório

Entidades principais

Ao criar uma política baseada em recurso para conceder acesso aos buckets, você deve usar o elemento `Principal` para especificar a pessoa ou a aplicação que pode fazer uma solicitação de uma ação ou operação no respectivo recurso. Para políticas de bucket de diretório, você pode usar as seguintes entidades principais:

- Uma conta da AWS
- Um usuário do IAM
- Um perfil do IAM
- Um usuário federado

Para obter mais informações, consultePrincipal no Guia do usuário do IAM.

Recursos

Os nomes de recurso da Amazon (ARNs) para buckets de diretório contêm o namespace `s3express`, a Região da AWS, o ID da conta da AWS e o nome do bucket de diretório, que inclui o ID da zona da AWS (um ID de zona de disponibilidade ou de zona local).

Para acessar e executar ações no bucket de diretório, você deve usar o seguinte formato de ARN:

```
arn:aws:s3express:region:account-id:bucket/base-bucket-name--zone-id--x-s3
```

Para acessar e executar ações no ponto de acesso para um bucket de diretório, você deve usar o seguinte formato de ARN:

```
arn:aws::s3express:region:account-id:accesspoint/accesspoint-basename--zone-id--xa-s3
```

Para obter mais informações sobre os ARNs, consulte Amazon Resource Names (ARNs) no Guia do usuário do IAM. Para obter mais informações sobre os recursos, consulte Elementos de política JSON do IAM: Resource no Guia do usuário do IAM.

Ações para buckets de diretório

Em uma política baseada em identidade ou recurso do IAM, defina quais ações do S3 serão permitidas ou negadas. As ações correspondem a operações de API específicas. Com buckets de

diretório, você deve usar o namespace do S3 Express One Zone, denominado `s3express`, para conceder permissões.

Quando você concede a permissão `s3express:CreateSession`, a operação de API `CreateSession` recupera um token de sessão temporário para todas as operações de API de endpoint zonal (em nível de objeto). O token de sessão retorna credenciais que são usadas para todas as outras operações de API de endpoint zonal. Por isso, você não concede permissões de acesso a operações de API zonais usando políticas do IAM. Em vez disso, `CreateSession` permite o acesso a todas as operações em nível de objeto. Consulte a lista de operações e permissões de API de endpoint zonal em Autenticar e autorizar solicitações.

Para saber mais sobre a operação de API `CreateSession`, consulte a CreateSession na Referência da API do Amazon Simple Storage Service.

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Ao usar uma ação em uma política, você geralmente permite ou nega acesso à operação de API com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação de API. O acesso às ações no nível do bucket só pode ser concedido em políticas baseadas em identidade do IAM (usuário ou perfil), não em políticas de bucket.

Consulte mais informações sobre como configurar políticas de ponto de acesso em Configurar políticas do IAM para usar pontos de acesso para buckets de diretório.

Para ter mais informações, consulte Actions, resources, and condition keys for Amazon S3 Express.

Políticas baseadas em identidade do IAM para buckets de diretório

Antes de criar buckets de diretório, você deve conceder as permissões necessárias aos usuários ou perfis do AWS Identity and Access Management (IAM). Esse exemplo de política permite acesso à operação de API `CreateSession` (para uso com as operações de API do endpoint zonal [nível de objeto]) e a todas as operações de API do endpoint regional (nível de bucket). Essa política permite que a operação de API `CreateSession` seja usada com todos os buckets de diretório, mas as operações de API de endpoint regional só são permitidas para uso com o bucket de diretório especificado. Para usar esse exemplo de política, substitua os *`user input placeholders`* por suas próprias informações.

```
{
     "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Sid": "AllowAccessRegionalEndpointAPIs",
            "Effect": "Allow",
            "Action": [
                "s3express:DeleteBucket",
                "s3express:DeleteBucketPolicy",
                "s3express:CreateBucket",
                "s3express:PutBucketPolicy",
                "s3express:GetBucketPolicy",
                "s3express:ListAllMyDirectoryBuckets"
            ],

            "Resource": "arn:aws:s3express:region:account_id:bucket/bucket-base-
name--zone-id--x-s3/*"
        },
        {
            "Sid": "AllowCreateSession",
            "Effect": "Allow",
            "Action": "s3express:CreateSession",
            "Resource": "*"
        }
    ]
}
```

Exemplos de políticas para buckets de diretório

Esta seção fornece exemplos de políticas de bucket de diretório. Para usar essas políticas, substitua os *user input placeholders* por suas próprias informações.

O exemplo de política de bucket a seguir permite que o ID de Conta da AWS *111122223333* use a operação de API `CreateSession` com a sessão padrão `ReadWrite` para o bucket de diretório especificado. Essa política concede acesso às operações de API de endpoint zonal (nível de objeto).

Example : política de bucket para permitir chamadas de **`CreateSession`** com a sessão padrão **`ReadWrite`**

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReadWriteAccess",
```

```
            "Effect": "Allow",
            "Resource": "arn:aws:s3express:us-west-2:account-id:bucket/bucket-base-name--zone-id--x-s3",
            "Principal": {
                "AWS": [
                    "111122223333"
                ]
            },
            "Action": [
                "s3express:CreateSession"
            ]
        }
    ]
}
```

Example : política de bucket para permitir chamadas de **`CreateSession`** com uma sessão **`ReadOnly`**

O exemplo de política de bucket a seguir permite que o ID de Conta da AWS *111122223333* use a operação de API `CreateSession`. Essa política usa a chave de condição `s3express:SessionMode` com o valor `ReadOnly` para definir uma sessão somente leitura.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReadOnlyAccess",
            "Effect": "Allow",
            "Principal": {
                "AWS": "111122223333"
            },
            "Action": "s3express:CreateSession",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "s3express:SessionMode": "ReadOnly"
                }
            }
        }
    ]
}
```

Example : política de bucket para permitir o acesso entre contas para chamadas de **`CreateSession`**

O exemplo de política de bucket a seguir permite que o ID de Conta da AWS *111122223333* use a operação de API `CreateSession` para o bucket de diretório especificado que pertence ao ID de Conta da AWS *444455556666*.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CrossAccount",
            "Effect": "Allow",
            "Principal": {
                "AWS": "111122223333"
            },
            "Action": [
                "s3express:CreateSession"
            ],
            "Resource": "arn:aws:s3express:us-west-2:444455556666:bucket/bucket-base-name--zone-id--x-s3"

        }
    ]
}
```

Autorizar operações de API de endpoint zonal com **`CreateSession`**

Para usar as operações da API do endpoint zonal (operações em nível de objeto ou plano de dados), exceto `CopyObject` e `HeadBucket`, é possível usar a operação de API `CreateSession` para criar e gerenciar sessões otimizadas para autorização de solicitações de dados com baixa latência. Para recuperar e usar um token de sessão, você deve permitir a ação `s3express:CreateSession` para o bucket de diretório em uma política baseada em identidade ou em uma política de bucket. Para obter mais informações, consulte Autorizar operações de API de endpoint regional com o IAM. Se você acessar a classe S3 Express One Zone pelo console do Amazon S3, pela AWS Command Line Interface (AWS CLI) ou usando os AWS SDKs, a classe S3 Express One Zone criará uma sessão em seu nome.

Se você usar a API REST do Amazon S3, poderá usar a operação de API `CreateSession` para obter credenciais de segurança temporárias que incluem um ID de chave de acesso, uma chave de acesso secreta, um token de sessão e um prazo de expiração. As credenciais temporárias fornecem as mesmas permissões que as credenciais de segurança de longo prazo, como as credenciais de usuário do IAM, mas as credenciais de segurança temporárias precisam incluir um token de sessão.

Modo de sessão

O modo de sessão define o escopo da sessão. Na política de bucket, você pode especificar a chave de condição `s3express:SessionMode` para controlar quem pode criar uma sessão de `ReadWrite` ou `ReadOnly`. Para obter mais informações sobre sessões de `ReadWrite` ou `ReadOnly`, consulte o parâmetro `x-amz-create-session-mode` para CreateSession na Referência da API do Amazon S3. Para obter mais informações sobre a política de bucket que deve ser criada, consulte Exemplos de políticas para buckets de diretório.

Token de sessão

Ao fazer uma chamada usando credenciais de segurança temporárias, ela deve incluir um token de sessão. O token de sessão é retornado junto com as credenciais temporárias. Um token de sessão tem como escopo o bucket de diretório e é usado para verificar se as credenciais de segurança são válidas e não expiraram. Para proteger as sessões, as credenciais de segurança temporárias expiram após 5 minutos.

`CopyObject` e `HeadBucket`

As credenciais de segurança temporárias têm como escopo um bucket de diretório específico e são habilitadas automaticamente para todas as chamadas de API de operação zonal (nível de objeto) para determinado bucket de diretório. Ao contrário de outras operações de API de endpoint zonal, `CopyObject` e `HeadBucket` não usam a autenticação de `CreateSession`. Todas as solicitações `CopyObject` e `HeadBucket` devem ser autenticadas e assinadas usando credenciais do IAM. No entanto, `CopyObject` e `HeadBucket` ainda são autorizados por `s3express:CreateSession`, como outras operações de API de endpoint zonal.

Para obter mais informações, consulte CreateSession na Referência da API do Amazon Simple Storage Service.

Práticas recomendadas de segurança para buckets de diretório

Há uma série de recursos de segurança a serem considerados ao trabalhar com buckets de diretório. As melhores práticas a seguir são diretrizes gerais e não representam uma solução completa de

segurança. Como essas práticas recomendadas podem não ser adequadas ou suficientes para o seu ambiente, trate-as como recomendações úteis em vez de requisitos.

Configurações padrão das funcionalidades Bloqueio de Acesso Público e Propriedade de Objetos

Os buckets de diretório oferecem suporte às funcionalidades Bloqueio de Acesso Público do S3 e Propriedade de Objetos do S3. Esses recursos do S3 são usados para auditoria e gerenciamento de acesso aos buckets e objetos.

Por padrão, todas as configurações da funcionalidade Bloqueio de Acesso Público são habilitadas para buckets de diretório. Além disso, a funcionalidade Propriedade de Objetos está definida como Imposto pelo proprietário do bucket, o que significa que as listas de controle de acesso (ACLs) estão desabilitadas. Essas configurações não podem ser modificadas. Para obter mais informações sobre esses recursos, consulte the section called “Bloquear o acesso público” e the section called “Controlar a propriedade do objeto”.

> **Note**
>
> Você não pode conceder acesso a objetos armazenados em buckets de diretório. Você pode conceder acesso somente aos seus buckets de diretório. O modelo de autorização para a classe S3 Express One Zone é diferente do modelo de autorização para o Amazon S3. Para obter mais informações, consulte Autorizar operações de API de endpoint zonal com `CreateSession`.

Autenticação e autorização

Os mecanismos de autenticação e autorização para buckets de diretório diferem, conforme você faz solicitações a operações de API de endpoint zonal ou operações de API de endpoint regional. As operações de API zonais são operações em nível de objeto (plano de dados). As operações de API regionais são operações em nível de bucket (ambiente de gerenciamento).

Você autentica e autoriza solicitações para as operações de API de endpoint zonal por meio de um novo mecanismo baseado em sessão que é otimizado para fornecer a menor latência. Com a autenticação baseada em sessão, os SDKs da AWS usam a operação de API `CreateSession` para solicitar credenciais temporárias que fornecem acesso de baixa latência ao bucket de diretório. Essas credenciais temporárias têm como escopo um bucket de diretório específico e expiram depois

de 5 minutos. Você pode usar essas credenciais temporárias para assinar chamadas de API zonais (nível de objeto). Para obter mais informações, consulte Autorizar operações de API de endpoint zonal com `CreateSession`.

Assinar solicitações com credenciais para gerenciamento de buckets de diretório

Use credenciais da classe para assinar solicitações de API de endpoint zonal (nível do objeto) com o AWS Signature Version 4, usando `s3express` como nome de serviço. Ao assinar as solicitações, use a chave secreta retornada por `CreateSession` e também forneça o token de sessão com `x-amzn-s3session-token header`. Para obter mais informações, consulte CreateSession.

Os AWS SDKs compatíveis gerenciam as credenciais e a assinatura em seu nome. Recomendamos usar os AWS SDKs para atualizar as credenciais e assinar solicitações para você.

Assinar solicitações com credenciais do IAM

Todas as chamadas de API regionais (nível de bucket) devem ser autenticadas e assinadas por credenciais do AWS Identity and Access Management (IAM) em vez de credenciais temporárias de sessão. As credenciais do IAM consistem no ID da chave de acesso e na chave de acesso secreta para as identidades do IAM. Todas as solicitações `CopyObject` e `HeadBucket` também devem ser autenticadas e assinadas usando credenciais do IAM.

Para alcançar a menor latência para as chamadas de operação zonal (nível do objeto), recomendamos usar as credenciais obtidas da chamada de `CreateSession` para assinar as solicitações, exceto para as solicitações de `CopyObject` e `HeadBucket`.

Usar o AWS CloudTrail

O AWS CloudTrail fornece um registro das ações executadas por um usuário, perfil ou AWS service (Serviço da AWS) no Amazon S3. É possível usar as informações coletadas pelo CloudTrail para determinar o seguinte:

- A solicitação feita ao Amazon S3
- O endereço IP do qual a solicitação foi feita.
- Quem fez a solicitação.
- Quando a solicitação foi feita
- Detalhes adicionais sobre a solicitação

Quando você configura a Conta da AWS, os eventos de gerenciamento do CloudTrail são habilitados por padrão. As operações de API de endpoint regional a seguir (operações de API em nível de bucket ou ambiente de gerenciamento) são registradas em log no CloudTrail.

- CreateBucket
- DeleteBucket
- DeleteBucketPolicy
- PutBucketPolicy
- GetBucketPolicy
- ListDirectoryBuckets
- ListMultipartUploads
- PutBucketEncryption
- GetBucketEncryption
- DeleteBucketEncryption

> **Note**
>
> `ListMultipartUploads` é uma operação de API de endpoint zonal. No entanto, ela é registrada no CloudTrail como um evento de gerenciamento. Para obter mais informações, consulte ListMultipartUploads na Referência da API do Amazon Simple Storage Service.

Por padrão, as trilhas do CloudTrail não registram eventos de dados, mas é possível configurar as trilhas para registrar eventos de dados para buckets de diretório especificados, ou para registrar eventos de dados para todos os buckets de diretório na sua conta AWS. As operações de API de endpoint zonal a seguir (operações de API em nível de objeto ou plano de dados) são registradas no CloudTrail.

- AbortMultipartUpload
- CompleteMultipartUpload
- CreateSession
- CopyObject
- CreateMultipartUpload
- DeleteObject

- DeleteObjects
- GetObject
- GetObjectAttributes
- HeadBucket
- HeadObject
- ListObjectsV2
- ListParts
- PutObject
- UploadPart
- UploadPartCopy

Consulte mais informações sobre como usar o AWS CloudTrail com buckets de diretório em Logging with AWS CloudTrail for directory buckets.

Implementar o monitoramento usando as ferramentas de monitoramento da AWS

O monitoramento é uma parte importante para manter a confiabilidade, segurança, disponibilidade e performance do Amazon S3 e suas soluções da AWS. A AWS fornece várias ferramentas e serviços para ajudar a monitorar o Amazon S3 e outros Serviços da AWS. Por exemplo, é possível monitorar métricas do Amazon CloudWatch para o Amazon S3, particularmente as métricas de armazenamento `BucketSizeBytes` e `NumberOfObjects`.

Os objetos armazenados em buckets de diretório não serão refletidos nas métricas de armazenamento `BucketSizeBytes` e `NumberOfObjects` do Amazon S3. No entanto, as métricas de armazenamento `BucketSizeBytes` e `NumberOfObjects` são compatíveis com buckets de diretório. Para ver as métricas de sua escolha, você pode diferenciar entre as classes de armazenamento do Amazon S3 especificando uma dimensão `StorageType`. Para obter mais informações, consulte Monitoramento de métricas com o Amazon CloudWatch.

Para obter mais informações, consulte Monitoramento de métricas com o Amazon CloudWatch e Registrar em log e monitorar no Amazon S3.

Gerenciar o acesso a conjuntos de dados compartilhados em buckets de diretório por meio de pontos de acesso

Os Pontos de Acesso Amazon S3 simplificam o gerenciamento de acesso aos dados em grande escala para conjuntos de dados compartilhados no S3. Pontos de acesso são nomes de host exclusivos que você cria para impor permissões e controles de rede distintos a todas as solicitações feitas por meio de um ponto de acesso. Você pode criar centenas de pontos de acesso por bucket, cada um com um nome distinto e permissões personalizadas para cada aplicação. Cada ponto de acesso funciona em conjunto com a política de bucket anexada ao bucket subjacente.

Em buckets de diretório, um nome de ponto de acesso consiste em um nome base que você fornece, seguido do ID da zona (zona de disponibilidade ou zona local da AWS) em que o bucket de diretório está localizado e de `--xa-s3`. Por exemplo, .*`accesspointname`*`--`*`zoneID`*`--xa-s3` Após a criação do ponto de acesso, não é possível alterar o nome ou o ID da zona.

Com os pontos de acesso para buckets de diretório, é possível usar o escopo do ponto de acesso para restringir o acesso a operações de API ou prefixos específicos. Você pode especificar qualquer quantidade de prefixos, mas a extensão total de caracteres de todos os prefixos não deve ultrapassar 256 bytes.

Você pode configurar qualquer ponto de acesso para aceitar solicitações somente de uma nuvem privada virtual (VPC). Isso restringe o acesso aos dados do Amazon S3 a uma rede privada.

Nesta seção, os tópicos explicam como usar pontos de acesso para buckets de diretório. Para obter informações sobre buckets de diretório, consulte Trabalhar com buckets de diretório.

Tópicos

- Regras de nomenclatura, restrições e limitações dos pontos de acesso para buckets de diretório
- Referência a pontos de acesso para buckets de diretório
- Operações de objeto referentes a pontos de acesso para buckets de diretório
- Configurar políticas do IAM para usar pontos de acesso para buckets de diretório
- Monitorar e registrar em log pontos de acesso para buckets de diretório
- Como criar pontos de acesso para buckets de diretório
- Gerenciar pontos de acesso para buckets de diretório

Regras de nomenclatura, restrições e limitações dos pontos de acesso para buckets de diretório

Os pontos de acesso simplificam o gerenciamento do acesso a dados em escala para conjuntos de dados compartilhados no Amazon S3. Os tópicos a seguir fornecem informações sobre as regras de nomenclatura dos pontos de acesso, bem como as restrições e limitações.

Tópicos

- Regras de nomenclatura dos pontos de acesso para buckets de diretório
- Restrições e limitações referentes a pontos de acesso para buckets de diretório

Regras de nomenclatura dos pontos de acesso para buckets de diretório

O ponto de acesso deve ser criado na mesma zona local em que o bucket está. Um nome de ponto de acesso deve ser exclusivo na zona.

Os nomes de pontos de acesso devem ser compatíveis com DNS e atender às seguintes condições:

- Devem começar com um número ou uma letra minúscula
- O nome base que você fornece deve ter de três a cinquenta caracteres de extensão.
- Não pode começar nem terminar com hífen (`-`)
- Não podem conter sublinhados (_), letras maiúsculas, espaços ou pontos (`.`).
- Deve terminar com o sufixo *`zoneid`*`--xa--s3`.

Restrições e limitações referentes a pontos de acesso para buckets de diretório

Os pontos de acesso para buckets de diretório têm as seguintes restrições e limitações:

- Cada ponto de acesso está associado a um bucket de diretório. Após a criação de um ponto de acesso, não é possível associá-lo a um bucket diferente. No entanto, você pode excluir um ponto de acesso e criar outro com o mesmo nome e associá-lo a um bucket diferente.
- Depois de criar um ponto de acesso, não é possível alterar sua configuração de nuvem privada virtual (VPC).
- As políticas de ponto de acesso estão limitadas a 20 KB.
- Os prefixos do escopo do ponto de acesso são limitados a uma extensão total de 256 bytes.

- É possível criar até 10 mil pontos de acesso por Conta da AWS por Região da AWS. Se você precisar de mais de 10 mil pontos de acesso para uma única conta em uma única região, poderá solicitar um aumento de cota de serviço. Para obter mais informações sobre cotas de serviço e como solicitar um aumento, consulte AWS Service Quotas na Referência geral da AWS.
- Você só pode usar pontos de acesso para executar operações em objetos. Não é possível usar pontos de acesso para executar operações de bucket do Amazon S3, como modificar ou excluir buckets. Para ver uma lista completa das operações permitidas, consulte Operações de objeto referentes a pontos de acesso para buckets de diretório.
- Você pode se referir aos pontos de acesso pelo nome, pelo alias do ponto de acesso ou pelo URI no estilo de hospedagem virtual. Não é possível endereçar pontos de acesso pelo ARN. Para obter mais informações, consulte Referência a pontos de acesso para buckets de diretório.
- As operações de API que controlam a funcionalidade de ponto de acesso (por exemplo, `PutAccessPointPolicy` e `GetAccessPointPolicy`) devem especificar a conta da AWS à qual o ponto de acesso pertence.
- É necessário usar o AWS Signature Version 4 ao fazer solicitações a um ponto de acesso usando a API REST. Para obter mais informações sobre como autenticar solicitações, consulte Autenticação de solicitações (AWS Signature Version 4) na Referência de APIs do Amazon Simple Storage Service.
- Os pontos de acesso permitem solicitações apenas por HTTPS. O Amazon S3 responderá automaticamente com um redirecionamento HTTP em todas as solicitações feitas por HTTP a fim de atualizar a solicitação para HTTPS.
- Os pontos de acesso não oferecem suporte ao acesso anônimo.
- Se você criar um ponto de acesso para um bucket pertencente a outra conta (um ponto de acesso entre contas), o ponto de acesso entre contas não concederá acesso aos dados enquanto o proprietário do bucket não conceder permissão para acessar o bucket. O proprietário do bucket sempre mantém o controle total sobre o acesso aos dados e deve atualizar a política do bucket para autorizar solicitações do ponto de acesso entre contas. Para ver um exemplo de política de bucket, consulte Configurar políticas do IAM para usar pontos de acesso para buckets de diretório.

Referência a pontos de acesso para buckets de diretório

Depois de criar um ponto de acesso, você pode usá-lo como um endpoint para realizar operações de objeto. Com relação a pontos de acesso para buckets de diretório, o alias do ponto de acesso é igual ao nome do ponto de acesso. Você pode usar o nome do ponto de acesso em vez do nome do

bucket para todas as operações de dados. Para obter uma lista das operações compatíveis, consulte Operações de objeto referentes a pontos de acesso para buckets de diretório.

Referência a pontos de acesso por meio de URIs no estilo de hospedagem virtual

Os pontos de acesso são compatíveis apenas com o endereçamento em estilo de host virtual. Os pontos de acesso usam o mesmo formato dos endpoints de bucket de diretório. Para obter mais informações, consulte Endpoints regionais e zonais para buckets de diretório.

Os Pontos de Acesso S3 não comportam acesso por HTTP. Eles comportam apenas o acesso seguro por HTTPS.

Operações de objeto referentes a pontos de acesso para buckets de diretório

Você pode usar pontos de acesso para acessar um objeto usando as operações de dados do S3 a seguir.

- AbortMultipartUpload
- CompleteMultipartUpload
- CopyObject
- CreateMultipartUpload
- CreateSession
- DeleteObject
- DeleteObjects
- GetObject
- GetObjectAttributes
- HeadBucket
- HeadObject
- ListMultipartUploads
- ListObjectsV2
- ListParts
- PutObject
- UploadPart

- UploadPartCopy

Configurar políticas do IAM para usar pontos de acesso para buckets de diretório

Os pontos de acesso comportam políticas de recursos do AWS Identity and Access Management (IAM) que permitem controlar o uso do ponto de acesso por recurso, usuário ou outras condições. Para que uma aplicação ou usuário acesse objetos por meio de um ponto de acesso, tanto o ponto de acesso quanto o a política do bucket subjacente devem permitir a solicitação.

> **Important**
>
> Adicionar um ponto de acesso a um bucket não altera o comportamento do bucket quando ele é acessado diretamente pelo nome do bucket. Todas as operações existentes no bucket continuarão a funcionar como antes. As restrições que você incluir em uma política de ponto de acesso ou em um escopo de ponto de acesso se aplicam somente a solicitações feitas por meio desse ponto de acesso.

Ao usar políticas de recursos do IAM, solucione avisos de segurança, erros, avisos gerais e sugestões do AWS Identity and Access Management Access Analyzer antes de salvar a política. O IAM Access Analyzer executa verificações de política para validar sua política em relação à gramática das políticas e às práticas recomendadas do IAM. Essas verificações geram descobertas e fornecem recomendações que ajudam a criar políticas que sejam funcionais e estejam em conformidade com as práticas recomendadas de segurança.

Para saber mais sobre a validação de políticas usando o IAM Access Analyzer, consulte Validação de políticas do IAM Access Analyzer no Guia do usuário do IAM. Para visualizar uma lista de avisos, erros e sugestões retornados pelo IAM Access Analyzer, consulte Referência de verificação de políticas do IAM Access Analyzer.

Exemplos de política de ponto de acesso para buckets de diretório

As políticas de ponto de acesso a seguir demonstram como controlar as solicitações um bucket de diretório. As políticas de ponto de acesso exigem ARNs de bucket ou ARNs de ponto de acesso. Não é possível usar aliases de ponto de acesso nas políticas. Abaixo é apresentado um exemplo de ARN de ponto de acesso:

```
arn:aws:s3express:region:account-id:accesspoint/myaccesspoint--zoneID--xa-s3
```

Você pode visualizar o ARN do ponto de acesso nos detalhes do ponto de acesso. Para obter mais informações, consulte Visualizar detalhes dos pontos de acesso para buckets de diretório.

> **Note**
>
> As permissões concedidas em uma política de ponto de acesso entram em vigor somente se o bucket subjacente também permitir o mesmo acesso. É possível fazer isso de duas maneiras:
>
> 1. (Recomendado) Delegue o controle de acesso do bucket para o ponto de acesso conforme descrito em Delegar controle de acesso a pontos de acesso.
> 2. Adicione as mesmas permissões contidas na política de ponto de acesso à política do bucket subjacente.

Example 1: política de controle de serviços para limitar os pontos de acesso a origens de rede de VPC

A política de controle de serviços a seguir requer que todos os novos pontos de acesso sejam criados com uma origem de rede de nuvem privada virtual (VPC). Com essa política em vigor, os usuários da sua organização não podem criar nenhum ponto de acesso acessível pela internet.

```
{
    "Version": "2012-10-17",
    "Statement": [
    {
        "Effect": "Deny",
        "Action": "s3express:CreateAccessPoint",
        "Resource": "*",
        "Condition": {
            "StringNotEquals": {
                "s3express:AccessPointNetworkOrigin": "VPC"
            }
        }
    }
  ]
```

```
}
```

Example 2: política de ponto de acesso para limitar o acesso ao bucket por pontos de acesso com uma origem de rede da VPC

A política de ponto de acesso a seguir limita todo o acesso ao bucket *amzn-s3-demo-bucket--zoneID--x-s3* por um ponto de acesso com uma origem de rede da VPC.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Principal": "*",
            "Action": "s3express:CreateSession",
            "Effect": "Deny",
            "Resource": "arn:aws:s3express:region:111122223333:bucket/amzn-s3-demo-
bucket--zoneID--x-s3",
            "Condition": {
                "StringNotEqualsIfExists": {
                    "s3express:AccessPointNetworkOrigin": "VPC"
                }
            }
        }
    ]
}
```

Chaves de condição

Os pontos de acesso para buckets de diretório têm chaves de condição que podem ser usadas em políticas do IAM para controlar o acesso aos recursos. As chaves de condição a seguir representam somente parte de uma política do IAM. Para obter exemplos de políticas completas, consulte Exemplos de política de ponto de acesso para buckets de diretório, Delegar controle de acesso a pontos de acesso e Conceder permissões para pontos de acesso entre contas.

`s3express:DataAccessPointArn`

Este exemplo mostra como filtrar o acesso pelo nome do recurso da Amazon (ARN) de um ponto de acesso e faz a correspondência com todos os pontos de acesso referentes à Conta da AWS *111122223333* na região *region*:

```
"Condition" : {
```

```
    "StringLike": {
        "s3express:DataAccessPointArn":
 "arn:aws:s3express:region:111122223333:accesspoint/*"
    }
}
```

s3express:DataAccessPointAccount

Este exemplo mostra um operador de string que você pode utilizar para estabelecer correspondência com o ID da conta do proprietário de um ponto de acesso. O exemplo a seguir estabelece correspondência com todos os pontos de acesso pertencentes à Conta da AWS *111122223333*.

```
"Condition" : {
    "StringEquals": {
        "s3express:DataAccessPointAccount": "111122223333"
    }
}
```

s3express:AccessPointNetworkOrigin

Este exemplo mostra um operador de string que você pode utilizar para estabelecer correspondência com a origem da rede, `Internet` ou VPC. O exemplo a seguir corresponde apenas a pontos de acesso com uma origem de VPC.

```
"Condition" : {
    "StringEquals": {
        "s3express:AccessPointNetworkOrigin": "VPC"
    }
}
```

s3express:Permissions

Você pode usar `s3express:Permissions` para restringir o acesso a operações de API no escopo do ponto de acesso. As seguintes operações de API são compatíveis:

- `PutObject`
- `GetObject`
- `DeleteObject`
- `ListBucket` (obrigatório para `ListObjectsV2`)

- `GetObjectAttributes`
- `AbortMultipartUpload`
- `ListBucketMultipartUploads`
- `ListMultipartUploadParts`

> **Note**
>
> Ao utilizar chaves de condição de vários valores, recomendamos que você use `ForAllValues` com instruções `Allow` e `ForAnyValue` com instruções `Deny`. Para obter mais informações, consulte Chaves de contexto de múltiplos valores no “Guia do usuário do IAM”.

Consulte mais informações sobre como usar chaves de condição com o Amazon S3 em Actions, resources, and condition keys for Amazon S3 na Referência de autorização do serviço.

Para ter mais informações sobre as permissões para operações de API do S3 de acordo com os tipos de recurso do S3, consulte Permissões obrigatórias para operações de API do Amazon S3.

Delegar controle de acesso a pontos de acesso

É possível delegar o controle de acesso da política de bucket à política de ponto de acesso. O exemplo de política de bucket a seguir permite acesso total a todos os pontos de acesso pertencentes à conta do proprietário do bucket. Após a aplicação da política, todo acesso a esse bucket é controlado por políticas de ponto de acesso. Recomendamos configurar seus buckets dessa maneira para todos os casos de uso que não exigem acesso direto ao bucket.

Example política de bucket que delega controle de acesso a pontos de acesso

```
{
    "Version": "2012-10-17",
    "Statement" : [
    {
        "Effect": "Allow",
        "Principal" : { "AWS": "*" },
        "Action" : "*",
        "Resource" : [ "Bucket ARN",
        "Condition": {
            "StringEquals" : { "s3express:DataAccessPointAccount" : "Bucket owner's
 account ID" }
```

```
        }
    }]
}
```

Conceder permissões para pontos de acesso entre contas

Para criar um ponto de acesso para um bucket pertencente a outra conta, primeiro você deve criar o ponto de acesso especificando o nome do bucket e o ID do proprietário da conta. Depois, o proprietário do bucket deve atualizar a política do bucket para autorizar solicitações do ponto de acesso. Criar um ponto de acesso é semelhante à criação de um DNS CNAME, pois o ponto de acesso não fornece acesso ao conteúdo do bucket. Todo acesso ao bucket é controlado pela política de bucket. O exemplo de política de bucket a seguir permite solicitações `GET` e `LIST` no bucket de um ponto de acesso pertencente a uma Conta da AWS confiável.

Substitua *`Bucket ARN`* pelo ARN do bucket.

Example de política de bucket que delega permissões a outra Conta da AWS

```
{
    "Version": "2012-10-17",
    "Statement" : [
    {
        "Effect": "Allow",
        "Principal" : { "AWS": "*" },
        "Action" : "s3express:CreateSession",
        "Resource" : [ "Bucket ARN" ],
        "Condition": {
            "StringEquals" : {
                "s3express:DataAccessPointAccount": "Access point owner's account ID"
            },
            "ForAllValues:StringEquals": {
                "s3express:Permissions": [
                    "GetObject",
                    "ListBucket"
                ]
            }
        }
    }]
}
```

Monitorar e registrar em log pontos de acesso para buckets de diretório

Você pode registrar em log as solicitações feitas por meio de pontos de acesso e as solicitações feitas às APIs que gerenciam os pontos de acesso, como `CreateAccessPoint` e `GetAccessPointPolicy`, usando o AWS CloudTrail. As entradas de log do CloudTrail para solicitações feitas por meio de pontos de acesso incluem o ARN (que inclui o nome do ponto de acesso) na seção `resources` do log.

Por exemplo, suponha que você tenha a seguinte configuração:

- Um bucket chamado *`amzn-s3-demo-bucket`*`--`*`zone-id`*`--x-s3` na região `region` que contém o objeto denominado `my-image.jpg`.
- Um ponto de acesso chamado `my-bucket-ap--zoneID--xa-s3` que está associado a *`amzn-s3-demo-bucket`*`--`*`zone-id`*`--x-s3`
- O ID de Conta da AWS `123456789012`

O seguinte exemplo mostra a seção `resources` de uma entrada de log do CloudTrail da configuração anterior:

```
"resources": [
        {"type": "AWS::S3Express::Object",

            "ARN": "arn:aws:s3express-region:123456789012:bucket/amzn-s3-demo-
bucket--zone-id--x-s3/my-image.jpg"
        },
        {"accountId": "c",
            "type": "AWS::S3Express::DirectoryBucket",
            "ARN": "arn:aws::s3express:region:123456789012:bucket/amzn-s3-demo-
bucket--zone-id--x-s3"
        },
        {"accountId": "123456789012",
            "type": "AWS::S3::AccessPoint",
            "ARN": "arn:aws:s3express:region:123456789012:accesspoint/my-bucket-ap--
zoneID--xa-s3"
        }
    ]
```

Para obter mais informações sobre o AWS CloudTrail, consulte O que é AWS CloudTrail? no Guia do Usuário doAWS CloudTrail.

Como criar pontos de acesso para buckets de diretório

Assim como os buckets de diretório, os pontos de acesso podem ser criados em zonas de disponibilidade ou em zonas locais dedicadas. O ponto de acesso deve ser criado na mesma região do bucket de diretório associado a ele.

Um ponto de acesso está associado a exatamente um bucket de diretório do Amazon S3. Se quiser usar um bucket de diretório em sua Conta da AWS, primeiro você deve criar um bucket de diretório. Para ter mais informações sobre como criar buckets de diretório, consulte Criar buckets de diretório em uma zona de disponibilidade ou Criar um bucket de diretório em uma zona local.

Você também pode criar um ponto de acesso entre contas associado a um bucket em outra Conta da AWS, desde que você saiba o nome do bucket e o ID da conta do proprietário do bucket. No entanto, a criação de pontos de acesso entre contas não concederá acesso aos dados no bucket até que você receba as permissões do proprietário do bucket. O proprietário do bucket deve conceder à conta do proprietário do ponto de acesso (sua conta) acesso ao bucket por meio da política do bucket. Para obter mais informações, consulte Conceder permissões para pontos de acesso entre contas.

Você pode criar um ponto de acesso para qualquer bucket de diretório com o AWS Management Console, a AWS CLI, a API REST ou os SDKs da AWS. Cada ponto de acesso é associado a um único bucket de diretório, e você pode criar centenas de pontos de acesso por bucket. Ao criar um ponto de acesso, você escolhe o nome do ponto de acesso e o bucket de diretório ao qual associá-lo. O nome do ponto de acesso consiste em um nome base que você fornece e um sufixo que inclui o ID da zona local em o bucket está localizado, seguido de `--xa-s3`. Por exemplo, *`myaccesspoint`*`-`*`zoneID`*`--xa-s3`. Você também pode restringir o acesso ao ponto de acesso por meio de uma nuvem privada virtual (VPC). Em seguida, você pode começar imediatamente a ler e gravar dados por meio do ponto de acesso usando o respectivo nome, assim como você usa o nome de um bucket de diretório.

É possível usar o escopo do ponto de acesso para restringir o acesso ao bucket de diretório por meio do ponto de acesso a operações de API ou prefixos específicos. Se você não adicionar um escopo ao ponto de acesso, todos os prefixos no bucket de diretório e todas as operações de API poderão ser executados em objetos no bucket quando acessados por meio do ponto de acesso. Depois de criar o ponto de acesso, você pode adicionar, modificar ou excluir o escopo usando a AWS CLI, os SDKs da AWS ou a API REST. Para obter mais informações, consulte Gerenciar o escopo dos pontos de acesso para buckets de diretório.

Depois de criar o ponto de acesso, você pode configurar a política de recursos do IAM do ponto de acesso. Para obter mais informações, consulte Visualizar, editar ou excluir políticas de pontos de acesso.

Usar o console do S3

> **Note**
>
> Você também pode criar um ponto de acesso para um bucket de diretórios na tela de buckets de diretório. Ao fazer isso, o nome do bucket de diretório é fornecido e você não precisa escolher um bucket ao criar o ponto de acesso. Para obter mais informações, consulte Listar buckets de diretório.

Como criar um ponto de acesso para buckets de diretório

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Na barra de navegação na parte superior da página, escolha o nome da Região da AWS exibida no momento. Em seguida, escolha a região na qual você deseja criar um ponto de acesso. O ponto de acesso deve ser criado na mesma região em que o bucket associado.
3. No painel de navegação à esquerda, escolha Buckets de diretório.
4. Na página Access Points (Pontos de acesso), escolha Create access point (Criar ponto de acesso).
5. Você pode criar um ponto de acesso para um bucket de diretório na sua conta ou em outra conta. Para criar um ponto de acesso para um bucket de diretório em outra conta.

   > **Note**
   >
   > Se você estiver usando um bucket em outra Conta da AWS, o proprietário do bucket deverá atualizar a política do bucket para autorizar solicitações do ponto de acesso. Para ver um exemplo de política de bucket, consulte Conceder permissões para pontos de acesso entre contas.

   a. No campo Bucket de diretório, escolha Especifique um bucket em outra conta.

b. No campo ID da conta do proprietário do bucket, insira o ID da Conta da AWS à qual o bucket pertence.

c. No campo Nome do bucket, insira o nome do bucket, incluindo o nome base e o ID da zona. Por exemplo, *.bucket-base-name--zone-id--x-s3*

6. Para criar um ponto de acesso para um bucket de diretório em sua conta:

a. No campo Bucket de diretório, selecione Escolha um bucket nesta conta.

b. No campo Nome do bucket, insira o nome do bucket, incluindo o nome base e o ID da zona. Por exemplo, *.bucket-base-name--zone-id--x-s3* Para escolher o bucket em um alista, selecione Procurar no S3 e escolha o bucket de diretório.

7. Em Nome do ponto de acesso, no campo Nome base, insira o nome do ponto de acesso. O ID da zona e o nome completo do ponto de acesso são exibidos. Para obter mais informações sobre nomenclatura de pontos de acesso, consulte Regras de nomenclatura dos pontos de acesso para buckets de diretório.

8. Em Origem da rede, escolha Nuvem privada virtual (VPC) ou Internet. Se você escolher Nuvem privada virtual (VPC), no campo ID da VPC, insira o ID da VPC que você quer usar com o ponto de acesso.

9. (Opcional) Em Escopo do ponto de acesso, para aplicar um escopo a esse ponto de acesso, escolha Limitar o escopo desse ponto de acesso usando prefixos ou permissões.

a. Para limitar o acesso aos prefixos no bucket de diretório, em Prefixos, insira um ou mais prefixos. Para adicionar outro prefixo, escolha Adicionar prefixo. Para remover um filtro, escolha Remover.

> **Note**
>
> O escopo de um ponto de acesso tem um limite de 512 caracteres no total para todos os prefixos. Você pode ver a quantidade de caracteres restantes abaixo de Adicionar prefixo.

b. Em Permissões, escolha uma ou mais operações de API que o ponto de acesso permitirá. Para remover uma operação de dados, escolha o X ao lado do nome da operação de dados.

10. Para não aplicar um escopo ao ponto de acesso e permitir acesso a todos os prefixos no bucket de diretório e a todas as operações de API por meio do ponto de acesso, em Escopo do ponto de acesso, escolha Aplicar acesso ao bucket inteiro.

11. Escolha Crie um ponto de acesso para o bucket de diretórios. O nome do ponto de acesso e outras informações sobre ele aparecem na lista Pontos de acesso para buckets de diretório.

Como usar o AWS CLI

O exemplo de comando a seguir cria um ponto de acesso chamado *example-ap* para o bucket *amzn-s3-demo-bucket--zone-id--x-s3* na conta *111122223333*.

```
aws s3control create-access-point --name example-ap--zoneID--xa-s3 --account-
id 111122223333 --bucket amzn-s3-demo-bucket--zone-id--x-s3
```

Para restringir o acesso ao ponto de acesso por meio de uma VPC, inclua o parâmetro `--vpc` e o ID da VPC.

```
aws s3control create-access-point --name example-ap--zoneID--xa-s3 --account-
id 111122223333 --bucket amzn-s3-demo-bucket--zone-id--x-s3 --vpc vpc-id
```

Ao criar um ponto de acesso para um bucket entre contas, inclua o parâmetro `--bucket-account-id`. O exemplo de comando a seguir cria um ponto de acesso na Conta da AWS *111122223333* para o bucket *amzn-s3-demo-bucket--zone-id--x-s3*, pertencente à Conta da AWS *444455556666*.

```
aws s3control create-access-point --name example-ap--zoneID--xa-s3 --account-
id 111122223333 --bucket amzn-s3-demo-bucket--zone-id--x-s3 --bucket-account-
id 444455556666
```

Para ter mais informações e exemplos, consulte create-access-point na “Referência de comandos da AWS CLI”.

Uso da API REST

O exemplo de comando a seguir criar um ponto de acesso chamado *example-ap* para o bucket *amzn-s3-demo-bucket--zone-id--x-s3* na *111122223333* e restringe o acesso por meio da VPC *vpc-id* (opcional).

```
PUT /v20180820/accesspoint/example-ap--zoneID--xa-s3 HTTP/1.1
Host: s3express-control.region.amazonaws.com
x-amz-account-id: 111122223333
```

```
<?xml version="1.0" encoding="UTF-8"?>
<CreateAccessPointRequest>
   <Bucket>amzn-s3-demo-bucket--zone-id--x-s3s</Bucket>
   <BucketAccountId>111122223333</BucketAccountId>
   <VpcConfiguration>
       <VpcId>vpc-id</VpcId>
   </VpcConfiguration>
</CreateAccessPointRequest>
```

Resposta:

```
HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<CreateAccessPointResult>
   <AccessPointArn>
       "arn:aws:s3express:region:111122223333:accesspoint/example-ap--zoneID--xa-s3"
   </AccessPointArn>
   <Alias>example-ap--zoneID--xa-s3</Alias>
</CreateAccessPointResult>
```

Uso dos SDKs da AWS

Você pode usar os SDKs da AWS para criar um ponto de acesso. Para ter mais informações, consulte a lista de SDKs compatíveis na “Referência de API do Amazon Simple Storage Service”.

Gerenciar pontos de acesso para buckets de diretório

Esta seção explica como gerenciar pontos de acesso para buckets de diretório usando a AWS Command Line Interface, a API REST do Amazon S3 ou o SDK da AWS.

Tópicos

- Listar pontos de acesso para buckets de diretório
- Visualizar detalhes dos pontos de acesso para buckets de diretório
- Visualizar, editar ou excluir políticas de pontos de acesso
- Gerenciar o escopo dos pontos de acesso para buckets de diretório
- Excluir o ponto de acesso para buckets de diretório

Listar pontos de acesso para buckets de diretório

Esta seção explica como listar os pontos de acesso para buckets de diretório usando o AWS Management Console, a AWS Command Line Interface (AWS CLI), a API REST ou os SDKs da AWS.

Usar o console do S3

Como listar os pontos de acesso na Conta da AWS

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Na barra de navegação na parte superior da página, escolha o nome da Região da AWS exibida no momento. Em seguida, escolha a região para a qual você deseja listar os pontos de acesso.
3. No painel de navegação, no lado esquerdo do console, escolha Pontos de acesso para buckets de diretório.
4. (Opcional) Pesquise pontos de acesso pelo nome. Somente os pontos de acesso na Região da AWS selecionada aparecerão aqui.
5. Escolha o nome do ponto de acesso que você deseja gerenciar.

Como usar o AWS CLI

O exemplo de comando `list-access-points-for-directory-buckets` a seguir mostra como você pode usar a AWS CLI para listar os pontos de acesso pertencentes a uma conta da AWS e associados a um bucket de diretório.

O comando a seguir lista os pontos de acesso para a Conta da AWS *11112222333* que estão anexados ao bucket *amzn-s3-demo-bucket--zone-id---zone-id--x-s3*.

```
aws s3control list-access-points-for-directory-buckets --account-id 111122223333 --
directory-bucket amzn-s3-demo-bucket--zone-id--x-s3
```

Para ter mais informações e exemplos, consulte list-access-points-for-directory-buckets na “Referência de comandos da AWS CLI”.

Uso da API REST

O exemplo de comando a seguir mostra como você pode usar a API REST para listar os pontos de acesso.

```
GET /v20180820/directoryaccesspoint?directoryBucket=amzn-s3-demo-bucket--zone-id--x-s3
&maxResults=maxResults HTTP/1.1
Host: s3express-control.region.amazonaws.com
x-amz-account-id: 111122223333
```

Example de resposta **ListAccessPointsForDirectoryBuckets**

```
HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<ListDirectoryAccessPointsResult>
    <AccessPointList>
        <AccessPoint>
            <AccessPointArn>arn:aws:s3express:region:111122223333:accesspoint/example-
access-point--zoneID--xa-s3</AccessPointArn>
            <Alias>example-access-point--zoneID--xa-s3</Alias>
            <Bucket>amzn-s3-demo-bucket--zone-id--x-s3</Bucket>
            <BucketAccountId>111122223333</BucketAccountId>
            <Name>example-access-point--zoneID--xa-s3</Name>
            <NetworkOrigin>VPC</NetworkOrigin>
            <VpcConfiguration>
                <VpcId>VPC-1</VpcId>
            </VpcConfiguration>
        </AccessPoint>
    </AccessPointList>
</ListDirectoryAccessPointsResult>
```

Uso dos SDKs da AWS

É possível usar os SDKs da AWS para listar os pontos de acesso. Para ter mais informações, consulte a lista de SDKs compatíveis na “Referência de API do Amazon Simple Storage Service”.

Visualizar detalhes dos pontos de acesso para buckets de diretório

Esta seção explica como visualizar detalhes de um ponto de acesso para buckets de diretório usando o AWS Management Console, a AWS CLI, os SDKs da AWS ou a API REST.

Usar o console do S3

Visualize os detalhes de um ponto de acesso para buckets de diretório para ver as seguintes informações sobre o ponto de acesso e o bucket de diretório correspondente:

- Propriedades:
  - Nome do bucket de diretório
  - ID da conta do proprietário do bucket de diretório
  - Região da AWS
  - Tipo de localização do bucket de diretório
  - Nome da localização do bucket de diretório
  - Data de criação do ponto de acesso
  - Origem da rede
  - ID da VPC
  - URI do S3
  - ARN do ponto de acesso
  - Alias do ponto de acesso
- Permissões:
  - Descobertas do analisador de acesso externo do IAM
  - Escopo do ponto de acesso
  - Política de ponto de acesso

Como visualizar os detalhes de um ponto de acesso na Conta da AWS

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Na barra de navegação na parte superior da página, escolha o nome da Região da AWS exibida no momento. Em seguida, escolha a região para a qual você deseja listar os pontos de acesso.
3. No painel de navegação, no lado esquerdo do console, escolha Pontos de acesso para buckets de diretório.
4. (Opcional) Pesquise pontos de acesso pelo nome. Somente os pontos de acesso na Região da AWS selecionada aparecerão aqui.
5. Escolha o nome do ponto de acesso que você deseja gerenciar.

6. Selecione a guia Propriedades ou a guia Permissões.

Como usar o AWS CLI

O exemplo de comando `get-access-point` a seguir mostra como você pode usar a AWS CLI para visualizar os detalhes de um ponto de acesso.

O comando a seguir lista os detalhes do ponto de acesso *my-access-point--zoneID--xa-s3* para a Conta da AWS *111122223333*.

```
aws s3control get-access-point --name my-access-point--zoneID--xa-s3 --account-
id 111122223333
```

Example da saída do comando **`get-access-point`**

```
{
    "Name": "example-access-point--zoneID--xa-s3",
    "Bucket": "amzn-s3-demo-bucket--zone-id--x-s3",
    "NetworkOrigin": "Internet",
    "PublicAccessBlockConfiguration": {
        "BlockPublicAcls": true,
        "IgnorePublicAcls": true,
        "BlockPublicPolicy": true,
        "RestrictPublicBuckets": true
    },
    "CreationDate": "2025-04-23T18:26:22.146000+00:00",
    "Alias": "example-access-point--zoneID--xa-s3",
    "AccessPointArn": "arn:aws:s3express:region:111122223333:accesspoint/example-
access-point--zoneID--xa-s3",
    "BucketAccountId": "296805379465"
}
```

Para obter mais informações e exemplos, consulte get-access-point na Referência de comandos da AWS CLI.

Uso da API REST

É possível usar a API REST para visualizar os detalhes de um ponto de acesso. Para obter mais informações, consulte GetAccessPoint na Referência da API do Amazon Simple Storage Service.

Uso dos SDKs da AWS

É possível usar os SDKs da AWS para visualizar os detalhes dos pontos de acesso. Para ter mais informações, consulte a lista de SDKs compatíveis na “Referência de API do Amazon Simple Storage Service”.

Visualizar, editar ou excluir políticas de pontos de acesso

Você pode usar uma política de ponto de acesso do AWS Identity and Access Management (IAM) para controlar a entidade principal e o recurso que podem acessar o ponto de acesso. O escopo do ponto de acesso gerencia os prefixos e as permissões de API para o ponto de acesso. Você pode criar, editar e excluir uma política de ponto de acesso usando a AWS Command Line Interface, a API REST ou os SDKs da AWS. Consulte mais informações sobre escopo de ponto de acesso em Gerenciar o escopo dos pontos de acesso para buckets de diretório.

> **Note**
>
> Como os buckets de diretório usam autorização baseada em sessão, sua política sempre deve incluir a ação `s3express:CreateSession`.

Usar o console do S3

Como visualiza, editar ou excluir uma política de ponto de acesso

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Na barra de navegação na parte superior da página, escolha o nome da Região da AWS exibida no momento. Em seguida, escolha a região para a qual você deseja listar os pontos de acesso.
3. No painel de navegação, no lado esquerdo do console, escolha Pontos de acesso para buckets de diretório.
4. (Opcional) Pesquise pontos de acesso pelo nome. Somente os pontos de acesso na Região da AWS selecionada aparecerão aqui.
5. Escolha o nome do ponto de acesso que você deseja gerenciar.
6. Selecione a guia Permissões.
7. Para criar ou editar a política de ponto de acesso, em Política de ponto de acesso, escolha Editar. Edite a política. Selecione Salvar.

8. Para excluir a política de ponto de acesso, em Política de ponto de acesso, escolha Excluir. Na janela Excluir política de ponto de acesso, digite **`confirm`** e escolha Excluir.

Como usar o AWS CLI

Você pode usar os comandos `get-acccess-point-policy`, `put-access-point-policy` e `delete-access-point-policy` para visualizar, editar ou excluir uma política de ponto de acesso. Para obter mais informações, consulte get-access-point-policy, put-access-point-policy ou delete-access-point-policy na “Referência de comandos da AWS CLI”.

Uso da API REST

Você pode usar as operações `GetAccessPointPolicy`, `DeleteAccessPointPolicy` e `PutAccessPointPolicy` da API REST para visualizar, excluir ou editar uma política de ponto de acesso. Para obter mais informações, consulte PutAccessPointPolicy, GetAccessPointPolicy ou DeleteAccessPointPolicy na “Referência de API do Amazon Simple Storage Service”.

Uso dos SDKs da AWS

Você pode usar os comandos SDKs da AWS para visualizar, excluir ou editar uma política de ponto de acesso. Para ter mais informações, consulte a lista de SDKs compatíveis com GetAccessControlPolicy, DeleteAccessControlPolicy e PutAccessControlPolicy na “Referência de API do Amazon Simple Storage Service”.

Gerenciar o escopo dos pontos de acesso para buckets de diretório

Esta seção explica como visualizar e modificar o escopo dos pontos de acesso para buckets de diretório usando a AWS Command Line Interface, a API REST ou os SDKs da AWS. Você pode usar o escopo do ponto de acesso para restringir o acesso a operações de API ou prefixos específicos.

Tópicos

- Visualizar o escopo dos pontos de acesso para buckets de diretório
- Modificar o escopo dos pontos de acesso para buckets de diretório
- Excluir o escopo dos pontos de acesso para buckets de diretório

Visualizar o escopo dos pontos de acesso para buckets de diretório

Você pode usar o AWS Management Console, a AWS Command Line Interface, a API REST ou SDKs da AWS para visualizar o escopo do ponto de acesso para buckets de diretório.

Usar o console do S3

Como usar o AWS CLI

O exemplo de comando `get-access-point-scope` a seguir mostra como você pode usar a AWS CLI para visualizar o escopo de um ponto de acesso.

O comando a seguir mostra o escopo do ponto de acesso *my-access-point*--*zoneID*--xa-s3 para a Conta da AWS *111122223333*.

```
aws s3control get-access-point-scope --name my-access-point--zoneID--xa-s3 --account-
id 111122223333
```

Para ter mais informações e exemplos, consulte get-access-point-scope na “Referência de comandos da AWS CLI”.

Example resultado de **`get-access-point-scope`**

```
{
    "Scope": {
        "Permissions": [
            "ListBucket",
            "PutObject"
        ]
  "Prefixes": [
            "Prefix": "MyPrefix1*",
            "Prefix": "MyObjectName.csv"
        ]
    }
}
```

Uso da API REST

O exemplo de solicitação `GetAccessPointScope` a seguir mostra como você pode usar a API REST para visualizar o escopo de um ponto de acesso.

A solicitação a seguir mostra o escopo do ponto de acesso *my-access-point*--*region*-*zoneID*--xa-s3 para a Conta da AWS *111122223333*.

```
GET /v20180820/accesspoint/my-access-point--zoneID--xa-s3/scope HTTP/1.1
Host: s3express-control.region.amazonaws.com
x-amz-account-id: 111122223333
```

Example resultado de **`GetAccessPointScope`**

```
HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<GetAccessPointScopeResult>
    <Scope>
        <Prefixes>
            <Prefix>MyPrefix1*</Prefix>
            <Prefix>MyObjectName.csv</Prefix>
        </Prefixes>
        <Permissions>
            <Permission>ListBucket</Permission>
            <Permission>PutObject</Permission>
        </Permissions>
        <Scope>
</GetAccessPointScopeResult>
```

Uso dos SDKs da AWS

É possível usar os SDKs da AWS para visualizar o escopo dos pontos de acesso. Para ter mais informações, consulte a lista de SDKs compatíveis na “Referência de API do Amazon Simple Storage Service”.

Modificar o escopo dos pontos de acesso para buckets de diretório

Você pode usar a AWS Command Line Interface, a API REST ou os SDKs da AWS para modificar o escopo dos pontos de acesso para buckets de diretório. O escopo de ponto de acesso é usado para restringir o acesso a prefixos específicos, operações de API ou uma combinação de ambos.

Você pode incluir uma ou mais das seguintes operações de API como permissões:

- `PutObject`
- `GetObject`
- `DeleteObject`

- `ListBucket` (obrigatório para `ListObjectsV2`)
- `GetObjectAttributes`
- `AbortMultipartUploads`
- `ListBucketMultipartUploads`
- `ListMultipartUploadParts`

> **Note**
>
> - Você pode especificar qualquer quantidade de prefixos, mas a extensão total de caracteres de todos os prefixos deve ser inferior a 256 bytes.
> - Ao modificar o escopo de um ponto de acesso, você substitui o escopo existente.

Como usar o AWS CLI

O exemplo de comando `put-access-point-scope` a seguir mostra como você pode usar a AWS CLI para modificar o escopo de um ponto de acesso.

O comando a seguir modifica o escopo do ponto de acesso *my-access-point*--*zoneID*--xa-s3 para a Conta da AWS *111122223333*.

> **Note**
>
> Você pode utilizar curingas em prefixos usando o caractere asterisco (*). Se você quiser usar o caractere asterisco como literal, adicione um caractere de barra invertida (\) de escape antes dele.
> Além disso, todos os prefixos finalizam com um "*" implícito, o que significa que todos os caminhos dentro do prefixo serão incluídos.

```
aws s3control put-access-point-scope --name my-access-point--zoneID--xa-s3 --account-id 111122223333 --scope Prefixes=string,Permissions=string
```

Para ter mais informações e exemplos, consulte put-access-point-scope na "Referência de comandos da AWS CLI".

Uso da API REST

O exemplo de solicitação `PutAccessPointScope` a seguir mostra como você pode usar a API REST para modificar o escopo de um ponto de acesso.

A solicitação a seguir modifica o escopo do ponto de acesso *my-access-point*--*zoneID*--xa-s3 para a Conta da AWS *111122223333*.

> **Note**
>
> Você pode utilizar curingas em prefixos usando o caractere asterisco (*). Se você quiser usar o caractere asterisco como literal, adicione um caractere de barra invertida (\) de escape antes dele.
> Além disso, todos os prefixos finalizam com um "*" implícito, o que significa que todos os caminhos dentro do prefixo serão incluídos.

```
PUT /v20180820/accesspoint/my-access-point--zoneID--xa-s3/scope HTTP/1.1
Host: s3express-control.region.amazonaws.com
x-amz-account-id: 111122223333
<?xml version="1.0" encoding="UTF-8"?>
<PutAccessPointScopeRequest>
        <Scope>
            <Prefixes>
                <Prefix>Jane/*</Prefix>
            </Prefixes>
            <Permissions>
                <Permission>PutObject</Permission>
                <Permission>GetObject</Permission>
            </Permissions>
            <Scope>
    </PutAccessPointScopeRequest>
```

Uso dos SDKs da AWS

É possível usar a AWS, os SDKs da AWS CLI ou a API REST para modificar o escopo do ponto de acesso. Para ter mais informações, consulte a lista de SDKs compatíveis na "Referência de API do Amazon Simple Storage Service".

Excluir o escopo dos pontos de acesso para buckets de diretório

Você pode usar a AWS Command Line Interface, a API REST ou os SDKs da AWS para excluir o escopo dos pontos de acesso para buckets de diretório.

> **Note**
>
> Quando você exclui o escopo de um ponto de acesso, todos os prefixos e permissões são excluídos.

Como usar o AWS CLI

O exemplo de comando `delete-access-point-scope` a seguir mostra como você pode usar a AWS CLI para excluir o escopo do ponto de acesso.

O comando a seguir exclui o escopo do ponto de acesso *my-access-point*--*zoneID*--xa-s3 para a Conta da AWS *111122223333*.

```
aws s3control delete-access-point-scope --name my-access-point--region-zoneID--xa-s3 --
account-id 111122223333
```

Para ter mais informações e exemplos, consulte delete-access-point-scope na “Referência de comandos da AWS CLI”.

Uso da API REST

A solicitação a seguir exclui o escopo do ponto de acesso *my-access-point*--*zoneID*--xa-s3 para a Conta da AWS *111122223333*.

```
DELETE /v20180820/accesspoint/my-access-point--zoneID--xa-s3/scope HTTP/1.1
Host: s3express-control.region.amazonaws.com
x-amz-account-id: 111122223333
```

Uso dos SDKs da AWS

É possível usar os SDKs da AWS para excluir o escopo dos pontos de acesso. Para ter mais informações, consulte a lista de SDKs compatíveis na “Referência de API do Amazon Simple Storage Service”.

Excluir o ponto de acesso para buckets de diretório

Esta seção explica como excluir um ponto de acesso usando o AWS Management Console, a AWS Command Line Interface, a API REST ou os SDKs da AWS.

> **Note**
>
> Antes de excluir um bucket de diretório anexado ao ponto de acesso, é necessário excluir o ponto de acesso.

Usar o console do S3

Como excluir pontos de acesso para buckets de diretório em sua Conta da AWS

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Na barra de navegação na parte superior da página, escolha o nome da Região da AWS exibida no momento. Em seguida, escolha a região para a qual você deseja listar os pontos de acesso.
3. No painel de navegação, no lado esquerdo do console, escolha Pontos de acesso para buckets de diretório.
4. (Opcional) Pesquise pontos de acesso pelo nome. Somente os pontos de acesso na Região da AWS selecionada aparecerão aqui.
5. Escolha o nome do ponto de acesso que você deseja excluir.
6. Escolha Excluir.
7. Para confirmar a exclusão, digite **`confirm`** e escolha Excluir.

Como usar o AWS CLI

O exemplo de comando `delete-access-point` a seguir mostra como você pode usar a AWS CLI para excluir um ponto de acesso.

O comando a seguir exclui o escopo do ponto de acesso *`my-access-point`*--*`zoneID`*--xa-s3 para a Conta da AWS *`111122223333`*.

```
aws s3control delete-access-point --name my-access-point--zoneID--xa-s3 --account-
id 111122223333
```

Para obter mais informações e exemplos, consulte delete-access-point na Referência de comandos da AWS CLI.

Uso da API REST

É possível usar a API REST para excluir os pontos de acesso. Para obter mais informações, consulte DeleteAccessPoint na Referência da API do Amazon Simple Storage Service.

Uso dos SDKs da AWS

É possível usar os SDKs da AWS para excluir os pontos de acesso. Para ter mais informações, consulte a lista de SDKs compatíveis na “Referência de API do Amazon Simple Storage Service”.

Registro em log com o AWS CloudTrail para buckets de diretório

O Amazon S3 é integrado ao AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, um perfil ou um serviço da AWS. O CloudTrail captura todas as chamadas de API para o Amazon S3 como eventos. Ao fazer uso das informações coletadas pelo CloudTrail, é possível determinar a solicitação feita ao Amazon S3, o endereço IP que a realizou, quando ela foi feita e detalhes adicionais. Quando ocorre alguma atividade de evento aceita no Amazon S3, essa atividade é registrada em um evento do CloudTrail. É possível usar a trilha do AWS CloudTrail para registrar em log eventos de gerenciamento e eventos de dados para buckets de diretório. Para ter mais informações, consulte Eventos do CloudTrail no Amazon S3 e What is AWS CloudTrail? no Guia do usuário do AWS CloudTrail.

Eventos de gerenciamento do CloudTrail para buckets de diretório

Por padrão, o CloudTrail registra em log as ações nos buckets de diretório como eventos de gerenciamento. A `eventsource` de eventos de gerenciamento do CloudTrail para buckets de diretório é `s3express.amazonaws.com`. Quando você configura a conta AWS, os eventos de gerenciamento do CloudTrail são habilitados por padrão. As operações de API de endpoint regional a seguir (operações de API em nível de bucket ou ambiente de gerenciamento) são registradas em log no CloudTrail.

- `CreateBucket`
- `DeleteBucket`
- `DeleteBucketPolicy`
- `PutBucketPolicy`

- `GetBucketPolicy`
- `ListDirectoryBuckets`
- `ListMultipartUploads`
- `GetBucketEncryption`
- `PutBucketEncryption`
- `DeleteBucketEncryption`

> **Note**
>
> `ListMultipartUploads` é uma operação de API de endpoint zonal. No entanto, essa operação da API é registrada no CloudTrail como um evento de gerenciamento. Para obter mais informações, consulte `ListMultipartUploads` na Referência da API do Amazon Simple Storage Service.

Para ter mais informações sobre eventos de gerenciamento do CloudTrail, consulte Logging management events no Manual do usuário do AWS CloudTrail.

Eventos de dados do CloudTrail para buckets de diretório

Os Eventos de dados fornecem informações sobre as operações de recursos realizadas em um recurso (por exemplo, leitura ou gravação em um objeto do Amazon S3). Também são conhecidas como operações de plano de dados. Eventos de dados geralmente são atividades de alto volume. Por padrão, as trilhas do CloudTrail não registram eventos de dados, mas é possível configurar as trilhas para registrar eventos de dados para objetos armazenados em buckets de uso geral e buckets de diretórios. Para ter mais informações, consulte Habilitar o registro em log de objetos em um bucket usando o console.

Ao registrar em log eventos de dados de uma trilha no CloudTrail, você pode optar por usar seletores de eventos avançados ou básicos. Para registrar eventos de dados de objetos armazenados em buckets de diretório, é necessário usar seletores de eventos avançados. Ao configurar seletores de recursos avançados, você escolherá ou especificará o tipo de recurso `AWS::S3Express::Object`.

As operações de API de endpoint zonal a seguir (operações de API em nível de objeto ou plano de dados) são registradas no CloudTrail.

- `AbortMultipartUpload`

- CompleteMultipartUpload
- CreateSession
- CopyObject
- CreateMultipartUpload
- DeleteObject
- DeleteObjects
- GetObject
- GetObjectAttributes
- HeadBucket
- HeadObject
- ListObjectsV2
- ListParts
- PutObject
- RenameObject
- UploadPart
- UploadPartCopy

Para ter mais informações sobre eventos de dados do CloudTrail, consulte Logging data events no Manual do usuário do AWS CloudTrail.

Consulte mais informações sobre eventos do CloudTrail para buckets de diretório nos seguintes tópicos:

Tópicos

- Exemplos de arquivos de log do CloudTrail para buckets de diretório

Exemplos de arquivos de log do CloudTrail para buckets de diretório

O arquivo de log do CloudTrail inclui informações sobre a operação da API solicitada, a data e a hora da operação, os parâmetros de solicitação, etc. Este tópico apresenta exemplos de eventos de dados do CloudTrail e de eventos de gerenciamento para buckets de diretório.

Tópicos

- Exemplos de arquivos de log de eventos do CloudTrail para buckets de diretório

Exemplos de arquivos de log de eventos do CloudTrail para buckets de diretório

Veja a seguir um exemplo de arquivo de log do CloudTrail que demonstra CreateSession.


```
    {
        "eventVersion": "1.09",
        "userIdentity": {
          "type": "AssumedRole",
          "principalId": "AROAIDPPEZS35WEXAMPLE:AssumedRoleSessionName",
          "arn": "arn:aws:sts::111122223333assumed-role/RoleToBeAssumed/MySessionName",
          "accountId": "111122223333",
          "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
          "sessionContext": {
            "sessionIssuer": {
              "type": "Role",
              "principalId": "AROAIDPPEZS35WEXAMPLE",
              "arn": "arn:aws:iam::111122223333:role/RoleToBeAssumed",
              "accountId": "111122223333",
              "userName":"RoleToBeAssumed
            },

            "attributes": {
              "creationDate": "2024-07-02T00:21:16Z",
            "mfaAuthenticated": "false"
            }
          }
        },
        "eventTime": "2024-07-02T00:22:11Z",
        "eventSource": "s3express.amazonaws.com",
        "eventName": "CreateSession",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "72.21.198.68",
        "userAgent": "aws-sdk-java/2.20.160-SNAPSHOT
 Linux/5.10.216-225.855.amzn2.x86_64 OpenJDK_64-Bit_Server_VM/11.0.23+9-LTS
 Java/11.0.23 vendor/Amazon.com_Inc. md/internal exec-env/AWS_Lambda_java11 io/sync
 http/Apache cfg/retry-mode/standard",
        "requestParameters": {
          "bucketName": "bucket-base-name--usw2-az1--x-s3".
            "host": "bucket-base-name--usw2-az1--x-s3.s3express-usw2-az1.us-
west-2.amazonaws.com",
            "x-amz-create-session-mode": "ReadWrite"
        },
        "responseElements": {
            "credentials": {
```

```
                "accessKeyId": "AKIAI44QH8DHBEXAMPLE"
                "expiration": ""Mar 20, 2024, 11:16:09 PM",
                "sessionToken": "<session token string>"
            },
        },
        "additionalEventData": {
            "SignatureVersion": "SigV4",
            "cipherSuite": "TLS_AES_128_GCM_SHA256",
            "bytesTransferredIn": 0,
            "AuthenticationMethod": "AuthHeader",
            "xAmzId2": "q6xhNJYmhg",
            "bytesTransferredOut": 1815,
            "availabilityZone": "usw2-az1"
          },
          "requestID": "28d2faaf-3319-4649-998d-EXAMPLE72818",
          "eventID": "694d604a-d190-4470-8dd1-EXAMPLEe20c1",
          "readOnly": true,
          "resources": [
            {
              "type": "AWS::S3Express::Object",
              "ARNPrefix": "arn:aws:s3express:us-west-2:111122223333:bucket-base-name--
usw2-az1--x-s3"
            },
            {
              "accountId": "111122223333"
              "type": "AWS::S3Express::DirectoryBucket",
              "ARN": "arn:aws:s3express:us-west-2:111122223333:bucket-base-name--usw2-
az1--x-s3"
             }
           ],
           "eventType": "AwsApiCall",
           "managementEvent": false,
           "recipientAccountId": "111122223333",
           "eventCategory": "Data",
           "tlsDetails": {
             "tlsVersion": "TLSv1.3",
             "cipherSuite": "TLS_AES_128_GCM_SHA256",
             "clientProvidedHostHeader": "bucket-base-name--usw2-az1--x-s3.s3express-
usw2-az1.us-west-2.amazonaws.com"
            }
          }
```

Para usar as operações da API do endpoint zonal (operações em nível de objeto ou plano de dados), é possível usar a operação da API `CreateSession` para criar e gerenciar sessões otimizadas para autorização de solicitações de dados com baixa latência. Também é possível usar `CreateSession` para reduzir a quantidade de registro em log. Para identificar quais operações de API zonal foram realizadas durante uma sessão, é possível combinar o `accessKeyId` em `responseElements` em seu arquivo de log `CreateSession` com o `accessKeyId` no arquivo de log de outras operações de API zonal. Para ter mais informações, consulte `CreateSession` authorization.

Veja a seguir um exemplo de arquivo de log do CloudTrail que demonstra a operação da API `GetObject` autenticada por `CreateSession`.


```
    {
        "eventVersion": "1.09",
        "userIdentity": {
          "type": "AssumedRole",
          "principalId": "AROAIDPPEZS35WEXAMPLE:AssumedRoleSessionName",
          "arn": "arn:aws:sts::111122223333assumed-role/RoleToBeAssumed/MySessionName",
          "accountId": "111122223333",
          "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
          "sessionContext": {
            "attributes": {
              "creationDate": "2024-07-02T00:21:49Z"
            }
          }
        },
        "eventTime": "2024-07-02T00:22:01Z",
        "eventSource": "s3express.amazonaws.com",
        "eventName": "GetObject",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "72.21.198.68",
        "userAgent": "aws-sdk-java/2.25.66 Linux/5.10.216-225.855.amzn2.x86_64
 OpenJDK_64-Bit_Server_VM/17.0.11+9-LTS Java/17.0.11 vendor/Amazon.com_Inc. md/internal
 exec-env/AWS_Lambda_java17 io/sync http/Apache cfg/retry-mode/legacy",
        "requestParameters": {
          "bucketName": "bucket-base-name--usw2-az1--x-s3",
          "x-amz-checksum-mode": "ENABLED",
          "Host": "bucket-base-name--usw2-az1--x-s3.s3express-usw2-az1.us-
west-2.amazonaws.com",
          "key": "test-get-obj-with-checksum"
        },
        "responseElements": null,
        "additionalEventData": {
```

```
          "SignatureVersion": "Sigv4",
          "CipherSuite": "TLS_AES_128_GCM_SHA256",
          "bytesTransferredIn": 0,
          "AuthenticationMethod": "AuthHeader",
          "x-amz-id-2": "oOy6w8K7LFsyFN",
          "bytesTransferredOut": 9,
          "availabilityZone": "usw2-az1",
          "sessionModeApplied": "ReadWrite"
        },
          "requestID": "28d2faaf-3319-4649-998d-EXAMPLE72818",
          "eventID": "694d604a-d190-4470-8dd1-EXAMPLEe20c1",
          "readOnly": true,
          "resources": [
            {
              "type": "AWS::S3Express::Object",
              "ARNPrefix": "arn:aws:s3express:us-west-2:111122223333:bucket-base-name--
usw2-az1--x-s3"
            },
            {
              "accountId": "111122223333",
              "type": "AWS::S3Express::DirectoryBucket",
              "ARN": "arn:aws:s3express:us-west-2:111122223333:bucket-base-name--usw2-
az1--x-s3"
             }
           ],
           "eventType": "AwsApiCall",
           "managementEvent": false,
           "recipientAccountId": "111122223333",
           "eventCategory": "Data",
           "tlsDetails": {
             "tlsVersion": "TLSv1.3",
             "cipherSuite": "TLS_AES_128_GCM_SHA256",
             "clientProvidedHostHeader": "bucket-base-name--usw2-az1--x-s3.s3express-
usw2-az1.us-west-2.amazonaws.com"
            }
          }
```


No exemplo de arquivo de log `GetObject` acima, o `accessKeyId` (AKIAI44QH8DHBEXAMPLE) corresponde ao `accessKeyId` sob `responseElements` no exemplo de arquivo de log CreateSession. O `accessKeyId` correspondente indica a sessão na qual a operação `GetObject` foi realizada.

O exemplo a seguir mostra uma entrada de log do CloudTrail que demonstra uma ação `DeleteObjects` em um bucket de diretório, invocado pelo S3 Lifecycle. Para obter mais informações, consulte Working with S3 Lifecycle for directory buckets.

```
eventVersion:"1.09",
  userIdentity:{

    type:"AWSService",
    invokedBy:"lifecycle.s3.amazonaws.com"
  },
  eventTime:"2024-09-11T00:55:54Z",
  eventSource:"s3express.amazonaws.com",
  eventName:"DeleteObjects",
  awsRegion:"us-east-2",
  sourceIPAddress:"lifecycle.s3.amazonaws.com",
  userAgent:"gamma.lifecycle.s3.amazonaws.com",
  requestParameters:{

    bucketName:"amzn-s3-demo-bucket--use2-az2--x-s3",
    'x-amz-expected-bucket-owner':"637423581905",
    Host:"amzn-s3-demo-bucket--use2-az2--x-s3.gamma.use2-az2.express.s3.aws.dev",
    delete:"",
    'x-amz-sdk-checksum-algorithm':"CRC32C"
  },
  responseElements:null,
  additionalEventData:{

    SignatureVersion:"Sigv4",
    CipherSuite:"TLS_AES_128_GCM_SHA256",
    bytesTransferredIn:41903,
    AuthenticationMethod:"AuthHeader",
    'x-amz-id-2':"9H5YWZY0",
    bytesTransferredOut:35316,
    availabilityZone:"use2-az2",
    sessionModeApplied:"ReadWrite"
  },
  requestID:"011eeadd04000191",
  eventID:"d3d8b116-219d-4ee6-a072-5f9950733c74",
  readOnly:false,
  resources:[

    {
```

```
      type:"AWS::S3Express::Object",
      ARNPrefix:"arn:aws:s3express:us-east-2:637423581905:bucket/amzn-s3-demo-bucket--
use2-az2--x-s3/"
    },
    {

      accountId:"637423581905",
      type:"AWS::S3Express::DirectoryBucket",
      ARN:"arn:aws:s3express:us-east-2:637423581905:bucket/amzn-s3-demo-bucket--use2-
az2--x-s3"
    }
  ],
  eventType:"AwsApiCall",
  managementEvent:false,
  recipientAccountId:"637423581905",
  sharedEventID:"59f877ac-1dd9-415d-b315-9bb8133289ce",
  eventCategory:"Data"
}
```

O exemplo a seguir mostra uma entrada de log do CloudTrail que demonstra uma solicitação `Access Denied` em uma ação `CreateSession` invocada pelo S3 Lifecycle. Para obter mais informações, consulte CreateSession.

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "gamma.lifecycle.s3.amazonaws.com"
    },
    "eventTime": "2024-09-11T18:13:08Z",
    "eventSource": "s3express.amazonaws.com",
    "eventName": "CreateSession",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "gamma.lifecycle.s3.amazonaws.com",
    "userAgent": "gamma.lifecycle.s3.amazonaws.com",
    "errorCode": "AccessDenied",
    "errorMessage": "Access Denied",
    "requestParameters": {
        "bucketName": "amzn-s3-demo-bucket--use2-az2--x-s3",
        "Host": "amzn-s3-demo-bucket--use2-az2--x-s3.gamma.use2-
az2.express.s3.aws.dev",
        "x-amz-create-session-mode": "ReadWrite",
        "x-amz-server-side-encryption": "AES256"
```

```
    },
    "responseElements": null,
    "additionalEventData": {
        "SignatureVersion": "Sigv4",
        "CipherSuite": "TLS_AES_128_GCM_SHA256",
        "bytesTransferredIn": 0,
        "AuthenticationMethod": "AuthHeader",
        "x-amz-id-2": "zuDDC1VNbC4LoNwUIc5",
        "bytesTransferredOut": 210,
        "availabilityZone": "use2-az2"
    },
    "requestID": "010932f174000191e24a0",
    "eventID": "dce7cc46-4cd3-46c0-9a47-d1b8b70e301c",
    "readOnly": true,
    "resources": [{
            "type": "AWS::S3Express::Object",
            "ARNPrefix": "arn:aws:s3express:us-east-2:637423581905:bucket/amzn-s3-demo-
bucket--use2-az2--x-s3/"
        },
        {
            "accountId": "637423581905",
            "type": "AWS::S3Express::DirectoryBucket",
            "ARN": "arn:aws:s3express:us-east-2:637423581905:bucket/amzn-s3-demo-
bucket--use2-az2--x-s3"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "637423581905",
    "sharedEventID": "da96b5bd-6066-4a8d-ad8d-f7f427ca7d58",
    "eventCategory": "Data"
}
```


Otimizar o desempenho do bucket de diretório

Para obter o melhor desempenho ao usar buckets de diretório, recomendamos seguir estas diretrizes.

Para ter mais informações sobre as práticas recomendadas para o S3 Express One Zone, consulte Práticas recomendadas para otimizar a performance da classe S3 Express One Zone.

Usar a autenticação baseada em sessão

Os buckets de diretório são compatíveis com um novo mecanismo de autorização baseado em sessão para autenticar e autorizar solicitações para um bucket de diretório. Com a autenticação baseada em sessão, os AWS SDKs usam automaticamente a operação de API `CreateSession` para criar um token temporário de sessão que pode ser usado para autorização de baixa latência de solicitações de dados a um bucket de diretório.

Os AWS SDKs usam a operação de API `CreateSession` para solicitar credenciais temporárias, depois criam e atualizam tokens para você automaticamente a cada 5 minutos. Para aproveitar os benefícios de desempenho dos buckets de diretório, recomendamos que você use os AWS SDKs para iniciar e gerenciar a solicitação de API `CreateSession`. Para obter mais informações sobre esse modelo baseado em sessão, consulte Autorizar operações de API de endpoint zonal com `CreateSession`.

Práticas recomendadas adicionais de soma de verificação do S3

Os buckets de diretório oferecem a opção de escolher o algoritmo de soma de verificação usado para validar seus dados durante o upload ou o download. Você pode selecionar um dos seguintes algoritmos de verificação de integridade de dados de hash seguro (SHA) ou de verificação de redundância cíclica (CRC): CRC32, CRC32C, SHA-1 e SHA-256. As somas de verificação baseadas em MD5 não são compatíveis com a classe de armazenamento S3 Express One Zone.

CRC32 é a soma de verificação padrão usada pelos AWS SDKs ao transmitir dados de ou para buckets de diretório. Recomendamos usar CRC32 e CRC32C para ter a melhor performance com buckets de diretório.

Usar a versão mais recente dos AWS SDKs e das bibliotecas de tempo de execução comuns

Vários dos AWS SDKs também fornecem as bibliotecas Common Runtime (CRT) da AWS para acelerar ainda mais a performance em clientes do S3. Esses SDKs incluem o AWS SDK for Java 2.x, o AWS SDK para C++ e o AWS SDK para Python (Boto3). O cliente do S3 baseado em CRT transfere objetos entre buckets de diretório com desempenho e confiabilidade aprimorados usando automaticamente a operação de API de carregamento fracionado e buscas de intervalo de bytes para automatizar as conexões de escalabilidade horizontal.

Para atingir o melhor desempenho com os buckets de diretório, recomendamos usar a versão mais recente dos AWS SDKs que incluem as bibliotecas de CRT ou usar a AWS Command Line Interface (AWS CLI).

Desenvolvimento com buckets de diretório

Depois de criar o bucket de diretório, você pode começar a desfrutar imediatamente de leituras e gravações de latência muito baixa. Você pode se comunicar com o bucket de diretório usando uma conexão de endpoint em uma nuvem privada virtual (VPC) ou pode usar operações de API zonais e regionais para gerenciar objetos e buckets de diretório. É possível trabalhar com buckets de diretório usando os AWS SDKs, o console do Amazon S3, a AWS Command Line Interface (AWS CLI) e APIs REST do Amazon S3.

Tópicos

- Endpoints regionais e zonais para buckets de diretório
- Trabalhar com buckets de diretório usando o console do S3, a AWS CLI e AWS SDKs
- Operações de API de bucket de diretório

Endpoints regionais e zonais para buckets de diretório

Para acessar endpoints regionais e zonais de buckets de diretório por meio de sua nuvem privada virtual (VPC), é possível usar endpoints da VPC de gateway. Depois de criar um endpoint de gateway, é possível adicioná-lo como um destino na tabela de rotas para o tráfego destinado da VPC ao bucket. Não há cobrança adicional pelo uso de endpoints do gateway. Para obter mais informações sobre como configurar endpoints de VPC do gateway, consulte Rede para buckets de diretório.

As operações de API no nível do bucket (ambiente de gerenciamento) estão disponíveis por meio de um endpoint regional e são chamadas de operações de API do endpoint regional. Exemplos de operações de API de endpoint regional são `CreateBucket` e `DeleteBucket`.

Você usa operações de API de endpoint zonal (nível de objeto ou plano de dados) para fazer upload e gerenciar objetos. As operações de API de endpoint zonal estão disponíveis por meio de um endpoint zonal. Exemplos de operações de API zonais são `PutObject` e `CopyObject`.

Para ter mais informações sobre os endpoints regionais e zonais para buckets de diretório em zonas de disponibilidade, consulte Endpoints regionais e zonais para buckets de diretório em uma zona de disponibilidade.

Para ter mais informações sobre os endpoints regionais e zonais para buckets de diretório em zonas locais, consulte Conceitos para buckets de diretório em zonas locais.

Trabalhar com buckets de diretório usando o console do S3, a AWS CLI e AWS SDKs

Você pode trabalhar com a classe de armazenamento S3 Express One Zone e os buckets de diretório usando os AWS SDKs, o console do Amazon S3, a AWS CLI (AWS Command Line Interface) e a API REST do Amazon S3.

Console do S3

Para começar a usar o console do S3, siga estas etapas:

- Criar buckets de diretório em uma zona de disponibilidade
- Esvaziar um bucket de diretório
- Excluir um bucket de diretório

Para ver um tutorial completo, consulte Tutorial: Conceitos básicos da classe S3 Express One Zone.

SDKs da AWS

A classe S3 Express One Zone é compatível com os seguintes AWS SDKs:

- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK for Java 2.x
- AWS SDK para JavaScript v3
- AWS SDK para .NET
- AWS SDK para PHP
- AWS SDK para Python (Boto3)
- AWS SDK para Ruby
- AWS SDK para Kotlin
- AWS SDK para Rust

Ao trabalhar com a classe S3 Express One Zone, recomendamos usar a versão mais recente dos AWS SDKs. Os AWS SDKs compatíveis com a classe S3 Express One Zone lidam com o estabelecimento, a atualização e o encerramento de sessões em seu nome. Isso significa que você pode começar imediatamente a usar as operações de API depois de fazer download e instalar os AWS SDKs e configurar as permissões necessárias do IAM. Para obter mais informações, consulte Autorizar operações de API de endpoint regional com o IAM.

Para obter informações sobre os AWS SDKs, inclusive sobre como baixá-los e instalá-los, consulte Aprenda a criar na AWS.

Para obter exemplos de AWS SDK, consulte os seguintes tópicos:

- Criar buckets de diretório em uma zona de disponibilidade
- Esvaziar um bucket de diretório
- Excluir um bucket de diretório

AWS Command Line Interface (AWS CLI)

Você pode usar a AWS Command Line Interface (AWS CLI) para criar buckets de diretório e usar as operações de API de endpoint regional e zonal compatíveis com a classe S3 Express One Zone.

Para começar a usar a AWS CLI, consulte Conceitos básicos da AWS CLI na Referência de comandos da AWS CLI.

> **Note**
>
> Para usar buckets de diretório com os comandos `aws s3` de alto nível, atualize a AWS CLI para a versão mais recente. Para obter mais informações sobre como instalar e configurar a AWS CLI, consulte Instalar ou atualize para a versão mais recente da AWS CLI na Referência de comandos da AWS CLI.

Para obter exemplos da AWS CLI, consulte os seguintes tópicos:

- Criar buckets de diretório em uma zona de disponibilidade
- Esvaziar um bucket de diretório
- Excluir um bucket de diretório

Operações de API de bucket de diretório

Para gerenciar bucket de diretório, você pode usar operações de API de endpoint regional (nível de bucket ou ambiente de gerenciamento). Para gerenciar objetos nos buckets de diretório, você poderá usar operações de API de endpoint zonal (nível do objeto ou plano de dados). Para obter mais informações, consulte Rede para buckets de diretório e Endpoints e endpoints de VPC do gateway.

Operações de API de endpoint regional

As seguintes operações de API de endpoint regional são compatíveis com buckets de diretório:

- CreateAccessPoint
- CreateBucket
- DeleteAccessPoint
- DeleteAccessPointPolicy
- DeleteAccessPointScope
- DeleteBucket
- DeleteBucketLifecycle
- DeleteBucketPolicy
- GetAccessPoint
- GetAccessPointPolicy
- GetAccessPointScope
- GetBucketLifecycleConfiguration
- GetBucketPolicy
- ListAccessPointsForDirectoryBuckets
- ListDirectoryBuckets
- ListTagsForResource
- PutAccessPointPolicy
- PutAccessPointScope
- PutBucketLifecycleConfiguration
- PutBucketPolicy
- DeleteBucketEncryption
- GetBucketEncryption

- PutBucketEncryption
- TagResource
- UntagResource

Operações de API de endpoint zonal

As seguintes operações de API de endpoint zonal podem ser usadas para buckets de diretório:

- CreateSession
- CopyObject
- DeleteObject
- DeleteObjects
- GetObject
- GetObjectAttributes
- HeadBucket
- HeadObject
- ListObjectsV2
- PutObject
- RenameObject
- AbortMultipartUpload
- CompleteMultiPartUpload
- CreateMultipartUpload
- ListMultipartUploads
- ListParts
- UploadPart
- UploadPartCopy

Usar tags com buckets de diretório do S3

Uma tag da AWS é um par de chave-valor que contém metadados sobre recursos, neste caso buckets de diretório do Amazon S3. Você pode marcar buckets de diretório do S3 ao criá-los ou gerenciar tags em buckets de diretório existentes. Não há cobrança adicional para usar tags

em buckets de diretório além das taxas de solicitação padrão da API do S3. Para obter mais informações, consulte Preço do Amazon S3.

Como as tags funcionam

Os buckets de diretório do Amazon S3 permitem dois tipos de tag:

- Tags geradas AWS: a AWS aplica automaticamente essas tags, e você não pode modificá-las ou removê-las. Para saber mais sobre tags geradas pela AWS, consulte Using AWS-generated tags.
- Tags definidas pelo usuário: é você quem aplica essas tags aos seus buckets de diretório do S3 ou a outros recursos e as gerencia.

Tags definidas pelo usuário

Uma tag definida pelo usuário é um par de chave-valor de tag que você usa para rotular seus recursos. As tags definidas pelo usuário consistem em uma chave obrigatória e um valor opcional. Estes são os principais componentes de uma tag definida pelo usuário:

A chave da tag

A chave de tags é o nome obrigatório da tag. Por exemplo, `project` é a chave da tag no seguinte par de chave-valor de tag:

Chave	Valor
`project`	`Trinity`

A chave da tag é uma string que diferencia maiúsculas e minúsculas e deve conter de 1 a 128 caracteres Unicode.

O valor da tag

O valor da tag é uma string opcional. Por exemplo, `Trinity` é o valor da tag neste par de chave-valor de tag:

Chave	Valor
`project`	`Trinity`

O valor da tag é uma string que diferencia maiúsculas e minúsculas e pode conter de 0 a 256 caracteres Unicode.

Para obter detalhes sobre os caracteres permitidos em tags definidas pelo usuário e outras restrições, consulte User-Defined Tag Restrictions no Guia do usuário do Gerenciamento de Faturamento e Custos da AWS.

O conjunto de tags

Cada bucket de diretório do S3 tem um conjunto de tags que contém todos os pares de chave e valor de tag atribuídos a esse bucket. Um conjunto de tags pode conter até cinquenta tags ou estar vazio.

Embora cada chave deva ser exclusiva em um conjunto de tags, você pode usar o mesmo valor várias vezes. Por exemplo, você pode ter o mesmo valor, `Trinity`, para as duas chaves de tag abaixo:

Chave	Valor
`project`	`Trinity`
`cost-center`	`Trinity`

Em um bucket, quando você adiciona uma tag que tem a mesma chave de uma tag existente, o novo valor substitui o antigo.

AWSA não aplica nenhum significado semântico às suas tags. Interpretamos as tags estritamente como sequências de caracteres.

Para adicionar, listar, modificar ou excluir tags, você pode usar o console do Amazon S3, a AWS Command Line Interface (AWS CLI) ou a API do Amazon S3.

Maneiras comuns de usar tags

Use tags em buckets de diretório do S3 para:

1. Alocação de custos: acompanhe os custos de armazenamento por tag de bucket no Gerenciamento de Faturamento e Custos da AWS.
2. Controle de acesso por atributo (ABAC): amplie as permissões de acesso e conceda acesso aos buckets de diretório do S3 com base nas respectivas tags.

> **Note**
>
> Você pode usar as mesmas tags para alocação de custos e controle de acesso.

Usar tags para alocação de custos

Acompanhe seus custos de armazenamento do Amazon S3 aplicando tags aos buckets de diretório do S3 e ativando essas tags para alocação de custos.

Para começar a rastrear os custos:

1. Adicione tags aos seus buckets de diretório do S3 ou use tags existentes. Para ter mais informações sobre como adicionar tags definidas pelo usuário aos seus buckets de diretório, consulte Como trabalhar com tags. Por exemplo, você pode rotular os buckets com uma tag que identifique um projeto ou um grupo de projetos.
2. Ative as tags para alocação de custos no console do Gerenciamento de Faturamento e Custos da AWS. Consulte Activating user-defined cost allocation tags no Guia do usuário do Gerenciamento de Faturamento e Custos da AWS. Você pode ativar tags definidas pelo usuário ou geradas pela AWS. Para ter mais informações, consulte Organizing and tracking costs using AWS cost allocation tags.

A AWS usa as tags ativadas para organizar os custos de seus recursos em várias ferramentas gerenciamento de faturamento e custos, como:

- Relatório de alocação de custos

  Oferece uma visualização geral dos custos organizados com base em nas tags ativadas. Para ter mais informações, consulte Using the monthly cost allocation report no Guia do usuário do AWS Billing.

- Relatório de Custos e Uso (CUR)

  Oferece o conjunto mais detalhado de dados de custo e uso da AWS, bem como detalhamento de custos baseado em tags. Para ter mais informações, consulte What are AWS Cost and Usage Reports? no Guia do usuário do AWS Data Exports.

Usar tags para controle de acesso por atributo (ABAC)

O controle de acesso por atributo (ABAC) é uma estratégia de autorização que define permissões com base em atributos (isto é, tags). Você pode anexar tags a entidades do AWS Identity and Access Management (IAM) (usuários ou perfis) e a recursos da AWS, como buckets de diretório do Amazon S3. Posteriormente, você controla as permissões para esses recursos usando condições baseadas em tags em políticas de controle de acesso para permitir ou negar operações quando essas condições forem atendidas.

ABAC para buckets de diretório do S3

Os buckets de diretório do Amazon S3 permitem o controle de acesso por atributo (ABAC) por meio de tags. Use chaves de condição baseadas em tags em políticas de bucket de diretório do S3, de suas organizações na AWS e do IAM. Para empresas, o ABAC no Amazon S3 permite a autorização em várias contas da AWS.

Nas suas políticas do IAM, você pode controlar o acesso aos buckets de diretório do S3 com base nas tags do bucket usando as seguintes chaves de condição globais:

- `aws:ResourceTag/key-name`
  - Use essa chave para comparar o par chave-valor da etiqueta especificado na política com o par chave-valor anexado ao recurso. Por exemplo, é possível exigir que o acesso a um recurso seja permitido somente se o recurso tiver a chave de tag `Dept` anexada com o valor `Marketing`. Para obter mais informações, consulte Controle de acesso aos recursos do AWS.
- `aws:RequestTag/key-name`
  - Use essa chave para comparar o par de chave/valor da tag que foi passado na solicitação com o par de tags especificado na política. Por exemplo, é possível verificar se a solicitação inclui a chave de tag `Dept` e se ela tem o valor `Accounting`. Para ter mais informações, consulte Controlar o acesso durante solicitações da AWS. Você pode usar essa chave de condição para restringir quais pares de chave-valor de tag podem ser transmitidos durante as operações de API `TagResource` e `CreateBucket`.
- `aws:TagKeys`
  - Use essa chave para comparar as chaves de tag em uma solicitação com as chaves especificadas na política. Ao usar políticas para controlar o acesso usando etiquetas, recomendamos o uso da chave de condição `aws:TagKeys` para definir quais chaves de etiquetas serão permitidas. Para ver exemplos de política e ter mais informações, consulte Controlar o acesso com base em chaves de tag. Você pode criar um bucket de diretório do S3

com tags. Para permitir a marcação durante a operação de API `CreateBucket`, você deve criar uma política que inclua as ações `s3express:TagResource` e `s3express:CreateBucket`. Em seguida, você pode usar a chave de condição `aws:TagKeys` para impor o uso de tags específicas na solicitação `CreateBucket`.

- `s3express:BucketTag/tag-key`
  - Use essa chave de condição para conceder permissões a dados específicos em buckets de diretório por meio de tags. Quando se usa um ponto de acesso para acessar um bucket de diretório, essa chave de condição faz referência às tags no bucket de diretório ao conceder permissões referentes ao ponto de acesso e ao bucket de diretório, enquanto `aws:ResourceTag/tag-key` faz referência apenas às tags do recurso ao qual está sendo concedida uma permissão.

Exemplo de política

Veja os exemplos de política de ABAC a seguir para buckets de diretório do Amazon S3.

1.1 Política do IAM para criar ou modificar buckets com tags específicas

Nessa política do IAM, usuários ou perfis com essa política só podem criar buckets de diretório do S3 se marcarem o bucket com a chave de tag `project` e o valor de tag `Trinity` na solicitação de criação do bucket. Eles também podem adicionar ou modificar tags em buckets de diretório existentes do S3, desde que a solicitação `TagResource` inclua o par de chave-valor de tag `project:Trinity`. Essa política não concede permissões de leitura, gravação ou exclusão nos buckets ou nos respectivos objetos.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CreateBucketWithTags",
      "Effect": "Allow",
      "Action": [
        "s3express:CreateBucket",
        "s3express:TagResource"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/project": [
```

```
            "Trinity"
          ]
        }
      }
    }
  ]
}
```

1.2 Política de bucket para restringir operações no bucket por meio de tags

Nessa política de bucket, as entidades principais do IAM (usuários e perfis) podem executar operações usando a ação `CreateSession` no bucket somente se o valor da tag `project` do bucket corresponder ao valor da tag `project` da entidade principal.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowObjectOperations",
      "Effect": "Allow",
      "Principal": {
        "AWS": "111122223333"
      },
      "Action": "s3express:CreateSession",
      "Resource": "arn:aws:s3express:us-west-2:111122223333:bucket/amzn-s3-demo-
bucket--usw2-az1--x-s3",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/project": "${aws:PrincipalTag/project}"
        }
      }
    }
  ]
}
```

1.3 Política do IAM para modificar tags em recursos existentes, mantendo a governança de marcação

Nessa política do IAM, as entidades principais do IAM (usuários e perfis) podem modificar tags em um bucket somente se o valor da tag `project` do bucket corresponder ao valor da tag `project` da entidade principal. Somente as quatro tags (`project`, `environment`, `owner` e `cost-center`) especificadas nas chaves de condição `aws:TagKeys` são permitidas para esses buckets de

diretório. Isso ajuda a impor a governança de tags, evita modificações não autorizadas nas tags e mantém o esquema de marcação consistente em todos os seus buckets.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EnforceTaggingRulesOnModification",
      "Effect": "Allow",
      "Action": [
        "s3express:TagResource"
      ],
      "Resource": "arn:aws:s3express:*:*:bucket/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/project": "${aws:PrincipalTag/project}"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": [
            "project",
            "environment",
            "owner",
            "cost-center"
          ]
        }
      }
    }
  ]
}
```

1.4 Uso da chave de condição s3express:BucketTag

Nessa política do IAM, a instrução de condição permite acesso aos dados do bucket somente se o bucket tiver a chave de tag `Environment` e o valor de tag `Production`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowAccessToSpecificAccessPoint",
      "Effect": "Allow",
      "Action": "*",
      "Resource": "arn:aws:s3express:*:*:accesspoint/*",
```

```
      "Condition": {
        "StringEquals": {
          "s3express:BucketTag/Environment": "Production"
        }
      }
    }
  ]
}
```

Como trabalhar com tags

Você pode adicionar ou gerenciar tags para buckets de diretório do S3 usando o console do Amazon S3, a AWS Command Line Interface (CLI) e os SDKs da AWS ou as APIs TagResource, UntagResource e ListTagsForResource do S3. Para obter mais informações, consulte:

Tópicos

- Criar buckets de diretórios com tags
- Adicionar uma tag a um bucket de diretório
- Visualizar tags de buckets de diretório
- Excluir uma tag de um bucket de diretório

Criar buckets de diretórios com tags

Você pode marcar buckets de diretório do Amazon S3 ao criá-los. Não há cobrança adicional para usar tags em buckets de diretório além das taxas de solicitação padrão da API do S3. Para obter mais informações, consulte Preço do Amazon S3. Para ter mais informações sobre marcação de buckets de diretório, consulte Usar tags com buckets de diretório do S3.

Permissões

Para criar um bucket de diretório com tags, você precisa ter as seguintes permissões:

- `s3express:CreateBucket`
- `s3express:TagResource`

Solucionar de problemas de erros

Se você encontrar um erro ao tentar criar um bucket de diretório com tags, é possível fazer o seguinte:

- Verifique se você tem as Permissões necessárias para criar o bucket de diretório e adicionar uma tag a ele.
- Confira sua política de usuário do IAM para ver se existe alguma condição de controle de acesso por atributo (ABAC). Pode ser necessário rotular seus buckets de diretório somente com chaves e valores de tag específicos. Para obter mais informações, consulte Usar tags para controle de acesso por atributo (ABAC).

Etapas

Você pode criar um bucket de diretório com tags aplicadas usando o console do Amazon S3, a AWS Command Line Interface (AWS CLI), a API REST do Amazon S3 e SDKs da AWS.

Usar o console do S3

Para criar um bucket de diretório com tags usando o console do Amazon S3:

1. Faça login no console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets de diretório.
3. Escolha Criar bucket para criar um bucket de diretório.
4. É possível criar dois tipos de bucket de diretório:

   Criar um bucket de diretório em uma zona de disponibilidade para uma workload de alto desempenho. Para obter mais informações, consulte Workloads de alto desempenho.

   Criar um bucket de diretório em uma zona local para uma workload de residência de dados. Para obter mais informações, consulte Workloads de residência de dados.
5. Para ambos os tipos de bucket de diretório, a opção Tags está presente na página Criar bucket ao criar um bucket de diretório.
6. Insira um nome para o bucket. Para obter mais informações, consulte

   Ao criar um bucket de diretório no Amazon S3, as regras de nomenclatura de buckets a seguir se aplicam. Para conferir as regras de nomenclatura para buckets de uso geral, consulte Regras de nomenclatura de buckets de uso geral.

Um nome de bucket de diretório consiste em um nome base que você fornece e um sufixo que contém o ID da zona da AWS (uma zona de disponibilidade ou zona local) em que o bucket está localizado e `--x-s3`. O *`zone-id`* pode ser o ID de uma zona de disponibilidade ou zona local.

```
base-name--zoneid--x-s3
```

Por exemplo, o seguinte nome de bucket de diretório contém o ID da zona de disponibilidade `usw2-az1`:

```
bucket-base-name--usw2-az1--x-s3
```

> **Note**
>
> Quando você cria um bucket de diretório usando o console, um sufixo é adicionado automaticamente ao nome base fornecido. Esse sufixo inclui o ID da zona (zona de disponibilidade ou zona local) que você escolheu.

> Ao criar um bucket de diretório usando uma API, é necessário fornecer o sufixo completo, incluindo o ID da zona de disponibilidade, na solicitação. Consulte uma lista dos IDs de zona em Endpoints.

As regras de nomenclatura a seguir se aplicam a buckets de diretório.

- O nome deve ser exclusivo na zona escolhida (zona de disponibilidade da AWS ou zona local da AWS).
- O nome deve ter entre 3 (mín.) e 63 (máx.) caracteres, incluindo o sufixo.
- Consistir em letras minúsculas, números e hifens (-).
- Inicie e termine com uma letra ou um número.
- Deve incluir o seguinte sufixo: `--`*`zone-id`*`--x-s3`.
- O nome do bucket não deve iniciar com o prefixo `xn--`.
- O nome do bucket não deve iniciar com o prefixo `sthree-`.
- O nome do bucket não deve iniciar com o prefixo `sthree-configurator`.
- O nome do bucket não deve iniciar com o prefixo `amzn-s3-demo-`.

- Os nomes de bucket não podem terminar com o sufixo `-s3alias`. Esse sufixo se reserva a nomes de alias de ponto de acesso. Para obter mais informações, consulte Alias de ponto de acesso.

- Os nomes de bucket não podem terminar com o sufixo `--ol-s3`. Esse sufixo é reservado a nomes de alias de ponto de acesso de objeto do Lambda. Para obter mais informações, consulte Como usar um alias no estilo do bucket para o ponto de acesso do Object Lambda do bucket do S3.
- Os nomes de bucket não podem terminar com o sufixo `.mrap`. Esse sufixo é reservado para nomes de ponto de acesso de várias regiões. Para obter mais informações, consulte Regras para nomear pontos de acesso multirregionais do Amazon S3.

.

7. Escolha Adicionar nova tag para abrir o editor de tags e inserir um par de chave-valor de tag. A chave de tag é necessária, mas o valor é opcional.
8. Para adicionar outra tag, selecione novamente Adicionar nova tag. É possível adicionar até cinquenta pares de chave-valor de tag.
9. Ao concluir a especificação das opções para seu novo bucket de diretório, escolha Criar bucket.

Uso dos SDKs da AWS

SDK for Java 2.x

Este exemplo mostra como criar um bucket de diretório com tags usando o AWS SDK for Java 2.x. Para usar o comando, substitua os *espaços reservados para entrada do usuário* por suas próprias informações.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3.S3Client;
import software.amazon.awssdk.services.s3.model.BucketInfo;
import software.amazon.awssdk.services.s3.model.BucketType;
import software.amazon.awssdk.services.s3.model.CreateBucketConfiguration;
import software.amazon.awssdk.services.s3.model.CreateBucketRequest;
import software.amazon.awssdk.services.s3.model.CreateBucketResponse;
import software.amazon.awssdk.services.s3.model.DataRedundancy;
import software.amazon.awssdk.services.s3.model.LocationInfo;
import software.amazon.awssdk.services.s3.model.LocationType;
import software.amazon.awssdk.services.s3.model.Tag;
```

```
public class CreateBucketWithTagsExample {
    public static void createBucketWithTagsExample() {
        S3Client s3 = S3Client.builder().region(Region.US_WEST_2).build();

        CreateBucketConfiguration bucketConfiguration =
 CreateBucketConfiguration.builder()
                .location(LocationInfo.builder()
                        .type(LocationType.AVAILABILITY_ZONE)
                        .name("usw2-az1").build())
                .bucket(BucketInfo.builder()
                        .type(BucketType.DIRECTORY)
                        .dataRedundancy(DataRedundancy.SINGLE_AVAILABILITY_ZONE)
                        .build())
                .tags(Tag.builder().key("MyTagKey").value("MyTagValue").build())
                .build();

        CreateBucketRequest createBucketRequest = CreateBucketRequest.builder()
                .bucket("amzn-s3-demo-bucket--usw2-az1--x-s3--usw2-az1--x-s3")
                .createBucketConfiguration(bucketConfiguration)
                .build();

        CreateBucketResponse response = s3.createBucket(createBucketRequest);
        System.out.println("Status code (should be 200):");
        System.out.println(response.sdkHttpResponse().statusCode());
    }
}
```

Uso da API REST

Para ter informações sobre a compatibilidade da API REST do Amazon S3 para criar um bucket de diretório com tags, consulte a seguinte seção na “Referência de API do Amazon Simple Storage Service”:

- CreateBucket

Como usar o AWS CLI

Para instalar a AWS CLI, consulte Instalar ou atualizar a versão mais recente da AWS CLI no Guia do usuário da versão 2 da AWS Command Line Interface.

O exemplo da CLI a seguir mostra como criar um bucket de diretório com tags usando o AWS CLI. Para usar o comando, substitua os *espaços reservados para entrada do usuário* por suas próprias informações.

Ao criar um bucket de diretório, você deve fornecer detalhes de configuração e usar a seguinte convenção de nomenclatura: *bucket-base-name*--*zone-id*--x-s3.

Solicitação:

```
aws s3api create-bucket \
--bucket bucket-base-name--zone-id--x-s3 \
--create-bucket-configuration "Location={Type=AvailabilityZone,Name=zone-
id},Bucket={DataRedundancy=SingleAvailabilityZone,Type=Directory},Tags=[{Key=mykey1,Value=myval
 {Key=mykey2,Value=myvalue2}]"
```

Resposta:

```
{
  "Location": "http://bucket--use1-az4--x-s3.s3express-use1-az4.us-
east-1.amazonaws.com/"
}
```

Adicionar uma tag a um bucket de diretório

É possível adicionar tags aos buckets de diretório do Amazon S3 e modificá-las. Não há cobrança adicional para usar tags em buckets de diretório além das taxas de solicitação padrão da API do S3. Para obter mais informações, consulte Preço do Amazon S3. Para ter mais informações sobre marcação de buckets de diretório, consulte Usar tags com buckets de diretório do S3.

Permissões

Para adicionar uma tag a um bucket de diretório, você precisa ter a seguinte permissão:

- `s3express:TagResource`

Solucionar de problemas de erros

Se você encontrar um erro ao tentar adicionar uma tag a um bucket de diretório, você pode fazer o seguinte:

- Verifique se você tem as Permissões necessárias para adicionar uma tag a um bucket de diretório.
- Se você tentou adicionar uma chave de tag que começa com o prefixo reservado `aws:` da AWS, altere-a e tente novamente.

Etapas

É possível adicionar tags a buckets de diretório usando o console do Amazon S3, a AWS Command Line Interface (AWS CLI), a API REST do Amazon S3 e SDKs da AWS.

Usar o console do S3

Para adicionar tags a um bucket de diretório usando o console do Amazon S3:

1. Faça login no console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets de diretório.
3. Escolha o nome do bucket.
4. Escolha a guia Properties (Propriedades).
5. Role até a seção Tags e escolha Adicionar nova tag.
6. Isso abre a página Adicionar tags. É possível adicionar até cinquenta pares de chave-valor de tag.
7. Se você adicionar uma nova tag com a mesma chave de uma tag existente, o valor da nova sobrescreverá o valor da tag existente.
8. Nessa página, também é possível editar os valor das tags existentes.
9. Depois de adicionar as tags, escolha Salvar alterações.

Uso dos SDKs da AWS

SDK for Java 2.x

Este exemplo mostra como adicionar tags a um bucket de diretório usando o AWS SDK for Java 2.x. Para usar o comando, substitua os *espaços reservados para entrada do usuário* por suas próprias informações.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.Tag;
import software.amazon.awssdk.services.s3control.model.TagResourceRequest;
import software.amazon.awssdk.services.s3control.model.TagResourceResponse;
```

```
public class TagResourceExample {
    public static void tagResourceExample() {
        S3ControlClient s3Control =
 S3ControlClient.builder().region(Region.US_WEST_2).build();

        TagResourceRequest tagResourceRequest = TagResourceRequest.builder()
                .resourceArn("arn:aws:s3express:us-west-2:111122223333:bucket/my-
directory-bucket--usw2-az1--x-s3")
                .accountId("111122223333")
                .tags(Tag.builder().key("MyTagKey").value("MyTagValue").build())
                .build();

        TagResourceResponse response = s3Control.tagResource(tagResourceRequest);
        System.out.println("Status code (should be 204):");
        System.out.println(response.sdkHttpResponse().statusCode());
    }
}
```

Uso da API REST

Para ter informações sobre a compatibilidade da API REST do Amazon S3 para adicionar tags a um bucket de diretório, consulte a seguinte seção na “Referência de API do Amazon Simple Storage Service”:

- TagResource

Como usar o AWS CLI

Para instalar a AWS CLI, consulte Instalar ou atualizar a versão mais recente da AWS CLI no Guia do usuário da versão 2 da AWS Command Line Interface.

O exemplo da CLI a seguir mostra como adicionar tags a um bucket de diretório usando a AWS CLI. Para usar o comando, substitua os *espaços reservados para entrada do usuário* por suas próprias informações.

Solicitação:

```
aws s3control tag-resource \
--account-id 111122223333 \
--resource-arn arn:aws:s3express:us-east-1:444455556666:bucket/prefix--use1-az4--x-s3 \
```

```
--tags "Key=mykey,Value=myvalue"
```

Resposta:

```
{
  "ResponseMetadata": {
      "RequestId": "EXAMPLE123456789",
      "HTTPStatusCode": 200,
      "HTTPHeaders": {
          "date": "Wed, 19 Jun 2025 10:30:00 GMT",
          "content-length": "0"
      },
      "RetryAttempts": 0
  }
}
```

Visualizar tags de buckets de diretório

É possível visualizar ou listar tags aplicadas aos buckets de diretório do S3. Para obter mais informações sobre tags, consulte Usar tags com buckets de diretório do S3.

Permissões

Para adicionar as tags aplicadas a um bucket de diretório, você precisa ter a seguinte permissão:

- `s3express:ListTagsForResource`

Solucionar de problemas de erros

Se você encontrar um erro ao tentar listar ou visualizar as tags de um bucket de diretório, é possível fazer o seguinte:

- Verifique se você tem as Permissões necessárias para visualizar ou listar as tags do bucket de diretório.

Etapas

Você pode visualizar tags aplicadas a buckets de diretório usando o console do Amazon S3, a AWS Command Line Interface (AWS CLI), a API REST do Amazon S3 e os SDKs da AWS.

Usar o console do S3

Para visualizar as tags aplicadas a um bucket de diretório usando o console do Amazon S3:

1. Faça login no console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets de diretório.
3. Escolha o nome do bucket.
4. Escolha a guia Properties (Propriedades).
5. Role até a seção Tags para visualizar todas as tags aplicadas ao bucket de diretório.
6. Por padrão, a seção Tags mostra as tags definidas elo usuário. Você pode selecionar a guia Tags geradas pela AWS para visualizar as tags aplicadas pelos serviços da AWS ao seu bucket de diretório.

Uso dos SDKs da AWS

Esta seção oferece um exemplo de como visualizar tags aplicadas a um bucket de diretório usando os SDKs da AWS.

SDK for Java 2.x

Este exemplo mostra como visualizar as tags aplicadas a um bucket de diretório usando o AWS SDK for Java 2.x.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.ListTagsForResourceRequest;
import software.amazon.awssdk.services.s3control.model.ListTagsForResourceResponse;

public class ListTagsForResourceExample {
    public static void listTagsForResourceExample() {
        S3ControlClient s3Control =
 S3ControlClient.builder().region(Region.US_WEST_2).build();

        ListTagsForResourceRequest listTagsForResourceRequest =
 ListTagsForResourceRequest.builder()
                .resourceArn("arn:aws:s3express:us-west-2:111122223333:bucket/my-
directory-bucket--usw2-az1--x-s3")
                .accountId("111122223333")
                .build();
```

```
        ListTagsForResourceResponse response =
 s3Control.listTagsForResource(listTagsForResourceRequest);
        System.out.println("Tags on my resource:");
        System.out.println(response.toString());
    }
}
```

Uso da API REST

Para ter informações sobre a compatibilidade da API REST do Amazon S3 para visualizar as tags aplicadas a um bucket de diretório, consulte a seguinte seção na “Referência de API do Amazon Simple Storage Service”:

- ListTagsforResource

Como usar o AWS CLI

Para instalar a AWS CLI, consulte Instalar ou atualizar a versão mais recente da AWS CLI no Guia do usuário da versão 2 da AWS Command Line Interface.

O exemplo de CLI a seguir mostra como visualizar as tags aplicadas a um bucket de diretório. Para usar o comando, substitua os *espaços reservados para entrada do usuário* por suas próprias informações.

Solicitação:

```
aws s3control list-tags-for-resource \
--account-id 111122223333 \
--resource-arn arn:aws:s3express:us-east-1:444455556666:bucket/prefix--use1-az4--x-s3 \
```

Resposta: tags presentes

```
{
  "Tags": [
      {
          "Key": "MyKey1",
          "Value": "MyValue1"
      },
      {
          "Key": "MyKey2",
          "Value": "MyValue2"
```

```
        },
        {
            "Key": "MyKey3",
            "Value": "MyValue3"
        }
    ]
}
```

Resposta: nenhuma tag presente

```
{
  "Tags": []
}
```

Excluir uma tag de um bucket de diretório

É possível remover tags dos buckets de diretório do S3. Uma tag da AWS é um par de chave-valor que contém metadados sobre recursos, neste caso buckets de diretório do Amazon S3. Para obter mais informações sobre tags, consulte Usar tags com buckets de diretório do S3.

> **Note**
>
> Se você excluir uma tag e depois descobrir que ela estava sendo usada para rastrear custos ou controlar o acesso, poderá adicionar a tag novamente ao bucket de diretório.

Permissões

Para excluir uma tag de um bucket de diretório, você precisa ter a seguinte permissão:

- `s3express:UntagResource`

Etapas

Você pode excluir tags de um bucket de diretório usando o console do Amazon S3, a AWS Command Line Interface (AWS CLI), a API REST do Amazon S3 e os SDKs da AWS.

Usar o console do S3

Para excluir tags de um bucket de diretório usando o console do Amazon S3:

1. Faça login no console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets de diretório.
3. Escolha o nome do bucket.
4. Escolha a guia Properties (Propriedades).
5. Role até a seção Tags e marque a caixa de seleção ao lado das tags que você gostaria de excluir.
6. Escolha Excluir.
7. O pop-up Excluir tags definidas pelo usuário é exibido e solicita que você confirme as tags selecionadas.
8. Escolha Delete para confirmar.

Uso dos SDKs da AWS

SDK for Java 2.x

Este exemplo mostra como excluir tags de um bucket de diretório usando o AWS SDK for Java 2.x. Para usar o comando, substitua os *espaços reservados para entrada do usuário* por suas próprias informações.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.UntagResourceRequest;
import software.amazon.awssdk.services.s3control.model.UntagResourceResponse;

public class UntagResourceExample {
    public static void untagResourceExample() {
        S3ControlClient s3Control =
 S3ControlClient.builder().region(Region.US_WEST_2).build();

        UntagResourceRequest untagResourceRequest = UntagResourceRequest.builder()
                .resourceArn("arn:aws:s3express:us-west-2:111122223333:bucket/my-
directory-bucket--usw2-az1--x-s3")
                .accountId("111122223333")
                .tagKeys("myTagKey")
                .build();

        UntagResourceResponse response =
 s3Control.untagResource(untagResourceRequest);
        System.out.println("Status code (should be 204):");
        System.out.println(response.sdkHttpResponse().statusCode());
```

```
    }
}
```

Uso da API REST

Para ter informações sobre a compatibilidade da API REST do Amazon S3 para excluir tags de um bucket de diretório, consulte a seguinte seção na “Referência de API do Amazon Simple Storage Service”:

- UnTagResource

Como usar o AWS CLI

Para instalar a AWS CLI, consulte Instalar ou atualizar a versão mais recente da AWS CLI no Guia do usuário da versão 2 da AWS Command Line Interface.

O exemplo da CLI a seguir mostra como excluir tags de um bucket de diretório usando a AWS CLI. Para usar o comando, substitua os *espaços reservados para entrada do usuário* por suas próprias informações.

Solicitação:

```
aws s3control untag-resource \
--account-id 111122223333 \
--resource-arn arn:aws:s3express:us-east-1:444455556666:bucket/prefix--use1-az4--x-s3 \
--tag-keys "tagkey1" "tagkey2"
```

Resposta:

```
{
  "ResponseMetadata": {
    "RequestId": "EXAMPLE123456789",
    "HTTPStatusCode": 204,
    "HTTPHeaders": {
        "date": "Wed, 19 Jun 2025 10:30:00 GMT",
        "content-length": "0"
    },
    "RetryAttempts": 0
  }
}
```

Trabalhar com a funcionalidade Tabelas do Amazon S3 e com buckets de tabela

A funcionalidade Tabelas do Amazon S3 fornece armazenamento do S3 otimizado para workloads de analytics, com recursos projetados para melhorar continuamente a performance das consultas e reduzir os custos de armazenamento de tabelas. A funcionalidade Tabelas do S3 foi criada especificamente para armazenar dados tabulares, como transações de compras diárias, dados de sensores de streaming ou impressões de anúncios. Os dados tabulares representam dados em colunas e linhas, como em uma tabela de banco de dados.

Os dados na funcionalidade Tabelas do S3 são armazenados em um novo tipo de bucket: um bucket de tabela, que armazena tabelas como sub-recursos. Os buckets de tabela oferecem suporte ao armazenamento de tabelas no formato Apache Iceberg. Usando instruções SQL padrão, você pode consultar as tabelas com mecanismos de consulta compatíveis com Iceberg, como Amazon Athena, Amazon Redshift e Apache Spark.

Tópicos

- Recursos da funcionalidade Tabelas do S3
- Serviços relacionados
- Tutorial: conceitos básicos da funcionalidade Tabelas do S3
- Buckets de tabela
- Manutenção da funcionalidade Tabelas do S3
- Namespaces de tabela
- Tabelas em buckets de tabela do S3
- Acessar dados da tabela
- Regiões da AWS, endpoints e cotas de serviço da funcionalidade Tabelas do S3
- Segurança para a funcionalidade Tabelas do S3
- Registro em log com o AWS CloudTrail para a funcionalidade Tabelas do S3

Recursos da funcionalidade Tabelas do S3

Armazenamento de tabelas com propósito específico

Os buckets de tabela do S3 são projetados especificamente para tabelas. Os buckets de tabela fornecem quantidades mais altas de transações por segundo (TPS) e melhor throughput de consultas em comparação com as tabelas autogerenciadas em buckets de uso geral do S3. Os buckets de tabela oferecem a mesma durabilidade, disponibilidade e escalabilidade de outros tipos de bucket do Amazon S3.

Suporte integrado para o Apache Iceberg

As tabelas nos buckets de tabela são armazenadas no formato Apache Iceberg. Você pode consultar essas tabelas usando SQL padrão em mecanismos de consulta compatíveis com Iceberg. O Iceberg tem uma variedade de recursos para otimizar a performance das consultas, incluindo evolução de esquemas e evolução de partições.

Com o Iceberg, você pode alterar a maneira como os dados são organizados para que possam evoluir com o tempo sem que precise reescrever as consultas ou reconstruir as estruturas de dados. O Iceberg foi projetado para ajudar a garantir a consistência e a confiabilidade dos dados por meio de suporte às transações. Para ajudar você a corrigir problemas ou realizar consultas de viagem no tempo, é possível acompanhar como os dados mudam ao longo do tempo e reverter para versões históricas.

Otimização automatizada de tabelas

Para otimizar as tabelas para consulta, o S3 executa continuamente operações automáticas de manutenção, como compactação, gerenciamento de snapshots e remoção de arquivos não referenciados. Essas operações aumentam a performance da tabela ao compactar objetos menores em menos arquivos maiores. As operações de manutenção também reduzem os custos de armazenamento ao limpar objetos não utilizados. Essa manutenção automatizada simplifica a operação de data lakes em grande escala, reduzindo a necessidade de manutenção manual das tabelas. Para cada tabela e bucket de tabela, você pode personalizar as configurações de manutenção.

Gerenciamento de acesso e segurança

Você pode gerenciar o acesso tanto para buckets de tabela quanto para tabelas individuais com o AWS Identity and Access Management (IAM) e as políticas de controle de serviço no AWS Organizations. A funcionalidade Tabelas do S3 usa um namespace de serviço diferente do Amazon S3: o namespace s3tables. Portanto, é possível criar políticas especificamente para a

funcionalidade Tabelas do S3 e seus recursos. Você pode criar políticas para conceder acesso a tabelas individuais, a todas as tabelas em um namespace de tabelas ou a buckets de tabela inteiros. Todas as configurações da funcionalidade Bloqueio de Acesso Público do Amazon S3 estão sempre habilitadas para buckets de tabela e não podem ser desabilitadas.

Integração com os serviços de analytics da AWS

É possível integrar automaticamente os buckets de tabela do Amazon S3 ao Amazon SageMaker Lakehouse por meio do console do S3. Essa integração permite que os serviços de analytics da AWS descubram e acessem dados de tabela automaticamente por meio do AWS Glue Data Catalog. Depois da integração, é possível trabalhar com as tabelas usando serviços de analytics, como o Amazon Athena, o Amazon Redshift, o QuickSight e outros. Para ter mais informações sobre como a integração funciona, consulte Usar tabelas do Amazon S3 com serviços de analytics da AWS.

Serviços relacionados

Você pode usar os Serviços da AWS a seguir com a funcionalidade Tabelas do S3 para oferecer suporte a aplicações de analytics específicas.

- Amazon Athena: o Athena é um serviço de consultas interativas que você pode usar para analisar dados no Amazon S3 usando SQL padrão. Você também pode usar o Athena para executar análises de dados de maneira interativa usando o Apache Spark sem a necessidade de planejamento, configuração ou gerenciamento de recursos. Ao executar aplicações do Apache Spark no Athena, você envia o código Spark para processamento e recebe os resultados de forma direta.
- AWS Glue: o AWS Glue é um serviço de integração de dados com tecnologia sem servidor que permite que você descubra, prepare, migre e integre dados de várias fontes. Você pode usar o AWS Glue para analytics, machine learning (ML) e desenvolvimento de aplicações. O AWS Glue também inclui outras ferramentas de produtividade e operações de dados para criação, execução de trabalhos e implementação de fluxos de trabalho de negócios.
- Amazon EMR: o Amazon EMR é uma plataforma de cluster gerenciada que simplifica a execução de frameworks de big data, como Apache Hadoop e Apache Spark, na AWS a fim de processar e analisar grandes volumes de dados.
- Amazon Redshift: o Amazon Redshift é um serviço de data warehouse na escala de petabytes na nuvem. Você pode usar o Amazon Redshift sem servidor para acessar e analisar dados sem

todas as configurações de um data warehouse provisionado. Os recursos são provisionados automaticamente e a capacidade do data warehouse escala de maneira inteligente para oferecer performance rápida até mesmo às workloads mais exigentes e imprevisíveis. O tempo em que o data warehouse fica ocioso não é cobrado, portanto você paga apenas pelo que usa. Você pode carregar dados e começar a consultar imediatamente no editor de consultas v2 do Amazon Redshift ou na sua ferramenta de business intelligence (BI) favorita.

- QuickSight: o QuickSight é um serviço de analytics de negócios para criar visualizações, executar análises ad hoc e extrair rapidamente insights dos dados. O QuickSight descobre facilmente as fontes de dados da AWS e oferece uma performance de consultas rápida e responsiva usando o SPICE (mecanismo de cálculo superrápido, paralelo e em memória) do QuickSight.
- AWS Lake Formation: o Lake Formation é um serviço gerenciado que simplifica o processo de configuração, proteção e gerenciamento de data lakes. O Lake Formation ajuda a descobrir suas fontes de dados para catalogar, limpar e transformar os dados. Com o Lake Formation, você pode gerenciar um controle de acesso refinado para os dados de um data lake no Amazon S3 e seus metadados no AWS Glue Data Catalog.

Tutorial: conceitos básicos da funcionalidade Tabelas do S3

Neste tutorial, você vai criar um bucket de tabela e integrar buckets de tabela em sua região com os serviços de analytics da AWS. Depois, você usará a AWS CLI para criar seu primeiro namespace e tabela no bucket de tabela. Por fim, você usará o AWS Lake Formation para conceder permissão na tabela a fim de poder começar a consultá-la com o Athena.

> **Tip**
>
> Caso esteja migrando dados tabulares de buckets de uso geral para buckets de tabela, a Biblioteca de Soluções da AWS tem uma solução guiada para ajudar você. Essa solução automatiza a movimentação de tabelas do Apache Iceberg e do Apache Hive registradas no AWS Glue Data Catalog e armazenadas em buckets de uso geral para buckets de tabela por meio do AWS Step Functions e o Amazon EMR com o Apache Spark. Consulte mais informações em Guidance for Migrating Tabular Data from Amazon S3 to S3 Tables na Biblioteca de Soluções da AWS.

Tópicos

- Etapa 1: criar um bucket de tabela e integrá-lo aos serviços de analytics da AWS

- Etapa 2: criar um namespace de tabela e uma tabela
- (Opcional) Etapa 3: conceder permissões do Lake Formation na tabela
- Etapa 4: consultar dados com SQL no Athena

Etapa 1: criar um bucket de tabela e integrá-lo aos serviços de analytics da AWS

Nesta etapa, use o console do Amazon S3 para criar seu primeiro bucket de tabela. Para conferir outras maneiras de criar um bucket de tabela, consulte Criar um bucket de tabela.

> **Note**
>
> Por padrão, o console do Amazon S3 integra automaticamente os buckets de tabela ao Amazon SageMaker Lakehouse, o que permite que os serviços de analytics da AWS descubram e acessem automaticamente seus dados de tabela do S3. Se criar seu primeiro bucket de tabela de maneira programática usando a AWS Command Line Interface (AWS CLI), os SDKs da AWS ou a API REST, você deverá concluir manualmente a integração dos serviços de analytics da AWS. Para obter mais informações, consulte Usar tabelas do Amazon S3 com serviços de analytics da AWS.

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Na barra de navegação na parte superior da página, escolha o nome da Região da AWS exibida no momento. Depois, escolha a região na qual você deseja criar o bucket de tabela.
3. No painel de navegação à esquerda, escolha Buckets de tabela.
4. Escolha Criar bucket de tabela.
5. Em Configuração geral, insira um nome para o bucket de tabela.

   O nome do bucket de tabela deve:

   - Ser exclusivo na sua Conta da AWS e na região atual.
   - Ter entre 3 e 63 caracteres.
   - Consistir apenas em letras minúsculas, números e hífens (-).
   - Inicie e termine com uma letra ou um número.

Após a criação do bucket, não é possível alterar o respectivo nome. O bucket de tabela pertence à Conta da AWS que o criou. Consulte mais informações sobre como nomear buckets de tabela em Regras de nomenclatura de buckets de tabela.

6. Na seção Integração com serviços de analytics da AWS, verifique se a caixa de seleção Habilitar integração está marcada.

   Se a opção Habilitar integração estiver selecionada quando você criar seu primeiro bucket de tabela usando o console, o Amazon S3 tentará integrar o bucket de tabela aos serviços de analytics da AWS. Essa integração permite que você use os serviços de analytics da AWS para acessar todas as tabelas na região atual. Para obter mais informações, consulte Usar tabelas do Amazon S3 com serviços de analytics da AWS.

7. Escolha Criar bucket.

Etapa 2: criar um namespace de tabela e uma tabela

Nesta etapa, você cria um namespace no bucket de tabela e, depois, cria uma tabela nesse namespace. É possível criar um namespace de tabela e uma tabela usando o console ou a AWS CLI.

> **Important**
>
> Ao criar tabelas, use apenas letras minúsculas nos nomes e nas definições das tabelas. Por exemplo, os nomes das colunas devem estar todos em minúsculas. Se o nome da tabela ou a definição da tabela contiver letras maiúsculas, a tabela não será compatível com o AWS Lake Formation ou o AWS Glue Data Catalog. Nesse caso, a tabela não estará visível para serviços de analytics da AWS, como o Amazon Athena, mesmo que os buckets de tabela estejam integrados aos serviços de analytics da AWS.
>
> Se a definição da tabela contiver letras maiúsculas, você receberá a seguinte mensagem de erro ao executar uma consulta `SELECT` no Athena: “GENERIC_INTERNAL_ERROR: Get table request failed: com.amazonaws.services.glue.model.ValidationException: Unsupported Federation Resource - Invalid table or column names”.

Usar o console do S3 e o Amazon Athena

O procedimento a seguir usa o console do Amazon S3 para criar um namespace e uma tabela com o Amazon Athena.

Como criar um namespace de tabela e uma tabela

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets de tabela.
3. Na página Buckets de tabela, escolha o bucket de tabela no qual você deseja criar uma tabela.
4. Na página de detalhes do bucket de tabela, escolha Criar tabela com o Athena.
5. Na caixa de diálogo Criar tabela com o Athena, escolha Criar um namespace e insira um nome no campo Nome do namespace. Os nomes de namespace devem ter de 1 a 255 caracteres e ser exclusivos no bucket de tabela. Os caracteres válidos são a–z, 0–9 e sublinhado (_). Sublinhados não são permitidos no início dos nomes de namespace.
6. Escolha Create namespace (Criar namespace).
7. Escolha Criar tabela com o Athena.
8. O console do Amazon Athena é aberto e o editor de consultas do Athena aparece. O editor de consultas é preenchido com uma consulta de exemplo que você pode usar para criar uma tabela. Modifique a consulta para especificar o nome da tabela e as colunas que você deseja que a tabela tenha.
9. Quando terminar de modificar a consulta, escolha Executar para criar a tabela.

Se a criação da tabela tiver sido bem-sucedida, o nome da nova tabela aparecerá na lista de tabelas do Athena. Ao voltar para o console do Amazon S3, a nova tabela aparecerá na lista Tabelas na página de detalhes do bucket de tabela depois que você atualizar a lista.

Como usar o AWS CLI

Para usar os exemplos de comando da AWS CLI a seguir para criar um namespace no bucket de tabela e, depois, criar uma tabela com um esquema nesse namespace, substitua os valores de *`user input placeholder`* pelos seus próprios.

Pré-requisitos

- Anexe a política `AmazonS3TablesFullAccess` à identidade do IAM.

- Instale a AWS CLI versão 2.23.10 ou posterior. Para obter mais informações, consulte Instalar ou atualizar a versão mais recente da AWS CLI no Guia do usuário do AWS Command Line Interface.

1. Crie um namespace no bucket de tabela executando o seguinte comando:

```
aws s3tables create-namespace \
--table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-table-bucket \
--namespace my_namespace
```

   - Confirme se o namespace foi criado com sucesso executando o seguinte comando:

```
aws s3tables list-namespaces \
--table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-table-bucket
```

2. Crie uma tabela com um esquema de tabela executando o seguinte comando:

```
aws s3tables create-table --cli-input-json file://mytabledefinition.json
```

   Para o arquivo `mytabledefinition.json`, use o seguinte exemplo de definição de tabela:

```
{
    "tableBucketARN": "arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-table-bucket",
    "namespace": "my_namespace",
    "name": "my_table",
    "format": "ICEBERG",
    "metadata": {
        "iceberg": {
            "schema": {
                "fields": [
                     {"name": "id", "type": "int","required": true},
                     {"name": "name", "type": "string"},
                     {"name": "value", "type": "int"}
                ]
            }
        }
    }
}
```

(Opcional) Etapa 3: conceder permissões do Lake Formation na tabela

Nesta etapa, você concede permissões do Lake Formation na nova tabela a outras entidades principais do IAM. Essas permissões autorizam que outras entidades principais, além de você, acessem os recursos do bucket de tabela usando o Athena e outros serviços de analytics da AWS. Para obter mais informações, consulte Conceder permissão em uma tabela ou um banco de dados. Se você for o único usuário que acessará as tabelas, poderá pular essa etapa.

1. Abra o console do AWS Lake Formation em https://console.aws.amazon.com/lakeformation/ e faça login como administrador do data lake. Consulte mais informações sobre como criar um administrador de data lake em Create a data lake administrator.
2. No painel de navegação, escolha Permissões de dados e Conceder.
3. Na página Conceder permissões, em Entidades principais, escolha Usuários e perfis do IAM e selecione o usuário ou o perfil do IAM que você deseja permitir que execute consultas na tabela.
4. Em Tags do LF ou recursos de catálogo, escolha Recursos do catálogo de dados nomeados.
5. Execute um destes procedimentos, dependendo se deseja conceder acesso a todas as tabelas da conta ou se deseja conceder acesso somente aos recursos dentro do bucket de tabela que você criou:
   - Em Catálogos, escolha um catálogo no nível da conta que você criou ao integrar o bucket de tabela. Por exemplo, .*111122223333*:s3tablescatalog
   - Em Catálogos, escolha o subcatálogo para o bucket de tabela. Por exemplo, .*111122223333*:s3tablescatalog/*amzn-s3-demo-table-bucket*
6. (Opcional) Se você escolheu o subcatálogo para o bucket de tabela, execute um ou ambos os procedimentos:
   - Em Bancos de dados, escolha o namespace do bucket de tabela que você criou.
   - Em Tabelas, escolha a tabela que você criou no bucket de tabelas ou escolha Todas as tabelas.
7. Será possível definir permissões em nível de catálogo, banco de dados ou tabela, dependendo de você ter escolhido um catálogo ou subcatálogo e, depois, um banco de dados ou uma tabela. Consulte mais informações sobre as permissões do Lake Formation em Managing Lake Formation permissions no Guia do desenvolvedor do AWS Lake Formation.

   Execute um destes procedimentos:
   - Em Permissões de catálogo, escolha Super para conceder a outra entidade principal todas as permissões no catálogo ou escolha permissões mais detalhadas, como Descrever.

- Em Permissões de banco de dados, você não pode escolher Super para conceder a outra entidade principal todas as permissões no banco de dados. Em vez disso, escolha permissões mais detalhadas, como Descrever.
- Em Permissões de tabela, escolha Super para conceder a outra entidade principal todas as permissões na tabela ou escolha permissões mais detalhadas, como Selecionar ou Descrever.

> **Note**
>
> Quando você concede permissões do Lake Formation em um recurso do catálogo de dados para uma conta externa ou diretamente para uma entidade principal do IAM em outra conta, o Lake Formation usa o serviço do AWS Resource Access Manager (AWS RAM) para compartilhar o recurso. Se a conta do concedido estiver na mesma organização da conta do concedente, o recurso compartilhado estará disponível imediatamente para o concedido. Se a conta do concedido não estiver na mesma organização, o AWS RAM envia um convite à conta do concedido para aceitar ou rejeitar a concessão do recurso. Em seguida, para disponibilizar o recurso compartilhado, o administrador do data lake deve usar o console AWS RAM ou AWS CLI para aceitar o convite na conta do concedido. Consulte mais informações sobre o compartilhamento de dados entre contas em Cross-account data sharing in Lake Formation no Guia do desenvolvedor do AWS Lake Formation.

8. Selecione Conceder.

Etapa 4: consultar dados com SQL no Athena

Você pode consultar a tabela com SQL no Athena. O Athena é compatível com consultas Data Definition Language (DDL), Data Manipulation Language (DML) e Data Query Language (DQL) para Tabelas do S3.

É possível acessar a consulta do Athena pelo console do Amazon S3 ou pelo console do Amazon Athena.

Usar o console do S3 e o Amazon Athena

O procedimento a seguir usa o console do Amazon S3 para acessar o editor de consultas do Athena e possibilitar que você consulte uma tabela com o Amazon Athena.

Como consultar uma tabela

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets de tabela.
3. Na página Buckets de tabela, escolha o bucket de tabela que contém a tabela que você deseja consultar.
4. Na página de detalhes do bucket de tabela, escolha o botão de opção ao lado do nome da tabela que você deseja consultar.
5. Escolha Consultar tabela com o Athena.
6. O console do Amazon Athena é aberto e o editor de consultas do Athena aparece com uma amostra de consulta SELECT carregada para você. Modifique essa consulta conforme necessário para seu caso de uso.
7. Para executar a consulta, escolha Run (Executar).

Usar o console do Amazon Athena

Como consultar uma tabela

1. Abra o console do Athena em https://console.aws.amazon.com/athena/.
2. Consulte a tabela. Veja a seguir uma amostra de consulta que você pode modificar. Substitua *user input placeholders* por suas próprias informações.

```
SELECT * FROM "s3tablescatalog/amzn-s3-demo-table-bucket"."my_namespace"."my_table"
 LIMIT 10
```

3. Para executar a consulta, escolha Run (Executar).

Buckets de tabela

Os buckets de tabela do Amazon S3 são um tipo de bucket do S3 que você pode usar para criar e armazenar tabelas como recursos do S3. Os buckets de tabela são usados para armazenar dados tabulares e metadados como objetos para uso em workloads de analytics. O S3 realiza a manutenção nos buckets de tabela automaticamente para ajudar a reduzir os custos de armazenamento de tabelas. Para obter mais informações, consulte Manutenção para buckets de tabela.

Para interagir com as tabelas armazenadas nos buckets de tabela, você pode integrar os buckets de tabela a aplicações de analytics compatíveis com Apache Iceberg. Os buckets de tabela se integram aos serviços de analytics da AWS por meio do AWS Glue Data Catalog. Para obter mais informações, consulte Usar tabelas do Amazon S3 com serviços de analytics da AWS. Você também pode interagir com as tabelas utilizando mecanismos de consulta de código aberto usando o Catálogo de Tabelas do Amazon S3 para Apache Iceberg. Para obter mais informações, consulte Acessar tabelas usando o endpoint Iceberg REST do serviço Tabelas do Amazon S3.

Cada bucket de tabela tem um nome do recurso da Amazon (ARN) exclusivo e uma política de recurso associada a ele. Os ARNs de buckets de tabela seguem este formato:

```
arn:aws:s3tables:Region:OwnerAccountID:bucket/bucket-name
```

Todas as tabelas e buckets de tabela são privados e não podem ser tornados públicos. Esses recursos só podem ser acessados por usuários que tenham recebido acesso explícito. Para conceder acesso, você pode usar políticas baseadas em recurso do IAM para tabelas e buckets de tabela, e políticas baseadas em identidade do IAM para usuários e perfis.

Por padrão, você pode criar até dez buckets de tabela por Região da AWS em uma Conta da AWS. Para solicitar um aumento da cota de tabelas e de buckets de tabela, entre em contato com o Suporte.

Há vários tipos de bucket do Amazon S3. Antes de criar um bucket, escolha o tipo de bucket que melhor se adapte aos requisitos de performance e da aplicação. Para obter mais informações sobre os vários tipos de bucket e os casos de uso apropriados para cada um, consulte Buckets.

Tópicos

- Regras de nomenclatura de buckets de tabela, tabelas e namespaces do Amazon S3
- Criar um bucket de tabela
- Excluir um bucket de tabela
- Visualizar detalhes sobre um bucket de tabela do Amazon S3
- Gerenciar políticas de buckets de tabela

Regras de nomenclatura de buckets de tabela, tabelas e namespaces do Amazon S3

Ao criar um bucket de tabela, escolha um nome de bucket e uma Região da AWS. O nome deve ser exclusivo dentro da conta na região escolhida. Depois de criar um bucket de tabela, você não poderá mais alterar o respectivo nome ou região. Os nomes dos buckets de tabela devem seguir regras de nomenclatura específicas. Para ter mais informações sobre as regras de nomenclatura para os buckets de tabela e para as tabelas e os namespaces dentro deles, consulte o tópico a seguir.

Tópicos

- Regras de nomenclatura de buckets de tabela
- Regras de nomenclatura para tabelas e namespaces

Regras de nomenclatura de buckets de tabela

Ao criar buckets de tabela do Amazon S3, especifique um nome de bucket de tabela. Como outros tipos de bucket, não é possível renomear os buckets de tabela. Ao contrário de outros tipos de bucket, os buckets de tabela não estão em um namespace global, então cada nome de bucket na conta só precisa ser exclusivo apenas na região da AWS atual.

Para conferir as regras de nomenclatura para buckets de uso geral, consulte Regras de nomenclatura de buckets de uso geral. Consulte as regras de nomenclatura de buckets de diretório em Regras de nomenclatura de buckets de diretório.

As regras de nomenclatura a seguir se aplicam aos buckets de tabela.

- Os nomes dos buckets devem ter entre 3 e 63 caracteres.
- Os nomes de bucket podem consistir apenas em letras minúsculas, números e hífenes (-).
- Os nomes dos buckets devem começar e terminar com uma letra ou um número.
- Os nomes de bucket não devem conter sublinhados (_) nem pontos (.).
- Os nomes de bucket não devem começar com os seguintes prefixos:
  - `xn--`
  - `sthree-`
  - `amzn-s3-demo-`
- Os nomes de bucket não devem terminar com os seguintes prefixos:

- `-s3alias`
- `--ol-s3`
- `--x-s3`
- `--table-s3`

Regras de nomenclatura para tabelas e namespaces

As seguintes regras de nomenclatura se aplicam a tabelas e namespaces dentro de buckets de tabela:

- Os nomes devem ter entre 1 e 255 caracteres.
- Os nomes só podem consistir em letras minúsculas, números e sublinhados (_). Sublinhados não são permitidos no início ou no final dos nomes de namespace.
- Os nomes devem começar e terminar com uma letra ou um número.
- Os nomes não devem conter hifens (-) nem pontos (.).
- O nome da tabela deve ser único dentro de um namespace.
- Um namespace deve ser único dentro de um bucket de tabela.
- Os nomes de namespaces não devem começar com o prefixo reservado `aws`. Não é possível usar `aws_s3_metadata` como namespace. `aws_s3_metadata` é um namespace reservado para tabelas de metadados. Para obter mais informações, consulte Acelerar a descoberta de dados com o S3 Metadata.

Criar um bucket de tabela

Os buckets de tabela do Amazon S3 são um tipo de bucket do S3 que você pode usar para criar e armazenar tabelas como recursos do S3. Para começar a usar a funcionalidade Tabelas do S3, crie um bucket de tabela para armazenar e gerenciar as tabelas. Ao criar um bucket de tabela, você escolhe um nome de bucket e uma Região da AWS. O nome do bucket de tabela deve ser exclusivo para a conta na região escolhida. Depois de criar um bucket de tabela, você não poderá mais alterar o respectivo nome ou região. Para ter mais informações sobre a nomeação de buckets de tabela, consulte Regras de nomenclatura de buckets de tabela, tabelas e namespaces do Amazon S3.

Os buckets de tabela têm o seguinte formato de nome do recurso da Amazon (ARN):

```
arn:aws:s3tables:region:owner-account-id:bucket/bucket-name
```

Por padrão, é possível criar até dez buckets de tabela por região em uma Conta da AWS. Para solicitar um aumento da cota de tabelas e de buckets de tabela, entre em contato com o Suporte.

Ao criar um bucket de tabela, você pode especificar o tipo de criptografia que será usado para criptografar as tabelas criadas nesse bucket. Para ter mais informações sobre as opções de criptografia de bucket, consulte the section called “Criptografia”.

Pré-requisitos para a criação de buckets de tabela

Para criar um bucket de tabela, primeiro é necessário fazer o seguinte:

- Você deve ter permissões do AWS Identity and Access Management (IAM) para `s3tables:CreateTableBucket`.

> **Note**
>
> Se você escolher SSE-KMS como o tipo de criptografia padrão, deverá ter permissões para `s3tables:PutTableBucketEncryption` e a permissão `DescribeKey` na chave do AWS KMS escolhida. Além disso, a chave AWS KMS que você usa precisa conceder permissão à funcionalidade Tabelas do S3 para que realize a manutenção automática de tabelas. Para obter mais informações, consulte Requisitos de permissão para criptografia SSE-KMS da funcionalidade Tabelas do S3.

Para criar um bucket de tabela, é possível usar o console do Amazon S3, a API REST do Amazon S3, a AWS Command Line Interface (AWS CLI) ou os SDKs da AWS.

Uso do console do S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Na barra de navegação na parte superior da página, escolha o nome da Região da AWS exibida no momento. Em seguida, escolha a região na qual você deseja criar um bucket.
3. No painel de navegação à esquerda, escolha Buckets de tabela.
4. Escolha Criar bucket de tabela para abrir a página Criar bucket de tabela.
5. Em Propriedades, insira um nome para o bucket de tabela.

   O nome do bucket de tabela deve:

- Ser exclusivo na sua conta e na região atual.
- Ter entre 3 e 63 caracteres.
- Consistir apenas em letras minúsculas, números e hífens (-).
- Inicie e termine com uma letra ou um número.

Depois de criado o bucket, você não pode mudar seu nome. A Conta da AWS que cria o bucket é a proprietária do bucket. Para ter mais informações sobre a nomeação de buckets de tabela, consulte Regras de nomenclatura de buckets de tabela, tabelas e namespaces do Amazon S3.

6. Se você quiser integrar os buckets de tabela aos serviços de analytics da AWS, selecione a opção Habilitar integração em Integração com serviços de analytics da AWS.

> **Note**
>
> Quando você cria seu primeiro bucket de tabela usando o console com a opção Habilitar integração selecionada, o Amazon S3 tenta integrar automaticamente o bucket de tabela aos serviços de analytics da AWS. Essa integração permite que você use os serviços de analytics da AWS para consultar todas as tabelas na região atual. Para obter mais informações, consulte Usar tabelas do Amazon S3 com serviços de analytics da AWS.

7. Para configurar a criptografia padrão, em Tipo de criptografia, selecione uma das seguintes opções:

   - Criptografia do lado do servidor com chave gerenciada pelo Amazon S3 (SSE-S3)
   - Criptografia do lado do servidor com chave do AWS Key Management Service (SSE-KMS)

   Para ter mais informações sobre as opções de criptografia para dados de tabela, consulte Proteger os dados de tabela do S3 com criptografia.

8. Escolha Criar bucket.

Como usar o AWS CLI

Esse exemplo mostra como criar um bucket de tabela usando a AWS CLI. Para usar esse exemplo, substitua os *`user input placeholders`* por suas próprias informações.

```
aws s3tables create-table-bucket \
```

```
    --region us-east-2 \
    --name amzn-s3-demo-bucket1
```

Por padrão, os buckets de tabela do S3 usam SSE-S3 como configuração de criptografia padrão, mas você pode usar o parâmetro opcional `--encryption-configuration` para especificar um tipo de criptografia diferente. O exemplo a seguir mostra como criar um bucket que usa a criptografia SSE-KMS. Para ter mais informações sobre configurações de criptografia para buckets de tabela, consulte Proteger os dados de tabela do S3 com criptografia.

```
aws s3tables create-table-bucket \
    --region us-east-2 \
    --name amzn-s3-demo-bucket1
    --encryption-configuration '{
                    "sseAlgorithm": "aws:kms",
                    "kmsKeyArn":
 "arn:aws:kms:Region:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab" }'
```

Excluir um bucket de tabela

Você pode usar as APIs do Amazon S3, a AWS Command Line Interface, ou os AWS SDKs para excluir um bucket de tabela. Antes de excluir um bucket de tabela, você deve excluir todos os namespaces e tabelas dentro do bucket.

Uso do AWS CLI

Esse exemplo mostra como excluir um bucket de tabela usando a AWS CLI. Para usar esse exemplo, substitua os *espaços reservados para entrada do usuário* por suas próprias informações.

```
aws s3tables delete-table-bucket \
    --region us-east-2 \
    --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-
bucket1
```

Visualizar detalhes sobre um bucket de tabela do Amazon S3

É possível visualizar os detalhes de um bucket de tabelas do Amazon S3 de maneira programática usando a API REST de Tabelas do S3, a AWS CLI ou os SDKs da AWS.

Uso do AWS CLI

Esse exemplo mostra como obter os detalhes de um bucket de tabela usando a AWS CLI. Para usar esse exemplo, substitua os *espaços reservados para entrada do usuário* por suas próprias informações.

```
aws s3tables get-table-bucket --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-bucket1
```

Gerenciar políticas de buckets de tabela

Você pode adicionar, excluir, atualizar e visualizar políticas para buckets de tabela do Amazon S3 usando a API REST do Amazon S3, os AWS SDKs e a AWS Command Line Interface (AWS CLI). Para obter mais informações, consulte os tópicos a seguir.

Para obter mais informações, consulte os tópicos a seguir. Para ter mais informações sobre as chaves de condição e ações do AWS Identity and Access Management (IAM) compatíveis com a funcionalidade Tabelas do Amazon S3, consulte Gerenciamento de acesso para a funcionalidade Tabelas do S3. Para conferir exemplos de políticas para buckets de tabela, consulte Políticas baseadas em recurso para a funcionalidade Tabelas do S3.

Adicionar uma política de bucket de tabela

Para adicionar uma política a um bucket de tabela, use o exemplo da AWS CLI a seguir.

Uso do AWS CLI

Esse exemplo mostra como criar uma política de bucket de tabela usando a AWS CLI. Para usar o comando, substitua os *user input placeholders* por suas próprias informações.

```
aws s3tables put-table-bucket-policy \
    --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-bucket1  \
    --resource-policy your-policy-JSON
```

Visualizar uma política de bucket de tabela

Para visualizar uma política que está anexada a um bucket de tabela, use o exemplo da AWS CLI a seguir.

Uso do AWS CLI

Esse exemplo mostra como visualizar a política que está anexada a um bucket de tabela usando a AWS CLI. Para usar o comando, substitua os *user input placeholders* por suas próprias informações.

```
aws s3tables get-table-bucket-policy --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-bucket1
```

Excluir uma política de bucket de tabela

Para excluir uma política que está anexada a um bucket de tabela, use o exemplo da AWS CLI a seguir.

Uso do AWS CLI

Esse exemplo mostra como excluir uma política de bucket de tabela usando a AWS CLI. Para usar o comando, substitua os *user input placeholders* por suas próprias informações.

```
aws s3tables delete-table-bucket-policy --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-bucket1
```

Manutenção da funcionalidade Tabelas do S3

O Amazon S3 executa a manutenção automaticamente para aprimorar o desempenho das tabelas em buckets de tabela do S3. A manutenção é realizada no bucket de tabela e em cada tabela e inclui o seguinte:

Manutenção em nível de bucket de tabela:

- Remoção de arquivos sem referência: limpa arquivos órfãos para otimizar o uso e os custos do armazenamento.

Manutenção em nível de tabela:

- Compactação de arquivos: consolida arquivos pequenos para melhorar o desempenho das consultas e reduzir os custos de armazenamento.
- Gerenciamento de snapshots: controla o histórico de versões da tabela e evita o aumento excessivo de metadados.

Essas opções não são permitidas por padrão. Você pode editar ou desabilitar essas operações por meio de arquivos de configuração de manutenção.

Tópicos

- Status de trabalhos de manutenção da funcionalidade Tabelas do S3
- Manutenção para buckets de tabela
- Manutenção de tabelas
- Considerações e limitações para trabalhos de manutenção

Status de trabalhos de manutenção da funcionalidade Tabelas do S3

Os trabalhos de manutenção da funcionalidade Tabelas do S3 são executados periodicamente para as tabelas ou os buckets de tabela do S3. Você pode consultar o status desses trabalhos com a API `GetTableMaintenanceJobStatus`.

Como obter o status de trabalhos de manutenção usando a AWS CLI

O exemplo a seguir obterá os status de trabalhos de manutenção usando a API `GetTableMaintenanceJobStatus`.

```
aws s3tables get-table-maintenance-job-status \
   --table-bucket-arn="arn:aws:s3tables:arn:aws::111122223333:bucket/amzn-s3-demo-bucket1" \
   --namespace="mynamespace" \
   --name="testtable"
```

Para obter mais informações, consulte get-table-maintenance-job-status na Referência de comandos da AWS CLI.

Os trabalhos de manutenção da funcionalidade Tabelas do S3 podem transitar entre quatro status possíveis:

- `Successful`
- `Failed`
- `Disabled`
- `Not_Yet_Run`

Os trabalhos com status de falha incluirão uma mensagem de falha. A lista a seguir descreve possíveis mensagens de falha.

- Foi encontrada uma exceção de validação do Iceberg ao tentar ler a tabela. Verifique se sua tabela está legível, segue a especificação do Iceberg e contém somente caminhos do S3 que começam com o alias de tabela do S3.
- No momento, o gerenciamento de snapshots do Iceberg não aceita tags ou referências definidas pelo usuário.
- A configuração de manutenção de tabelas do Iceberg é incompatível com as propriedades de tabela “history.expire.max-snapshot-age-ms” e “history.expire.min-snapshots-to-keep”.
- O gerenciamento de snapshots do Iceberg e a remoção de arquivos sem referência não são compatíveis quando a propriedade de tabela “gc.enabled” está definida como falsa. Essa propriedade não deve estar definida ou explicitamente definida como verdadeira.
- Falha na confirmação devido a metadados desatualizados. A manutenção será repetida na próxima oportunidade disponível.
- Acesso insuficiente para realizar manutenção de tabelas. A chave usada para criptografar a tabela deve estar ativa e ter uma política de recursos que conceda acesso à entidade principal de serviço `maintenance.s3tables.amazonaws.com` do S3.

  > **Note**
  >
  > Para ter mais informações sobre as permissões do AWS KMS para Tabelas do S3, consulte Requisitos de permissão para criptografia SSE-KMS da funcionalidade Tabelas do S3.

- Erro interno

Manutenção para buckets de tabela

O Amazon S3 oferece operações de manutenção para aprimorar o gerenciamento e a performance dos buckets de tabela. A opção a seguir é habilitada por padrão para todos os buckets de tabela. Você pode editar ou desabilitar essa opção especificando um arquivo de configuração de manutenção para o bucket de tabela.

A edição dessa configuração requer a permissão `s3tables:PutTableBucketMaintenanceConfiguration`.

Tópicos

- Remoção de arquivos sem referência
- Considerações e limitações

Remoção de arquivos sem referência

A remoção de arquivos sem referência identifica e exclui todos os objetos que não são referidos por nenhum snapshot de tabela. Como parte da política de remoção de arquivos sem referência, você pode configurar duas propriedades: `unreferencedDays` (três dias por padrão) e `nonCurrentDays` (dez dias por padrão).

Para qualquer objeto não referenciado pela tabela e mais antigo que a propriedade `unreferencedDays`, o S3 marca o objeto como desatualizado. O S3 exclui objetos desatualizados após o número de dias especificado pela propriedade `nonCurrentDays`.

> **Note**
>
> As exclusões de objetos desatualizados são permanentes, sem nenhuma maneira de recuperá-los.

Para visualizar ou recuperar objetos que foram marcados como desatualizados, você deve entrar em contato com o AWS Support. Para obter informações sobre como entrar em contato com o AWS Support, consulte Entrar em contato com a AWS ou a Documentação do AWS Support.

A remoção de arquivos não referenciados determina os objetos a serem excluídos de uma tabela somente com referência a essa tabela. Qualquer referência feita a esses objetos fora da tabela não impedirá que a remoção de arquivos não referenciados exclua um objeto.

Se você desativar a remoção de arquivos não referenciados, nenhum trabalho em andamento será afetado. A nova configuração entrará em vigor no próximo trabalho após a alteração da configuração. Para ter mais informações, consulte as informações sobre preços na Definição de preço do Amazon S3.

Você só pode configurar a remoção de arquivos não referenciados ao nível do bucket de tabela. Essa configuração se aplicará a todas as tabelas do bucket.

Como configurar a remoção de arquivos não referenciados usando a AWS CLI

O exemplo a seguir definirá `unreferencedDays` como 4 dias e `nonCurrentDays` como 10 dias usando a API `PutTableBucketMaintenanceConfiguration`.

```
aws s3tables put-table-bucket-maintenance-configuration \
   --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-
table-bucket \
   --type icebergUnreferencedFileRemoval \
   --value '{"status":"enabled","settings":{"icebergUnreferencedFileRemoval":
{"unreferencedDays":4,"nonCurrentDays":10}}}'
```

Para obter mais informações, consulte put-table-bucket-maintenance-configuration na Referência de comandos da AWS CLI.

Considerações e limitações

Para saber mais sobre considerações adicionais e limites para remoção de arquivos não referenciados, consulte the section called “Considerações e limitações”.

Manutenção de tabelas

O serviço Tabelas do S3 oferece operações de manutenção para aprimorar o gerenciamento e o desempenho de tabelas individuais. As opções a seguir estão habilitadas por padrão para todas as tabelas em buckets de tabela. Você pode editar ou desabilitar essas opções especificando arquivos de configuração de manutenção para a tabela do S3.

A edição dessa configuração requer as permissões `s3tables:GetTableMaintenanceConfiguration` e `s3tables:PutTableMaintenanceConfiguration`.

Tópicos

- Compactação
- Gerenciamento de snapshots
- Considerações e limitações

Compactação

A compactação é configurada no nível da tabela e combina vários objetos menores em menos objetos maiores a fim de melhorar o desempenho de consulta do Apache Iceberg. Ao combinar objetos, a compactação também aplica os efeitos das exclusões em nível de linha na tabela.

A compactação está habilitada por padrão para todas as tabelas, com um tamanho de arquivo de destino padrão de 512 MB ou um valor personalizado de 64 MB a 512 MB especificado por você. Os arquivos compactados são gravados como o snapshot mais recente da tabela.

Estratégias de compactação

Você pode escolher entre várias estratégias de compactação que podem aumentar ainda mais o desempenho da consulta, dependendo dos padrões de consulta e da ordem de classificação da tabela.

O serviço Tabelas do S3 permite estas estratégias de compactação para tabelas:

- Auto (padrão)
  - O Amazon S3 seleciona a melhor estratégia de compactação com base na ordem de classificação da tabela. Essa é a estratégia de compactação padrão para todas as tabelas.
  - Para tabelas com uma ordem de classificação definida nos respectivos metadados, `auto` aplicará automaticamente a compactação `sort`.
  - Para tabelas sem uma ordem de classificação, `auto` usará por padrão a compactação `binpack`.
- Binpack
  - Combina arquivos pequenos em arquivos maiores, geralmente visando tamanhos acima de 100 MB, enquanto aplica quaisquer exclusões pendentes. Essa é a estratégia de compactação padrão para tabelas não classificadas.
- Sort
  - Organiza os dados com base em colunas especificadas que são classificadas automaticamente por hierarquia durante a compactação, melhorando o desempenho da consulta para operações filtradas. Essa estratégia é recomendada quando suas consultas filtram colunas específicas com frequência. Quando você usa essa estratégia, o serviço Tabelas do S3 aplica automaticamente a classificação hierárquica nas colunas quando `sort_order` é definido nas propriedades da tabela.
- Z-order

- Otimiza a organização dos dados combinando vários atributos em um único valor escalar que pode ser usado para classificação, permitindo consultas eficientes em várias dimensões. Essa estratégia é recomendada quando você precisa consultar dados em várias dimensões simultaneamente. Ela exige que você defina uma ordem de classificação nas propriedades de tabela do Iceberg usando a propriedade de tabela `sort_order`.

A compactação incorrerá em custos adicionais. Para ter mais informações, consulte as informações sobre preços na Definição de preço do Amazon S3.

Exemplos de compactação

Os exemplos a seguir mostram configurações para compactação de tabelas.

Como configurar o tamanho do arquivo de destino de compactação usando a AWS CLI

O tamanho mínimo do arquivo de compactação de destino é 64 MB; o máximo é 512 MB.

O exemplo a seguir alterará o tamanho do arquivo de destino para 256 MB usando a API `PutTableMaintenanceConfiguration`.

```
aws s3tables put-table-maintenance-configuration \
   --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-
bucket1 \
   --type icebergCompaction \
   --namespace mynamespace \
   --name testtable \
   --value='{"status":"enabled","settings":{"icebergCompaction":
{"targetFileSizeMB":256}}}'
```

Para obter mais informações, consulte put-table-maintenance-configuration na Referência de comandos da AWS CLI.

Como configurar a estratégia de compactação usando a AWS CLI

O exemplo a seguir mudará a estratégia de compactação para `sort` usando a API `PutTableMaintenanceConfiguration`. Ao definir a compactação, você pode escolher entre as seguintes estratégias de compactação: `auto`, `binpack`, `sort` ou `z-order`

> **Note**
>
> Para definir a estratégia de compactação como `sort` ou `z-order`, você precisa atender aos seguintes pré-requisitos:
>
> - Uma ordem de classificação definida nas propriedades de tabela do Iceberg.
> - A permissão `s3tables:GetTableData`.

```
aws s3tables put-table-maintenance-configuration \
   --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-
table-bucket \
   --type icebergCompaction \
   --namespace mynamespace \
   --name testtable \
   --value='{"status":"enabled","settings":{"icebergCompaction":
{"strategy":"sort"}}}'
```

Para obter mais informações, consulte put-table-maintenance-configuration na Referência de comandos da AWS CLI.

Como desabilitar a compactação usando a AWS CLI

O exemplo a seguir desabilitará a compactação usando a API `PutTableMaintenanceConfiguration`.

```
aws s3tables put-table-maintenance-configuration \
   --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-
table-bucket \
   --type icebergCompaction \
   --namespace mynamespace \
   --name testtable \
   --value='{"status":"disabled","settings":{"icebergCompaction":
{"targetFileSizeMB":256}}}'
```

Para obter mais informações, consulte put-table-maintenance-configuration na Referência de comandos da AWS CLI.

Gerenciamento de snapshots

O gerenciamento de snapshots determina o número de snapshots ativos para uma tabela. Isso se baseia em `MinimumSnapshots` (1 por padrão) e em `MaximumSnapshotAge` (120 horas por padrão). O gerenciamento de snapshots expira e remove os snapshots de tabela com base nessas configurações.

Quando um snapshot expira, o Amazon S3 marca quaisquer objetos referenciados apenas por esse snapshot como desatualizados. Esses objetos desatualizados são excluídos após o número de dias especificado pela propriedade `NoncurrentDays` na política de remoção de arquivos não referenciados.

> **Note**
>
> As exclusões de objetos desatualizados são permanentes, sem nenhuma maneira de recuperá-los.

Para visualizar ou recuperar objetos que foram marcados como desatualizados, você deve entrar em contato com o AWS Support. Para obter informações sobre como entrar em contato com o AWS Support, consulte Entrar em contato com a AWS ou a Documentação do AWS Support.

O gerenciamento de snapshots determina os objetos a serem excluídos de uma tabela com referências apenas a essa tabela. Qualquer referência feita a esses objetos fora da tabela não impedirá que o gerenciamento de snapshots exclua um objeto.

> **Note**
>
> O gerenciamento de snapshots não oferece suporte a valores de retenção que você configura como propriedades de tabela do Iceberg no arquivo `metadata.json` ou por meio de um comando SQL `ALTER TABLE SET TBLPROPERTIES`, incluindo retenção baseada em ramificação ou tag. O gerenciamento de snapshots é desabilitado quando você configura uma política de retenção baseada em ramificação ou tag, ou configura uma política de retenção no arquivo `metadata.json` que seja maior do que os valores configurados por meio da API `PutTableMaintenanceConfiguration`. Nesses casos, o S3 não expirará nem removerá snapshots e você precisará excluir manualmente os snapshots ou remover as propriedades de tabela do Iceberg para evitar cobranças de armazenamento.

Você só pode configurar o gerenciamento de snapshots ao nível da tabela. Para ter mais informações, consulte as informações sobre preços na Definição de preço do Amazon S3.

Exemplos de gerenciamento de snapshots

Os exemplos a seguir mostram configurações para o gerenciamento de snapshots de tabela.

Como configurar o gerenciamento de snapshots usando a AWS CLI

O exemplo a seguir definirá `MinimumSnapshots` como 10 e `MaximumSnapshotAge` como 2.500 horas usando a API `PutTableMaintenanceConfiguration`.

```
aws s3tables put-table-maintenance-configuration \
--table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-
table-bucket \
--namespace my_namespace \
--name my_table \
--type icebergSnapshotManagement \
--value '{"status":"enabled","settings":{"icebergSnapshotManagement":
{"minSnapshotsToKeep":10,"maxSnapshotAgeHours":2500}}}'
```

Como desabilitar o gerenciamento de snapshots usando a AWS CLI

O exemplo a seguir desabilitará o gerenciamento de snapshots usando a API `PutTableMaintenanceConfiguration`.

```
aws s3tables put-table-maintenance-configuration \
--table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-
table-bucket \
--namespace my_namespace \
--name my_table \
--type icebergSnapshotManagement \
--value '{"status":"disabled","settings":{"icebergSnapshotManagement":
{"minSnapshotsToKeep":1,"maxSnapshotAgeHours":120}}}'
```

Para obter mais informações, consulte put-table-maintenance-configuration na Referência de comandos da AWS CLI.

Considerações e limitações

Para saber mais sobre considerações e limites adicionais para compactação e gerenciamento de snapshots, consulte the section called “Considerações e limitações”.

> **Note**
>
> O serviço Tabelas do S3 aplica o tamanho padrão do grupo de linhas de parquets de 128 MB.

Considerações e limitações para trabalhos de manutenção

O Amazon S3 oferece operações de manutenção para aprimorar a performance das tabelas e dos buckets de tabela do S3. Essas opções são compactação de arquivos, gerenciamento de snapshots e remoção de arquivos não referenciados. Veja a seguir as limitações e considerações para essas opções de gerenciamento.

Tópicos

- Considerações para compactação
- Considerações para gerenciamento de snapshots
- Considerações para remoção de arquivos não referenciados
- Limites para manutenção de tabelas e buckets de tabela do S3

Considerações para compactação

As considerações a seguir se aplicam à compactação. Para ter mais informações sobre compactação, consulte the section called “Manutenção de tabelas”.

- A compactação só é compatível com os tipos de arquivo Apache Parquet.
- A compactação não oferece suporte ao seguinte tipo de dados: Fixo.
- A compactação não oferece suporte aos seguintes tipos de compressão: `brotli` e `lz4`.

Considerações para gerenciamento de snapshots

As considerações a seguir se aplicam ao gerenciamento de snapshots. Para ter mais informações sobre o gerenciamento de snapshots, consulte the section called “Manutenção de tabelas”.

- Os snapshots serão preservados somente quando ambos os critérios forem satisfeitos: o número mínimo de snapshots a serem mantidos e o período de retenção especificado.

- O gerenciamento de snapshots exclui metadados de snapshots expirados do Apache Iceberg, evitando consultas de viagem no tempo para snapshots expirados e, opcionalmente, excluindo arquivos de dados associados.
- O gerenciamento de snapshots não oferece suporte a valores de retenção que você configura como propriedades de tabela do Iceberg no arquivo `metadata.json` ou por meio de um comando SQL `ALTER TABLE SET TBLPROPERTIES`, incluindo retenção baseada em ramificação ou tag. O gerenciamento de snapshots é desabilitado quando você configura uma política de retenção baseada em ramificação ou tag, ou configura uma política de retenção no arquivo `metadata.json` que seja maior do que os valores configurados por meio da API `PutTableMaintenanceConfiguration`. Nesses casos, o S3 não expirará nem removerá snapshots e você precisará excluir manualmente os snapshots ou remover as propriedades de tabela do Iceberg para evitar cobranças de armazenamento.

Considerações para remoção de arquivos não referenciados

As considerações a seguir se aplicam à remoção de arquivos não referenciados. Para ter mais informações sobre a remoção de arquivos não referenciados, consulte the section called “Manutenção de buckets de tabela”.

- A remoção de arquivos não referenciados exclui arquivos de dados e metadados que não são mais referenciados pelos metadados do Iceberg quando o horário de criação é anterior ao período de retenção.

Limites para manutenção de tabelas e buckets de tabela do S3

Operação de manutenção	Propriedade	Configurável ao nível do bucket de tabela?	Configurável ao nível da tabela?	Valor padrão	Valor mínimo
Compactação	targetFileSizeMB	Não	Sim	512 MB	64 MB
Gerenciamento de snapshots	minimumSnapshots	Não	Sim	1	1

Operação de manutenção	Propriedade	Configurável ao nível do bucket de tabela?	Configurável ao nível da tabela?	Valor padrão	Valor mínimo
Gerenciamento de snapshots	maximumSnapshotAge	Não	Sim	120 horas	1 hora
Remoção de arquivos não referenciados	unreferencedDays	Sim	Não	3 dias	1 dia
Remoção de arquivos não referenciados	nonCurrentDays	Sim	Não	10 dias	1 dia

> **Note**
>
> O serviço Tabelas do S3 aplica o tamanho padrão do grupo de linhas de parquets de 128 MB.

Namespaces de tabela

Ao criar tabelas em um bucket de tabela do Amazon S3, elas são organizadas em agrupamentos lógicos chamados namespaces. Ao contrário das tabelas e dos buckets de tabela do S3, os namespaces não são recursos. Namespaces são constructos que ajudam a organizar e gerenciar tabelas de forma escalável. Por exemplo, todas as tabelas pertencentes ao departamento de recursos humanos de uma empresa podem ser agrupadas em um valor de namespace comum de `hr`.

Para controlar o acesso a namespaces específicos, é possível usar políticas de recursos de buckets de tabela. Para obter mais informações, consulte the section called “Políticas baseadas em recursos”.

As seguintes regras se aplicam a namespaces de tabela:

- Cada namespace deve ser único em um bucket de tabela.
- É possível criar até 10.000 namespaces por bucket de tabela.
- Cada nome de tabela deve ser único em um namespace.
- Cada tabela só pode ter um nível de namespaces. Os namespaces não podem ser aninhados.
- Cada tabela pertence a um único namespace.
- Você pode mover as tabelas entre namespaces.

Tópicos

- Criar namespaces
- Excluir um namespace

Criar namespaces

Um namespace de tabela é um constructo lógico que serve para agrupar tabelas em um bucket de tabela do Amazon S3. Cada tabela pertence a um único namespace. Antes de criar uma tabela em um bucket de tabela, é necessário criar um namespace para agrupá-las. É possível criar um namespace usando o console do Amazon S3, a AWS Command Line Interface (AWS CLI), a API REST do Amazon S3, os SDKs da AWS ou mecanismos de consulta integrados.

Nomes do namespace

As seguintes regras de nomenclatura se aplicam aos namespaces:

- Os nomes devem ter entre 1 e 255 caracteres.
- Os nomes só podem consistir em letras minúsculas, números e sublinhados (_). Sublinhados não são permitidos no início ou no final dos nomes de namespace.
- Os nomes devem começar e terminar com uma letra ou um número.
- Os nomes não devem conter hifens (-) nem pontos (.).
- Um namespace deve ser único dentro de um bucket de tabela.
- Os nomes de namespaces não devem começar com o prefixo reservado `aws`. Não é possível usar `aws_s3_metadata` como namespace. `aws_s3_metadata` é um namespace reservado para tabelas de metadados. Para obter mais informações, consulte Acelerar a descoberta de dados com o S3 Metadata.

Consulte mais informações sobre nomes válidos de namespace em Regras de nomenclatura para tabelas e namespaces.

Usar o console do S3 e o Amazon Athena

O procedimento a seguir usa o fluxo de trabalho Criar tabela com o Athena para criar um namespace no console do Amazon S3. Se não quiser usar o Amazon Athena também para criar uma tabela no namespace, você poderá cancelar o fluxo de trabalho depois de criar o namespace.

Para criar um namespace

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets de tabela.
3. Na página Buckets de tabela, escolha o bucket no qual você deseja criar um namespace.
4. Na página de detalhes do bucket, escolha Criar tabela com o Athena.
5. Na caixa de diálogo Criar tabela com o Athena, escolha Criar um namespace e, depois, Criar namespace.
6. Insira um nome no campo Nome do namespace. Os nomes de namespace devem ter de 1 a 255 caracteres e ser exclusivos no bucket de tabela. Os caracteres válidos são a–z, 0–9 e sublinhado (_). Sublinhados não são permitidos no início ou no final dos nomes de namespace.
7. Escolha Create namespace (Criar namespace).
8. Se você também quiser criar uma tabela, escolha Criar tabela com o Athena. Consulte mais informações sobre como criar uma tabela com o Athena em the section called “Usar o console do S3 e o Amazon Athena”. Se não quiser criar uma tabela no momento, escolha Cancelar.

Como usar o AWS CLI

Esse exemplo mostra como criar um namespace de tabelas usando a AWS CLI. Para usar esse exemplo, substitua os *user input placeholders* por suas próprias informações.

```
aws s3tables create-namespace \
    --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-bucket1 \
    --namespace example_namespace
```

Usando um mecanismo de consulta

Você pode criar um namespace em uma sessão do Apache Spark conectada aos buckets de tabela do Amazon S3.

Esse exemplo mostra como criar uma tabela usando instruções `CREATE` em um mecanismo de consulta integrado à funcionalidade Tabelas do S3. Para usar esse exemplo, substitua os *espaços reservados para entrada do usuário* por suas próprias informações.

```
spark.sql("CREATE NAMESPACE IF NOT EXISTS s3tablesbucket.my_namespace")
```

Excluir um namespace

Antes de excluir um namespace de tabela de um bucket de tabela do Amazon S3, é necessário excluir todas as tabelas dentro do namespace ou movê-las para outro namespace. É possível excluir um namespace usando a API REST do Amazon S3, os SDKs da AWS, a AWS Command Line Interface (AWS CLI) ou mecanismos de consulta integrados.

Consulte mais informações sobre as permissões necessárias para excluir um namespace em DeleteNamespace na Referência de API do Amazon Simple Storage Service.

Como usar o AWS CLI

Esse exemplo mostra como excluir um namespace de tabelas usando a AWS CLI. Para usar esse exemplo, substitua os *user input placeholders* por suas próprias informações.

```
aws s3tables delete-namespace \
    --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-bucket1 \
    --namespace example_namespace
```

Tabelas em buckets de tabela do S3

Uma tabela do S3 representa um conjunto de dados estruturado que consiste nos dados da tabela subjacente e nos metadados relacionados. Esses dados são armazenados em um bucket de tabela como um sub-recurso. Todas as tabelas em um bucket de tabela são armazenadas no formato de tabela Apache Iceberg. O Amazon S3 gerencia a manutenção das tabelas por meio da compactação automática de arquivos e do gerenciamento de snapshots. Para obter mais informações, consulte Manutenção de tabelas.

Para tornar as tabelas em uma conta acessíveis pelos serviços de analytics da AWS, integre os buckets de tabela do Amazon S3 ao Amazon SageMaker Lakehouse. Essa integração permite que serviços de analytics da AWS, como o Amazon Athena e o Amazon Redshift, descubram e acessem dados de tabela automaticamente.

Quando você cria uma tabela, o Amazon S3 gera automaticamente um local de warehouse para ela. Trata-se de um local exclusivo do S3 que armazena os objetos associados à tabela. O seguinte exemplo mostra o formato de um local de warehouse:

```
s3://63a8e430-6e0b-46f5-k833abtwr6s8tmtsycedn8s4yc3xhuse1b--table-s3
```

Em um bucket de tabela, você pode organizar as tabelas em agrupamentos lógicos chamados namespaces. Para obter mais informações, consulte Namespaces de tabela.

Você pode renomear as tabelas, mas cada tabela tem um nome do recurso da Amazon (ARN) exclusivo e um ID de tabela exclusivo. Cada tabela também tem uma política de recursos anexada a ela. Você pode usar essa política para gerenciar o acesso à tabela.

Os ARNs das tabelas usam o seguinte formato:

```
arn:aws:s3tables:region:owner-account-id:bucket/bucket-name/table/table-id
```

Por padrão, você pode criar até 10.000 tabelas em um bucket de tabela. Para solicitar um aumento da cota de tabelas e de buckets de tabela, entre em contato com o Suporte.

O Amazon S3 oferece suporte aos seguintes tipos de tabelas em buckets de tabela:

Tabelas de clientes

As tabelas de cliente são tabelas em que você pode ler e gravar. Você pode recuperar dados dessas tabelas usando mecanismos de consulta integrados. Também pode inserir, atualizar ou excluir dados delas usando operações de API do S3 ou mecanismos de consulta integrados.

Tabelas da AWS

As tabelas da AWS são tabelas somente leitura que são geradas por um AWS service (Serviço da AWS) em seu nome. Essas tabelas são gerenciadas pelo Amazon S3 e não podem ser modificadas por nenhuma entidade principal do IAM fora do próprio Amazon S3. Você pode recuperar informações dessas tabelas, mas não pode modificar os dados nelas. As tabelas da

AWS incluem tabelas do S3 Metadata, que contêm metadados capturados dos objetos em um bucket de uso geral do S3. Para obter mais informações, consulte Acelerar a descoberta de dados com o S3 Metadata.

Tópicos

- Criar uma tabela do Amazon S3
- Excluir uma tabela do Amazon S3
- Gerenciar políticas de tabela

Criar uma tabela do Amazon S3

Uma tabela do Amazon S3 é um sub-recurso de um bucket de tabela. As tabelas são armazenadas no formato Apache Iceberg para que você possa trabalhar com elas usando mecanismos de consulta e outras aplicações compatíveis com o Apache Iceberg. O Amazon S3 otimiza continuamente as tabelas para ajudar a reduzir os custos de armazenamento e melhorar a performance das consultas de analytics.

Quando você cria uma tabela, o Amazon S3 gera automaticamente um local de warehouse para ela. Um local de warehouse é um local exclusivo do S3 onde é possível ler e gravar objetos associados à tabela. O seguinte exemplo mostra o formato de um local de warehouse:

```
s3://63a8e430-6e0b-46f5-k833abtwr6s8tmtsycedn8s4yc3xhuse1b--table-s3
```

As tabelas têm o seguinte formato de nome do recurso da Amazon (ARN):

```
arn:aws:s3tables:region:owner-account-id:bucket/bucket-name/table/table-id
```

Por padrão, você pode criar até 10.000 tabelas em um bucket de tabela. Para solicitar um aumento da cota de tabelas e de buckets de tabela, entre em contato com o Suporte.

É possível criar uma tabela usando o console do Amazon S3, a API REST do Amazon S3, os SDKs da AWS, a AWS Command Line Interface (AWS CLI) ou mecanismos de consulta conectados com os buckets de tabela.

Ao criar uma tabela, você pode especificar as respectivas configurações de criptografia, a menos que esteja criando a tabela com o Athena. Se você não especificar as configurações de criptografia,

a tabela será criptografada com as configurações padrão do bucket de tabela. Para obter mais informações, consulte Especificar criptografia para tabelas.

Pré-requisitos para a criação de tabelas

Para criar uma tabela, primeiro é necessário fazer o seguinte:

- Criar um bucket de tabela.
- Crie um namespace no bucket de tabela.
- Você deve ter permissões do AWS Identity and Access Management (IAM) para `s3tables:CreateTable` e `s3tables:PutTableData`.
-

> **Note**
>
> Se você estiver usando a criptografia SSE-KMS para a tabela, precisará de permissões para `s3tables:PutTableEncryption` e da permissão `DescribeKey` na chave do AWS KMS escolhida. Além disso, a chave AWS KMS que você usa precisa conceder permissão à funcionalidade Tabelas do S3 para que realize a manutenção automática de tabelas. Para obter mais informações, consulte Requisitos de permissão para criptografia SSE-KMS da funcionalidade Tabelas do S3.

Consulte mais informações sobre nomes válidos de tabela em Regras de nomenclatura para tabelas e namespaces.

> **Important**
>
> Ao criar tabelas, use apenas letras minúsculas nos nomes e nas definições das tabelas. Por exemplo, os nomes das colunas devem estar todos em minúsculas. Se o nome da tabela ou a definição da tabela contiver letras maiúsculas, a tabela não será compatível com o AWS Lake Formation ou o AWS Glue Data Catalog. Nesse caso, a tabela não estará visível para serviços de analytics da AWS, como o Amazon Athena, mesmo que os buckets de tabela estejam integrados aos serviços de analytics da AWS.
> Se a definição da tabela contiver letras maiúsculas, você receberá a seguinte mensagem de erro ao executar uma consulta `SELECT` no Athena: “GENERIC_INTERNAL_ERROR: Get table request failed: com.amazonaws.services.glue.model.ValidationException: Unsupported Federation Resource - Invalid table or column names”.

Usar o console do S3 e o Amazon Athena

O procedimento a seguir usa o console do Amazon S3 para criar uma tabela com o Amazon Athena. Se ainda não criou um namespace no bucket de tabela, você pode fazer isso como parte desse processo. Antes de realizar as etapas a seguir, integre os buckets de tabela aos serviços de analytics da AWS nessa região. Para obter mais informações, consulte the section called “Usar tabelas do S3 com serviços de analytics da AWS”.

> **Note**
>
> Quando você cria uma tabela usando o Athena, ela herda as configurações de criptografia padrão do bucket de tabela. Se você quiser usar um tipo de criptografia diferente, precisará criar a tabela usando outro método.

Para criar uma tabela do

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets de tabela.
3. Na página Buckets de tabela, escolha o bucket no qual você deseja criar uma tabela.
4. Na página de detalhes do bucket, escolha Criar tabela com o Athena.
5. Na caixa de diálogo Criar tabela com o Athena, execute um destes procedimentos:
   - Crie um namespace. Escolha Criar um namespace e insira um nome no campo Nome do namespace. Os nomes de namespace devem ter de 1 a 255 caracteres e ser exclusivos no bucket de tabela. Os caracteres válidos são a–z, 0–9 e sublinhado (_). Sublinhados não são permitidos no início dos nomes de namespace.
   - Escolha Create namespace (Criar namespace).
   - Especifique um namespace existente. Escolha Especificar um namespace existente neste bucket de tabela. Depois, selecione Escolher entre namespaces existentes ou Inserir um nome de namespace existente. Se você tiver mais de mil namespaces no bucket e ele não aparecer na lista, será necessário inserir o nome do namespace.
6. Escolha Criar tabela com o Athena.
7. O console do Amazon Athena é aberto e o editor de consultas do Athena aparece. O campo Catálogo deve ser preenchido com s3tablescatalog/ seguido do nome do bucket de tabela;

por exemplo, s3tablescatalog/***amzn-s3-demo-bucket***. O campo Banco de dados deve ser preenchido com o namespace que você criou ou selecionou anteriormente.

> **Note**
>
> Caso não veja esses valores nos campos Catálogo e Banco de dados, verifique se você integrou os buckets de tabela aos serviços de analytics da AWS nessa região. Para obter mais informações, consulte the section called “Usar tabelas do S3 com serviços de analytics da AWS”.

8. O editor de consultas é preenchido com uma consulta de exemplo que você pode usar para criar uma tabela. Modifique a consulta para especificar o nome da tabela e as colunas que você deseja que a tabela tenha.
9. Quando terminar de modificar a consulta, escolha Executar para criar a tabela.

> **Note**
>
> - Se você receber o erro “Insufficient permissions to execute the query. Principal does not have any privilege on specified resource” ao tentar executar uma consulta no Athena, você deverá receber as permissões necessárias do Lake Formation na tabela. Para obter mais informações, consulte the section called “Conceder permissão em uma tabela ou um banco de dados”.
> - Se você receber o erro “Iceberg cannot access the requested resource” ao tentar executar uma consulta no Athena, acesse o console do AWS Lake Formation e verifique se você se autoconcedeu permissões no catálogo do bucket de tabela e no banco de dados (namespace) que criou. Não especifique uma tabela ao conceder essas permissões. Para obter mais informações, consulte the section called “Conceder permissão em uma tabela ou um banco de dados”.
> - Se você receber a seguinte mensagem de erro ao executar uma consulta `SELECT` no Athena, isso significa que o nome da tabela ou os nomes de coluna na definição da tabela contêm letras maiúsculas: “GENERIC_INTERNAL_ERROR: Get table request failed: com.amazonaws.services.glue.model.ValidationException: Unsupported Federation Resource - Invalid table or column names”. Os nomes de tabela e de coluna devem estar todos em minúsculas.

Se a criação da tabela tiver sido bem-sucedida, o nome da nova tabela aparecerá na lista de tabelas do Athena. Ao voltar para o console do Amazon S3, a nova tabela aparecerá na lista Tabelas na página de detalhes do bucket de tabela depois que você atualizar a lista.

Como usar o AWS CLI

Este exemplo mostra como criar uma tabela com um esquema usando a AWS CLI e especificando os metadados da tabela com JSON. Para usar esse exemplo, substitua os *user input placeholders* por suas próprias informações.

```
aws s3tables create-table --cli-input-json file://mytabledefinition.json
```

Para o arquivo `mytabledefinition.json`, use o exemplo de definição de tabela a seguir. Para usar esse exemplo, substitua os *user input placeholders* por suas próprias informações.

```
{
    "tableBucketARN": "arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-
table-bucket",
    "namespace": "your_namespace",
    "name": "example_table",
    "format": "ICEBERG",
    "metadata": {
        "iceberg": {
            "schema": {
                "fields": [
                     {"name": "id", "type": "int","required": true},
                     {"name": "name", "type": "string"},
                     {"name": "value", "type": "int"}
                ]
            }
        }
    }
}
```

Usando um mecanismo de consulta

É possível criar uma tabela em um mecanismo de consulta compatível conectado aos buckets de tabela, como em uma sessão do Apache Spark no Amazon EMR.

O exemplo a seguir mostra como criar uma tabela com o Spark usando instruções `CREATE` e adicionar dados à tabela usando instruções `INSERT` ou lendo dados de um arquivo existente. Para usar esse exemplo, substitua os *user input placeholders* por suas próprias informações.

```
spark.sql(
" CREATE TABLE IF NOT EXISTS s3tablesbucket.example_namespace.`example_table` (
    id INT,
    name STRING,
    value INT
)
USING iceberg "
)
```

Depois de criar a tabela, você pode carregar dados nela. Escolha entre os seguintes métodos:

- Adicione dados à tabela usando a instrução `INSERT`.

```
spark.sql(
"""
    INSERT INTO s3tablesbucket.my_namespace.my_table
    VALUES
        (1, 'ABC', 100),
        (2, 'XYZ', 200)
""")
```

- Carregue um arquivo de dados existente.

  1. Leia os dados no Spark:

```
val data_file_location = "Path such as S3 URI to data file"
val data_file = spark.read.parquet(data_file_location)
```

  2. Grave os dados em uma tabela do Iceberg:

```
data_file.writeTo("s3tablesbucket.my_namespace.my_table").using("Iceberg").tableProperty
 ("format-version", "2").createOrReplace()
```

Excluir uma tabela do Amazon S3

Você pode excluir uma tabela usando a API REST do Amazon S3, o AWS SDK, a AWS CLI ou mecanismos de consulta integrados.

> **Note**
>
> A funcionalidade Tabelas do S3 não é compatível com a operação `DROP TABLE` com `purge=false`. Algumas versões do Spark sempre definem esse sinalizador como falso, mesmo ao executar comandos `DROP TABLE PURGE`. Você pode tentar novamente usando `DROP TABLE` com `purge=true` ou usar a API REST DeleteTable da funcionalidade Tabelas do S3 para excluir uma tabela.
> Quando você exclui uma tabela, os objetos associados a essa tabela se tornam desatualizados e podem levar até um dia para serem removidos.

Como usar o AWS CLI

Esse exemplo mostra como excluir uma tabela usando a AWS CLI. Para usar o comando, substitua os *espaços reservados para entrada do usuário* por suas próprias informações.

```
aws s3tables delete-table \
    --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-
table-bucket \
    --namespace example_namespace --name example_table
```

Usando um mecanismo de consulta

Você pode excluir uma tabela em uma sessão do Apache Spark conectada aos buckets de tabela do Amazon S3.

Esse exemplo mostra como excluir uma tabela usando o comando `DROP TABLE PURGE`. Para usar o comando, substitua os *espaços reservados para entrada do usuário* por suas próprias informações.

```
spark.sql(
" DROP TABLE [IF EXISTS] s3tablesbucket.example_namespace.example_table PURGE")
```

Gerenciar políticas de tabela

Você pode adicionar, excluir, atualizar e visualizar políticas para tabelas usando a API REST do Amazon S3, o AWS SDK e a AWS CLI. Para obter mais informações, consulte os tópicos a seguir. Para ter mais informações sobre as chaves de condição e ações do AWS Identity and Access Management (IAM) compatíveis com a funcionalidade Tabelas do Amazon S3, consulte

Gerenciamento de acesso para a funcionalidade Tabelas do S3. Para conferir exemplos de políticas de tabela, consulte Políticas baseadas em recurso para a funcionalidade Tabelas do S3.

Adicionar uma política de tabela

Para adicionar uma política de tabela a uma tabela, você pode usar a API REST do Amazon S3, o AWS SDK e a AWS CLI.

Uso do AWS CLI

Esse exemplo mostra como criar uma política de tabela usando a AWS CLI. Para usar o comando, substitua os *espaços reservados para entrada do usuário* por suas próprias informações.

```
aws s3tables put-table-policy \
    --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-bucket1 \
    --namespace my-namespace \
    --name my-table \
    --resource-policy your-policy-JSON
```

Visualizar uma política de tabela

Para visualizar a política de bucket anexada a uma tabela, você pode usar a API REST do Amazon S3, o AWS SDK e a AWS CLI.

Uso do AWS CLI

Esse exemplo mostra como visualizar a política que está anexada a uma tabela usando a AWS CLI. Para usar o comando, substitua os *espaços reservados para entrada do usuário* por suas próprias informações.

```
aws s3tables get-table-policy \
    --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-bucket1/table/tableID \
    --namespace my-namespace \
    --name my-table
```

Excluir uma política de tabela

Para excluir uma política que está anexada a uma tabela, você pode usar a API REST do Amazon S3, o SDK da AWS e a AWS CLI.

Uso do AWS CLI

Esse exemplo mostra como excluir uma política de tabela usando a AWS CLI. Para usar o comando, substitua os *espaços reservados para entrada do usuário* por suas próprias informações.

```
aws s3tables delete-table-policy \
    --table-ARN arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-bucket1/
table/tableID \
    --namespace your-namespace \
    --name your-table
```

Acessar dados da tabela

Há várias maneiras de acessar tabelas nos buckets de tabela do Amazon S3. É possível integrar tabelas a serviços de analytics da AWS usando o Amazon SageMaker Lakehouse ou acessar tabelas diretamente usando o endpoint Iceberg REST de tabelas do Amazon S3 ou o Catálogo de Tabelas do Amazon S3 para Apache Iceberg. O método de acesso que você usa dependerá da configuração do catálogo, do modelo de governança e das necessidades de controle de acesso. Apresentamos a seguir uma visão geral desses métodos de acesso.

Integração com o Amazon SageMaker Lakehouse

Esse é o método de acesso recomendado para trabalhar com tabelas em buckets de tabela do S3. A integração oferece gerenciamento unificado de tabelas, governança centralizada e controle de acesso refinado em vários serviços de analytics da AWS.

Acesso direto

Use esse método se precisar trabalhar com implementações de catálogos do AWS Partner Network (APN) e implementações de catálogos personalizados ou se precisar realizar apenas operações básicas de leitura/gravação em tabelas dentro de um único bucket de tabela.

> **Note**
>
> Para acessar tabelas, a identidade do IAM que você usa precisa ter acesso aos seus recursos de tabela e às ações da funcionalidade Tabelas do S3. Para obter mais informações, consulte Gerenciamento de acesso para a funcionalidade Tabelas do S3.

Acessar tabelas por meio da integração com o Amazon SageMaker Lakehouse

É possível integrar buckets de tabela do S3 ao Amazon SageMaker Lakehouse para acessar tabelas de serviços de analytics da AWS, como o Amazon Athena, o Amazon Redshift e o QuickSight. O Amazon SageMaker Lakehouse unifica todos os dados nos data lakes do Amazon S3 e nos data warehouses do Amazon Redshift, para que seja possível criar aplicações de analytics, machine learning (ML) e IA generativa em uma única cópia dos dados. A integração preenche o AWS Glue Data Catalog com os recursos da tabela e federa o acesso a esses recursos com o AWS Lake Formation. Consulte mais informações sobre integração em Usar tabelas do Amazon S3 com serviços de analytics da AWS.

A integração permite o controle de acesso refinado por meio do AWS Lake Formation para oferecer segurança adicional. O Lake Formation usa conjuntamente um modelo de permissões próprio e o modelo de permissões do IAM para controlar o acesso aos recursos de tabela e aos dados subjacentes. Isso significa que uma solicitação para acessar a tabela deve passar por verificações de permissão tanto do IAM quanto do Lake Formation. Consulte mais informações em Lake Formation permissions overview no Guia do desenvolvedor do AWS Lake Formation.

Os seguintes serviços de analytics da AWS podem acessar tabelas por meio dessa integração:

- Amazon Athena
- Amazon Redshift
- Amazon EMR
- QuickSight
- Amazon Data Firehose

Acessar tabelas usando o endpoint Iceberg REST do AWS Glue

Depois que os buckets de tabela do S3 estiverem integrados ao Amazon SageMaker Lakehouse, você também poderá usar o endpoint Iceberg REST do AWS Glue para se conectar às tabelas do S3 por meio de mecanismos de consulta de terceiros compatíveis com o Iceberg. Para obter mais informações, consulte Acessar tabelas do Amazon S3 usando o endpoint Iceberg REST do AWS Glue.

Recomendamos usar o endpoint Iceberg REST do AWS Glue quando você quiser acessar tabelas do Spark, do PyIceberg ou de outros clientes compatíveis com o Iceberg.

Os seguintes clientes podem acessar tabelas diretamente por meio do endpoint Iceberg REST do AWS Glue:

- Qualquer cliente do Iceberg, incluindo o Spark, o PyIceberg e outros.

Acessar tabelas diretamente

É possível acessar tabelas diretamente de mecanismos de consulta de código aberto por meio de métodos que conectam as operações de gerenciamento de Tabelas do S3 às suas aplicações de analytics do Apache Iceberg. Há dois métodos de acesso direto: o endpoint Iceberg REST do serviço Tabelas do Amazon S3 ou o Catálogo de Tabelas do Amazon S3 para Apache Iceberg. O endpoint REST é recomendado.

Recomendamos o acesso direto se você acessa tabelas em implementações de catálogos autogerenciados ou se precisa realizar apenas operações básicas de leitura/gravação em tabelas em um único bucket de tabela. Com relação a outros cenários de acesso, recomendamos a integração com o Amazon SageMaker Lakehouse.

O acesso direto às tabelas é gerenciado por meio de políticas baseadas em identidade do IAM ou políticas baseadas em recursos anexadas a tabelas e buckets de tabela. Você não precisa gerenciar as permissões do Lake Formation para tabelas ao acessá-las diretamente.

Acessar tabelas por meio do endpoint Iceberg REST do serviço Tabelas do Amazon S3

Você pode usar o endpoint Iceberg REST do serviço Tabelas do Amazon S3 para acessar as tabelas diretamente de qualquer cliente compatível com o Iceberg REST por meio de endpoints HTTP. Consulte mais informações em Acessar tabelas usando o endpoint Iceberg REST do serviço Tabelas do Amazon S3.

Os seguintes mecanismos de consulta e serviços de analytics da AWS podem acessar tabelas diretamente usando o endpoint Iceberg REST do serviço Tabelas do Amazon S3:

Mecanismos de consulta compatíveis

- Qualquer cliente do Iceberg, incluindo o Spark, o PyIceberg e outros.
- Amazon EMR
- AWS Glue ETL

Acessar tabelas diretamente por meio do Catálogo de Tabelas do Amazon S3 para Apache Iceberg

Você também pode acessar tabelas diretamente de mecanismos de consulta como o Apache Spark usando o catálogo de clientes de Tabelas do S3. Consulte mais informações em Acessar tabelas do Amazon S3 com o Catálogo de Tabelas do Amazon S3 para Apache Iceberg. No entanto, o S3 recomenda usar o endpoint Iceberg REST de Tabelas do Amazon S3 para acesso direto, pois ele é compatível com mais aplicações e não exige código específico de mecanismo ou linguagem.

Os seguintes mecanismos de consulta podem acessar tabelas diretamente usando o catálogo de cliente:

- Apache Spark

Usar tabelas do Amazon S3 com serviços de analytics da AWS

Para tornar as tabelas em uma conta acessíveis pelos serviços de analytics da AWS, integre os buckets de tabela do Amazon S3 ao Amazon SageMaker Lakehouse. Essa integração permite que os serviços de analytics da AWS descubram e acessem dados de tabela automaticamente. Você pode usar essa integração para trabalhar com tabelas nos seguintes serviços:

- Amazon Athena
- Amazon Redshift
- Amazon EMR
- QuickSight
- Amazon Data Firehose

> **Note**
>
> Essa integração usa os serviços AWS Glue e AWS Lake Formation e pode incorrer em custos de solicitação e armazenamento do AWS Glue. Para obter mais informações, consulte Preços do AWS Glue.
>
> Há preços adicionais para a execução de consultas nas tabelas do S3. Saiba mais nas informações sobre os preços do mecanismo de consulta que você está usando.

Como funciona a integração

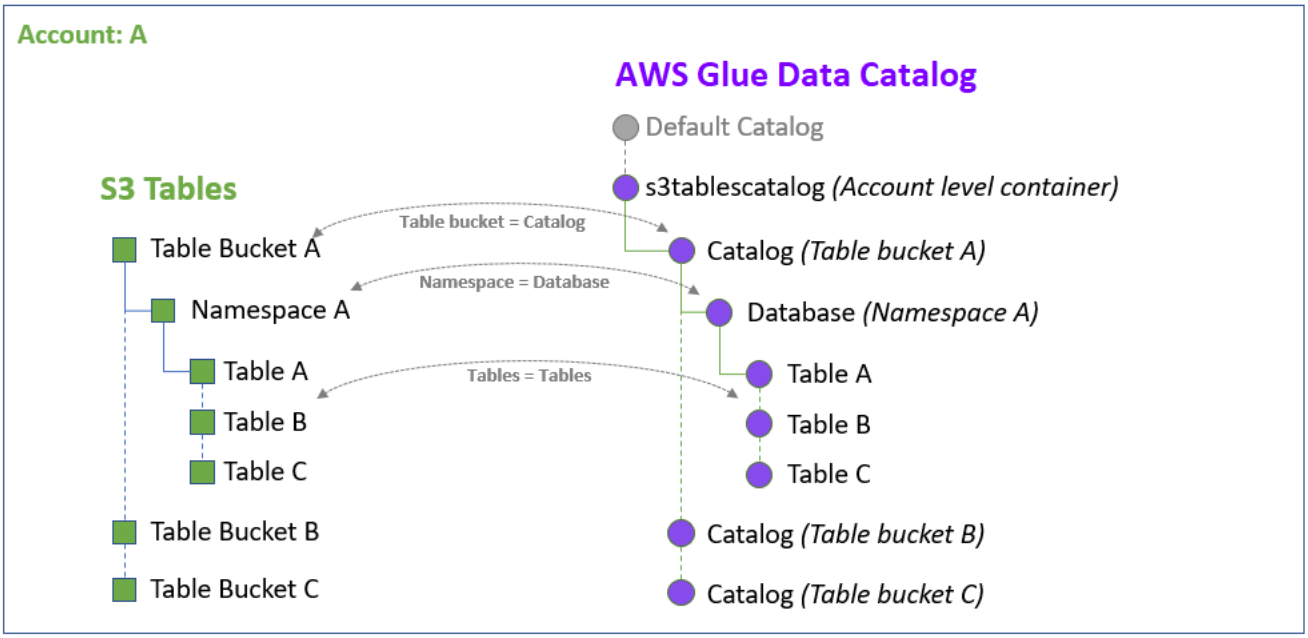
Quando você cria um bucket de tabela no console, o Amazon S3 inicializa as seguintes ações para integrar os buckets de tabela na região que você selecionou aos serviços de analytics da AWS:

1. Cria um perfil de serviço do AWS Identity and Access Management (IAM) que concede ao Lake Formation acesso a todos os buckets de tabela.
2. Usando o perfil de serviço, o Lake Formation registra os buckets de tabela na região atual. Isso permite que o Lake Formation gerencie o acesso, as permissões e a governança de todos os buckets de tabela atuais e futuros nessa região.
3. Adiciona o catálogo `s3tablescatalog` ao AWS Glue Data Catalog na região atual. Ao adicionar o catálogo `s3tablescatalog`, todos os buckets de tabela, namespaces e tabelas podem ser preenchidos no Catálogo de Dados.

> **Note**
>
> Essas ações são automatizadas por meio do console do Amazon S3. Se você realizar essa integração de forma programática, deverá executar manualmente todas essas ações.

Você integra os buckets de tabela uma vez por região da AWS. Após a conclusão da integração, todos os buckets de tabela, namespaces e tabelas atuais e futuros serão adicionados ao AWS Glue Data Catalog nessa região.

A ilustração a seguir mostra como o catálogo `s3tablescatalog` preenche automaticamente os buckets de tabela, os namespaces e as tabelas na região atual como objetos correspondentes no Catálogo de Dados. Os buckets de tabela são preenchidos como subcatálogos. Os namespaces em um bucket de tabela são preenchidos como bancos de dados nos respectivos subcatálogos. As tabelas são preenchidas como tabelas nos respectivos bancos de dados.



Como as permissões funcionam

Recomendamos integrar os buckets de tabela aos serviços de analytics da AWS para que você possa trabalhar com dados de tabela em vários serviços que usam o AWS Glue Data Catalog como um armazenamento de metadados. A integração permite um controle de acesso detalhado por meio do AWS Lake Formation. Essa abordagem de segurança significa que, para poder trabalhar com suas tabelas, além das permissões do AWS Identity and Access Management (IAM), você deve conceder à entidade principal do IAM permissões do Lake Formation nas tabelas.

Há dois tipos principais de permissões no AWS Lake Formation:

- As permissões de acesso a metadados controlam a capacidade de criar, ler, atualizar e excluir tabelas e bancos de dados de metadados no Catálogo de Dados.
- As permissões de acesso aos dados subjacentes controlam a capacidade de ler e gravar dados nos locais do Amazon S3 subjacentes para os quais os recursos do Catálogo de Dados apontam.

O Lake Formation usa conjuntamente um modelo de permissões próprio e o modelo de permissões do IAM para controlar o acesso aos recursos do Catálogo de Dados e aos dados subjacentes:

- Para que uma solicitação de acesso aos recursos do Catálogo de Dados ou os dados subjacentes seja bem-sucedida, ela deve passar pelas verificações de permissão do IAM e do Lake Formation.

- As permissões do IAM controlam o acesso a APIs e recursos do Lake Formation e do AWS Glue, enquanto as permissões do Lake Formation controlam o acesso aos recursos do Catálogo de Dados, aos locais do Amazon S3 e aos dados subjacentes.

As permissões do Lake Formation se aplicam somente na região em que foram concedidas, e uma entidade principal deve ser autorizada por um administrador do data lake ou por outra entidade principal com as permissões necessárias para receber as permissões do Lake Formation.

Para obter mais informações, consulte "Overview of Lake Formation permissions" (Visão geral das permissões do Lake Formation) no Guia do desenvolvedor do AWS Lake Formation.

Siga as etapas em the section called "Pré-requisitos da integração" e the section called "Integrar buckets de tabela aos serviços de analytics da AWS" para ter as permissões apropriadas para acessar o AWS Glue Data Catalog e seus recursos de tabela, bem como para trabalhar com serviços de analytics da AWS.

> **Important**
>
> Se você não for o usuário que realizou a integração dos buckets de tabela com os serviços de analytics da AWS para sua conta, deverá receber as permissões necessárias do Lake Formation na tabela. Para obter mais informações, consulte the section called "Conceder permissão em uma tabela ou um banco de dados".

Pré-requisitos da integração

Os pré-requisitos a seguir se aplicam para integrar buckets de tabela a serviços de analytics da AWS:

- Crie um bucket de tabela.
- Anexe a política AWSLakeFormationDataAdmin gerenciada pela AWS à entidade principal do AWS Identity and Access Management (IAM) para tornar esse usuário um administrador de data lake. Consulte mais informações sobre como criar um administrador de data lake em Create a data lake administrator no Guia do desenvolvedor do AWS Lake Formation.
- Adicione permissões para a operação `glue:PassConnection` à entidade principal do IAM.
- Adicione permissões para as operações `lakeformation:RegisterResource` e `lakeformation:RegisterResourceWithPrivilegedAccess` à entidade principal do IAM.

- Atualize a AWS Command Line Interface (AWS CLI) para a versão mais recente.

> **Important**
>
> Ao criar tabelas, use apenas letras minúsculas nos nomes e nas definições das tabelas. Por exemplo, os nomes das colunas devem estar todos em minúsculas. Se o nome da tabela ou a definição da tabela contiver letras maiúsculas, a tabela não será compatível com o AWS Lake Formation ou o AWS Glue Data Catalog. Nesse caso, a tabela não estará visível para serviços de analytics da AWS, como o Amazon Athena, mesmo que os buckets de tabela estejam integrados aos serviços de analytics da AWS.
>
> Se a definição da tabela contiver letras maiúsculas, você receberá a seguinte mensagem de erro ao executar uma consulta `SELECT` no Athena: “GENERIC_INTERNAL_ERROR: Get table request failed: com.amazonaws.services.glue.model.ValidationException: Unsupported Federation Resource - Invalid table or column names”.

Integrar buckets de tabela aos serviços de analytics da AWS

Essa integração deve ser feita uma vez por região da AWS.

> **Important**
>
> A integração dos serviços de analytics da AWS agora usa a opção `WithPrivilegedAccess` na operação de API `registerResource` do Lake Formation para registrar buckets de tabela do S3. Agora a integração também cria o catálogo `s3tablescatalog` no AWS Glue Data Catalog usando a opção `AllowFullTableExternalDataAccess` na operação de API `CreateCatalog` do AWS Glue.
>
> Se você configurou a integração com a versão prévia, pode continuar usando sua integração atual. No entanto, como o processo de integração atualizado oferece melhorias de desempenho, recomendamos a migração. Se quiser migrar para a integração atualizada, consulte the section called “Migrar para o processo de integração atualizado”.

Uso do console do S3

1. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.

2. No painel de navegação à esquerda, escolha Buckets de tabela.
3. Escolha Criar bucket de tabela.

   A página Criar bucket de tabela é aberta.
4. Insira um Nome do bucket de tabela e marque a caixa de seleção Habilitar integração.
5. Escolha Criar bucket de tabela. O Amazon S3 tentará integrar automaticamente os buckets de tabela nessa região.

Na primeira vez que você integra buckets de tabela em qualquer região, o Amazon S3 cria um perfil de serviço do IAM em seu nome. Esse perfil permite que o Lake Formation acesse todos os buckets de tabela na conta e federe o acesso às tabelas no AWS Glue Data Catalog.

Como usar o AWS CLI

Como integrar buckets de tabela usando a AWS CLI

As etapas a seguir mostram como usar a AWS CLI para integrar buckets de tabela. Para usar essas etapas, substitua *`user input placeholders`* por suas próprias informações.

1. Crie um bucket de tabela.

```
aws s3tables create-table-bucket \
--region us-east-1 \
--name amzn-s3-demo-table-bucket
```

2. Crie um perfil de serviço do IAM que permita que o Lake Formation acesse os recursos de tabela.

   a. Crie um arquivo chamado `Role-Trust-Policy.json` que contenha a seguinte política de confiança:

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Sid": "LakeFormationDataAccessPolicy",
        "Effect": "Allow",
        "Principal": {
          "Service": "lakeformation.amazonaws.com"
        },
```

```
        "Action": [
            "sts:AssumeRole",
            "sts:SetContext",
            "sts:SetSourceIdentity"
        ],
        "Condition": {
          "StringEquals": {
            "aws:SourceAccount": "111122223333"
          }
        }
      }
    ]
}
```

Crie um perfil de serviço do IAM usando o seguinte comando:

```
aws iam create-role \
--role-name S3TablesRoleForLakeFormation \
--assume-role-policy-document file://Role-Trust-Policy.json
```

b. Crie um arquivo chamado `LF-GluePolicy.json` que contenha a seguinte política:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "LakeFormationPermissionsForS3ListTableBucket",
            "Effect": "Allow",
            "Action": [
                "s3tables:ListTableBuckets"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "LakeFormationDataAccessPermissionsForS3TableBucket",
            "Effect": "Allow",
            "Action": [
                "s3tables:CreateTableBucket",
                "s3tables:GetTableBucket",
                "s3tables:CreateNamespace",
                "s3tables:GetNamespace",
```

```
                "s3tables:ListNamespaces",
                "s3tables:DeleteNamespace",
                "s3tables:DeleteTableBucket",
                "s3tables:CreateTable",
                "s3tables:DeleteTable",
                "s3tables:GetTable",
                "s3tables:ListTables",
                "s3tables:RenameTable",
                "s3tables:UpdateTableMetadataLocation",
                "s3tables:GetTableMetadataLocation",
                "s3tables:GetTableData",
                "s3tables:PutTableData"
            ],
            "Resource": [
                "arn:aws:s3tables:us-east-1:111122223333:bucket/*"
            ]
        }
    ]
}
```

Anexe a política ao perfil usando o seguinte comando:

```
aws iam put-role-policy \
--role-name S3TablesRoleForLakeFormation  \
--policy-name LakeFormationDataAccessPermissionsForS3TableBucket \
--policy-document file://LF-GluePolicy.json
```

3. Crie um arquivo chamado `input.json` que contenha o seguinte:

```
{
    "ResourceArn": "arn:aws:s3tables:us-east-1:111122223333:bucket/*",

    "WithFederation": true,
    "RoleArn": "arn:aws:iam::111122223333:role/S3TablesRoleForLakeFormation"
}
```

Registre os buckets de tabela no Lake Formation usando o seguinte comando:

```
aws lakeformation register-resource \
--region us-east-1 \
--with-privileged-access \
--cli-input-json file://input.json
```

4. Crie um arquivo chamado `catalog.json` que contenha o seguinte catálogo:

```
{
   "Name": "s3tablescatalog",
   "CatalogInput": {
      "FederatedCatalog": {
          "Identifier": "arn:aws:s3tables:us-east-1:111122223333:bucket/*",
          "ConnectionName": "aws:s3tables"
       },
       "CreateDatabaseDefaultPermissions":[],
       "CreateTableDefaultPermissions":[],
       "AllowFullTableExternalDataAccess": "True"
   }
}
```

   Crie o catálogo `s3tablescatalog` usando o comando a seguir. Ao criar esse catálogo, o AWS Glue Data Catalog é preenchido com objetos correspondentes a buckets de tabela, namespaces e tabelas.

```
aws glue create-catalog \
--region us-east-1 \
--cli-input-json file://catalog.json
```

5. Verifique se o catálogo `s3tablescatalog` foi adicionado no AWS Glue usando o seguinte comando:

```
aws glue get-catalog --catalog-id s3tablescatalog
```

Migrar para o processo de integração atualizado

O processo de integração dos serviços de analytics da AWS foi atualizado. Se você configurou a integração com a versão prévia, pode continuar usando sua integração atual. No entanto, como o processo de integração atualizado oferece melhorias de desempenho, recomendamos que realize a migração usando as etapas a seguir. Consulte mais informações sobre o processo de migração ou integração em Creating an Amazon S3 Tables catalog in the AWS Glue Data Catalog no Guia do desenvolvedor do AWS Lake Formation.

1. Abra o console do AWS Lake Formation em https://console.aws.amazon.com/lakeformation/ e faça login como administrador do data lake. Consulte mais informações sobre como criar um

administrador de data lake em Create a data lake administrator no Guia do desenvolvedor do AWS Lake Formation.

2. Exclua o catálogo `s3tablescatalog` fazendo o seguinte:

   - No painel de navegação à esquerda, selecione Catálogos.
   - Selecione o botão de opção ao lado do catálogo `s3tablescatalog` na lista Catálogos. No menu Ações, escolha Excluir.

3. Cancele o registro da localização dos dados do catálogo `s3tablescatalog` fazendo o seguinte:

   - No painel de navegação à esquerda, acesse a seção Administração e selecione Locais de data lake.
   - Selecione o botão de opção ao lado da localização do data lake `s3tablescatalog`; por exemplo, `s3://tables:region:account-id:bucket/*`.
   - No menu Ações, selecione Remover.
   - Na caixa de diálogo de confirmação exibida, selecione Remover.

4. Agora que você excluiu o catálogo `s3tablescatalog` e a localização do data lake, pode seguir as etapas para integrar os buckets de tabela aos serviços de analytics da AWS usando o processo de integração atualizado.

> **Note**
>
> Se você quiser trabalhar com tabelas criptografadas com SSE-KMS em serviços integrados de analytics da AWS, o perfil que você utiliza precisa ter permissão para usar sua chave do AWS KMS para operações de criptografia. Para obter mais informações, consulte Conceder permissões a entidades principais do IAM para trabalhar com tabelas criptografadas em serviços integrados de analytics da AWS.

Próximas etapas

- Crie um namespace .
- Criar uma tabela.

Conceder permissões do Lake Formation nos recursos de tabela

Depois que os buckets de tabela são integrados aos serviços de analytics da AWS, o Lake Formation gerencia o acesso aos recursos da tabela. O Lake Formation usa um modelo de permissões próprio (permissões do Lake Formation) que permite um controle de acesso detalhado aos recursos do Catálogo de Dados. O Lake Formation exige que cada entidade principal do IAM (usuário ou perfil) seja autorizada a realizar ações nos recursos gerenciados pelo Lake Formation. Para obter mais informações, consulte "Overview of Lake Formation permissions" (Visão geral das permissões do Lake Formation) no Guia do desenvolvedor do AWS Lake Formation. Consulte informações sobre o compartilhamento de dados entre contas em Cross-account data sharing in Lake Formation no Guia do desenvolvedor do AWS Lake Formation.

Para que as entidades principais do IAM possam acessar tabelas nos serviços de analytics da AWS, você deve conceder a elas permissões do Lake Formation nesses recursos.

> **Note**
>
> Se você é o usuário que realizou a integração do bucket de tabela, já tem permissões do Lake Formation para as tabelas. Se você é a única entidade principal que acessará as tabelas, pode ignorar esta etapa. Você só precisa conceder permissões do Lake Formation em suas tabelas a outras entidades principais do IAM. Isso permite que outras entidades principais acessem a tabela ao executar consultas. Para obter mais informações, consulte Conceder permissão em uma tabela ou um banco de dados.

É necessário conceder a outras entidades principais do IAM as permissões do Lake Formation nos recursos de tabela para trabalhar com eles nos seguintes serviços:

- Amazon Redshift
- Amazon Data Firehose
- Amazon QuickSight
- Amazon Athena

Conceder permissão em uma tabela ou um banco de dados

Você pode conceder a uma entidade principal permissões do Lake Formation em uma tabela ou um banco de dados em um bucket de tabela por meio do console do Lake Formation ou da AWS CLI.

> **Note**
>
> Quando você concede permissões do Lake Formation em um recurso do catálogo de dados para uma conta externa ou diretamente para uma entidade principal do IAM em outra conta, o Lake Formation usa o serviço do AWS Resource Access Manager (AWS RAM) para compartilhar o recurso. Se a conta do concedido estiver na mesma organização da conta do concedente, o recurso compartilhado estará disponível imediatamente para o concedido. Se a conta do concedido não estiver na mesma organização, o AWS RAM envia um convite à conta do concedido para aceitar ou rejeitar a concessão do recurso. Em seguida, para disponibilizar o recurso compartilhado, o administrador do data lake deve usar o console AWS RAM ou AWS CLI para aceitar o convite na conta do concedido. Consulte mais informações sobre o compartilhamento de dados entre contas em Cross-account data sharing in Lake Formation no Guia do desenvolvedor do AWS Lake Formation.

Console

1. Abra o console do AWS Lake Formation em https://console.aws.amazon.com/lakeformation/ e faça login como administrador do data lake. Consulte mais informações sobre como criar um administrador de data lake em Create a data lake administrator no Guia do desenvolvedor do AWS Lake Formation.
2. No painel de navegação, escolha Permissões de dados e Conceder.
3. Na página Conceder permissões, em Entidades principais, execute um dos seguintes procedimentos:
   - Para o Amazon Athena ou o Amazon Redshift, escolha Usuários e perfis do IAM e selecione a entidade principal do IAM que você usa para consultas.
   - Para o Amazon Data Firehose, escolha Usuários e perfis do IAM e selecione o perfil de serviço que você criou para fazer streaming para as tabelas.
   - Para o QuickSight, escolha Usuários e grupos SAML e insira o nome do recurso da Amazon (ARN) do usuário administrador do QuickSight.
4. Em Tags do LF ou recursos de catálogo, escolha Recursos do catálogo de dados nomeados.
5. Em Catálogos, escolha o subcatálogo que você criou ao integrar seu bucket de tabela; por exemplo, `account-id:s3tablescatalog/amzn-s3-demo-bucket`.
6. Em Bancos de dados, escolha o namespace do bucket de tabela do S3 que você criou.
7. (Opcional) Em Tabelas, escolha a tabela do S3 que você criou no bucket de tabela.

> **Note**
>
> Se você estiver criando uma tabela no editor de consultas do Athena, não selecione uma tabela.

8. Execute um destes procedimentos:
   - Se você especificou uma tabela na etapa anterior, em Permissões de tabela, escolha Super.
   - Se você não especificou uma tabela na etapa anterior, acesse Permissões do banco de dados. Para o compartilhamento de dados entre contas, não é possível escolher Super para conceder à outra entidade principal todas as permissões no banco de dados. Em vez disso, escolha permissões mais detalhadas, como Descrever.
9. Selecione Conceder.

CLI

1. Você deve executar os comandos da AWS CLI a seguir como administrador do data lake. Consulte mais informações em Create a data lake administrator no Guia do desenvolvedor do AWS Lake Formation.
2. Execute o comando a seguir para conceder permissões do Lake Formation em uma tabela no bucket de tabela do S3 a uma entidade principal do IAM para acessar a tabela. Para usar esse exemplo, substitua os *user input placeholders* por suas próprias informações.

```
aws lakeformation grant-permissions \
--region us-east-1 \
--cli-input-json \
'{
    "Principal": {
        "DataLakePrincipalIdentifier": "user or role ARN, for example,
 arn:aws:iam::account-id:role/example-role"
    },
    "Resource": {
        "Table": {
            "CatalogId": "account-id:s3tablescatalog/amzn-s3-demo-bucket",
            "DatabaseName": "S3 table bucket namespace, for example,
 test_namespace",
            "Name": "S3 table bucket table name, for example test_table"
        }
```

```
    },
    "Permissions": [
        "ALL"
    ]
}'
```

Acessar tabelas do Amazon S3 usando o endpoint Iceberg REST do AWS Glue

Depois que os buckets de tabela do S3 estiverem integrados ao AWS Glue Data Catalog, você poderá usar o endpoint Iceberg REST do AWS Glue para se conectar às tabelas do S3 por meio de clientes compatíveis com o Apache Iceberg, como PyIceberg ou Spark. O endpoint Iceberg REST do AWS Glue implementa a Especificação da API Catalog Open do Iceberg REST, que fornece uma interface padronizada para interagir com tabelas do Iceberg. Para acessar as tabelas do S3 usando o endpoint, você precisa configurar as permissões por meio de uma combinação de políticas do IAM e concessões do AWS Lake Formation. As seções a seguir explicam como configurar o acesso, incluindo instruções sobre como criar o perfil do IAM necessário, definir as políticas essenciais e estabelecer permissões do Lake Formation para acesso em nível de banco de dados e de tabela.

Consulte uma explicação completa sobre como usar o PyIceberg em Access data in Amazon S3 Tables using PyIceberg through the AWS Glue Iceberg REST endpoint.

Pré-requisitos

- Integrar os buckets de tabela aos serviços de analytics da AWS
- Criar um namespace de tabela
- Ter acesso a uma conta de administrador do data lake

Criar um perfil do IAM para o cliente

Para acessar tabelas por meio de endpoints do AWS Glue, você precisa criar um perfil do IAM com permissões para ações do AWS Glue e do Lake Formation. Este procedimento explica como criar esse perfil e configurar suas permissões.

1. Abra o console do IAM, em https://console.aws.amazon.com/iam/.
2. No painel de navegação à esquerda, escolha Políticas.
3. Escolha Criar uma política e selecione JSON no editor de políticas.

4. Adicione a seguinte política em linha que concede permissões para acessar ações do AWS Glue e do Lake Formation:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "glue:GetCatalog",
                "glue:GetDatabase",
                "glue:GetDatabases",
                "glue:GetTable",
                "glue:GetTables",
                "glue:CreateTable",
                "glue:UpdateTable"
            ],
            "Resource": [
                "arn:aws:glue:<region>:<account-id>:catalog",
                "arn:aws:glue:<region>:<account-id>:catalog/s3tablescatalog",
                "arn:aws:glue:<region>:<account-id>:catalog/
s3tablescatalog/<s3_table_bucket_name>",
                "arn:aws:glue:<region>:<account-id>:table/
s3tablescatalog/<s3_table_bucket_name>/<namespace>/*",
                "arn:aws:glue:<region>:<account-id>:database/
s3tablescatalog/<s3_table_bucket_name>/<namespace>"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "lakeformation:GetDataAccess"
            ],
            "Resource": "*"
        }
    ]
}
```

5. Depois de criar a política, crie um perfil do IAM e escolha Política de confiança personalizada como Tipo de entidade confiável.

6. Insira o seguinte em Política de confiança personalizada:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::<accountid>:role/<Admin_role>"
            },
            "Action": "sts:AssumeRole",
            "Condition": {}
        }
    ]
}
```

Definir o acesso no Lake Formation

O Lake Formation oferece controles de acesso detalhado para tabelas do data lake. Quando você integrou o bucket do S3 ao AWS Glue Data Catalog, as tabelas foram automaticamente registradas como recursos no Lake Formation. Para acessar essas tabelas, você deve conceder permissões específicas do Lake Formation à sua identidade do IAM, além das permissões de política do IAM.

As etapas a seguir explicam como aplicar os controles de acesso do Lake Formation para permitir que o cliente do Iceberg se conecte às tabelas. Você deve fazer login como administrador do data lake para aplicar essas permissões.

Permitir que mecanismos externos acessem os dados da tabela

No Lake Formation, você deve habilitar o acesso total à tabela para que mecanismos externos acessem os dados. Isso permite que aplicações de terceiros obtenham credenciais temporárias do Lake Formation ao usar um perfil do IAM que tenha permissões completas na tabela solicitada.

Abra o console do Lake Formation em https://console.aws.amazon.com/lakeformation/.

1. Abra o console do Lake Formation em https://console.aws.amazon.com/lakeformation/ e faça login como administrador de data lake.
2. No painel de navegação, em Administração, selecione Configurações de integração de aplicações.
3. Selecione Permitir que mecanismos externos acessem dados em locais do Amazon S3 com acesso total à tabela. Em seguida, escolha Salvar.

Conceder permissões do Lake Formation nos recursos de tabela

Depois, conceda permissões do Lake Formation ao perfil do IAM que você criou para o cliente compatível com o Iceberg. Essas permissões possibilitarão que o perfil crie e gerencie tabelas no namespace. Você precisa fornecer permissões em nível de banco de dados e de tabela:

Como conceder permissões de banco de dados

1. Abra o console do AWS Lake Formation em https://console.aws.amazon.com/lakeformation/ e faça login como administrador do data lake.
2. No painel de navegação, escolha Permissões de dados e Conceder.
3. Na página Conceder permissões, em Entidades principais, escolha Usuários e perfis do IAM e selecione o perfil do IAM que você criou para acesso ao REST endpoint do Iceberg do AWS Glue.
4. Em Tags do LF ou recursos de catálogo, escolha Recursos do catálogo de dados nomeados.
5. Em Catálogos, escolha o catálogo de dados do AWS Glue que foi criado para o bucket de tabela. Por exemplo, .`<accoundID>`:s3tablescatalog/`<table-bucket-name>`
6. Para Bancos de dados, escolha `mynamespace`.
7. Em Permissões de tabela, selecione Criar tabela e Descrever.
8. Selecione Conceder.

Como conceder permissões de tabela

1. Abra o console do AWS Lake Formation em https://console.aws.amazon.com/lakeformation/ e faça login como administrador do data lake.
2. No painel de navegação, escolha Permissões de dados e Conceder.
3. Na página Conceder permissões, em Entidades principais, escolha Usuários e perfis do IAM e selecione o perfil do IAM que você criou para acesso ao REST endpoint do Iceberg do AWS Glue.
4. Em Tags do LF ou recursos de catálogo, escolha Recursos do catálogo de dados nomeados.
5. Em Catálogos, escolha o catálogo de dados do AWS Glue que foi criado para o bucket de tabela. Por exemplo, .`<accoundID>`:s3tablescatalog/`<table-bucket-name>`
6. Em Bancos de dados, escolha o namespace do bucket de tabela do S3 que você criou.
7. Em Tabelas, escolha ALL_TABLES.
8. Em Permissões de tabela, escolha Super.

9. Selecione Conceder.

Configurar o ambiente para usar o endpoint

Depois de configurar o perfil do IAM com as permissões necessárias para o acesso à tabela, você pode usá-lo para executar clientes do Iceberg em sua máquina local configurando a AWS CLI com o perfil por meio do seguinte comando:

```
aws sts assume-role --role-arn "arn:aws:iam::<accountid>:role/<glue-irc-role>" --role-session-name <glue-irc-role>
```

Para acessar tabelas por meio do endpoint REST do AWS Glue, você precisa inicializar um catálogo em seu cliente compatível com o Iceberg. Essa inicialização requer a especificação de propriedades personalizadas, incluindo propriedades do Sigv4, o URI do endpoint e o local do warehouse. Especifique essas propriedades da seguinte forma:

- Propriedades do Sigv4: o Sigv4 deve estar habilitado e o nome de assinatura é `glue`.
- Local do warehouse: o bucket de tabela, especificado no formato *<accountid>*`:s3tablescatalog/`*<table-bucket-name>*.
- URI do endpoint: consulte o Guia de referência dos endpoints de serviço do AWS Glue para o endpoint específico da região.

O exemplo a seguir mostra como inicializar um catálogo do pyIceberg.

```
rest_catalog = load_catalog(
        s3tablescatalog,
**{
"type": "rest",
"warehouse": "<accountid>:s3tablescatalog/<table-bucket-name>",
"uri": "https://glue.<region>.amazonaws.com/iceberg",
"rest.sigv4-enabled": "true",
"rest.signing-name": "glue",
"rest.signing-region": region
        }
)
```

Consulte mais informações sobre a implementação do endpoint Iceberg REST do AWS Glue em Conectar ao Catálogo de Dados usando o endpoint Iceberg REST do AWS Glue no Guia do usuário do AWS Glue.

Acessar tabelas usando o endpoint Iceberg REST do serviço Tabelas do Amazon S3

É possível conectar o cliente do Iceberg REST ao endpoint Iceberg REST do serviço Tabelas do Amazon S3 e fazer chamadas à REST API para criar, atualizar ou consultar tabelas em buckets de tabela do S3. O endpoint implementa um conjunto de APIs Iceberg REST padronizadas descritas na especificação da API Catalog Open do Apache Iceberg REST. Ele converte operações da Iceberg REST API em operações correspondentes do serviço Tabelas do S3.

> **Note**
>
> O endpoint Iceberg REST do serviço Tabelas do Amazon S3 pode ser usado para acessar tabelas em implementações de catálogo da AWS Partner Network (APN) ou implementações de catálogo personalizadas. Ele também pode ser usado se você precisar apenas de acesso básico de leitura/gravação a um único bucket de tabela. Em outros cenários de acesso, recomendamos usar o endpoint Iceberg REST do AWS Glue para se conectar às tabelas, que fornece gerenciamento unificado de tabelas, governança centralizada e controle de acesso refinado. Para ter mais informações, consulte Acessar tabelas do Amazon S3 usando o endpoint Iceberg REST do AWS Glue.

Configuração do endpoint

Você se conecta ao endpoint Iceberg REST do serviço Tabelas do Amazon S3 usando o endpoint de serviço. Os endpoints Iceberg REST de Tabelas do S3 têm o seguinte formato:

```
https://s3tables.<REGION>.amazonaws.com/iceberg
```

Consulte os endpoints específicos da região em Regiões da AWS e endpoints da funcionalidade Tabelas do S3.

Propriedades de configuração do catálogo

Ao usar um cliente do Iceberg para conectar um mecanismo de analytics ao endpoint de serviço, é necessário especificar as propriedades de configuração a seguir ao inicializar o catálogo. Substitua os *valores de espaços reservados* por suas informações de região e bucket de tabela.

- O endpoint específico da região como o URI do endpoint: `https://s3tables.<REGION>.amazonaws.com/iceberg`
- O ARN do bucket de tabela como localização do warehouse: `arn:aws:s3tables:<region>:<accountID>:bucket/<bucketname>`
- Propriedades do Sigv4 para autenticação. O nome de assinatura do SigV4 para as solicitações do endpoint de serviço é `s3tables`.

Os exemplos a seguir mostram como configurar diferentes clientes para usar o endpoint Iceberg REST do serviço Tabelas do Amazon S3.

PyIceberg

Para usar o endpoint Iceberg REST desse serviço com o PyIceberg, especifique as seguintes propriedades de configuração da aplicação:

```
rest_catalog = load_catalog(
  catalog_name,
  **{
    "type": "rest",
    "warehouse":"arn:aws:s3tables:<Region>:<accountID>:bucket/<bucketname>",
    "uri": "https://s3tables.<Region>.amazonaws.com/iceberg",
    "rest.sigv4-enabled": "true",
    "rest.signing-name": "s3tables",
    "rest.signing-region": "<Region>"
  }
)
```

Apache Spark

Para usar o endpoint Iceberg REST do serviço Tabelas do Amazon S3 com o Spark, especifique as propriedades de configuração a seguir da aplicação, substituindo os *valores de espaço reservado* por suas informações de região e bucket de tabela.

```
spark-shell \
```

```
  --packages "org.apache.iceberg:iceberg-spark-
runtime-3.5_2.12:1.4.1,software.amazon.awssdk:bundle:2.20.160,software.amazon.awssdk:url-
connection-client:2.20.160" \
  --master "local[*]" \
  --conf
 "spark.sql.extensions=org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions"
 \
  --conf "spark.sql.defaultCatalog=spark_catalog" \
   --conf "spark.sql.catalog.spark_catalog=org.apache.iceberg.spark.SparkCatalog" \
  --conf "spark.sql.catalog.spark_catalog.type=rest" \
  --conf "spark.sql.catalog.spark_catalog.uri=https://
s3tables.<Region>.amazonaws.com/iceberg" \
  --conf
 "spark.sql.catalog.spark_catalog.warehouse=arn:aws:s3tables:<Region>:<accountID>:bucket/
<bucketname>" \
  --conf "spark.sql.catalog.spark_catalog.rest.sigv4-enabled=true" \
  --conf "spark.sql.catalog.spark_catalog.rest.signing-name=s3tables" \
  --conf "spark.sql.catalog.spark_catalog.rest.signing-region=<Region>" \
  --conf "spark.sql.catalog.spark_catalog.io-
impl=org.apache.iceberg.aws.s3.S3FileIO" \
  --conf
 "spark.hadoop.fs.s3a.aws.credentials.provider=org.apache.hadoop.fs.s3a.SimpleAWSCredentialP
 \
  --conf "spark.sql.catalog.spark_catalog.rest-metrics-reporting-enabled=false"
```

Autenticar e autorizar o acesso ao endpoint

As solicitações de API aos endpoints de serviço de Tabelas do S3 são autenticadas usando o AWS Signature Version 4 (SigV4). Consulte AWS Signature Version 4 para solicitações de API para saber mais sobre o AWS SigV4.

O nome de assinatura do SigV4 para solicitações de endpoint Iceberg REST do serviço Tabelas do Amazon S3 é `s3tables`.

As solicitações ao endpoint Iceberg REST do serviço Tabelas do Amazon S3 são autorizadas usando ações `s3tables` do IAM correspondentes às operações de API REST. Essas permissões podem ser definidas em políticas baseadas em identidade do IAM ou em políticas baseadas em recurso anexadas a tabelas e buckets de tabela. Para ter mais informações, consulte Gerenciamento de acesso para a funcionalidade Tabelas do S3.

Você pode acompanhar as solicitações feitas às tabelas por meio do endpoint REST com o AWS CloudTrail. As solicitações serão registradas como a ação correspondente do IAM no S3. Por exemplo, uma API `LoadTable` gerará um evento de gerenciamento para a operação `GetTableMetadataLocation` e um evento de dados para a operação `GetTableData`. Para ter mais informações, consulte Registro em log com o AWS CloudTrail para a funcionalidade Tabelas do S3.

Parâmetros de caminho e prefixo

As APIs do catálogo Iceberg REST têm um prefixo de formato livre nos respectivos URLs de solicitação. Por exemplo, a chamada de API `ListNamespaces` usa o formato de URL `GET/v1/{prefix}/namespaces`. Para tabelas do S3, o `{prefix}` do caminho REST é sempre o ARN do bucket de tabelas codificado em URL.

Por exemplo, para o ARN do bucket de tabela `arn:aws:s3tables:`*`us-east-1`*`:111122223333:bucket/`*`bucketname`*, o prefixo seria `arn%3Aaws%3As3tables%3A`*`us-east-1`*`%3A`*`111122223333`*`%3Abucket%2F`*`bucketname`*.

Parâmetro do caminho do namespace

Os namespaces no caminho de API do catálogo do Iceberg REST podem ter vários níveis. No entanto, o serviço Tabelas do S3 só é compatível com namespaces de nível único. Para acessar um namespace em uma hierarquia de catálogos de vários níveis, é possível se conectar a um catálogo de vários níveis acima do namespace ao fazer referência ao namespace. Isso possibilita que qualquer mecanismo de consulta que permita a notação em três partes de `catalog.namespace.table` acesse objetos na hierarquia de catálogos do serviço Tabelas do S3 sem problemas de compatibilidade em comparação com o uso do namespace de vários níveis.

Operações de API do Iceberg REST compatíveis

A tabela a seguir contém as APIs REST do Iceberg compatíveis e mostra como elas correspondem às ações do serviço Tabelas do S3.

Operação REST do Iceberg	Caminho REST	Ação do IAM em Tabelas do S3	Nome do evento do CloudTrail
`getConfig`	`GET /v1/config`	`s3tables:GetTableBucket`	`s3tables:GetTableBucket`

Operação REST do Iceberg	Caminho REST	Ação do IAM em Tabelas do S3	Nome do evento do CloudTrail
listNamespaces	GET /v1/{prefix}/namespaces	s3tables:ListNamespaces	s3tables:ListNamespaces
createNamespace	POST /v1/{prefix}/namespaces	s3tables:CreateNamespace	s3tables:CreateNamespace
loadNamespaceMetadata	GET /v1/{prefix}/namespaces/{namespace}	s3tables:GetNamespace	s3tables:GetNamespace
dropNamespace	DELETE /v1/{prefix}/namespaces/{namespace}	s3tables:DeleteNamespace	s3tables:DeleteNamespace
listTables	GET /v1/{prefix}/namespaces/{namespace}/tables	s3tables:ListTables	s3tables:ListTables
createTable	POST /v1/{prefix}/namespaces/{namespace}/tables	s3tables:CreateTable , s3tables:PutTableData	s3tables:CreateTable , s3tables:PutObject
loadTable	GET /v1/{prefix}/namespaces/{namespace}/tables/{table}	s3tables:GetTableMetadataLocation , s3tables:GetTableData	s3tables:GetTableMetadataLocation , s3tables:GetObject

Operação REST do Iceberg	Caminho REST	Ação do IAM em Tabelas do S3	Nome do evento do CloudTrail
updateTable	POST /v1/{prefix}/namespaces/{namespace}/tables/{table}	s3tables:UpdateTableMetadataLocation, s3tables:PutTableData, s3tables:GetTableData	s3tables:UpdateTableMetadataLocation, s3tables:PutObject, s3tables:GetObject
dropTable	DELETE /v1/{prefix}/namespaces/{namespace}/tables/{table}	s3tables:DeleteTable	s3tables:DeleteTable
renameTable	POST /v1/{prefix}/tables/rename	s3tables:RenameTable	s3tables:RenameTable
tableExists	HEAD /v1/{prefix}/namespaces/{namespace}/tables/{table}	s3tables:GetTable	s3tables:GetTable
namespaceExists	HEAD /v1/{prefix}/namespaces/{namespace}	s3tables:GetNamespace	s3tables:GetNamespace

Considerações e limitações

Veja a seguir as considerações e limitações ao usar o endpoint Iceberg REST do serviço Tabelas do Amazon S3.

Considerações

- Comportamento da API CreateTable: a opção `stage-create` não é permitida para essa operação e resulta em um erro `400 Bad Request`. Isso significa que não é possível criar uma tabela com base em resultados de consultas usando `CREATE TABLE AS SELECT` (CTAS).
- Comportamento da API DeleteTable: você só pode excluir tabelas com a limpeza habilitada. A exclusão de tabelas com `purge=false` não é permitida e resulta em um erro `400 Bad Request`. Algumas versões do Spark sempre definem esse sinalizador como falso, mesmo ao executar comandos `DROP TABLE PURGE`. Você pode tentar com `DROP TABLE PURGE` ou usar a operação DeleteTable de Tabelas do S3 para excluir uma tabela.
- O endpoint só permite operações de metadados de tabela padrão. Para manutenção de tabelas, como gerenciamento de snapshots e compactação, use as operações de API de manutenção de Tabelas do S3. Para ter mais informações, consulte Manutenção da funcionalidade Tabelas do S3.

Limitações

- Namespaces multinível não são compatíveis.
- A autenticação baseada em OAuth não é compatível.
- Somente a propriedade `owner` é compatível com namespaces.
- As APIs relacionadas à visualização definidas na especificação da API Open do Apache Iceberg REST não são compatíveis.
- A execução de operações em uma tabela com um tamanho de arquivo `metadata.json` maior que 5 MB não é permitida e retornará um erro `400 Bad Request`. Para controlar o tamanho dos arquivos `metadata.json`, use as operações de manutenção de tabelas. Para ter mais informações, consulte Manutenção da funcionalidade Tabelas do S3.

Acessar tabelas do Amazon S3 com o Catálogo de Tabelas do Amazon S3 para Apache Iceberg

É possível acessar tabelas do S3 por meio de mecanismos de consulta de código aberto, como o Apache Spark, usando o catálogo de cliente do Catálogo de Tabelas do Amazon S3 para Apache Iceberg. O Catálogo de Tabelas do Amazon S3 para Apache Iceberg é uma biblioteca de código aberto hospedada pelo AWS Labs. Ele traduz as operações do Apache Iceberg nos mecanismos de consulta (como descoberta de tabelas, atualizações de metadados e adição ou remoção de tabelas) em operações de API da funcionalidade Tabelas do S3.

O Catálogo de Tabelas do Amazon S3 para Apache Iceberg é distribuído como um Maven JAR chamado `s3-tables-catalog-for-iceberg.jar`. É possível criar o JAR do catálogo de cliente no Repositório do AWS Labs GitHub ou baixá-lo no Maven. Ao se conectar às tabelas, o JAR do catálogo de cliente é usado como uma dependência quando você inicializa uma sessão do Spark para o Apache Iceberg.

Usar o Catálogo de Tabelas do Amazon S3 para Apache Iceberg com o Apache Spark

É possível usar o Catálogo de Tabelas do Amazon S3 para Apache Iceberg como catálogo de cliente para se conectar a tabelas de aplicações de código aberto ao inicializar uma sessão do Spark. Na configuração da sessão, você especifica dependências em relação ao Iceberg e ao Amazon S3, e cria um catálogo personalizado que usa o bucket de tabela como warehouse de metadados.

Pré-requisitos

- Uma identidade do IAM com acesso ao bucket de tabela e a ações da funcionalidade Tabelas do S3. Para obter mais informações, consulte Gerenciamento de acesso para a funcionalidade Tabelas do S3.

Como inicializar uma sessão do Spark usando o Catálogo de Tabelas do Amazon S3 para Apache Iceberg

- Inicialize o Spark usando o comando a seguir. Para usar o comando, substitua o *número de versão* do Catálogo de Tabelas do Amazon S3 para Apache Iceberg pela versão mais recente do Repositório do AWS Labs GitHub e o *ARN do bucket de tabela* pelo ARN da sua própria tabela.

```
spark-shell \
--packages org.apache.iceberg:iceberg-spark-
runtime-3.5_2.12:1.6.1,software.amazon.s3tables:s3-tables-catalog-for-iceberg-
runtime:0.1.4 \
--conf spark.sql.catalog.s3tablesbucket=org.apache.iceberg.spark.SparkCatalog \
--conf spark.sql.catalog.s3tablesbucket.catalog-
impl=software.amazon.s3tables.iceberg.S3TablesCatalog \
--conf spark.sql.catalog.s3tablesbucket.warehouse=arn:aws:s3tables:us-
east-1:111122223333:bucket/amzn-s3-demo-table-bucket \
--conf
 spark.sql.extensions=org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions
```

Consultar tabelas do S3 com o Spark SQL

Usando o Spark, você pode executar operações DQL, DML e DDL em tabelas do S3. Ao consultar tabelas, você usa o nome da tabela totalmente qualificado, bem como o nome do catálogo da sessão, seguindo este padrão:

CatalogName.*NamespaceName*.*TableName*

Os exemplos de consultas a seguir mostram algumas maneiras de interagir com as tabelas do S3. Para usar esses exemplos de consultas no mecanismo de consulta, substitua os valores dos *espaços reservados para entrada do usuário* pelos seus próprios.

Como consultar tabelas com o Spark

- Crie um namespace

```
spark.sql(" CREATE NAMESPACE IF NOT EXISTS s3tablesbucket.my_namespace")
```

- Criar uma tabela

```
spark.sql(" CREATE TABLE IF NOT EXISTS s3tablesbucket.my_namespace.`my_table`
( id INT, name STRING, value INT ) USING iceberg ")
```

- Consultar uma tabela

```
spark.sql(" SELECT * FROM s3tablesbucket.my_namespace.`my_table` ").show()
```

- Inserir dados em uma tabela

```
spark.sql(
"""
    INSERT INTO s3tablesbucket.my_namespace.my_table
    VALUES
        (1, 'ABC', 100),
        (2, 'XYZ', 200)
""")
```

- Carregue um arquivo de dados existente em uma tabela.

  1. Leia os dados no Spark.

```
val data_file_location = "Path such as S3 URI to data file"
```

```
val data_file = spark.read.parquet(data_file_location)
```

2. Grave os dados em uma tabela do Iceberg.

```
data_file.writeTo("s3tablesbucket.my_namespace.my_table").using("Iceberg").tableProperty
 ("format-version", "2").createOrReplace()
```

Consultar tabelas do Amazon S3 com o Amazon Athena

O Amazon Athena é um serviço de consultas interativas que você pode usar para analisar dados no Amazon S3 usando SQL padrão. Para obter mais informações, consulte O que é o Amazon Athena? no Guia do usuário do Amazon Athena.

Depois que os buckets de tabela são integrados aos serviços de analytics da AWS, é possível executar consultas Data Definition Language (DDL), Data Manipulation Language (DML) e Data Query Language (DQL) em tabelas do S3 usando o Athena. Consulte mais informações sobre como consultar tabelas em um bucket de tabela em Registrar catálogos de buckets de tabela do S3 no Guia do usuário do Amazon Athena.

Também é possível executar consultas no Athena pelo console do Amazon S3.

Usar o console do S3 e o Amazon Athena

O procedimento a seguir usa o console do Amazon S3 para acessar o editor de consultas do Athena e possibilitar que você consulte uma tabela com o Amazon Athena.

> **Note**
>
> Antes de realizar as etapas a seguir, integre os buckets de tabela aos serviços de analytics da AWS nessa região. Para obter mais informações, consulte the section called “Usar tabelas do S3 com serviços de analytics da AWS”.

Como consultar uma tabela

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets de tabela.

3. Na página Buckets de tabela, escolha o bucket que contém a tabela que você deseja consultar.
4. Na página de detalhes do bucket, escolha o botão de opção ao lado do nome da tabela que você deseja consultar.
5. Escolha Consultar tabela com o Athena.
6. O console do Amazon Athena é aberto e o editor de consultas do Athena aparece com uma amostra de consulta SELECT carregada para você. Modifique essa consulta conforme necessário para seu caso de uso.

   No editor de consultas, o campo Catálogo deve ser preenchido com s3tablescatalog/ seguido do nome do bucket de tabela; por exemplo, s3tablescatalog/***amzn-s3-demo-bucket***. O campo Banco de dados deve ser preenchido com o namespace em que a tabela está armazenada.

   > **Note**
   >
   > Caso não veja esses valores nos campos Catálogo e Banco de dados, verifique se você integrou os buckets de tabela aos serviços de analytics da AWS nessa região. Para obter mais informações, consulte the section called “Usar tabelas do S3 com serviços de analytics da AWS”.

7. Para executar a consulta, escolha Run (Executar).

   > **Note**
   >
   > - Se você receber o erro “Insufficient permissions to execute the query. Principal does not have any privilege on specified resource” ao tentar executar uma consulta no Athena, você deverá receber as permissões necessárias do Lake Formation na tabela. Para obter mais informações, consulte the section called “Conceder permissão em uma tabela ou um banco de dados”.
   > - Se você receber o erro “Iceberg cannot access the requested resource” ao tentar executar a consulta, acesse o console do AWS Lake Formation e verifique se você se autoconcedeu permissões no catálogo do bucket de tabela e no banco de dados (namespace) que criou. Não especifique uma tabela ao conceder essas permissões. Para obter mais informações, consulte the section called “Conceder permissão em uma tabela ou um banco de dados”.
   > - Se você receber a seguinte mensagem de erro ao executar uma consulta SELECT no Athena, isso significa que o nome da tabela ou os nomes de coluna na definição

da tabela contêm letras maiúsculas: “GENERIC_INTERNAL_ERROR: Get table request failed: com.amazonaws.services.glue.model.ValidationException: Unsupported Federation Resource - Invalid table or column names”. Os nomes de tabela e de coluna devem estar todos em minúsculas.

Acessar tabelas do Amazon S3 com o Amazon Redshift

O Amazon Redshift é um serviço de data warehouse rápido, totalmente gerenciado e em escala de petabytes que torna simples e econômica a análise eficiente de todos os seus dados usando as ferramentas de business intelligence existentes. O Redshift sem servidor permite acessar e analisar dados sem precisar de todas as configurações de um data warehouse provisionado. Para ter mais informações, consulte Conceitos básicos de data warehouses de tecnologia sem servidor no Guia de conceitos básicos do Amazon Redshift.

Consultar tabelas do Amazon S3 com o Amazon Redshift

Pré-requisitos

- Integre os buckets de tabela aos serviços de analytics da AWS.
  - Crie um namespace .
  - Criar uma tabela.
- Conceder permissões do Lake Formation nos recursos de tabela.

Depois de concluir os pré-requisitos, você poderá começar a usar o Amazon Redshift para consultar tabelas de uma das seguintes maneiras:

- Usando o Editor de Consultas V2 do Amazon Redshift.
- Conectando-se a um data warehouse do Amazon Redshift usando ferramentas de cliente SQL.
- Usar a API de dados do Amazon Redshift

Acessar tabelas do Amazon S3 com o Amazon EMR

O Amazon EMR (anteriormente chamado de Amazon Elastic MapReduce) é uma plataforma de cluster gerenciada que simplifica a execução de frameworks de big data, como o Apache Hadoop e Apache Spark, na AWS para processar e analisar grandes quantidades de dados. Ao usar essas

estruturas e projetos de código aberto relacionados, é possível processar dados para finalidades de analytics e workloads de inteligência de negócios. O Amazon EMR também permite transformar e mover grandes volumes de dados para dentro e para fora de outros datastores e bancos de dados da AWS.

Você pode usar clusters do Apache Iceberg no Amazon EMR para trabalhar com tabelas do S3, conectando-se a buckets de tabela em uma sessão do Spark. Para se conectar aos buckets de tabela no Amazon EMR, é possível usar a integração de serviços de analytics da AWS por meio do AWS Glue Data Catalog, ou você pode usar o catálogo de cliente de código aberto do Catálogo de Tabelas do Amazon S3 para Apache Iceberg.

> **Note**
>
> A funcionalidade Tabelas do S3 é compatível com o Amazon EMR versão 7.5 ou superior.

Conectar-se a buckets de tabela do S3 com o Spark em um cluster do Iceberg no Amazon EMR

Neste procedimento, você configura um cluster do Amazon EMR definido para Apache Iceberg, depois inicializa uma sessão do Spark que se conecta aos buckets de tabela. É possível configurar isso usando os serviços de analytics da AWS por meio do AWS Glue, ou você pode usar o catálogo de cliente de código aberto do Catálogo de Tabelas do Amazon S3 para Apache Iceberg. Para ter mais informações sobre o catálogo de cliente, consulte Acessar tabelas usando o endpoint Iceberg REST do serviço Tabelas do Amazon S3.

Escolha um método de uso de tabelas com o Amazon EMR entre as opções a seguir.

Amazon S3 Tables Catalog for Apache Iceberg

Os pré-requisitos a seguir se aplicam para consultar tabelas com o Spark no Amazon EMR usando o Catálogo de Tabelas do Amazon S3 para Apache Iceberg.

Pré-requisitos

- Anexe a política `AmazonS3TablesFullAccess` ao perfil do IAM que você usa para o Amazon EMR.

Como configurar um cluster do Amazon EMR para consultar tabelas com o Spark

1. Crie um cluster com a configuração a seguir. Para usar esse exemplo, substitua os *user input placeholders* por suas próprias informações.

```
aws emr create-cluster --release-label emr-7.5.0 \
--applications Name=Spark \
--configurations file://configurations.json \
--region us-east-1 \
--name My_Spark_Iceberg_Cluster \
--log-uri s3://amzn-s3-demo-bucket/ \
--instance-type m5.xlarge \
--instance-count 2 \
--service-role EMR_DefaultRole \
--ec2-attributes \

InstanceProfile=EMR_EC2_DefaultRole,SubnetId=subnet-1234567890abcdef0,KeyName=my-key-pair
```

`configurations.json`:

```
[{
"Classification":"iceberg-defaults",
"Properties":{"iceberg.enabled":"true"}
}]
```

2. Conecte-se ao nó primário do Spark usando SSH.
3. Para inicializar uma sessão do Spark para o Iceberg que estabelece conexão com o bucket de tabela, insira o comando a seguir. Substitua o *user input placeholders* pelo ARN do bucket de tabela.

```
spark-shell \
--packages software.amazon.s3tables:s3-tables-catalog-for-iceberg-runtime:0.1.3
 \
--conf spark.sql.catalog.s3tablesbucket=org.apache.iceberg.spark.SparkCatalog \
--conf spark.sql.catalog.s3tablesbucket.catalog-
impl=software.amazon.s3tables.iceberg.S3TablesCatalog \
--conf spark.sql.catalog.s3tablesbucket.warehouse=arn:aws:s3tables:us-
east-1:111122223333:bucket/amzn-s3-demo-bucket1 \
--conf spark.sql.defaultCatalog=s3tablesbucket \
```

```
--conf
 spark.sql.extensions=org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions
```

4. Consulte as tabelas com Spark SQL. Para conferir exemplos, consulte the section called "Consultar tabelas do S3 com o Spark SQL".

AWS analytics services integration

Os pré-requisitos a seguir se aplicam para consultar tabelas com o Spark no Amazon EMR usando a integração de serviços de analytics da AWS.

Pré-requisitos

- Integre os buckets de tabela aos serviços de analytics da AWS.
- Crie o perfil de serviço padrão para o Amazon EMR (`EMR_DefaultRole_V2`). Para conferir detalhes, consulte Service role for Amazon EMR (EMR role).
- Crie o perfil de instância do Amazon EC2 para o Amazon EMR (`EMR_EC2_DefaultRole`). Consulte detalhes em Service role for cluster EC2 instances (EC2 instance profile).
  - Anexe a política `AmazonS3TablesFullAccess` a `EMR_EC2_DefaultRole`.

Como configurar um cluster do Amazon EMR para consultar tabelas com o Spark

1. Crie um cluster com a configuração a seguir. Para usar esse exemplo, substitua os valores de *`user input placeholder`* por suas próprias informações.

```
aws emr create-cluster --release-label emr-7.5.0 \
--applications Name=Spark \
--configurations file://configurations.json \
--region us-east-1 \
--name My_Spark_Iceberg_Cluster \
--log-uri s3://amzn-s3-demo-bucket/ \
--instance-type m5.xlarge \
--instance-count 2 \
--service-role EMR_DefaultRole \
--ec2-attributes \

InstanceProfile=EMR_EC2_DefaultRole,SubnetId=subnet-1234567890abcdef0,KeyName=my-key-pair
```

`configurations.json`:

```
[{
"Classification":"iceberg-defaults",
"Properties":{"iceberg.enabled":"true"}
}]
```

2. Conecte-se ao nó primário do Spark usando SSH.
3. Insira o comando a seguir para inicializar uma sessão do Spark para o Iceberg que estabelece conexão com as tabelas. Substitua os *`user input placeholders`* por suas próprias informações.

```
spark-shell \
--conf
 spark.sql.extensions=org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions
 \
--conf spark.sql.defaultCatalog=s3tables \
--conf spark.sql.catalog.s3tables=org.apache.iceberg.spark.SparkCatalog \
--conf spark.sql.catalog.s3tables.catalog-
impl=org.apache.iceberg.aws.glue.GlueCatalog \
--conf spark.sql.catalog.s3tables.client.region=us-east-1 \
--conf spark.sql.catalog.s3tables.glue.id=111122223333
```

4. Consulte as tabelas com Spark SQL. Para conferir exemplos, consulte the section called "Consultar tabelas do S3 com o Spark SQL".

> **Note**
>
> Se você estiver usando o comando `DROP TABLE PURGE` com o Amazon EMR:
>
> - Amazon EMR versão 7.5
>
> Defina a configuração `spark.sql.catalog.`*`your-catalog-name`*`.cache-enabled` do Spark como `false`. Se essa configuração estiver definida como `true`, execute o comando em uma nova sessão ou aplicação para que o cache da tabela não seja ativado.
> - Amazon EMR versões posteriores a 7.5

Não há suporte ao `DROP TABLE`. É possível usar a API REST `DeleteTable` de Tabelas do S3 para excluir uma tabela.

Visualizar dados de tabela com o QuickSight

O QuickSight é um serviço rápido de analytics de negócios para criar visualizações, executar analytics ad hoc e extrair insights dos dados rapidamente. O QuickSight detecta facilmente fontes de dados da AWS, permite que as organizações sejam escaladas para centenas de milhares de usuários e proporciona performance de consultas rápida e responsiva usando o SPICE (mecanismo de cálculo superrápido, paralelo e em memória) do QuickSight. Para ter mais informações, consulte What is QuickSight? no Guia do usuário do QuickSight.

Depois de integrar os buckets de tabela aos serviços de analytics da AWS, você pode criar conjuntos de dados com base nas tabelas e trabalhar com eles no QuickSight usando o SPICE ou consultas SQL diretas do mecanismo de consulta. O QuickSight oferece suporte ao Athena como fonte de dados para tabelas do S3.

Configurar permissões para que o QuickSight acesse tabelas

Antes de trabalhar com dados de tabela do S3 no QuickSight, é necessário conceder permissões ao perfil de serviço e ao usuário administrador do QuickSight e conceder permissões do Lake Formation nas tabelas que você deseja acessar.

Conceder permissões ao perfil de serviço do QuickSight

Ao configurar o QuickSight pela primeira vez na conta, a AWS cria um perfil de serviço que permite que o QuickSight acesse fontes de dados em outros serviços da AWS, como Athena ou Amazon Redshift. O nome de perfil padrão é `aws-quicksight-service-role-v0`.

1. Abra o console do IAM, em https://console.aws.amazon.com/iam/.
2. Escolha Perfis e selecione o perfil de serviço do QuickSight. O nome padrão é `aws-quicksight-service-role-v0`.
3. Selecione Adicionar permissões e, em seguida, Criar política em linha.
4. Selecione JSON para abrir o editor de políticas JSON, depois adicione a política a seguir.

```
{
  "Version": "2012-10-17",
```

```
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": "glue:GetCatalog",
      "Resource": "*"
    }
  ]
}
```

5. Selecione Próximo, insira um Nome da política e escolha Criar política.

Como configurar permissões para o usuário administrador do QuickSight

1. Execute o comando da AWS CLI a seguir para localizar o ARN do usuário administrador do QuickSight.

```
aws quicksight list-users --aws-account-id 111122223333 --namespace default --
region region
```

2. Conceda permissões do Lake Formation a esse ARN. Para obter detalhes, consulte Conceder permissões do Lake Formation nos recursos de tabela.

Usar dados de tabela no QuickSight

Você pode se conectar aos dados da tabelas usando o Athena como fonte de dados.

Pré-requisitos

- Integre os buckets de tabela aos serviços de analytics da AWS.
  - Crie um namespace .
  - Criar uma tabela.
  - Configurar permissões para que o QuickSight acesse tabelas.
- Inscreva-se no QuickSight.

1. Faça login na sua conta do QuickSight em https://quicksight.aws.amazon.com/.
2. No painel, escolha Nova análise.
3. Escolha Novo conjunto de dados.

4. Selecione Athena.
5. Insira um Nome da fonte de dados e escolha Criar fonte de dados.
6. Escolha Usar SQL personalizado. Você não poderá selecionar a tabela no painel Escolher sua tabela.
7. Insira uma consulta SQL do Athena que capture as colunas que você deseja visualizar e escolha Confirmar consulta. Por exemplo, use a seguinte consulta para selecionar todas as colunas:

```
SELECT * FROM "s3tablescatalog/table-bucket-name".namespace.table-name
```

8. Escolha Visualizar para analisar os dados e começar a criar painéis. Para ter mais informações, consulte Visualizing data in QuickSight e Exploring interactive dashboards in QuickSight.

Fazer streaming de dados para tabelas com o Amazon Data Firehose

O Amazon Data Firehose é um serviço totalmente gerenciado para entrega de dados de streaming em tempo real a determinados destinos, como Amazon S3, Amazon Redshift, Amazon OpenSearch Service, Splunk, Tabelas do Apache Iceberg e endpoints HTTP personalizados ou endpoints HTTP pertencentes a provedores de serviços de terceiros compatíveis. Com o Amazon Data Firehose, você não precisa escrever aplicações nem gerenciar recursos. Configure os produtores de dados para enviar dados ao Firehose e ele entregará automaticamente os dados ao destino especificado. Você também pode configurar o Firehose para transformar os dados antes de entregá-los. Consulte mais informações sobre o Amazon Data Firehose em What is Amazon Data Firehose?.

Esse é o método de acesso para trabalhar com o serviço Tabelas do S3.

1. Integre os buckets de tabela aos serviços de analytics da AWS.
2. Configure o Firehose para entregar dados nas tabelas do S3. Para fazer isso, crie um perfil de serviço do AWS Identity and Access Management (IAM) que permita que o Firehose acesse suas tabelas.
3. Conceda ao perfil de serviço do Firehose permissões explícitas referentes á tabela ou ao namespace da tabela. Para ter mais informações, consulte Conceder permissões do Lake Formation nos recursos de tabela.
4. Crie um fluxo do Firehose que encaminhe os dados para a tabela.

Criar um perfil para o Firehose usar tabelas do S3 como destino

O Firehose precisa de um perfil de serviço do IAM com permissões específicas para acessar tabelas do AWS Glue e gravar dados nas tabelas do S3. É necessário fornecer esse perfil do IAM ao criar um fluxo do Firehose.

1. Abra o console do IAM, em https://console.aws.amazon.com/iam/.
2. No painel de navegação à esquerda, escolha Políticas.
3. Escolha Criar uma política e selecione JSON no editor de políticas.
4. Adicione a seguinte política em linha que concede permissões a todos os bancos de dados e tabelas no catálogo de dados. Se você quiser, poderá conceder permissões somente para tabelas e bancos de dados específicos. Para usar essa política, substitua os *user input placeholders* por suas próprias informações.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "S3TableAccessViaGlueFederation",
      "Effect": "Allow",
      "Action": [
        "glue:GetTable",
        "glue:GetDatabase",
        "glue:UpdateTable"
      ],
      "Resource": [
        "arn:aws:glue:region:account-id:catalog/s3tablescatalog/*",
        "arn:aws:glue:region:account-id:catalog/s3tablescatalog",
        "arn:aws:glue:region:account-id:catalog",
        "arn:aws:glue:region:account-id:database/*",
        "arn:aws:glue:region:account-id:table/*/*"
      ]
    },
    {
      "Sid": "S3DeliveryErrorBucketPermission",
      "Effect": "Allow",
      "Action": [
        "s3:AbortMultipartUpload",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
```

```
        "s3:ListBucketMultipartUploads",
        "s3:PutObject"
      ],
      "Resource": [
        "arn:aws:s3:::error delivery bucket",
        "arn:aws:s3:::error delivery bucket/*"
      ]
    },
    {
      "Sid": "RequiredWhenUsingKinesisDataStreamsAsSource",
      "Effect": "Allow",
      "Action": [
        "kinesis:DescribeStream",
        "kinesis:GetShardIterator",
        "kinesis:GetRecords",
        "kinesis:ListShards"
      ],
      "Resource": "arn:aws:kinesis:region:account-id:stream/stream-name"
    },
    {
      "Sid":
"RequiredWhenDoingMetadataReadsANDDataAndMetadataWriteViaLakeformation",
      "Effect": "Allow",
      "Action": [
        "lakeformation:GetDataAccess"
      ],
      "Resource": "*"
    },
    {
      "Sid": "RequiredWhenUsingKMSEncryptionForS3ErrorBucketDelivery",
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource": [
        "arn:aws:kms:region:account-id:key/KMS-key-id"
      ],
      "Condition": {
        "StringEquals": {
          "kms:ViaService": "s3.region.amazonaws.com"
        },
        "StringLike": {
```

```
          "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::error delivery bucket/
prefix*"
        }
      }
    },
    {
      "Sid": "LoggingInCloudWatch",
      "Effect": "Allow",
      "Action": [
        "logs:PutLogEvents"
      ],
      "Resource": [
        "arn:aws:logs:region:account-id:log-group:log-group-name:log-stream:log-
stream-name"
      ]
    },
    {
      "Sid": "RequiredWhenAttachingLambdaToFirehose",
      "Effect": "Allow",
      "Action": [
        "lambda:InvokeFunction",
        "lambda:GetFunctionConfiguration"
      ],
      "Resource": [
        "arn:aws:lambda:region:account-id:function:function-name:function-version"
      ]
    }
  ]
}
```

A política tem uma instrução que permite acesso ao Kinesis Data Streams, invocando funções do Lambda e acesso a chaves do AWS KMS. Se você não usar nenhum desses recursos, poderá remover as respectivas declarações.

Se o registro de erros em log estiver habilitado, o Firehose também enviará erros de entrega de dados para seu grupo de logs e fluxos do CloudWatch. Para isso, é necessário configurar os nomes do grupo de logs e do fluxo de logs. Para os nomes do grupo de logs e do fluxo de logs, consulte Monitor Amazon Data Firehose Using CloudWatch Logs.

5. Depois de criar a política, crie um perfil do IAM com a opção Serviço da AWS como Tipo de entidade confiável.
6. Em Serviço ou Caso de Uso, escolha Kinesis. Em Caso de uso, escolha Kinesis Firehose.

7. Selecione Próximo e escolha a política que você criou anteriormente.
8. Dê um nome à sua função. Revise os detalhes do perfil e escolha Criar perfil. O perfil terá a política de confiança a seguir.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sts:AssumeRole"
            ],
            "Principal": {
                "Service": [
                    "firehose.amazonaws.com"
                ]
            }
        }
    ]
}
```

Configurar um fluxo do Firehose para tabelas do S3

O procedimento a seguir mostra como criar um fluxo do Firehose para entregar dados às tabelas do S3 usando o console. Os pré-requisitos a seguir são necessários para configurar um fluxo do Firehose para tabelas do S3.

Pré-requisitos

- Integre os buckets de tabela aos serviços de analytics da AWS.
  - Crie um namespace .
  - Criar uma tabela.
- Crie o perfil para que o Firehose acesse as tabelas do S3.
- Conceda permissões do Lake Formation ao perfil de serviço do Firehose que você criou para acessar tabelas.

Para fornecer informações de roteamento ao Firehose ao configurar um fluxo, use namespace como o nome do banco de dados e o nome de uma tabela nesse namespace. Você pode usar esses

valores na seção “Chave exclusiva” de uma configuração de fluxo do Firehose a fim de rotear dados para uma única tabela. Você também pode usar esses valores a fim de rotear para uma tabela usando expressões de consulta JSON. Para ter mais informações, consulte Route incoming records to a single Iceberg table.

Como configurar um fluxo do Firehose para tabelas do S3 (console)

1. Abra o console do Firehose em https://console.aws.amazon.com/firehose/.
2. Escolha Criar fluxo do Firehose.
3. Em Origem, escolha uma das seguinte opções:
   - Amazon Kinesis Data Streams
   - Amazon MSK
   - PUT direto
4. Em Destino, selecione Tabelas do Apache Iceberg.
5. Insira um Nome do fluxo do Firehose.
6. Defina as Configurações da origem.
7. Em Configurações de destino, escolha Conta atual para transmitir para tabelas em sua conta ou Entre contas para tabelas em outra conta.
   - Para tabelas na Conta atual, selecione o Catálogo de Tabelas do S3 no menu suspenso Catálogo.
   - Para tabelas Entre contas, insira o ARN do catálogo para o qual você deseja transmitir em outra conta.
8. Configure os nomes do banco de dados e da tabela usando a Configuração de chave exclusiva, expressões JSONQuery ou em uma função do Lambda. Consulte mais informações em Route incoming records to a single Iceberg table e Route incoming records to different Iceberg tables no Guia do desenvolvedor do Amazon Data Firehose.
9. Em Configurações de backup, especifique um Bucket de backup do S3.
10. Em Funções do IAM existentes na seção Configurações avançadas, selecione o perfil do IAM que você criou para o Firehose.
11. Escolha Criar fluxo do Firehose.

Consulte mais informações sobre as outras configurações que você pode definir para um fluxo em Set up the Firehose stream no Guia do desenvolvedor do Amazon Data Firehose.

Executar trabalhos de ETL em tabelas do Amazon S3 com o AWS Glue

O AWS Glue é um serviço de integração de dados com tecnologia sem servidor que facilita aos usuários de analytics a descoberta, preparação, transferência e integração de dados de várias fontes. Você pode usar os trabalhos do AWS Glue para executar pipelines de extração, transformação e carregamento (ETL) a fim de carregar dados em data lakes. Para obter mais informações sobre o AWS Glue, consulte O que é o AWS Glue? no Guia do desenvolvedor do AWS Glue.

Um trabalho do AWS Glue encapsula um script que se conecta aos dados de origem, os processa e, depois, os grava no destino de dados. Normalmente, um trabalho executa scripts de extração, transformação e carga (ETL). Os trabalhos podem executar scripts projetados para os ambientes de runtime do Apache Spark. É possível monitorar trabalhos para entender as métricas do runtime, status de conclusão, duração e hora de início.

Você pode usar trabalhos do AWS Glue para processar dados em nas tabelas do S3 conectando-se às suas tabelas por meio da integração com serviços de analytics da AWS ou conectando-se diretamente por meio do endpoint Iceberg REST da funcionalidade Tabelas do Amazon S3 ou do Catálogo de Tabelas do Amazon S3 para Apache Iceberg. Este guia aborda as etapas básicas para começar a usar o AWS Glue com a funcionalidade Tabelas do S3, incluindo:

Tópicos

- Pré-requisitos
- Criar um script para se conectar aos buckets de tabela
- Criar um trabalho do AWS Glue que consulte tabelas

> **Note**
>
> A funcionalidade Tabelas do S3 é compatível com o AWS Glue versão 5.0 ou superior.

Pré-requisitos

Para poder consultar tabelas por meio de um trabalho do AWS Glue, é necessário configurar um perfil do IAM que o AWS Glue possa usar para executar o trabalho e fazer upload do JAR do Catálogo de Tabelas do Amazon S3 para Apache Iceberg em um bucket do S3 que o AWS Glue possa acessar ao executar o trabalho.

- Integre os buckets de tabela aos serviços de analytics da AWS.
- Crie um perfil do IAM para o AWS Glue.
  - Anexe a política gerenciada `AmazonS3TablesFullAccess` à função.
  - Anexe a política gerenciada `AmazonS3FullAccess` à função.
- (Opcional) Se você estiver usando o Catálogo de Tabelas do Amazon S3 para Apache Iceberg, precisará baixar o JAR do catálogo de cliente e carregá-lo em um bucket do S3.

  Baixar o JAR do catálogo

  1. Verifique a versão mais recente no Maven Central. Você pode fazer download do JAR pelo Maven Central usando um navegador ou o comando a seguir. Substitua o *número da versão* pela versão mais recente.

     ```
     wget https://repo1.maven.org/maven2/software/amazon/s3tables/s3-tables-catalog-for-iceberg-runtime/0.1.5/s3-tables-catalog-for-iceberg-runtime-0.1.5.jar
     ```

  2. Faça upload do JAR baixado para um bucket do S3 que o perfil do IAM do AWS Glue possa acessar. Você pode usar o comando da AWS CLI a seguir para fazer upload do JAR. Substitua o *número da versão* pela versão mais recente e o *nome do bucket* e o *caminho* por suas próprias informações.

     ```
     aws s3 cp s3-tables-catalog-for-iceberg-runtime-0.1.5.jar s3://amzn-s3-demo-bucket/jars/
     ```

Criar um script para se conectar aos buckets de tabela

Para acessar os dados da tabela ao executar um trabalho de ETL do AWS Glue, configure uma sessão do Spark para o Apache Iceberg que estabeleça conexão com o bucket de tabela do S3. Você pode modificar um script existente para se conectar ao bucket de tabela ou criar um script. Para ter mais informações sobre como criar scripts do AWS Glue, consulte Tutorial: gravar um script do AWS Glue para Spark no Guia do desenvolvedor do AWS Glue.

Também é possível configurar a sessão para se conectar aos buckets de tabela por meio de qualquer um dos seguintes métodos de acesso à funcionalidade Tabelas do S3:

- Integração da funcionalidade Tabelas do S3 com serviços de analytics da AWS
- Endpoint Iceberg REST da funcionalidade Tabelas do Amazon S3

- Catálogo de Tabelas do Amazon S3 para Apache Iceberg

Escolha um dos métodos de acesso a seguir para ver instruções de configuração e exemplos de configuração.

AWS analytics services integration

Um dos pré-requisitos para consultar tabelas com o Spark no AWS Glue usando a integração de serviços de analytics da AWS é integrar os buckets de tabela a serviços de analytics da AWS

Você pode configurar a conexão com seu bucket de tabela por meio de uma sessão do Spark em um trabalho ou com mágicas do AWS Glue Studio em uma sessão interativa. Para usar os exemplos a seguir, substitua os *valores de espaço reservado* pelas informações do seu bucket de tabela.

Usar um script do PySpark

Use o trecho de código a seguir em um script do PySpark para configurar um trabalho do AWS Glue e se conectar ao seu bucket de tabela usando a integração.

```
spark = SparkSession.builder.appName("SparkIcebergSQL") \
    .config("spark.sql.extensions",
 "org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions") \
    .config("spark.sql.defaultCatalog","s3tables") \
    .config("spark.sql.catalog.s3tables",
 "org.apache.iceberg.spark.SparkCatalog") \
    .config("spark.sql.catalog.s3tables.catalog-impl",
 "org.apache.iceberg.aws.glue.GlueCatalog") \
    .config("spark.sql.catalog.s3tables.glue.id",
 "111122223333:s3tablescatalog/amzn-s3-demo-table-bucket") \
    .config("spark.sql.catalog.s3tables.warehouse", "s3://amzn-s3-demo-table-
bucket/warehouse/") \
    .getOrCreate()
```

Usar de uma sessão interativa do AWS Glue

Se você estiver usando uma sessão interativa de caderno com o AWS Glue 5.0, especifique as mesmas configurações usando a mágica do `%%configure` em uma célula antes da execução do código.

```
%%configure
```

```
{"conf":
 "spark.sql.extensions=org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions
 --conf spark.sql.defaultCatalog=s3tables --conf
 spark.sql.catalog.s3tables=org.apache.iceberg.spark.SparkCatalog --conf
 spark.sql.catalog.s3tables.catalog-impl=org.apache.iceberg.aws.glue.GlueCatalog
 --conf spark.sql.catalog.s3tables.glue.id=111122223333:s3tablescatalog/amzn-s3-
demo-table-bucket --conf spark.sql.catalog.s3tables.warehouse=s3://amzn-s3-demo-
table-bucket/warehouse/"}
```

Amazon S3 Tables REST do Iceberg endpoint

Você pode configurar a conexão com seu bucket de tabela por meio de uma sessão do Spark em um trabalho ou com mágicas do AWS Glue Studio em uma sessão interativa. Para usar os exemplos a seguir, substitua os *valores de espaço reservado* pelas informações do seu bucket de tabela.

Usar um script do PySpark

Use o trecho de código a seguir em um script do PySpark para configurar um trabalho do AWS Glue e se conectar ao seu bucket de tabela usando o endpoint.

```
spark = SparkSession.builder.appName("glue-s3-tables-rest") \
    .config("spark.sql.extensions",
 "org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions") \
    .config("spark.sql.defaultCatalog", "s3_rest_catalog") \
    .config("spark.sql.catalog.s3_rest_catalog",
 "org.apache.iceberg.spark.SparkCatalog") \
    .config("spark.sql.catalog.s3_rest_catalog.type", "rest") \
    .config("spark.sql.catalog.s3_rest_catalog.uri", "https://
s3tables.Region.amazonaws.com/iceberg") \
    .config("spark.sql.catalog.s3_rest_catalog.warehouse",
 "arn:aws:s3tables:Region:111122223333:s3tablescatalog/amzn-s3-demo-table-
bucket") \
    .config("spark.sql.catalog.s3_rest_catalog.rest.sigv4-enabled", "true") \
    .config("spark.sql.catalog.s3_rest_catalog.rest.signing-name", "s3tables") \
    .config("spark.sql.catalog.s3_rest_catalog.rest.signing-region", "Region") \
    .config('spark.sql.catalog.s3_rest_catalog.io-
impl','org.apache.iceberg.aws.s3.S3FileIO') \
    .config('spark.sql.catalog.s3_rest_catalog.rest-metrics-reporting-
enabled','false') \
    .getOrCreate()
```

Usar de uma sessão interativa do AWS Glue

Se você estiver usando uma sessão interativa de caderno com o AWS Glue 5.0, especifique as mesmas configurações usando a mágica do `%%configure` em uma célula antes da execução do código. Substitua os valores de espaços reservados pelas informações do seu próprio bucket de tabela.

```
%%configure
{"conf":
 "spark.sql.extensions=org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions
 --conf spark.sql.defaultCatalog=s3_rest_catalog --conf
 spark.sql.catalog.s3_rest_catalog=org.apache.iceberg.spark.SparkCatalog
 --conf spark.sql.catalog.s3_rest_catalog.type=rest --conf
 spark.sql.catalog.s3_rest_catalog.uri=https://s3tables.Region.amazonaws.com/
iceberg --conf
 spark.sql.catalog.s3_rest_catalog.warehouse=arn:aws:s3tables:Region:111122223333:s3table
amzn-s3-demo-table-bucket --conf spark.sql.catalog.s3_rest_catalog.rest.sigv4-
enabled=true --conf spark.sql.catalog.s3_rest_catalog.rest.signing-name=s3tables
 --conf spark.sql.catalog.s3_rest_catalog.rest.signing-region=Region --conf
 spark.sql.catalog.s3_rest_catalog.io-impl=org.apache.iceberg.aws.s3.S3FileIO --
conf spark.sql.catalog.s3_rest_catalog.rest-metrics-reporting-enabled=false"}
```

Amazon S3 Tables Catalog for Apache Iceberg

Um pré-requisito para se conectar a tabelas usando o Catálogo de Tabelas do Amazon S3 para Apache Iceberg é primeiro baixar o JAR do catálogo mais recente e carregá-lo em um bucket do S3. Em seguida, ao criar seu trabalho, adicione o caminho para o JAR do catálogo de cliente como um parâmetro especial. Para ter mais informações sobre parâmetros de trabalho no AWS Glue, consulte Special parameters used in AWS Glue jobs no Guia do desenvolvedor do AWS Glue.

Você pode configurar a conexão com seu bucket de tabela por meio de uma sessão do Spark em um trabalho ou com mágicas do AWS Glue Studio em uma sessão interativa. Para usar os exemplos a seguir, substitua os *valores de espaço reservado* pelas informações do seu bucket de tabela.

Usar um script do PySpark

Use o trecho de código a seguir em um script do PySpark para configurar um trabalho do AWS Glue e se conectar ao seu bucket de tabela usando o JAR. Substitua os valores de espaços reservados pelas informações do seu próprio bucket de tabela.

```
spark = SparkSession.builder.appName("glue-s3-tables") \
    .config("spark.sql.extensions",
 "org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions") \
    .config("spark.sql.defaultCatalog", "s3tablesbucket") \
    .config("spark.sql.catalog.s3tablesbucket",
 "org.apache.iceberg.spark.SparkCatalog") \
    .config("spark.sql.catalog.s3tablesbucket.catalog-impl",
 "software.amazon.s3tables.iceberg.S3TablesCatalog") \
    .config("spark.sql.catalog.s3tablesbucket.warehouse",
 "arn:aws:s3tables:Region:111122223333:bucket/amzn-s3-demo-table-bucket") \
    .getOrCreate()
```

Usar de uma sessão interativa do AWS Glue

Se você estiver usando uma sessão interativa de caderno com o AWS Glue 5.0, especifique as mesmas configurações usando a mágica do `%%configure` em uma célula antes da execução do código. Substitua os valores de espaços reservados pelas informações do seu próprio bucket de tabela.

```
%%configure
{"conf":
 "spark.sql.extensions=org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions
 --conf spark.sql.defaultCatalog=s3tablesbucket --conf
 spark.sql.catalog.s3tablesbucket=org.apache.iceberg.spark.SparkCatalog
 --conf spark.sql.catalog.s3tablesbucket.catalog-
impl=software.amazon.s3tables.iceberg.S3TablesCatalog --conf
 spark.sql.catalog.s3tablesbucket.warehouse=arn:aws:s3tables:Region:111122223333:bucket/
amzn-s3-demo-table-bucket", "extra-jars": "s3://amzn-s3-demo-bucket/jars/s3-
tables-catalog-for-iceberg-runtime-0.1.5.jar"}
```

Scripts de amostra

Os scripts de exemplo do PySpark a seguir podem usados para testar a consulta de tabelas do S3 com um trabalho do AWS Glue. Esses scripts se conectam ao bucket de tabela e executam

consultas para: criar um namespace, criar uma tabela de exemplo, inserir dados na tabela e retornar os dados da tabela. Para usar os script, substitua os *valores de espaço reservado* pelas informações do seu próprio bucket de tabela.

Escolha entre os scripts a seguir com base no seu método de acesso à funcionalidade Tabelas do S3.

S3 Tables integration with AWS analytics services

```
from pyspark.sql import SparkSession

spark = SparkSession.builder.appName("SparkIcebergSQL") \
    .config("spark.sql.extensions",
 "org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions") \
    .config("spark.sql.defaultCatalog","s3tables")
    .config("spark.sql.catalog.s3tables", "org.apache.iceberg.spark.SparkCatalog") \
    .config("spark.sql.catalog.s3tables.catalog-impl",
 "org.apache.iceberg.aws.glue.GlueCatalog") \
    .config("spark.sql.catalog.s3tables.glue.id",
 "111122223333:s3tablescatalog/amzn-s3-demo-table-bucket") \
    .config("spark.sql.catalog.s3tables.warehouse", "s3://amzn-s3-demo-table-bucket/
bucket/amzn-s3-demo-table-bucket") \
    .getOrCreate()

namespace = "new_namespace"
table = "new_table"

spark.sql("SHOW DATABASES").show()

spark.sql(f"DESCRIBE NAMESPACE {namespace}").show()

spark.sql(f"""
    CREATE TABLE IF NOT EXISTS {namespace}.{table} (
       id INT,
       name STRING,
       value INT
    )
""")

spark.sql(f"""
    INSERT INTO {namespace}.{table}
    VALUES
       (1, 'ABC', 100),
```

```
       (2, 'XYZ', 200)
""")

spark.sql(f"SELECT * FROM {namespace}.{table} LIMIT 10").show()
```

Amazon S3 Tables REST do Iceberg endpoint

```
from pyspark.sql import SparkSession

spark = SparkSession.builder.appName("glue-s3-tables-rest") \
    .config("spark.sql.extensions",
 "org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions") \
    .config("spark.sql.defaultCatalog", "s3_rest_catalog") \
    .config("spark.sql.catalog.s3_rest_catalog",
 "org.apache.iceberg.spark.SparkCatalog") \
    .config("spark.sql.catalog.s3_rest_catalog.type", "rest") \
    .config("spark.sql.catalog.s3_rest_catalog.uri", "https://
s3tables.Region.amazonaws.com/iceberg") \
    .config("spark.sql.catalog.s3_rest_catalog.warehouse",
 "arn:aws:s3tables:Region:111122223333:bucket/amzn-s3-demo-table-bucket") \
    .config("spark.sql.catalog.s3_rest_catalog.rest.sigv4-enabled", "true") \
    .config("spark.sql.catalog.s3_rest_catalog.rest.signing-name", "s3tables") \
    .config("spark.sql.catalog.s3_rest_catalog.rest.signing-region", "Region") \
    .config('spark.sql.catalog.s3_rest_catalog.io-
impl','org.apache.iceberg.aws.s3.S3FileIO') \
    .config('spark.sql.catalog.s3_rest_catalog.rest-metrics-reporting-
enabled','false') \
    .getOrCreate()

namespace = "s3_tables_rest_namespace"
table = "new_table_s3_rest"

spark.sql("SHOW DATABASES").show()

spark.sql(f"DESCRIBE NAMESPACE {namespace}").show()

spark.sql(f"""
    CREATE TABLE IF NOT EXISTS {namespace}.{table} (
       id INT,
       name STRING,
       value INT
    )
""")
```

```
spark.sql(f"""
    INSERT INTO {namespace}.{table}
    VALUES
       (1, 'ABC', 100),
       (2, 'XYZ', 200)
""")

spark.sql(f"SELECT * FROM {namespace}.{table} LIMIT 10").show()
```

Amazon S3 Tables Catalog for Apache Iceberg

```
from pyspark.sql import SparkSession

#Spark session configurations
spark = SparkSession.builder.appName("glue-s3-tables") \
    .config("spark.sql.extensions",
 "org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions") \
    .config("spark.sql.defaultCatalog", "s3tablesbucket") \
    .config("spark.sql.catalog.s3tablesbucket",
 "org.apache.iceberg.spark.SparkCatalog") \
    .config("spark.sql.catalog.s3tablesbucket.catalog-impl",
 "software.amazon.s3tables.iceberg.S3TablesCatalog") \
    .config("spark.sql.catalog.s3tablesbucket.warehouse",
 "arn:aws:s3tables:Region:111122223333:bucket/amzn-s3-demo-table-bucket") \
    .getOrCreate()

#Script
namespace = "new_namespace"
table = "new_table"

spark.sql(f"CREATE NAMESPACE IF NOT EXISTS s3tablesbucket.{namespace}")
spark.sql(f"DESCRIBE NAMESPACE {namespace}").show()

spark.sql(f"""
    CREATE TABLE IF NOT EXISTS {namespace}.{table} (
       id INT,
       name STRING,
       value INT
    )
""")
```

```
spark.sql(f"""
    INSERT INTO {namespace}.{table}
    VALUES
       (1, 'ABC', 100),
       (2, 'XYZ', 200)
""")

spark.sql(f"SELECT * FROM {namespace}.{table} LIMIT 10").show()
```

Criar um trabalho do AWS Glue que consulte tabelas

Os procedimentos a seguir mostram como configurar trabalhos do AWS Glue que se conectam aos buckets de tabela do S3. Você pode fazer isso usando a AWS CLI ou usando o console com o editor de script do AWS Glue Studio. Para ter mais informações, consulte Criar trabalhos no AWS Glue no Guia do usuário do AWS Glue.

Usar o editor de script do AWS Glue Studio

O procedimento a seguir mostra como usar o editor de scripts do AWS Glue Studio para criar um trabalho de ETL que consulta as tabelas do S3.

Pré-requisitos

- Pré-requisitos
- Criar um script para se conectar aos buckets de tabela

1. Abra o console do AWS Glue em https://console.aws.amazon.com/glue/.
2. No painel de navegação, escolha Trabalhos de ETL.
3. Escolha Editor de scripts, depois selecione Fazer upload de script e faça upload do script PySpark que você criou para consultar tabelas do S3.
4. Selecione a guia Detalhes do trabalho e insira as informações a seguir em Propriedades básicas.
   - Em Nome, insira um nome para o trabalho.
   - Em Perfil do IAM, selecione o perfil que você criou para o AWS Glue.
5. (Opcional) Se estiver usando o Catálogo de Tabelas do Amazon S3 para o método de acesso Apache Iceberg, expanda Propriedades avançadas e, em Caminho de JARs dependentes, insira

o URI do S3 do JAR do catalogo de cliente client catalog jar que você carregou em um bucket do S3 como pré-requisito. Por exemplo, s3://*amzn-s3-demo-bucket1*/*jars*/s3-tables-catalog-for-iceberg-runtime-*0.1.5*.jar

6. Selecione Salvar para criar o trabalho.
7. Escolha Executar para iniciar o trabalho e revise o status do trabalho na guia Execuções.

Como usar o AWS CLI

O procedimento a seguir mostra como usar a AWS CLI para criar um trabalho de ETL que consulta as tabelas do S3. Para usar os comandos, substitua os *valores de espaços reservados* por suas próprias informações.

Pré-requisitos

- Pré-requisitos
- Criar um script para se conectar aos buckets de tabela e faça upload dele em um bucket do S3.

1. Crie um trabalho do AWS Glue.

```
aws glue create-job \
--name etl-tables-job \
--role arn:aws:iam::111122223333:role/AWSGlueServiceRole \
--command '{
    "Name": "glueetl",
    "ScriptLocation": "s3://amzn-s3-demo-bucket1/scripts/glue-etl-query.py",
    "PythonVersion": "3"
}' \
--default-arguments '{
    "--job-language": "python",
    "--class": "GlueApp"
}' \
--glue-version "5.0"
```

> **Note**
>
> (Opcional) Se você estiver usando o Catálogo de Tabelas do Amazon S3 para o método de acesso Apache Iceberg, adicione o JAR do catálogo de cliente a `--default-arguments` usando o parâmetro `--extra-jars`. Substitua os *espaços reservados de entrada* por suas próprias informações ao adicionar o parâmetro.

```
                            "--extra-jars": "s3://amzn-s3-demo-bucket/jar-
path/s3-tables-catalog-for-iceberg-runtime-0.1.5.jar"
```

2. Inicie o trabalho.

```
aws glue start-job-run \
--job-name etl-tables-job
```

3. Para revisar o status do trabalho, copie o ID de execução do comando anterior e insira-o no comando a seguir.

```
aws glue get-job-run --job-name etl-tables-job \
--run-id jr_ec9a8a302e71f8483060f87b6c309601ea9ee9c1ffc2db56706dfcceb3d0e1ad
```

Regiões da AWS, endpoints e cotas de serviço da funcionalidade Tabelas do S3

As seções a seguir incluem as Regiões da AWS compatíveis e as cotas de serviço da funcionalidade Tabelas do S3.

Tópicos

- Regiões da AWS e endpoints da funcionalidade Tabelas do S3
- Cotas da funcionalidade Tabelas do S3

Regiões da AWS e endpoints da funcionalidade Tabelas do S3

Para obter uma lista das regiões em que o serviço Tabelas do S3 está disponível no momento, consulte Amazon S3 endpoints. Para se conectar a um serviço da AWS de forma programática, use um endpoint. Para obter mais informações, consulte Endpoints de serviço da AWS. Para ter mais informações sobre os endpoints do Amazon S3, consulte Amazon S3 endpoints.

Nome da região	Região	Endpoint	Protocolo	Compatibilidade com versões do Signature
África (Cidade do Cabo)	af-south-1	`s3tables.af-south-1.amazonaws.com`	HTTPS	4
Ásia-Pacífico (Hong Kong)	ap-east-1	`s3tables.ap-east-1.amazonaws.com`	HTTPS	4
Ásia-Pacífico (Tóquio)	ap-northeast-1	`s3tables.ap-northeast-1.amazonaws.com`	HTTPS	4
Ásia-Pacífico (Seul)	ap-northeast-2	`s3tables.ap-northeast-2.amazonaws.com`	HTTPS	4
Ásia-Pacífico (Osaka)	ap-northeast-3	`s3tables.ap-northeast-3.amazonaws.com`	HTTPS	4
Ásia-Pacífico (Mumbai)	ap-south-1	`s3tables.ap-south-1.amazonaws.com`	HTTPS	4
Ásia-Pacífico (Hyderabad)	ap-south-2	`s3tables.ap-south-`	HTTPS	4

Nome da região	Região	Endpoint	Protocolo	Compatibilidade com versões do Signature
		2.amazonaws.com		
Ásia-Pacífico (Singapura)	ap-southeast-1	s3tables.ap-southeast-1.amazonaws.com	HTTPS	4
Ásia-Pacífico (Sydney)	ap-southeast-2	s3tables.ap-southeast-2.amazonaws.com	HTTPS	4
Ásia-Pacífico (Jacarta)	ap-southeast-3	s3tables.ap-southeast-3.amazonaws.com	HTTPS	4
Ásia-Pacífico (Melbourne)	ap-southeast-4	s3tables.ap-southeast-4.amazonaws.com	HTTPS	4
Ásia-Pacífico (Malásia)	ap-southeast-5	s3tables.ap-southeast-5.amazonaws.com	HTTPS	4
Ásia-Pacífico (Tailândia)	ap-southeast-7	s3tables.ap-southeast-7.amazonaws.com	HTTPS	4

Nome da região	Região	Endpoint	Protocolo	Compatibilidade com versões do Signature
Canadá (Central)	ca-central-1	`s3tables.ca-central-1.amazonaws.com`	HTTPS	4
Oeste do Canadá (Calgary)	ca-west-1	`s3tables.ca-west-1.amazonaws.com`	HTTPS	4
Europa (Frankfurt)	eu-central-1	`s3tables.eu-central-1.amazonaws.com`	HTTPS	4
Europa (Zurique)	eu-central-2	`s3tables.eu-central-2.amazonaws.com`	HTTPS	4
Europa (Estocolmo)	eu-north-1	`s3tables.eu-north-1.amazonaws.com`	HTTPS	4
Europa (Milão)	eu-south-1	`s3tables.eu-south-1.amazonaws.com`	HTTPS	4
Europa (Espanha)	eu-south-2	`s3tables.eu-south-2.amazonaws.com`	HTTPS	4

Nome da região	Região	Endpoint	Protocolo	Compatibilidade com versões do Signature
Europa (Irlanda)	eu-west-1	`s3tables.eu-west-1.amazonaws.com`	HTTPS	4
Europa (Londres)	eu-west-2	`s3tables.eu-west-2.amazonaws.com`	HTTPS	4
Europa (Paris)	eu-west-3	`s3tables.eu-west-3.amazonaws.com`	HTTPS	4
Israel (Tel Aviv)	il-central-1	`s3tables.il-central-1.amazonaws.com`	HTTPS	4
Oriente Médio (Emirados Árabes Unidos)	me-central-1	`s3tables.me-central-1.amazonaws.com`	HTTPS	4
Oriente Médio (Barém)	me-south-1	`s3tables.me-south-1.amazonaws.com`	HTTPS	4
México (Central)	mx-central-1	`s3tables.mx-central-1.amazonaws.com`	HTTPS	4

Nome da região	Região	Endpoint	Protocolo	Compatibilidade com versões do Signature
América do Sul (São Paulo)	sa-east-1	`s3tables.sa-east-1.amazonaws.com`	HTTPS	4
Leste dos EUA (Norte da Virgínia)	us-east-1	`s3tables.us-east-1.amazonaws.com`	HTTPS	4
Leste dos EUA (Ohio)	us-east-2	`s3tables.us-east-2.amazonaws.com`	HTTPS	4
Oeste dos EUA (N. da Califórnia)	us-west-1	`s3tables.us-west-1.amazonaws.com`	HTTPS	4
Oeste dos EUA (Oregon)	us-west-2	`s3tables.us-west-2.amazonaws.com`	HTTPS	4

Cotas da funcionalidade Tabelas do S3

As cotas, também chamadas de limites, correspondem ao número máximo de recursos ou operações de serviço para uma Conta da AWS. Veja a seguir as cotas para os recursos da funcionalidade Tabelas do S3. Para ter mais informações sobre as cotas do Amazon S3, consulte Amazon S3 quotas.

Name	Padrão	Ajustável	Descrição
Buckets de tabela	10	Para solicitar um aumento na cota, entre em contato com o Suporte.	O número de buckets de tabela do Amazon S3 que você pode criar por Região da AWS em uma conta.
Namespaces	10.000	Para solicitar um aumento na cota, entre em contato com o Suporte.	O número de namespaces de tabelas do Amazon S3 que você pode criar por bucket de tabela.
Tabelas	10.000	Para solicitar um aumento na cota, entre em contato com o Suporte.	O número de tabelas do Amazon S3 que você pode criar por bucket de tabela.

Segurança para a funcionalidade Tabelas do S3

O Amazon S3 fornece uma variedade de recursos e ferramentas de segurança. A lista a seguir apresenta os recursos e as ferramentas compatíveis com a funcionalidade Tabelas do S3. A aplicação adequada dessas ferramentas pode ajudar a garantir que os recursos permaneçam protegidos e só possam ser acessados pelos usuários pretendidos.

Políticas baseadas em identidade

As políticas baseadas em identidade são anexadas a um usuário, grupo ou função do IAM. Você pode usar políticas baseadas em identidade para conceder a uma identidade do IAM acesso a tabelas ou buckets de tabela. Por padrão, usuários e perfis não têm permissão para criar nem modificar tabelas e buckets de tabela. Eles também não podem executar tarefas usando o console do S3, a AWS CLI ou as APIs REST do Amazon S3. É possível criar usuários, grupos e perfis do IAM em sua conta e anexar políticas de acesso a eles. Depois, você pode conceder acesso aos recursos. Para criar e acessar tabelas e buckets de tabela, um administrador do IAM deve conceder

as permissões necessárias aos usuários ou ao perfil do AWS Identity and Access Management (IAM). Para ter mais informações, consulte Access management for S3 Tables.

Políticas baseadas em recursos

Políticas baseadas em recurso são anexadas a um recurso. Você pode criar políticas baseadas em recurso para as tabelas e os buckets de tabela. Você pode usar uma política de bucket de tabela para controlar as permissões de acesso à API ao nível do bucket de tabela e do namespace. Você também pode usar uma política de bucket de tabela para controlar as permissões de API ao nível da tabela em várias tabelas de um bucket. Dependendo da definição da política, as permissões anexadas ao bucket podem ser aplicadas a todas as tabelas ou a tabelas específicas no bucket. Você também pode usar uma política de tabela para conceder permissões de acesso à API ao nível da tabela a tabelas individuais do bucket.

Quando a funcionalidade Tabelas do S3 recebe uma solicitação para executar uma operação de tabela ou de bucket de tabela, primeiro ela verifica se o solicitante tem as permissões necessárias. Ela avalia todas as políticas de acesso, políticas de usuário e políticas baseadas em recurso relevantes para decidir se autoriza a solicitação (política de usuário do IAM, política de perfil do IAM, política de bucket de tabela e política de tabela). Com as políticas de bucket de tabela e as políticas de tabela, é possível personalizar o acesso aos recursos para garantir que somente as identidades que você aprovou possam acessar os recursos e executar ações neles. Para ter mais informações, consulte Access management for S3 Tables.

Políticas de controle de serviços (SCPs) do AWS Organizations para a funcionalidade Tabelas do S3

Você pode usar a funcionalidade Tabelas do Amazon S3 em políticas de controle de serviços (SCPs) para gerenciar as permissões dos usuários na sua organização. De maneira semelhante às políticas do IAM e de recursos, todas as ações ao nível da tabela e do bucket são referenciadas como parte do namespace `s3tables` nas políticas. Para obter mais informações, consulte Políticas de controle de serviços (SCPs) no Guia do usuário do AWS Organizations.

Tópicos

- Proteger os dados de tabela do S3 com criptografia
- Gerenciamento de acesso para a funcionalidade Tabelas do S3
- Conectividade de VPC para a funcionalidade Tabelas do S3
- Considerações e limitações de segurança para a funcionalidade Tabelas do S3

Proteger os dados de tabela do S3 com criptografia

Usar a criptografia do lado do servidor com chaves do AWS KMS (SSE-KMS) em buckets de tabela

Tópicos

- Como o SSE-KMS funciona para tabelas e buckets de tabela
- Impor e definir o escopo de uso do SSE-KMS para tabelas e buckets de tabela
- Monitorar e auditor da criptografia SSE-KMS para tabelas e buckets de tabela
- Requisitos de permissão para criptografia SSE-KMS da funcionalidade Tabelas do S3
- Especificar a criptografia do lado do servidor com chaves do AWS KMS (SSE-KMS) em buckets de tabela

Os buckets de tabela têm uma configuração de criptografia padrão que automaticamente criptografa tabelas usando criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3). Essa criptografia se aplica a todas as tabelas nos buckets de tabela do S3 e não tem custo para você.

Se precisar de maior controle sobre suas chaves de criptografia, como gerenciar a alternância de chaves e as concessões de política de acesso, poderá configurar os buckets de tabela para usar a criptografia do lado do servidor com chaves do AWS Key Management Service (AWS KMS) (SSE-KMS). Os controles de segurança do AWS KMS podem ajudá-lo a satisfazer os requisitos de conformidade relacionados à criptografia. Para obter mais informações sobre SSE-KMS, consulte Usar criptografia do lado do servidor com o AWS KMS (SSE-KMS).

Como o SSE-KMS funciona para tabelas e buckets de tabela

O SSE-KMS com buckets de tabela difere do SSE-KMS em buckets de uso geral nos seguintes aspectos:

- Você pode especificar configurações de criptografia para buckets de tabela e tabelas individuais.
- Você só pode usar chaves gerenciadas pelo cliente com o SSE-KMS. Não são permitidas chaves gerenciadas pela AWS.
- Você deve conceder permissões a determinados perfis e entidades principais de serviço da AWS para acessarem sua chave do AWS KMS. Para obter mais informações, consulte Requisitos de permissão para criptografia SSE-KMS da funcionalidade Tabelas do S3. Isso inclui conceder acesso a:

  - Entidade principal de manutenção do S3: para realizar a manutenção em tabelas criptografadas.
  - Perfil de integração da funcionalidade Tabelas do S3: para trabalhar com tabelas criptografadas em serviços de analytics da AWS.
  - Perfil de acesso ao cliente: para acesso direto a tabelas criptografadas de clientes Apache Iceberg.
  - Entidade principal do S3 Metadata: para atualizar tabelas de metadados criptografadas do S3.
- As tabelas criptografadas usam chaves em nível de tabela que minimizam o número de solicitações feitas ao AWS KMS para tornar o trabalho com tabelas criptografadas com SSE-KMS mais econômico.

Criptografia SSE-KMS para buckets de tabela

Ao criar um bucket de tabela, você pode escolher o SSE-KMS como o tipo de criptografia padrão e selecionar uma chave do KMS específica para ser usada na criptografia. Todas as tabelas criadas nesse bucket herdarão automaticamente essas configurações de criptografia do bucket de tabela. A qualquer momento, você pode usar o AWS CLI, a API do S3 ou os SDKs da AWS para modificar ou remover as configurações de criptografia padrão em um bucket de tabela. Ao modificar as configurações de criptografia em um bucket de tabela, essas configurações se aplicam somente às novas tabelas criadas nesse bucket. As configurações de criptografia para tabelas preexistentes não são alteradas. Para obter mais informações, consulte Especificar criptografia para buckets de tabela.

Criptografia SSE-KMS para tabelas

Você também tem a opção de criptografar uma tabela individual com uma chave do KMS diferente, independentemente da configuração de criptografia padrão do bucket. Para definir a criptografia para uma tabela individual, você deve especificar a chave de criptografia desejada ao criar a tabela. Se quiser alterar a criptografia de uma tabela existente, precisará criar uma tabela com a chave desejada e copiar os dados da tabela antiga para a nova. Para obter mais informações, consulte Especificar criptografia para tabelas.

Ao usar a criptografia do AWS KMS, a funcionalidade Tabelas do S3 cria automaticamente chaves de dados exclusivas em nível de tabela que criptografam novos objetos associados a cada tabela. Essas chaves são usadas por um período limitado, minimizando a necessidade de solicitações adicionais ao AWS KMS durante as operações de criptografia e reduzindo o custo da criptografia. Isso é semelhante a Chaves de bucket S3 para SSE-KMS.

Impor e definir o escopo de uso do SSE-KMS para tabelas e buckets de tabela

Você pode usar políticas baseadas em recursos da funcionalidade Tabelas do S3, políticas de chave do KMS, políticas baseadas em identidade do IAM ou qualquer combinação delas para impor o uso do SSE-KMS a tabelas e buckets de tabela do S3. Para ter mais informações sobre políticas de identidade e recursos destinados a tabelas, consulte Gerenciamento de acesso para a funcionalidade Tabelas do S3. Para ter mais informações sobre políticas de chave, consulte Key policies no Guia do desenvolvedor do AWS Key Management Service. Os exemplos a seguir mostram como você pode usar políticas para impor o uso do SSE-KMS.

Impor o uso do SSE-KMS para todas as tabelas com uma política de bucket de tabela

Este é um exemplo de política de bucket de tabela que impede que os usuários criem tabelas em um bucket de tabela específico, a menos que criptografem tabelas com uma chave do AWS KMS específica. Para usar essa política, substitua os *espaços reservados para entrada do usuário* por suas próprias informações:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EnforceKMSEncryption",
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "s3tables:CreateTable"
      ],
      "Resource": [
        "<table-bucket-arn>/*"
      ],
      "Condition": {
        "StringNotEquals": {
          "s3tables:sseAlgorithm": "aws:kms",
          "s3tables:kmsKeyArn": "<kms-key-arn>"
        }
      }
    }
  ]
}
```

Exigir que os usuários usem a criptografia SSE-KMS com uma política do IAM

Essa política de identidade do IAM exige que os usuários usem uma chave do AWS KMS específica para criptografia ao criar ou configurar recursos da funcionalidade Tabelas do S3. Para usar essa política, substitua os *espaços reservados para entrada do usuário* por suas próprias informações:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RequireKMSKeyOnTables",
      "Action": [
          "s3tables:CreateTableBucket",
          "s3tables:PutTableBucketEncryption",
          "s3tables:CreateTable"
      ]
      "Effect": "Deny",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
            "s3tables:sseAlgorithm": "aws:kms",
            "s3tables:kmsKeyArn": "<key_arn>"
        }
      }
    }
  ]
}
```

Restringir o uso de uma chave a um bucket de tabela específico com uma política de chave do KMS

Este exemplo de política de chave do KMS permite que a chave seja usada por um usuário específico somente para operações de criptografia em um bucket de tabela específico. Esse tipo de política é útil para limitar o acesso a uma chave em cenários entre contas. Para usar essa política, substitua os *espaços reservados para entrada do usuário* por suas próprias informações:

```
{
  "Version": "2012-10-17",
  "Id": "Id",
  "Statement": [
    {
      "Sid": "AllowPermissionsToKMS",
```

```
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
      },
      "Action": [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:EncryptionContext:aws:s3:arn": "<table-bucket-arn>/*"
        }
      }
    }
  ]
}
```

Monitorar e auditor da criptografia SSE-KMS para tabelas e buckets de tabela

Para auditar o uso das chaves do AWS KMS para seus dados criptografados por SSE-KMS, você pode usar logs do AWS CloudTrail. Você pode obter informações sobre suas operações criptográficas, como `GenerateDataKey` e `Decrypt`. O CloudTrail oferece suporte a vários valores de atributos para filtrar a pesquisa, como nome do evento, nome de usuário e origem do evento.

Você pode rastrear solicitações de configuração de criptografia para tabelas e buckets de tabela do Amazon S3 usando eventos do CloudTrail. Os seguintes nomes de eventos de API são usados nos logs do CloudTrail:

- `s3tables:PutTableBucketEncryption`
- `s3tables:GetTableBucketEncryption`
- `s3tables:DeleteTableBucketEncryption`
- `s3tables:GetTableEncryption`
- `s3tables:CreateTable`
- `s3tables:CreateTableBucket`

> **Note**
>
> Não é possível usar buckets de tabela no EventBridge.

Requisitos de permissão para criptografia SSE-KMS da funcionalidade Tabelas do S3

Ao usar a criptografia do lado do servidor com chaves do AWS Key Management Service (AWS KMS) (SSE-KMS) para tabelas nos buckets de tabela do S3, é necessário conceder permissões a diferentes identidades em sua conta. No mínimo, sua identidade de acesso e a entidade principal de manutenção da funcionalidade Tabelas do S3 precisam acessar sua chave. As outras permissões necessárias dependem do seu caso de uso.

Permissões obrigatórias

Para acessar uma tabela criptografada com uma chave do KMS, você precisa destas permissões nessa chave:

- `kms:GenerateDataKey`
- `kms:Decrypt`

> **Important**
>
> Para usar o SSE-KMS em tabelas, a entidade principal do serviço de manutenção da funcionalidade Tabelas do Amazon S3 (`maintenance.s3tables.amazonaws.com`) precisa das permissões `kms:GenerateDataKey` e `kms:Decrypt` na chave.

Permissões adicionais

Estas permissões adicionais são necessárias dependendo do seu caso de uso:

- Permissões para a integração de serviços de analytics da AWS: se você trabalha com tabelas criptografadas com SSE-KMS em serviços de analytics da AWS, seu perfil de integração precisa de permissão para usar sua chave do KMS.
- Permissões para acesso direto: se você trabalha diretamente com tabelas criptografadas com SSE-KMS, por meio de métodos como o endpoint de Tabelas do Amazon S3 Iceberg REST ou o Catálogo de Tabelas do Amazon S3 para Apache Iceberg, será necessário permitir que o perfil do IAM que seu cliente usa acesse sua chave.
- Permissões para tabelas do S3 Metadata: se você usa a criptografia SSE-KMS para tabelas de metadados do S3, precisará fornecer à entidade principal do serviço de metadados do S3 (`metadata.s3.amazonaws.com`) acesso à sua chave do KMS. Isso permite que o S3 Metadata atualize tabelas criptografadas para que elas reflitam as alterações mais recentes nos dados.

> **Note**
>
> Para chaves do KMS entre contas, seu perfil do IAM precisa de permissão de acesso à chave e autorização explícita na política de chave. Para ter mais informações sobre permissões entre contas referentes a chaves do KMS, consulte Allowing external AWS accounts to use a KMS key no Guia do desenvolvedor do AWS Key Management Service.

Tópicos

- Conceder à entidade principal do serviço de manutenção da funcionalidade Tabelas do S3 permissões para sua chave do KMS
- Conceder permissões a entidades principais do IAM para trabalhar com tabelas criptografadas em serviços integrados de analytics da AWS
- Conceder às entidades principais do IAM permissões para trabalhar diretamente com tabelas criptografadas
- Conceder permissões à entidade principal do serviço S3 Metadata para usar sua chave do KMS

Conceder à entidade principal do serviço de manutenção da funcionalidade Tabelas do S3 permissões para sua chave do KMS

Essa permissão é necessária para criar tabelas criptografadas com SSE-KMS e permitir a manutenção automática de tabelas, como compactação, gerenciamento de snapshots e remoção de arquivos sem referência nas tabelas criptografadas.

> **Note**
>
> Sempre que você faz uma solicitação para criar uma tabela criptografada com SSE-KMS, a funcionalidade Tabelas do S3 verifica se a entidade principal `maintenance.s3tables.amazonaws.com` tem acesso à sua chave do KMS. Para realizar essa verificação, um objeto de zero byte é criado temporariamente no bucket de tabela. Esse objeto será removido automaticamente pelas operações de manutenção de remoção de arquivos sem referência. Se a chave do KMS especificada para criptografia não tiver acesso de manutenção, a operação createTable falhará.

Para conceder acesso de manutenção em tabelas criptografadas com SSE-KMS, você pode usar o exemplo de política de chave a seguir. Nessa política, a entidade principal de serviço

`maintenance.s3tables.amazonaws.com` recebe permissão para usar uma chave do KMS específica para criptografar e descriptografar tabelas em um bucket de tabela específico. Para usar essa política, substitua os *espaços reservados para entrada do usuário* por suas próprias informações:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EnableKeyUsage",
            "Effect": "Allow",
            "Principal": {
                "Service": "maintenance.s3tables.amazonaws.com"
            },
            "Action": [
                "kms:GenerateDataKey",
                "kms:Decrypt"
            ],
            "Resource": "<kms-key-arn>",
            "Condition": {
                "StringLike": {
                    "kms:EncryptionContext:aws:s3:arn":"<table-or-table-bucket-arn>/*"
                }
            }
        }
    ]
}
```

Conceder permissões a entidades principais do IAM para trabalhar com tabelas criptografadas em serviços integrados de analytics da AWS

Para trabalhar com tabelas do S3 em serviços de analytics da AWS, integre os buckets de tabela ao Amazon SageMaker Lakehouse. Essa integração permite que os serviços de analytics da AWS descubram e acessem dados de tabela automaticamente. Para ter mais informações sobre integração, consulte Usar tabelas do Amazon S3 com serviços de analytics da AWS.

Quando você trabalha com tabelas criptografadas com SSE-KMS nesses serviços, o perfil que você usa precisa ter permissão para usar sua chave do AWS KMS para operações de criptografia. Você pode aplicar essas permissões ao perfil `S3TablesRoleForLakeFormation` criado durante a integração ou ao seu próprio perfil do IAM.

O exemplo de política do IAM em linha a seguir pode ser usado para permitir que o perfil de serviço `S3TablesRoleForLakeFormation` use uma chave do KMS específica em sua conta para operações de criptografia. Para usar os comandos, substitua os *valores de espaço reservado para entrada* por suas próprias informações.

```
{
  "Sid": "AllowTableRoleAccess",
  "Effect": "Allow",
  "Principal": {
 "AWS": "arn:aws:iam::111122223333:role/service-role/S3TablesRoleForLakeFormation"
  },
  "Action": [
      "kms:GenerateDataKey",
      "kms:Decrypt"
  ],
  "Resource": "<kms-key-arn>"
}
```

Conceder às entidades principais do IAM permissões para trabalhar diretamente com tabelas criptografadas

Ao trabalhar com tabelas criptografadas usando métodos de acesso direto ou de terceiros, você deve conceder ao perfil que você usa acesso à sua chave do KMS. Os exemplos a seguir mostram como conceder acesso por meio de uma política do IAM ou de uma política de chave do KMS.

IAM policy

Anexe essa política em linha ao perfil do IAM para permitir acesso à chave do KMS. Para usar essa política, substitua os *valores de espaço reservado para entrada* pelo ARN de sua chave do KMS.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
        "Effect": "Allow",
        "Action": [
            "kms:Decrypt",
            "kms:GenerateDataKey"
         ],
        "Resource": "<kms-key-arn>"
        }
```

```
    ]
}
```

KMS key policy

Anexe essa política em linha a uma chave do KMS para permitir que o perfil do AWS KMS especificado use a chave. Para usar os essa política, substitua os *valores de espaço reservado para entrada* por seu perfil do IAM.

```
{
    "Sid": "Allow use of the key",
    "Effect": "Allow",
    "Principal": {
        "AWS": [
            "arn:aws:iam::<catalog-account-id>:role/<role-name>"
        ]
    },
    "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey",
    ],
    "Resource": "*"
}
```

Conceder permissões à entidade principal do serviço S3 Metadata para usar sua chave do KMS

Para permitir que o Amazon S3 atualize tabelas de metadados criptografadas com SSE-KMS e realize a manutenção dessas tabelas de metadados, você pode usar o exemplo de política de chave a seguir. Nessa política, você permite que as entidades principais de serviço `metadata.s3.amazonaws.com` e `maintenance.s3tables.amazonaws.com` criptografem e descriptografem tabelas em um bucket de tabela específico usando uma chave específica. Para usar essa política, substitua os *espaços reservados para entrada do usuário* por suas próprias informações:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EnableKeyUsage",
            "Effect": "Allow",
            "Principal": {
```

```
                "Service": [
                    "maintenance.s3tables.amazonaws.com",
                    "metadata.s3.amazonaws.com"
                ]
            },
            "Action": [
                "kms:GenerateDataKey",
                "kms:Decrypt"
            ],
            "Resource": "<kms-key-arn>",
            "Condition": {
                "StringLike": {
                    "kms:EncryptionContext:aws:s3:arn":"<table-or-table-bucket-arn>/*"
                }
            }
        }
    ]
}
```

Especificar a criptografia do lado do servidor com chaves do AWS KMS (SSE-KMS) em buckets de tabela

Todos os buckets da funcionalidade Tabelas do Amazon S3 têm criptografia configurada por padrão e todas as novas tabelas criadas em um bucket de tabela são automaticamente criptografadas em repouso. A criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3) é a configuração de criptografia padrão para todos os buckets de diretório. Se você quiser especificar um tipo de criptografia diferente, é possível usar a criptografia do lado do servidor com chaves do AWS Key Management Service (AWS KMS) (SSE-KMS).

Você pode especificar a criptografia SSE-KMS em solicitações `CreateTableBucket` ou `CreateTable` ou definir a configuração de criptografia padrão no bucket de tabela em uma solicitação `PutTableBucketEncryption`.

> **Important**
>
> Para permitir a manutenção automática em tabelas e buckets de tabela criptografados com SSE-KMS, você deve conceder permissão à entidade principal de serviço maintenance.s3tables.amazonaws.com para usar sua chave do KMS. Para obter mais informações, consulte Requisitos de permissão para criptografia SSE-KMS da funcionalidade Tabelas do S3.

Especificar criptografia para buckets de tabela

Você pode especificar o SSE-KMS como o tipo de criptografia padrão ao criar um bucket de tabela. Para ter exemplos, consulte Criar um bucket de tabela. Depois de criar um bucket de tabela, você pode especificar o uso do SSE-KMS como a configuração de criptografia padrão usando operações da API REST, SDKs da AWS e a AWS Command Line Interface (AWS CLI).

> **Note**
>
> Quando você especifica o SSE-KMS como o tipo de criptografia padrão, a chave usada para criptografia deve permitir acesso à entidade principal do serviço de manutenção da funcionalidade Tabelas do S3. Se a entidade principal do serviço de manutenção não tiver acesso, você não conseguirá criar tabelas nesse bucket de tabela. Para obter mais informações, consulte Conceder à entidade principal do serviço de manutenção da funcionalidade Tabelas do S3 permissões para sua chave do KMS .

Usar a AWS CLI

Para usar o exemplo de comando a seguir da AWS CLI, substitua os *espaços reservados para entrada do usuário* por suas próprias informações.

```
aws s3tables put-table-bucket-encryption \
    --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-table-bucket; \
    --encryption-configuration '{
        "sseAlgorithm": "aws:kms",
        "kmsKeyArn": "arn:aws:kms:us-east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    }' \
    --region us-east-1
```

Você pode remover a configuração de criptografia padrão de um bucket de tabela usando a operação de API DeleteTableBucketEncryption. Ao remover as configurações de criptografia, as novas tabelas criadas no bucket de tabela usarão a criptografia SSE-S3 padrão.

Especificar criptografia para tabelas

Você pode aplicar a criptografia SSE-KMS ao criar uma tabela usando mecanismos de consulta, operações da API REST, SDKs da AWS e a AWS Command Line Interface (AWS CLI). As configurações de criptografia que você especifica ao criar uma tabela têm precedência sobre a configuração de criptografia padrão do bucket de tabela.

> **Note**
>
> Ao usar a criptografia SSE-KMS para uma tabela, a chave utilizada para criptografia deve permitir que a entidade principal do serviço de manutenção da funcionalidade Tabelas do S3 a acesse. Se a entidade principal do serviço de manutenção não tiver acesso, você não conseguirá criar a tabela. Para obter mais informações, consulte Conceder à entidade principal do serviço de manutenção da funcionalidade Tabelas do S3 permissões para sua chave do KMS .

Permissões obrigatórias do

As seguintes permissões são necessárias para criar tabelas criptografadas:

- `s3tables:CreateTable`
- `s3tables:PutTableEncryption`

Como usar o AWS CLI

O exemplo a seguir da AWS CLI cria uma tabela com um esquema básico e a criptografa com uma chave do AWS KMS gerenciada pelo cliente. Para usar o comando, substitua os *espaços reservados para entrada do usuário* por suas próprias informações.

```
aws s3tables create-table \
  --table-bucket-arn "arn:aws:s3tables:Region:ownerAccountId:bucket/amzn-s3-demo-table-bucket" \
  --namespace "mydataset" \
  --name "orders" \
  --format "ICEBERG" \
  --encryption-configuration '{
    "sseAlgorithm": "aws:kms",
    "kmsKeyArn":
 "arn:aws:kms:Region:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
```

```
}' \
--metadata '{
  "iceberg": {
    "schema": {
      "fields": [
        {
          "name": "order_id",
          "type": "string",
          "required": true
        },
        {
          "name": "order_date",
          "type": "timestamp",
          "required": true
        },
        {
          "name": "total_amount",
          "type": "decimal(10,2)",
          "required": true
        }
      ]
    }
  }
}'
```

A proteção de dados refere-se à proteção enquanto eles estão em trânsito (à medida que são transferidos para e do Amazon S3) e em repouso (enquanto estão armazenados em discos em data centers do Amazon S3). A funcionalidade Tabelas do S3 sempre protege os dados em trânsito usando Transport Layer Security (1.2 e posterior) por meio de HTTPS. Para proteger dados em repouso em buckets de tabela do S3, você tem as seguintes opções:

Criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3)

Todos os buckets de tabela do Amazon S3 têm criptografia configurada por padrão. A opção padrão para a criptografia do lado do servidor é com as chaves gerenciadas pelo Amazon S3 (SSE-S3). Essa criptografia não tem custo e se aplica a todas as tabelas nos buckets de tabela do S3, a menos que você especifique outra forma de criptografia. Cada objeto é criptografado com uma chave exclusiva. Como uma proteção adicional, a SSE-S3 criptografa a própria chave com uma chave-raiz que alterna regularmente. A SSE-S3 usa uma das cifras de bloco mais fortes disponíveis, o padrão de criptografia avançada de 256 bits (AES-256), para criptografar os dados.

Criptografia no lado do servidor com chaves do AWS KMS (SSE-KMS)

Você pode optar por configurar buckets de tabela ou tabelas para usar a criptografia do lado do servidor com chaves do AWS Key Management Service (AWS KMS) (SSE-KMS). Os controles de segurança do AWS KMS podem ajudá-lo a satisfazer os requisitos de conformidade relacionados à criptografia. O SSE-KMS oferece maior controle sobre as chaves de criptografia, permitindo que você faça o seguinte:

- Crie, visualize, edite, monitore, habilite ou desabilite, alterne e programe a exclusão de chaves do KMS.
- Definir políticas que controlam como e por quem as chaves do KMS podem ser usadas.
- Rastreie o uso de chaves no AWS CloudTrail para verificar se as chaves do KMS estão sendo usadas corretamente.

A funcionalidade Tabelas do S3 permite o uso de chaves gerenciadas pelo cliente no SSE-KMS para criptografar tabelas. Não é possível usar chaves gerenciadas pela AWS. Para ter mais informações sobre o uso do SSE-KMS para tabelas e buckets de tabela do S3, consulte Usar a criptografia do lado do servidor com chaves do AWS KMS (SSE-KMS) em buckets de tabela.

Gerenciamento de acesso para a funcionalidade Tabelas do S3

Na funcionalidade Tabelas do S3, os recursos incluem buckets de tabela e as tabelas contidas neles. O usuário-raiz da Conta da AWS que criou o recurso (proprietário do recurso) e os usuários do AWS Identity and Access Management (IAM) dentro dessa conta que têm as permissões necessárias podem acessar um recurso que eles criaram. O proprietário do recurso especifica quem mais pode acessar o recurso e as ações que podem realizar no recurso. O Amazon S3 tem várias ferramentas de gerenciamento de acesso que você pode usar para conceder a outros usuários acesso aos recursos do S3. Os tópicos a seguir fornecem uma visão geral dos recursos, das ações do IAM e das chaves de condição para a funcionalidade Tabelas do S3. Também apresentam exemplos de políticas baseadas em recurso e em identidade para a funcionalidade Tabelas do S3.

Tópicos

- Recursos
- Ações para a funcionalidade Tabelas do S3
- Chaves de condição para a funcionalidade Tabelas do S3
- Políticas baseadas em identidade do IAM para a funcionalidade Tabelas do S3
- Políticas baseadas em recurso para a funcionalidade Tabelas do S3

- Políticas gerenciadas pela AWS para o serviço Tabelas do S3
- Conceder acesso com semântica SQL

Recursos

Os recursos da funcionalidade Tabelas do S3 incluem buckets de tabela e as tabelas contidas neles.

- Buckets de tabela: os buckets de tabela são projetados especificamente para tabelas e fornecem quantidades mais altas de transações por segundo (TPS) e melhor throughput de consultas em comparação com as tabelas autogerenciadas em buckets de uso geral do S3. Os buckets de tabela oferecem as mesmas características de durabilidade, disponibilidade, escalabilidade e performance dos buckets de uso geral do Amazon S3.
- Tabelas: as tabelas nos buckets de tabela são armazenadas no formato Apache Iceberg. Você pode consultar essas tabelas usando SQL padrão em mecanismos de consulta compatíveis com Iceberg.

Os nomes de recursos da Amazon (ARNs) para tabelas e buckets de tabela contêm o namespace `s3tables`, a Região da AWS, o ID da Conta da AWS e o nome do bucket. Para acessar e executar ações nas tabelas e nos buckets de tabela, você deve usar os seguintes formatos de ARN:

- Formato do ARN de tabela:

```
arn:aws:s3tables:us-west-2:111122223333:bucket/amzn-s3-demo-bucket/
table/demo-tableID
```

Ações para a funcionalidade Tabelas do S3

Em uma política baseada em identidade ou em recurso, defina quais ações da funcionalidade Tabelas do S3 são permitidas ou negadas para entidades principais do IAM específicas. As ações de tabelas correspondem às operações de API ao nível do bucket e da tabela. Todas as ações fazem parte de um namespace do IAM exclusivo: `s3tables`.

Ao usar uma ação em uma política, você geralmente permite ou nega acesso à operação de API com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação de API. Por exemplo, as ações `s3tables:GetTableData` incluem permissões para as operações de API `GetObject`, `ListParts` e `ListMultiparts`.

Veja a seguir as ações compatíveis com buckets de tabela. Você pode especificar as ações a seguir no elemento `Action` de uma política do IAM ou de recurso.

Ação	Descrição	Nível de acesso	Acesso entre contas
`s3tables:CreateTableBucket`	Concede permissões para criar um bucket de tabela.	`Write`	Não
`s3tables:GetTableBucket`	Concede permissão para recuperar o ARN do bucket de tabela, o nome do bucket de tabela e a data de criação.	`Write`	Sim
`s3tables:ListTableBuckets`	Concede permissão para listar todos os buckets de tabela da conta.	`Read`	Não
`s3tables:CreateNamespace`	Concede permissão para criar um namespace em um	`Read`	Sim

Ação	Descrição	Nível de acesso	Acesso entre contas
	bucket de tabela.		
`s3tables:GetNamespace`	Concede permissão para recuperar os detalhes de um namespace.	`Read`	Sim
`s3tables:ListNamespaces`	Concede permissão para listar todos os namespaces no bucket de tabela.	`Read`	Sim
`s3tables:DeleteNamespace`	Concede permissão para excluir um namespace em um bucket de tabela.	`Write`	Sim
`s3tables:DeleteTableBucket`	Concede permissão para excluir o bucket.	`Write`	Sim

Ação	Descrição	Nível de acesso	Acesso entre contas
`s3tables:PutTableBucketPolicy`	Concede permissão para adicionar ou substituir uma política de bucket.	`Permissions Management`	Não
`s3tables:GetTableBucketPolicy`	Concede permissão para recuperar a política de bucket.	`Read`	Não
`s3tables:DeleteTableBucketPolicy`	Concede permissão para excluir a política do bucket.	`Permissions Management`	Não
`s3tables:GetTableBucketMaintenanceConfiguration`	Concede permissão para recuperar a configuração de manutenção de um bucket de tabela.	`Read`	Sim

Ação	Descrição	Nível de acesso	Acesso entre contas
`s3tables:PutTableBucketMaintenanceConfiguration`	Concede permissão para adicionar ou substituir a configuração de manutenção de um bucket de tabela.	`Write`	Sim
`s3tables:PutTableBucketEncryption`	Concede permissão para adicionar ou substituir a configuração de criptografia de um bucket de tabela.	`Write`	Não
`s3tables:GetTableBucketEncryption`	Concede permissão para recuperar a configuração de criptografia de um bucket de tabela.	`Read`	Não

Ação	Descrição	Nível de acesso	Acesso entre contas
`s3tables:DeleteTableBucketEncryption`	Concede permissão para excluir a configuração de criptografia de um bucket de tabela.	`Write`	Não

As ações a seguir são compatíveis com tabelas:

Ação	Descrição	Nível de acesso	Acesso entre contas
`s3tables:GetTableMaintenanceConfiguration`	Concede permissão para recuperar a configuração de manutenção de uma tabela.	`Read`	Sim
`s3tables:PutTableMaintenanceConfiguration`	Concede permissão para adicionar ou substituir a configuração de manutenção de uma tabela.	`Write`	Sim

Ação	Descrição	Nível de acesso	Acesso entre contas
`s3tables:PutTablePolicy`	Concede permissão para adicionar ou substituir uma política de tabela.	`Permissions Management`	Não
`s3tables:GetTablePolicy`	Concede permissão para recuperar a política da tabela.	`Read`	Não
`s3tables:DeleteTablePolicy`	Concede permissão para excluir a política da tabela.	`Permissions management`	Não
`s3tables:CreateTable`	Concede permissão para criar uma tabela em um bucket de tabela.	`Write`	Sim

Ação	Descrição	Nível de acesso	Acesso entre contas
`s3tables:GetTable`	Concede permissão para recuperar as informações de uma tabela.	`Read`	Sim
`s3tables:GetTableMetadataLocation`	Concede permissão para recuperar o ponteiro-raiz da tabela (arquivo de metadados).	`Read`	Sim
`s3tables:ListTables`	Concede permissão para listar todas as tabelas em um bucket de tabela.	`Read`	Sim
`s3tables:RenameTable`	Concede permissões para alterar o nome de uma tabela.	`Write`	Sim

Ação	Descrição	Nível de acesso	Acesso entre contas
`s3tables:UpdateTableMetadataLocation`	Concede permissão para atualizar o ponteiro-raiz da tabela (arquivo de metadados).	`Write`	Sim
`s3tables:GetTableData`	Concede permissão para ler os metadados da tabela e os objetos de dados armazenados no bucket de tabela.	`Read`	Sim
`s3tables:PutTableData`	Concede permissão para gravar os metadados da tabela e os objetos de dados armazenados no bucket de tabela.	`Write`	Sim

Ação	Descrição	Nível de acesso	Acesso entre contas
`s3tables:GetTableEncryption`	Concede permissão para recuperar as configurações de criptografia de um bucket de tabela.	`Write`	Não
`s3tables:PutTableEncryption`	Concede permissão para adicionar criptografia a uma tabela.	`Write`	Não

Para realizar ações de leitura e gravação ao nível da tabela, a funcionalidade Tabelas do S3 oferece suporte a operações de API do Amazon S3, como `GetObject` e `PutObject`. A tabela a seguir fornece uma lista de ações ao nível do objeto. Ao conceder permissões de leitura e gravação nas tabelas, use as ações a seguir.

Ação	APIs de objetos do S3		
`s3tables:GetTableData`	`GetObject`, `ListParts`, `HeadObject`		
`s3tables:PutTableData`	`PutObject`,		

Ação	APIs de objetos do S3		
	`CreateMultipartUpload`, `CompleteMultipartUpload`, `UploadPart`, `AbortMultipartUpload`		

Por exemplo, se um usuário tiver permissões `GetTableData`, ele poderá ler todos os arquivos associados à tabela, como o arquivo de metadados, o manifesto, os arquivos da lista de manifestos e os arquivos de dados parquet.

Chaves de condição para a funcionalidade Tabelas do S3

A funcionalidade Tabelas do S3 oferece suporte a chaves de contexto de condição globais da AWS.

Além disso, a funcionalidade Tabelas do S3 define as seguintes chaves de condição que você pode usar em uma política de acesso.

Chave de condição	Descrição	Tipo	
`s3tables:tableName`	Filtra o acesso pelos nomes das tabelas no bucket de tabela. Você pode usar a chave	`String`	

Chave de condição	Descrição	Tipo	
	de condição `s3tables:tableName` para escrever políticas do IAM ou de bucket de tabela que restrinjam o acesso de usuários ou aplicações somente a tabelas que atendam a essa condição de nome. É importante observar que, se você usar a chave de condição `s3tables:tableName` para controlar o acesso, as alterações nos nomes das tabelas poderão		

Chave de condição	Descrição	Tipo	
	afetar essas políticas. Exemplo de valor: `"s3tables:tableName":"department*"`		

Chave de condição	Descrição	Tipo	
`s3tables:namespace`	Filtra o acesso pelos namespaces criados no bucket de tabela. Você pode usar a chave de condição `s3tables:namespace` para criar políticas do IAM, de tabela ou de bucket de tabela que restringem o acesso de usuários ou aplicações às tabelas que fazem parte de um namespace específico. Exemplo de valor: `"s3tables:namespace":"hr"`	`String`	

Chave de condição	Descrição	Tipo	
	É importante observar que, se você usar a chave de condição `s3tables:namespace` para controlar o acesso, as alterações nos namespaces poderão afetar essas políticas.		

Chave de condição	Descrição	Tipo	
`s3tables:SSEAlgorithm`	Filtra o acesso pelo algoritmo de criptografia do lado do servidor usado para criptografar uma tabela. Você pode usar a chave de condição `s3tables:SSEAlgorithm` para escrever políticas do IAM, de tabela ou de bucket de tabela que restrinjam o acesso de usuários ou aplicações a tabelas criptografadas com determinado tipo de criptografia. Exemplo de valor:	`String`	

Chave de condição	Descrição	Tipo	
	`"s3tables:SSEAlgorithm":"aws:kms"` É importante observar que, se você usar a chave de condição `s3tables:SSEAlgorithm` para controlar o acesso, as alterações na criptografia poderão afetar essas políticas.		

Chave de condição	Descrição	Tipo	
`s3tables:KMSKeyArn`	Filtra o acesso pelo ARN da chave do AWS KMS usada para criptografar uma tabela. Você pode usar a chave de condição `s3tables:KMSKeyArn` para escrever políticas do IAM, de tabela ou de bucket de tabela que restrinjam o acesso de usuários ou aplicações a tabelas criptografadas com uma chave do KMS específica. É importante observar	ARN	

Chave de condição	Descrição	Tipo	
	que, se você usar a chave de condição `s3tables:KMSKeyArn` para controlar o acesso, as alterações na chave do KMS poderão afetar essas políticas.		

Políticas baseadas em identidade do IAM para a funcionalidade Tabelas do S3

Por padrão, usuários e perfis não têm permissão para criar nem modificar tabelas e buckets de tabela. Eles também não podem executar tarefas usando o console do S3, a AWS Command Line Interface (AWS CLI) ou as APIs REST do Amazon S3. Para criar e acessar tabelas e buckets de tabela, um administrador do AWS Identity and Access Management (IAM) deve conceder as permissões necessárias aos usuários ou ao perfil do IAM. Para saber como criar uma política baseada em identidade do IAM usando esses exemplos de documento de política JSON, consulte Criação de políticas do IAM no Guia do Usuário do IAM.

O tópico a seguir inclui exemplos de políticas baseadas em identidade do IAM. Para usar os exemplos de política a seguir, substitua os *espaços reservados para entrada do usuário* por suas próprias informações.

Tópicos

- Exemplo 1: permitir acesso para criar e usar buckets de tabela
- Exemplo 2: permitir acesso para criar e usar tabelas em um bucket de tabela

Exemplo 1: permitir acesso para criar e usar buckets de tabela

.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "AllowBucketActions",
        "Effect": "Allow",
        "Action": [
            "s3tables:CreateTableBucket",
            "s3tables:PutTableBucketPolicy",
            "s3tables:GetTableBucketPolicy",
            "s3tables:ListTableBuckets",
            "s3tables:GetTableBucket"
        ],

        "Resource": "arn:aws:s3tables:region:account_id:bucket/*"
    }]
}
```

Exemplo 2: permitir acesso para criar e usar tabelas em um bucket de tabela

```
{
     "Version": "2012-10-17",
     "Statement": [
         {
             "Sid": "AllowBucketActions",
             "Effect": "Allow",
             "Action": [
                 "s3tables:CreateTable",
                 "s3tables:PutTableData",
                 "s3tables:GetTableData",
                 "s3tables:GetTableMetadataLocation",
                 "s3tables:UpdateTableMetadataLocation",
                 "s3tables:GetNamespace",
                 "s3tables:CreateNamespace"
             ],

             "Resource": [
               "arn:aws:s3tables:region:account_id:bucket/amzn-s3-demo-bucket",
               "arn:aws:s3tables:region:account_id:bucket/amzn-s3-demo-bucket/table/*"
            ]
```

```
        }
    ]
}
```

Políticas baseadas em recurso para a funcionalidade Tabelas do S3

A funcionalidade Tabelas do S3 fornece políticas baseadas em recurso para gerenciar o acesso aos buckets de tabela e às tabelas: políticas de bucket de tabela e políticas de tabela. Você pode usar uma política de bucket de tabela para conceder permissões de acesso à API ao nível do bucket de tabela, do namespace ou da tabela. As permissões anexadas ao bucket de tabela podem ser aplicadas a todas as tabelas no bucket ou a tabelas específicas no bucket, dependendo da definição da política. Você pode usar uma política de tabela para conceder permissões ao nível da tabela.

Quando a funcionalidade Tabelas do S3 recebe uma solicitação, primeiro ela verifica se o solicitante tem as permissões necessárias. Ela avalia todas as políticas de acesso, políticas de usuário e políticas baseadas em recurso relevantes para decidir se autoriza a solicitação (política de usuário do IAM, política de perfil do IAM, política de bucket de tabela e política de tabela). Por exemplo, se uma política de bucket de tabela concede a um usuário permissões para realizar todas as ações nas tabelas do bucket (inclusive `DeleteTable`), mas uma tabela individual tiver uma política de tabela que nega a ação `DeleteTable` para todos os usuários, um usuário não pode excluir a tabela.

O tópico a seguir inclui exemplos de políticas de tabela e de bucket de tabela. Para usar essas políticas, substitua os *`espaços reservados para entrada do usuário`* por suas próprias informações.

> **Note**
>
> - Toda política que concede permissões para modificar tabelas deve incluir permissões para `GetTableMetadataLocation` a fim de acessar o arquivo-raiz da tabela. Para obter mais informações, consulte `GetTableMetadataLocation`.
> - Sempre que você realizar uma atividade de gravação ou exclusão em uma tabela, inclua permissões para `UpdateTableMetadataLocation` na política de acesso.
> - Recomendamos usar uma política de bucket de tabela para controlar o acesso às ações ao nível do bucket e uma política de tabela para controlar o acesso às ações ao nível da tabela. Nos casos em que você deseja definir o mesmo conjunto de permissões em várias tabelas, recomendamos o uso de uma política de bucket de tabela.

Tópicos

- Exemplo 1: a política de bucket de tabela permite acesso a PutBucketMaintenanceConfiguration para buckets em uma conta
- Exemplo 2: política de bucket de tabela para permitir acesso de leitura (SELECT) às tabelas armazenadas no namespace hr
- Exemplo 3: política de tabela para permitir que um usuário exclua uma tabela

Exemplo 1: a política de bucket de tabela permite acesso a **`PutBucketMaintenanceConfiguration`** para buckets em uma conta

O exemplo de política de bucket de tabela a seguir permite que o `data steward` do IAM exclua objetos não referenciados de todos os buckets em uma conta ao permitir acesso a `PutBucketMaintenanceConfiguration`.

```
{
     "Version": "2012-10-17",
     "Statement": [
         {
             "Effect": "Allow",
             "Principal": {
               "AWS": "arn:aws:iam::account_id:role/datasteward"
             },
             "Action": ["s3tables:PutTableBucketMaintenanceConfiguration"],
             "Resource":"arn:aws:s3tables:region:account_id:bucket/*"
     }]
 }
```

Exemplo 2: política de bucket de tabela para permitir acesso de leitura (SELECT) às tabelas armazenadas no namespace **`hr`**

Veja a seguir um exemplo de política de bucket de tabela permite que Jane, uma usuária do ID de Conta da AWS `123456789012`, acesse tabelas armazenadas no namespace `hr` em um bucket de tabela.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
```

```
            "Principal": {
                "AWS": "arn:aws:iam::123456789012:user/Jane"
            },
            "Action": [
                "s3tables:GetTableData",
                "s3tables:GetTableMetadataLocation"
            ],
            "Resource": "arn:aws:s3tables:region:account_id:bucket/amzn-s3-demo-table-
bucket/table/*",
            "Condition": {
                "StringLike": {"s3tables:namespace": "hr"}
            }
        }
    ]
}
```

Exemplo 3: política de tabela para permitir que um usuário exclua uma tabela

O exemplo a seguir é uma política de tabela que permite que o perfil do IAM `data steward` exclua uma tabela.

```
{
     "Version": "2012-10-17",
     "Id": "DeleteTable",
     "Statement": [
      {
       "Effect": "Allow",
       "Principal": {
         "AWS": "arn:aws:iam::account_id:role/datasteward"
        },
        "Action": [
           "s3tables:DeleteTable",
           "s3tables:UpdateTableMetadataLocation",
           "s3tables:PutTableData",
           "s3tables:GetTableMetadataLocation"

        ],
        "Resource":"arn:aws:s3tables:region:account_id:bucket/amzn-s3-demo-bucket1/
table/tableUUID"
     }]
}
```

Políticas gerenciadas pela AWS para o serviço Tabelas do S3

Uma política gerenciada pela AWS é uma política independente criada e administrada pela AWS. As políticas gerenciadas pela AWS são criadas para fornecer permissões a vários casos de uso comuns e permitir a atribuição de permissões a usuários, grupos e perfis.

Lembre-se de que as políticas gerenciadas pela AWS podem não conceder permissões de privilégio mínimo para casos de uso específicos, por estarem disponíveis para uso por todos os clientes da AWS. Recomendamos que você reduza ainda mais as permissões definindo as políticas gerenciadas pelo cliente que são específicas para seus casos de uso.

Você não pode alterar as permissões definidas em políticas gerenciadas pela AWS. Se a AWS atualiza as permissões definidas em um política gerenciada por AWS, a atualização afeta todas as identidades de entidades principais (usuários, grupos e perfis) às quais a política estiver vinculada. É provável que a AWS atualize uma política gerenciada por AWS quando um novo AWS service (Serviço da AWS) for lançado, ou novas operações de API forem disponibilizadas para os serviços existentes.

Para obter mais informações, consulte Políticas gerenciadas pela AWS no Guia do usuário do IAM.

Política gerenciada da AWS: AmazonS3TablesFullAccess

É possível anexar a política `AmazonTablesS3FullAccess` às identidades do IAM. Essa política concede permissões que possibilitam acesso total à funcionalidade Tabelas do Amazon S3.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3tables:*"
            ],
            "Resource": "*"
        }
    ]
}
```

Política gerenciada da AWS: AmazonS3TablesReadOnlyAccess

É possível anexar a política `AmazonS3TablesReadOnlyAccess` às identidades do IAM. Essa política concede permissões que oferecem acesso somente leitura à funcionalidade Tabelas do Amazon S3.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3tables:Get*",
                "s3tables:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

Política gerenciada da AWS: AmazonS3TablesLakeFormationServiceRole

É possível anexar a política `AmazonS3TablesLakeFormationServiceRole` às identidades do IAM. Essa política concede permissões que autorizam o acesso do perfil de serviço do AWS Lake Formation ao serviço Tabelas do S3. As permissões do AWS KMS são usadas para autorizar o acesso do Lake Formation a tabelas criptografadas.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PermissionsForS3ListTableBuckets",
            "Effect": "Allow",
            "Action": [
                "s3tables:ListTableBuckets"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "111122223333"
```

```
                }
            }
        },
        {
            "Sid": "DataAccessPermissionsForS3TablesResources",
            "Effect": "Allow",
            "Action": [
                "s3tables:CreateTableBucket",
                "s3tables:GetTableBucket",
                "s3tables:CreateNamespace",
                "s3tables:GetNamespace",
                "s3tables:ListNamespaces",
                "s3tables:DeleteNamespace",
                "s3tables:DeleteTableBucket",
                "s3tables:CreateTable",
                "s3tables:DeleteTable",
                "s3tables:GetTable",
                "s3tables:ListTables",
                "s3tables:RenameTable",
                "s3tables:UpdateTableMetadataLocation",
                "s3tables:GetTableMetadataLocation",
                "s3tables:GetTableData",
                "s3tables:PutTableData"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "111122223333"
                }
            }
        },
        {
            "Sid": "KMSDataAccessPermissionsForS3TablesResources",
            "Effect": "Allow",
            "Action": [
                "kms:GenerateDataKey",
                "kms:Decrypt"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "kms:ViaService": [
```

```
                        "s3.*.amazonaws.com"
                    ],
                    "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3tables:*:*:bucket/*/
table/*"
                },
                "StringEquals": {
                    "aws:ResourceAccount": "111122223333"
                }
            }
        },
        {
            "Sid": "KMSDescribeKeyAccessPermissionsForS3TablesResources",
            "Effect": "Allow",
            "Action": [
                "kms:DescribeKey"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "kms:ViaService": [
                        "s3tables.*.amazonaws.com"
                    ]
                },
                "StringEquals": {
                    "aws:ResourceAccount": "111122223333"
                }
            }
        }
    ]
}
```

Atualizações da funcionalidade Tabelas do Amazon S3 para políticas gerenciadas pela AWS

Veja detalhes sobre as atualizações nas políticas gerenciadas pela AWS para a funcionalidade Tabelas do Amazon S3 desde que as alterações começaram a ser controladas para essa funcionalidade.

Alteração	Descrição	Data
Adição de `AmazonS3TablesLakeFormation`	O serviço Tabelas do S3 adicionou uma nova política gerenciada pela AWS	19 de maio de 2025

Alteração	Descrição	Data
`ServiceRole` à funcionalidade Tabelas do Amazon S3.	chamada `AmazonS3TablesLakeFormationServiceRole`. Essa política concede permissões que autorizam o acesso do perfil de serviço do Lake Formation ao serviço Tabelas do S3.	
Adição de `AmazonTablesS3FullAccess` à funcionalidade Tabelas do Amazon S3.	A funcionalidade Tabelas do S3 adicionou uma nova política gerenciada pela AWS chamada `AmazonTablesS3FullAccess`. Essa política concede permissões que possibilitam acesso total à funcionalidade Tabelas do Amazon S3.	3 de dezembro de 2024
Adição de `AmazonS3TablesReadOnlyAccess` à funcionalidade Tabelas do Amazon S3.	A funcionalidade Tabelas do S3 adicionou uma nova política gerenciada pela AWS chamada `AmazonS3TablesReadOnlyAccess`. Essa política concede permissões que oferecem acesso somente leitura à funcionalidade Tabelas do Amazon S3.	3 de dezembro de 2024
Início do controle de alterações na funcionalidade Tabelas do Amazon S3.	A funcionalidade Tabelas do Amazon S3 passou a controlar as alterações relacionadas às políticas gerenciadas pela AWS.	3 de dezembro de 2024

Conceder acesso com semântica SQL

Você pode conceder permissões às tabelas usando a semântica SQL nas políticas de tabela e de bucket de tabela. Alguns exemplos de semântica SQL que você pode usar são `CREATE`, `INSERT`, `DELETE`, `UPDATE` e `ALTER`. A tabela a seguir fornece uma lista de ações de API associadas à semântica SQL que você pode usar para conceder permissões aos usuários.

A funcionalidade Tabelas do S3 oferece suporte parcial às permissões usando a semântica SQL. Por exemplo, a API `CreateTable` cria apenas uma tabela vazia no bucket de tabela. São necessárias permissões adicionais, como `UpdateTableMetadata`, `PutTableData` e `GetTableMetadataLocation`, para poder definir o esquema de tabela. Essas permissões adicionais também significam que você concederá ao usuário acesso para inserir linhas na tabela. Se quiser controlar o acesso exclusivamente com base na semântica SQL, recomendamos usar AWS Lake Formation ou alguma outra solução de terceiros integrada à funcionalidade Tabelas do S3.

Atividade ao nível da tabela	Ações do IAM		
`SELECT`	`s3tables:GetTableData` , `s3tables:GetTableMetadataLocation`		
`CREATE`	`s3tables:CreateTable` , `s3tables:UpdateTableMetadataLocation` , `s3tables:PutTableData` ,		

Atividade ao nível da tabela	Ações do IAM		
	s3tables: GetTableMetadataLocation ,		
INSERT	s3tables: UpdateTableMetadataLocation , s3tables: PutTableData , s3tables: GetTableMetadataLocation		
UPDATE	s3tables: UpdateTableMetadataLocation , s3tables: PutTableData , s3tables: GetTableMetadataLocation		

Atividade ao nível da tabela	Ações do IAM		
ALTER,RENAME	s3tables:UpdateTableMetadataLocation , s3tables:PutTableData , s3tables:GetTableMetadataLocation , s3tables:RenameTable		
DELETE,DROP	s3tables:DeleteTable , s3tables:UpdateTableMetadataLocation , s3tables:PutTableData , s3tables:GetTableMetadataLocation		

Conectividade de VPC para a funcionalidade Tabelas do S3

Todas as tabelas na funcionalidade Tabelas do S3 estão no formato Apache Iceberg e são compostas por dois tipos de objeto do S3. Esses dois tipos de objeto são arquivos de dados que armazenam os dados e arquivos de metadados que rastreiam informações sobre os arquivos de dados em diferentes momentos. Todas as operações de buckets de tabela, namespaces e tabelas (por exemplo, `CreateNamespace`, `CreateTable` e assim por diante) são roteadas por meio de um endpoint da funcionalidade Tabelas do S3 (`s3tables.region.amazonaws.com`) e todas as operações ao nível do objeto que leem ou gravam os arquivos de dados e metadados continuam sendo roteadas por meio de um endpoint de serviço do S3 (`s3.region.amazonaws.com`).

Para acessar a funcionalidade Tabelas do S3, o Amazon S3 oferece suporte a dois tipos de endpoint da VPC usando o AWS PrivateLink: endpoints de gateway e endpoints de interface. Um endpoint de gateway é um gateway que você especifica na tabela de rotas para acessar o S3 por meio da VPC pela rede da AWS. Os endpoints de interface estendem a funcionalidade dos endpoints de gateway usando endereços IP privados para rotear solicitações ao Amazon S3 de dentro da VPC on-premises ou de uma VPC em outra Região da AWS usando emparelhamento da VPC ou o AWS Transit Gateway.

Para acessar a funcionalidade Tabelas do S3 de uma VPC, recomendamos criar dois endpoints da VPC (um para o S3 e outro para a funcionalidade Tabelas do S3). Você pode criar um endpoint de gateway ou de interface para rotear operações ao nível do arquivo (objeto) para o S3 e um endpoint de interface para rotear operações ao nível do bucket e da tabela para a funcionalidade Tabelas do S3. Você pode criar e usar endpoints da VPC para solicitações ao nível do arquivo usando o S3. Para ter mais informações, consulte Gateway endpoints no Guia do usuário do AWS PrivateLink.

Para saber mais sobre como usar o AWS PrivateLink para criar e trabalhar com endpoints na funcionalidade Tabelas do S3, consulte os tópicos a seguir. Para criar um endpoint da VPC de interface, consulte Create a VPC endpoint (Criar um endpoint da VPC) no Guia do AWS PrivateLink.

Tópicos

- Criar endpoints da VPC para a funcionalidade Tabelas do S3
- Acessar tabelas e buckets de tabela por meio de endpoints usando a AWS CLI
- Configurar uma rede de VPC ao usar mecanismos de consulta
- Restringir o acesso à funcionalidade Tabelas do S3 na rede da VPC

Criar endpoints da VPC para a funcionalidade Tabelas do S3

Quando você cria um endpoint da VPC, a funcionalidade Tabelas do S3 gera dois tipos de nomes DNS específicos do endpoint: regionais e zonais.

- Um nome DNS regional tem o seguinte formato: `VPCendpointID.s3tables.AWSregion.vpce.amazonaws.com`. Por exemplo, para o ID do endpoint da VPC `vpce-1a2b3c4d`, o nome DNS gerado será semelhante a `vpce-1a2b3c4d-5e6f.s3tables.us-east-1.vpce.amazonaws.com`.
- Um nome DNS zonal tem o seguinte formato: `VPCendpointID-AvailabilityZone.s3tables.AWSregion.vpce.amazonaws.com`. Por exemplo, para o ID do endpoint da VPC `vpce-1a2b3c4d-5e6f.`, o nome DNS gerado será semelhante a `vpce-1a2b3c4d-5e6f-us-east-1a.s3tables.us-east-1.vpce.amazonaws.com`.

  Um nome DNS zonal inclui a zona de disponibilidade. Você pode usar os nomes DNS zonais quando a arquitetura isola zonas de disponibilidade. Os nomes DNS do S3 específicos do endpoint podem ser resolvidos por meio do domínio DNS público do S3.

Você também pode usar as opções de DNS privado para simplificar o roteamento de tráfego do S3 pelos endpoints da VPC e ajudar a aproveitar o caminho de rede de menor custo disponível para a aplicação. O DNS privado mapeia o endpoint público da funcionalidade Tabelas do S3, por exemplo, `s3tables.region.amazonaws.com`, para um IP privado na VPC. Você pode usar as opções de DNS privado para rotear o tráfego regional do S3 sem atualizar os clientes do S3 para usar os nomes DNS específicos dos endpoints de interface.

> **Note**
>
> O AWS PrivateLink para Amazon S3 não é compatível com o uso de endpoints de camada dupla do Amazon S3. Consulte mais informações em Using Amazon S3 dual-stack endpoints na Referência de API do Amazon S3.

Acessar tabelas e buckets de tabela por meio de endpoints usando a AWS CLI

Você pode usar a AWS Command Line Interface (AWS CLI) para acessar tabelas e buckets de tabela por meio dos endpoints de interface. Com a AWS CLI, os comandos `aws s3` roteiam o tráfego pelo endpoint do Amazon S3. Os comandos `aws s3tables` da AWS CLI usam o endpoint da funcionalidade Tabelas do Amazon S3.

Um exemplo de um endpoint da VPC `s3tables` é `vpce-0123456afghjipljw-nmopsqea.s3tables.region.vpce.amazonaws.com`.

Um endpoint da VPC `s3tables` não inclui um nome de bucket. Você pode acessar o endpoint da VPC `s3tables` usando os comandos `aws s3tables` da AWS CLI.

Um exemplo de um endpoint da VPC `s3` é `amzn-s3-demo-bucket.vpce-0123456afghjipljw-nmopsqea.s3.region.vpce.amazonaws.com`.

Você pode acessar o endpoint da VPC `s3` usando os comandos `aws s3` da AWS CLI.

Usar a AWS CLI

Para acessar tabelas e buckets de tabela por meio de endpoints de interface usando a AWS CLI, use os parâmetros `-region` e `--endpoint-url`. Para realizar ações ao nível da tabela e do bucket de tabela, use o URL de endpoint da funcionalidade Tabelas do S3. Para realizar ações ao nível do objeto, use o URL de endpoint do Amazon S3.

Nos exemplos a seguir, substitua os *espaços reservados para entrada do usuário* por suas próprias informações.

Exemplo 1: usar um URL de endpoint para listar os buckets de tabela de uma conta

```
aws s3tables list-table-buckets --endpoint https://vpce-0123456afghjipljb-aac.s3tables.us-east-1.vpce.amazonaws.com –region us-east-1
```

Exemplo 2: usar um URL de endpoint para listar as tabelas em seu bucket

```
aws s3tables list-tables --table-bucket-arn arn:aws:s3tables:us-east-1:123456789301:bucket/amzn-s3-demo-bucket --endpoint
 https://vpce-0123456afghjipljb-aac.s3tables.us-east-1.vpce.amazonaws.com --region us-east-1
```

Configurar uma rede de VPC ao usar mecanismos de consulta

Use as etapas a seguir para configurar uma rede de VPC ao usar mecanismos de consulta.

1. Para começar, você pode criar ou atualizar uma VPC. Para obter mais informações, consulte Criar uma VPC.

2. Para operações ao nível da tabela e do bucket de tabela que são roteadas para a funcionalidade Tabelas do S3, crie um endpoint de interface. Para obter mais informações, consulte Acessar um serviço da AWS usando um endpoint da VPC de interface.
3. Para todas as operações ao nível do objeto que são roteadas para o Amazon S3, crie um endpoint de gateway ou um endpoint de interface. Para ter mais informações sobre os endpoints de gateway, consulte Create a gateway endpoint.
4. Depois, configure recursos de dados e inicialize um cluster do Amazon EMR. Para ter mais informações, consulte Getting started with Amazon EMR.
5. Em seguida, você pode enviar uma aplicação do Spark com uma configuração adicional selecionando os nomes DNS no endpoint da VPC. Por exemplo, `spark.sql.catalog.ice_catalog.s3tables.endpoint` e `https://interface-endpoint.s3tables.us-east-1.vpce.amazonaws.com`. Para ter mais informações, consulte Submit work to your Amazon EMR cluster.

Restringir o acesso à funcionalidade Tabelas do S3 na rede da VPC

Semelhante às políticas baseadas em recurso, você pode anexar uma política de endpoint ao endpoint da VPC que controla o acesso às tabelas e aos buckets de tabela. No exemplo a seguir, a política de endpoint de interface restringe o acesso somente a buckets de tabela específicos.

```
{
    "Version": "2012-10-17",
    "Id": "Policy141511512309",
    "Statement": [{
        "Sid": "Access-to-specific-bucket-only",
        "Principal": "*",
        "Action": "s3tables:*",
        "Effect": "Allow",
        "Resource": [
            "arn:aws:s3tables:region:account_id:bucket/amzn-s3-demo-bucket",
            "arn:aws:s3tables:region:account_id:bucket/amzn-s3-demo-bucket/*"
        ]
    }]
}
```

Considerações e limitações de segurança para a funcionalidade Tabelas do S3

A lista a seguir descreve quais recursos e funções de segurança e controle de acesso são incompatíveis ou limitados para a funcionalidade Tabelas do S3.

- As políticas de acesso público não são compatíveis. Os usuários não podem modificar políticas de bucket ou de tabela para permitir acesso público.
- Os URLs pré-assinados para acessar objetos associados a uma tabela não são compatíveis.
- As tags não são compatíveis com tabelas e buckets de tabela. Portanto, não há suporte ao controle de acesso baseado em atributo e à alocação baseada em tags.
- Solicitações feitas por HTTP não são compatíveis. O Amazon S3 responde automaticamente com um redirecionamento HTTP em todas as solicitações feitas por HTTP a fim de atualizar as solicitações para HTTPS.
- É necessário usar o AWS Signature Version 4 ao fazer solicitações a um ponto de acesso usando as APIs REST.
- As solicitações feitas pelo protocolo de internet versão 6 (IPv6) são compatíveis apenas com ações ao nível do objeto em endpoints de armazenamento de tabelas, e não com ações ao nível da tabela e do bucket.
- As políticas de acesso a tabelas e buckets de tabela são limitadas a 20 KB.

Registro em log com o AWS CloudTrail para a funcionalidade Tabelas do S3

O Amazon S3 é integrado ao AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, um perfil ou um serviço da AWS. O CloudTrail captura todas as chamadas de API para o Amazon S3 como eventos. Ao fazer uso das informações coletadas pelo CloudTrail, é possível determinar a solicitação feita ao Amazon S3, o endereço IP que a realizou, quando ela foi feita e detalhes adicionais. Quando ocorre alguma atividade de evento aceita no Amazon S3, essa atividade é registrada em um evento do CloudTrail. É possível usar a trilha do AWS CloudTrail para registrar eventos de gerenciamento e de dados em log para a funcionalidade Tabelas do S3. Para ter mais informações, consulte Eventos do CloudTrail no Amazon S3 e What is AWS CloudTrail? no Guia do usuário do AWS CloudTrail.

Eventos de gerenciamento do CloudTrail para a funcionalidade Tabelas do S3

Os eventos de gerenciamento fornecem informações sobre operações de gerenciamento executadas em recursos na sua conta da AWS.

Por padrão, o CloudTrail registra eventos de gerenciamento em log para a funcionalidade Tabelas do S3. O `eventsource` para eventos de gerenciamento do CloudTrail para a funcionalidade Tabelas do S3 é `s3tables.amazonaws.com`. Quando você configura a conta AWS, os eventos de gerenciamento do CloudTrail são habilitados por padrão. Os seguintes eventos de gerenciamento são registrados em log no CloudTrail.

- `CreateNamespace`
- `CreateTable`
- `CreateTableBucket`
- `DeleteNamespace`
- `DeleteTable`
- `DeleteTableBucket`
- `DeleteTableBucketPolicy`
- `DeleteTablePolicy`
- `GetNamespace`
- `GetTable`
- `GetTableBucket`
- `GetTableBucketMaintenanceConfiguration`
- `GetTableBucketPolicy`
- `GetTableMaintenanceConfiguration`
- `GetTableMaintenanceJobStatus`
- `GetTableMetadataLocation`
- `GetTablePolicy`
- `ListNamespaces`
- `ListTableBuckets`
- `ListTables`
- `PutTableBucketMaintenanceConfiguration`

- PutTableMaintenanceConfiguration
- PutBucketPolicy
- PutTablePolicy
- RenameTable
- UpdateTableMetadataLocation

Para ter mais informações sobre eventos de gerenciamento do CloudTrail, consulte Logging management events no Guia do usuário do AWS CloudTrail.

Eventos de dados do CloudTrail para a funcionalidade Tabelas do S3

Os eventos de dados fornecem informações sobre as operações realizadas em um recurso ou dentro dele. Por padrão, as trilhas do CloudTrail não registram eventos de dados em log, mas é possível configurar as trilhas para que façam isso.

Ao registrar eventos de dados em log para uma trilha no CloudTrail, você escolherá ou especificará o tipo de recurso. A funcionalidade Tabelas do S3 tem dois tipos de recurso, `AWS::S3Tables::Table` e `AWS::S3Tables::TableBucket`.

Os eventos de dados a seguir são registrados em log no CloudTrail.

- AbortMultipartUpload
- CompleteMultipartUpload
- CreateMultipartUpload
- GetObject
- HeadObject
- ListParts
- PutObject
- UploadPart

Para ter mais informações sobre os eventos de dados do CloudTrail, consulte Logging data events no Guia do usuário do AWS CloudTrail.

Para ter mais informações sobre os eventos do CloudTrail para a funcionalidade Tabelas do S3, consulte os seguintes tópicos:

Tópicos

- Exemplos de arquivos de log de eventos de dados do AWS CloudTrail para a funcionalidade Tabelas do S3

Exemplos de arquivos de log de eventos de dados do AWS CloudTrail para a funcionalidade Tabelas do S3

O arquivo de log do AWS CloudTrail inclui informações sobre a operação de API solicitada, a data e a hora da operação, os parâmetros de solicitação etc. Este tópico fornece exemplos de arquivos de log para eventos de dados do CloudTrail para a funcionalidade Tabelas do S3.

Tópicos

- Exemplo: arquivo de log do CloudTrail para evento de dados de GetObject
- Exemplo: arquivo de log do CloudTrail para evento de dados de PutObject

Exemplo: arquivo de log do CloudTrail para evento de dados de **`GetObject`**

Veja a seguir um exemplo de arquivo de log do CloudTrail que demonstra a operação de API `GetObject`.


```
{
    "eventVersion": "1.11",
    "userIdentity": {
      "type": "IAMUser",
      "principalId": "123456789012",
      "arn": "arn:aws:iam::111122223333:user/"myUserName",
      "accountId": "111122223333",
      "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
      "userName":"myUserName"
    },
    "eventTime": "2024-11-22T17:12:25Z",
    "eventSource": "s3tables.amazonaws.com",
    "eventName": "GetObject",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "[aws-cli/2.18.5]",
    "requestParameters": {
        "Host": "tableWarehouseLocation.s3.us-east-1.amazonaws.com",
        "key": "product-info.json"
```

```
        },
        "responseElements":  null,
        "additionalEventData": {
            "SignatureVersion": "SigV4",
            "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
            "bytesTransferredIn": 0,
            "AuthenticationMethod": "AuthHeader",
            "xAmzId2": "q6xhNJYmhg",
            "bytesTransferredOut": 28441

          },
          "requestID": "07D681123BD12AED",
          "eventID": "f2b287f3-0df1-1234-a2f4-c4bdfed47657",
          "readOnly": true,
          "resources": [{
              "accountId": "111122223333",
              "type": "AWS::S3Tables::TableBucket",
               "ARN": "arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-
bucket1"
           }, {
              "accountId": "111122223333",
              "type": "AWS::S3Tables::Table",
              "ARN": "arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-
bucket/table/111aa1111-22bb-33cc-44dd-5555eee66ffff"

           }],
           "eventType": "AwsApiCall",
           "managementEvent": false,
           "recipientAccountId": "444455556666",
           "eventCategory": "Data",
           "tlsDetails": {
             "tlsVersion": "TLSv1.2",
             "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
             "clientProvidedHostHeader": "tableWarehouseLocation.s3.us-
east-1.amazonaws.com"
          }
    }
```

Exemplo: arquivo de log do CloudTrail para evento de dados de **`PutObject`**

Veja a seguir um exemplo de arquivo de log do CloudTrail que demonstra a operação de API `PutObject`.

```
{
        "eventVersion": "1.11",
        "userIdentity": {
          "type": "IAMUser",
          "principalId": "123456789012",
          "arn":  "arn:aws:iam::444455556666:user/"myUserName",
          "accountId": "444455556666",
          "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
          "userName":"myUserName"
        },
        "eventTime": "2024-11-22T17:12:25Z",
        "eventSource": "s3tables.amazonaws.com",
        "eventName": "PutObject",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "192.0.2.0",
        "userAgent": "[aws-cli/2.18.5]",
        "requestParameters": {
            "Host": "tableWarehouseLocation.s3.us-east-1.amazonaws.com",
            "key": "product-info.json"
        },
        "responseElements":  {
            "x-amz-server-side-encryption": "AES256",
            "x-amz-version-id": "13zAFMdccAjt3MWd6ehxgCCCDRdkAKDw"
        },
        "additionalEventData": {
            "SignatureVersion": "SigV4",
            "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
            "bytesTransferredIn": 28441,
            "AuthenticationMethod": "AuthHeader",
            "xAmzId2": "q6xhCJYmhg",
            "bytesTransferredOut": 0

          },
          "requestID": "28d2faaf-1234-4649-997d-EXAMPLE72818",
          "eventID": "694d604a-d190-1234-0dd1-EXAMPLEe20c1",
          "readOnly": false,
          "resources": [{
              "accountId": "444455556666",
              "type": "AWS::S3Tables::TableBucket",
               "ARN": "arn:aws:s3tables:us-east-1:444455556666:bucket/amzn-s3-demo-
bucket1"
           }, {
              "accountId": "444455556666",
```

```
              "type": "AWS::S3Tables::Table",
              "ARN": "arn:aws:s3tables:us-east-1:444455556666:bucket/amzn-s3-demo-
bucket1/table/b89ec883-b1d9-4b37-9cd7-b86f590123f4"
           }],
           "eventType": "AwsApiCall",
           "managementEvent": false,
           "recipientAccountId": "111122223333",
           "eventCategory": "Data",
           "tlsDetails": {
             "tlsVersion": "TLSv1.2",
             "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
             "clientProvidedHostHeader": "tableWarehouseLocation.s3.us-
east-1.amazonaws.com"
            }
          }
```

Controle de acesso no Amazon S3

Na AWS, um recurso é uma entidade com a qual você pode trabalhar. No Amazon Simple Storage Service (S3), buckets e objetos são os recursos originais do Amazon S3. É provável que todo cliente do S3 tenha buckets com objetos. A adição de novas funcionalidades ao S3 também acompanha novos recursos adicionais, mas nem todo cliente usa esses recursos específicos. Para obter mais informações sobre os recursos do Amazon S3, consulte Recursos do S3.

Por padrão, todos os recursos do Amazon S3 são privados. Além disso, por padrão, o usuário-raiz da Conta da AWS que criou o recurso (proprietário do recurso) e os usuários do IAM dentro dessa conta com as permissões necessárias podem acessar um recurso que eles criaram. O proprietário do recurso decide quem mais pode acessar o recurso e as ações que outras pessoas podem realizar no recurso. O S3 tem várias ferramentas de gerenciamento de acesso que você pode usar para conceder a outras pessoas acesso aos seus recursos do S3.

As seções a seguir fornecem uma visão geral dos recursos do S3, das ferramentas de gerenciamento de acesso do S3 disponíveis e dos melhores casos de uso para cada ferramenta de gerenciamento de acesso. As listas nessas seções buscam ser abrangentes e incluir todos os recursos, ferramentas de gerenciamento de acesso e casos de uso comuns de gerenciamento de acesso do S3. Ao mesmo tempo, essas seções foram projetadas para serem diretórios que levam você aos detalhes técnicos desejados. Se você já tiver uma boa compreensão de alguns dos tópicos a seguir, poderá pular para a seção que se aplica a você.

Para ter mais informações sobre as permissões referentes a operações de API do S3 de acordo com os tipos de recurso do S3, consulte Permissões obrigatórias para operações de API do Amazon S3.

Tópicos

- Recursos do S3
- Identidades
- Ferramentas de gerenciamento de acesso
- Ações
- Casos de uso do gerenciamento de acesso
- Solução de problemas de gerenciamento de acesso

Recursos do S3

Os recursos originais do Amazon S3 são os buckets e os objetos que eles contêm. À medida que novas funcionalidades são adicionadas ao S3, novos recursos também são adicionados. Veja a seguir uma lista completa dos recursos do S3 e suas respectivas funcionalidades.

Tipo de recurso	Funcionalidade do Amazon S3	Descrição
`bucket`	Atributos principais	Um bucket é um contêiner de objetos. Para armazenar um objeto no S3, crie um bucket e faça upload de um ou mais objetos no bucket. Para obter mais informações, consulte Criar, configurar e trabalhar com buckets de uso geral do Amazon S3.
`object`		Um objeto pode ser um arquivo e qualquer metadado que descreva esse arquivo. Quando um objeto estiver no bucket, você poderá abri-lo, fazer download dele e movê-lo. Para obter mais informações, consulte Trabalhar com objetos no Amazon S3.
`accesspoint`	Pontos de acesso	Os pontos de acesso são endpoints de rede nomeados e anexados a buckets que você pode usar para realizar operações de objeto do Amazon S3, como `GetObject` e `PutObject` . Cada ponto de acesso tem permissões e controles de rede distintos e uma política de ponto de acesso personalizada que funciona em conjunto com a política de bucket anexada ao bucket subjacente. Você pode configurar qualquer ponto de acesso para aceitar solicitações somente de uma nuvem privada virtual (VPC) ou definir configurações personalizadas de bloqueio de acesso público para cada ponto de acesso. Para obter mais informações, consulte Gerenciar o acesso a conjuntos de dados compartilhados com pontos de acesso.

Tipo de recurso	Funcionalidade do Amazon S3	Descrição
`objectlambdaaccesspoint`		Um ponto de acesso do Object Lambda é um ponto de acesso para um bucket que também está associado a uma função do Lambda. Com o ponto de acesso do Object Lambda, você pode adicionar seu próprio código às solicitações `GET`, `LIST` e `HEAD` do Amazon S3 para modificar e processar dados à medida que eles são retornados a uma aplicação. Para obter mais informações, consulte Criar pontos de acesso do Object Lambda.
`multiregionaccesspoint`		Os pontos de acesso multirregionais fornecem um endpoint global que as aplicações podem usar para atender a solicitações de buckets do S3 localizados em várias regiões da AWS. Você pode usar pontos de acesso multirregionais para criar aplicações de várias regiões com a mesma arquitetura usada em uma única região, depois executar essas aplicações em qualquer lugar do mundo. Em vez de enviar solicitações pela internet pública congestionada, as solicitações de aplicações feitas para um endpoint global de ponto de acesso multirregional são roteadas automaticamente pela rede global da AWS para o bucket do Amazon S3 mais próximo. Para obter mais informações, consulte Gerenciar o tráfego multirregional com Pontos de Acesso Multirregionais.

Tipo de recurso	Funcionalidade do Amazon S3	Descrição
`job`	Operações em lote do S3	Um trabalho é um recurso da funcionalidade Operações em Lote do S3. É possível usar a funcionalidade Operações em Lote do S3 para executar operações em lote de grande escala em listas de objetos do Amazon S3 que você especificar. O Amazon S3 rastreia o progresso do trabalho de operação em lote, envia notificações e armazena um relatório de conclusão detalhado de todas as ações, fornecendo uma experiência totalmente gerenciada, auditável e sem servidor. Para obter mais informações, consulte Executar operações de objetos em massa com o Operações em Lote.
`storagelensconfiguration`	Lente de Armazenamento do S3	Uma configuração da funcionalidade Lente de Armazenamento do S3 coleta métricas de armazenamento e dados do usuário de todas as contas da organização. A funcionalidade Lente de Armazenamento do S3 fornece aos administradores uma visão única do uso e da atividade do armazenamento de objetos em centenas ou até milhares de contas de uma organização, com detalhes para gerar insights em vários níveis de agregação. Para obter mais informações, consulte Avaliação de sua atividade de armazenamento e uso com a Lente de Armazenamento do Amazon S3.
`storagelensgroup`		Um grupo da Lente de Armazenamento do S3 agrega métricas usando filtros personalizados com base nos metadados de objetos. Os grupos da Lente de Armazenamento do S3 ajudam a investigar as características dos dados, como distribuição de objetos por idade, tipos de arquivo mais comuns e muito mais. Para obter mais informações, consulte Trabalhar com grupos da Lente de Armazenamento do S3 para filtrar e agregar métricas.

Tipo de recurso	Funcionalidade do Amazon S3	Descrição
`accessgrantsinstance`	Concessões de Acesso do S3	Uma instância da funcionalidade Concessões de Acesso do S3 é um contêiner para as concessões do S3 que você cria. Com funcionalidade Concessões de Acesso do S3, você pode criar concessões aos seus dados do Amazon S3 para identidades do IAM em sua conta, identidades do IAM em outras contas (entre contas) e identidades de diretório adicionadas ao AWS IAM Identity Center pelo seu diretório corporativo. Para obter mais informações sobre a funcionalidade Concessões de Acesso do S3, consulte Gerenciar o acesso com a funcionalidade Concessões de Acesso do S3.
`accessgrantslocation`		Um Local de Concessões de Acesso é um bucket, um prefixo dentro de um bucket ou um objeto que você registra em sua instância da funcionalidade Concessões de Acesso do S3. Para poder criar uma concessão a um local, primeiro é necessário registrá-lo na instância da funcionalidade Concessões de Acesso do S3. Depois, com a funcionalidade Concessões de Acesso do S3, você pode conceder acesso ao bucket, prefixo ou objeto para identidades do IAM em sua conta, identidades do IAM em outras contas (entre contas) e identidades de diretório adicionadas ao AWS IAM Identity Center pelo seu diretório corporativo. Para obter mais informações sobre a funcionalidade Concessões de Acesso do S3, consulte Gerenciar o acesso com a funcionalidade Concessões de Acesso do S3.

Tipo de recurso	Funcionalidade do Amazon S3	Descrição
`accessgrant`		Uma concessão de acesso é uma concessão individual aos seus dados do Amazon S3. Com funcionalidade Concessões de Acesso do S3, você pode criar concessões aos seus dados do Amazon S3 para identidades do IAM em sua conta, identidades do IAM em outras contas (entre contas) e identidades de diretório adicionadas ao AWS IAM Identity Center pelo seu diretório corporativo. Para obter mais informações sobre a funcionalidade Concessões de Acesso do S3, consulte Gerenciar o acesso com a funcionalidade Concessões de Acesso do S3.

Buckets

Há dois tipos de bucket do Amazon S3: os buckets de uso geral e os buckets de diretório.

- Os buckets de uso geral são o tipo original de bucket do S3 e são recomendados para a maioria dos casos de uso e padrões de acesso. Os buckets de uso geral também permitem que objetos sejam armazenados em todas as classes de armazenamento, exceto na classe S3 Express One Zone. Para obter mais informações sobre as classes de armazenamento do S3, consulte Compreender e gerenciar classes de armazenamento do Amazon S3.
- Os buckets de diretório usam a classe de armazenamento S3 Express One Zone, que é recomendada se sua aplicação é sensível à performance e se beneficia de latências inferiores a dez milissegundos para `PUT` e `GET`. Para ter mais informações, consulte Trabalhar com buckets de diretório, S3 Express One Zone e Autorizar operações de API de endpoint regional com o IAM.

Categorizar os recursos do S3

O Amazon S3 oferece funcionalidades para categorizar e organizar seus recursos do S3. Além de ser útil para organizar os recursos, a categorização também permite que você defina regras de gerenciamento de acesso com base nas categorias de recursos. Em particular, prefixos e marcações são duas funcionalidades de organização de armazenamento que você pode usar ao definir permissões de gerenciamento de acesso.

> **Note**
>
> As informações a seguir se aplicam a buckets de uso geral. Os buckets de diretório não oferecem suporte à marcação e têm limitações de prefixo. Para obter mais informações, consulte Autorizar operações de API de endpoint regional com o IAM.

- Prefixos: um prefixo no Amazon S3 é uma string de caracteres no início do nome de uma chave de objeto que é usado para organizar os objetos armazenados em buckets do S3. Você pode usar um caractere delimitador, como uma barra (`/`), para indicar o final do prefixo no nome da chave de objeto. Por exemplo, você pode ter nomes de chave de objeto que começam com o prefixo `engineering/` ou nomes de chave de objeto que começam com o prefixo `marketing/campaigns/`. O uso de um delimitador no final do prefixo, como um caractere de barra `/`, simula as convenções de nomenclatura de pastas e arquivos. No entanto, no S3, o prefixo faz parte do nome da chave de objeto. Em buckets do S3 de uso geral, não há uma hierarquia real de pastas.

  O Amazon S3 oferece suporte à organização e ao agrupamento de objetos por meio de seus prefixos. Também é possível gerenciar o acesso aos objetos por meio de seus prefixos. Por exemplo, é possível limitar o acesso somente aos objetos com nomes que começam com um prefixo específico.

  Para obter mais informações, consulte Organizar objetos usando prefixos. O console do S3 usa o conceito de pastas, que, em buckets de uso geral, são prefixos previamente incluídos no nome da chave de objeto. Para obter mais informações, consulte Organizar objetos no console do Amazon S3 usando pastas.
- Etiquetas: cada etiqueta é um par de chave/valor que é atribuído aos recursos. Por exemplo, você pode marcar alguns recursos com a etiqueta `topicCategory=engineering`. Você pode usar a marcação para ajudar na alocação de custos, na categorização e organização e no controle de acesso. A marcação de buckets é usada somente para alocação de custos. Você pode marcar objetos, trabalhos e as funcionalidades Lente de Armazenamento e Concessões de Acesso do S3 para fins de organização ou controle de acesso. Na funcionalidade Concessões de Acesso do S3, também é possível usar a marcação para alocação de custos. Como exemplo de controle do acesso aos recursos usando as etiquetas deles, você pode compartilhar somente os objetos que têm uma etiqueta específica ou uma combinação de etiquetas.

  Para obter mais informações, consulte Controle do acesso aos recursos da AWS usando tags de recursos no Guia do usuário do IAM.

Identidades

No Amazon S3, o proprietário do recurso é a identidade que criou o recurso, como um bucket ou um objeto. Por padrão, somente o usuário-raiz da conta que criou o recurso e as identidades do IAM dentro da conta que têm a permissão necessária podem acessar o recurso do S3. Os proprietários de recursos podem conceder acesso aos seus recursos do S3 para outras identidades.

Identidades que não possuem um recurso podem solicitar acesso a esse recurso. As solicitações para um recurso são autenticadas ou não autenticadas. As solicitações autenticadas devem incluir um valor de assinatura que autentica o remetente da solicitação, enquanto solicitações não autenticadas não exigem assinatura. Recomendamos que você conceda acesso somente a usuários autenticados. Consulte mais informações sobre a autenticação de solicitações em Making requests na Referência da API do Amazon S3.

> **Important**
>
> Recomendamos que você não use credenciais de usuário raiz da Conta da AWS para fazer solicitações autenticadas. Em vez disso, crie um perfil do IAM e conceda acesso total a ele. Usuários com esse perfil são conhecidos como usuários administradores. Em vez de usar credenciais de usuário raiz da Conta da AWS, você pode usar credenciais atribuídas ao perfil administrador para interagir com a AWS e realizar tarefas, como criar um bucket, criar usuários e conceder permissões a eles. Para obter mais informações, consulte Credenciais de usuário-raiz da Conta da AWS e credenciais de usuário do IAM na Referência geral da AWS e Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.

As identidades que acessam seus dados no Amazon S3 podem ser uma das seguintes:

Conta da AWS proprietária

A Conta da AWS que criou o recurso. Por exemplo, a conta que criou o bucket. Essa conta é a proprietária do recurso. Para obter mais informações, consulte Usuário-raiz da conta da AWS.

Identidades do IAM na mesma conta da Conta da AWS proprietária

Ao configurar contas para novos membros da equipe que precisam de acesso ao S3, a Conta da AWS proprietária pode usar o AWS Identity and Access Management (IAM) para criar usuários, grupos e perfis. Depois, a Conta da AWS proprietária pode compartilhar recursos com essas

identidades do IAM. A conta proprietária também pode especificar permissões para conceder às identidades do IAM, o que permite ou nega as ações que podem ser executadas nos recursos compartilhados.

As identidades do IAM fornecem mais recursos, incluindo a capacidade de exigir que os usuários insiram credenciais de login antes de acessar recursos compartilhados. Usando as identidades do IAM, é possível implementar uma forma de autenticação multifator (MFA) do IAM para oferecer suporte a uma base de identidade sólida. Uma prática recomendada do IAM é a criação de perfis para gerenciamento de acesso em vez de conceder permissões a cada usuário individual. Você atribui usuários individuais ao perfil apropriado. Para obter mais informações, consulte Práticas recomendadas de segurança no IAM.

Outras contas da AWS proprietárias e suas identidades do IAM (acesso entre contas)

A Conta da AWS proprietária também pode conceder acesso aos recursos para outras contas da AWS proprietárias ou identidades do IAM que pertençam a outra conta da AWS.

> **Note**
>
> Delegação de permissão: se uma Conta da AWS for proprietária de um recurso, ela poderá conceder essas permissões a outra Conta da AWS. Essa conta poderá delegar essas permissões, ou um subconjunto delas, para usuários da mesma conta. Isso é chamado de delegação de permissão. No entanto, uma conta que recebe permissões de outra conta não pode delegar essas permissões “entre contas” para outra Conta da AWS.

Usuários anônimos (acesso público)

A Conta da AWS proprietária pode tornar os recursos públicos. Tornar um recurso público tecnicamente compartilha o recurso com o usuário anônimo. Os buckets criados desde abril de 2023 bloqueiam todo o acesso público por padrão, a menos que você altere essa configuração. Recomendamos que você configure os buckets para bloquear o acesso público e que conceda acesso somente a usuários autenticados. Para obter mais informações sobre como bloquear o acesso público, consulte Bloquear o acesso público ao armazenamento do Amazon S3.

Serviços da AWS

O proprietário do recurso pode conceder acesso a um recurso do Amazon S3 para outro serviço da AWS. Por exemplo, você pode conceder a permissão `s3:PutObject` ao serviço AWS

CloudTrail para gravação de arquivos de log no seu bucket. Para obter mais informações, consulte Fornecimento de acesso a um produto da AWS.

Identidades do diretório corporativo

O proprietário do recurso pode conceder aos usuários ou perfis do seu diretório corporativo acesso a um recurso do S3 usando a funcionalidade Concessões de Acesso do S3. Para obter mais informações sobre como adicionar um diretório corporativo ao AWS IAM Identity Center, consulte What is IAM Identity Center?

Proprietários de bucket ou recurso

A Conta da AWS que você usa para criar buckets e carregar objetos é a proprietária desses recursos. Um proprietário do bucket pode conceder permissões entre contas à outra Conta da AWS (ou aos usuários em outra conta) para carregar objetos.

Quando o proprietário de um bucket permite que outra conta faça upload de objetos em um bucket, o proprietário do bucket é dono de todos os objetos enviados para esse bucket por padrão. No entanto, se as configurações Imposto pelo proprietário do bucket e Proprietário do bucket preferido estiverem desativadas, a Conta da AWS que faz upload dos objetos será proprietária desses objetos, e o proprietário do bucket não terá permissões sobre os objetos pertencentes a outra conta, com as seguintes exceções:

- O proprietário do bucket paga as faturas. O proprietário do bucket pode negar acesso a todos os objetos ou excluir objetos no bucket, independentemente de quem o possui.
- O proprietário do bucket pode arquivar todos os objetos ou restaurar os objetos arquivados, independentemente de quem os possui. Arquivo refere-se à classe de armazenamento usada para armazenar os objetos. Para obter mais informações, consulte Gerenciar o ciclo de vida dos objetos.

Ferramentas de gerenciamento de acesso

O Amazon S3 fornece uma variedade de recursos e ferramentas de segurança. Veja a seguir uma lista abrangente desses recursos e ferramentas. Você não precisa de todas essas ferramentas de gerenciamento de acesso, mas deve usar uma ou mais para conceder acesso aos seus recursos do Amazon S3. A aplicação adequada dessas ferramentas pode ajudar a garantir que seus recursos só possam ser acessados pelos usuários pretendidos.

A ferramenta de gerenciamento de acesso mais usada é a política de acesso. Uma política de acesso pode ser uma política baseada em recurso vinculada a um recurso da AWS, como uma política de bucket para um bucket. Uma política de acesso também pode ser uma política baseada em identidade anexada a uma identidade do AWS Identity and Access Management (IAM), como um usuário, grupo ou perfil do IAM. Escreva uma política de acesso para conceder a Contas da AWS e usuários, grupos e perfis do IAM permissão para realizar operações em um recurso. Por exemplo, você pode conceder a permissão `PUT Object` para outra Conta da AWS de modo que o usuário possa fazer upload de objetos em seu bucket.

A política de acesso descreve quem tem acesso a quê. Quando o Amazon S3 recebe uma solicitação, ele precisa avaliar todas as políticas de acesso para determinar se deve autorizar ou negar a solicitação. Para obter mais informações sobre como o Amazon S3 avalia essas políticas, consulte Como o Amazon S3 autoriza uma solicitação.

Veja a seguir as ferramentas de gerenciamento de acesso disponíveis no Amazon S3.

Política de bucket

Uma política de bucket do Amazon S3 é uma política baseada em recurso do AWS Identity and Access Management (IAM), formatada em JSON, que é anexada a determinado bucket. Use políticas de bucket para conceder a outras Contas da AWS ou identidades do IAM permissões de acesso ao bucket e aos objetos contidos nele. Muitos casos de uso de gerenciamento de acesso do S3 podem ser atendidos usando uma política de bucket. Com as políticas de bucket, é possível personalizar o acesso ao bucket para ajudar a garantir que somente as identidades que você aprovou possam acessar recursos e executar ações neles. Para obter mais informações, consulte Políticas de bucket para o Amazon S3.

A seguir há um exemplo de política de bucket. Expresse a política de bucket usando um arquivo JSON. Esse exemplo de política concede uma permissão de leitura do perfil do IAM a todos os objetos no bucket. Ela contém uma instrução chamada `BucketLevelReadPermissions`, que permite a ação `s3:GetObject` (permissão de leitura) nos objetos em um bucket chamado `amzn-s3-demo-bucket1`. Ao especificar um perfil do IAM como `Principal`, essa política concede acesso a todos os usuários do IAM com esse perfil. Para usar esse exemplo de política, substitua os *`user input placeholders`* por suas próprias informações.

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
```

```
      "Sid":"BucketLevelReadPermissions",
      "Effect":"Allow",
      "Principal": {
     "AWS": "arn:aws:iam::123456789101:role/s3-role"
      },
      "Action":["s3:GetObject"],
      "Resource":["arn:aws:s3:::amzn-s3-demo-bucket1/*"]
    }]
  }
```

> **Note**
>
> Ao criar políticas, evite o uso de caracteres curinga (*) no elemento `Principal`, porque ele permite que qualquer pessoa acesse os recursos do Amazon S3. Em vez disso, é melhor listar explicitamente usuários ou grupos que têm permissão para acessar o bucket ou listar condições que devem ser atendidas usando uma cláusula de condição na política. Além disso, em vez de incluir um caractere curinga para as ações de seus usuários ou grupos, conceda a eles permissões específicas quando aplicável.

Política baseada em identidade

Uma política de usuário do IAM ou baseada em identidade é um tipo de política do AWS Identity and Access Management(IAM). Uma política baseada em identidade é uma política em formato JSON anexada a usuários, grupos ou perfis do IAM em sua conta da AWS. Você pode usar políticas baseadas em identidade para conceder a uma identidade do IAM acesso a buckets ou objetos. É possível criar usuários, grupos e perfis do IAM em sua conta e anexar políticas de acesso a eles. Depois, você pode conceder acesso a recursos da AWS, incluindo recursos do Amazon S3. Para obter mais informações, consulte Políticas baseadas em identidade do Amazon S3.

Veja a seguir um exemplo de uma política baseada em identidade. O exemplo de política permite que o perfil do IAM associado execute seis ações diferentes do Amazon S3 (permissões) em um bucket e nos objetos contidos nele. Se você anexar essa política a um perfil do IAM em sua conta e atribuir o perfil a alguns de seus usuários do IAM, os usuários com esse perfil poderão realizar essas ações nos recursos (buckets) especificados na política. Para usar esse exemplo de política, substitua os *user input placeholders* por suas próprias informações.

```
{
  "Version": "2012-10-17",
```

```
  "Statement": [
  {
    "Sid": "AssignARoleActions",
    "Effect": "Allow",
    "Action": [
   "s3:PutObject",
   "s3:GetObject",
   "s3:ListBucket",
   "s3:DeleteObject",
   "s3:GetBucketLocation"
    ],
    "Resource": [
   "arn:aws:s3:::amzn-s3-demo-bucket1/*",
   "arn:aws:s3:::amzn-s3-demo-bucket1"
    ]
    },
  {
    "Sid": "AssignARoleActions2",
    "Effect": "Allow",
    "Action": "s3:ListAllMyBuckets",
    "Resource": "*"
  }
  ]
}
```

Concessões de Acesso do S3

Use a funcionalidade Concessões de Acesso do S3 para criar concessões de acesso aos seus dados do Amazon S3 para identidades em diretórios de identidades corporativas, como Active Directory, e para identidades do AWS Identity and Access Management (IAM). A funcionalidade Concessões de Acesso do S3 ajuda você a gerenciar permissões de dados em grande escala. Além disso, a funcionalidade Concessões de Acesso do S3 registra a identidade do usuário final e a aplicação usada para acessar os dados do S3 em logs do AWS CloudTrail. Isso fornece um histórico de auditoria detalhado até a identidade do usuário final para todos os acessos aos dados em seus buckets do S3. Para obter mais informações, consulte Gerenciar o acesso com a funcionalidade Concessões de Acesso do S3.

Pontos de acesso

A funcionalidade Pontos de Acesso Amazon S3 simplifica o gerenciamento do acesso a dados em escala para aplicações que usam conjuntos de dados compartilhados no S3. Os pontos de acesso são endpoints de rede nomeados que são anexados a um bucket. Você pode usar os pontos

de acesso para executar operações em objetos do S3 em grande escala, como fazer upload e recuperar objetos. Um bucket pode ter até 10.000 pontos de acesso anexados, e é possível impor permissões distintas e controles de rede a cada ponto de acesso para fornecer controle detalhado sobre o acesso aos objetos do S3. A funcionalidade Pontos de Acesso do S3 pode ser associada a buckets na mesma conta ou em outra conta confiável. As políticas de pontos de acesso são políticas baseadas em recurso que são avaliadas em conjunto com a política de bucket correspondente. Para obter mais informações, consulte Gerenciar o acesso a conjuntos de dados compartilhados com pontos de acesso.

Lista de controle de acesso (ACL)

Uma ACL é uma lista de concessões que identifica o concessionário e a permissão concedida. As ACLs concedem permissões básicas de leitura ou gravação a outras Contas da AWS. As ACLs usam um esquema XML específico do Amazon S3. Uma ACL é um tipo de política do AWS Identity and Access Management (IAM). Uma ACL de objeto é usada para gerenciar o acesso a um objeto, e uma ACL de bucket é usada para gerenciar o acesso a um bucket. No caso das políticas de bucket, há uma única política para o bucket todo, mas as ACLs de objeto são especificadas por objeto. Recomendamos manter as ACLs desativadas, exceto em circunstâncias incomuns em que seja necessário controlar o acesso para cada objeto individualmente. Para obter mais informações sobre como usar ACLs, consulte Controlar a propriedade de objetos e desabilitar ACLs para seu bucket.

> **Warning**
>
> A maioria dos casos de uso modernos no Amazon S3 não exige o uso de ACLs.

Esta é uma ACL de bucket de exemplo. A concessão na ACL mostra um proprietário de bucket com permissão de controle total.

```
<?xml version="1.0" encoding="UTF-8"?>
 <AccessControlPolicy xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Owner>
   <ID>Owner-Canonical-User-ID</ID>
   <DisplayName>owner-display-name</DisplayName>
  </Owner>
 <AccessControlList>
  <Grant>
   <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="Canonical
 User">
    <ID>Owner-Canonical-User-ID</ID>
```

```
    <DisplayName>display-name</DisplayName>
   </Grantee>
   <Permission>FULL_CONTROL</Permission>
  </Grant>
 </AccessControlList>
</AccessControlPolicy>
```

Propriedade de Objeto

Para gerenciar o acesso a um objeto, você precisa ser o proprietário desse objeto. Você pode usar a configuração Propriedade de Objeto ao nível do bucket para controlar a propriedade de objetos carregados no bucket. Além disso, use a Propriedade de Objeto para ativar as ACLs. Por padrão, a Propriedade de Objeto é definida como a configuração Imposto pelo proprietário do bucket e todas as ACLs estão desativadas. Quando as ACLs estão desativadas, o proprietário do bucket possui todos os objetos do bucket e gerencia exclusivamente o acesso aos dados. Para gerenciar o acesso, o proprietário do bucket usa políticas ou outra ferramenta de gerenciamento de acesso, excluindo as ACLs. Para obter mais informações, consulte Controlar a propriedade de objetos e desabilitar ACLs para seu bucket.

Há três configurações para a Propriedade de Objeto que podem ser usadas tanto para controlar a propriedade de objetos carregados no bucket como para ativar as ACLs:

ACLs desativadas

- Imposto pelo proprietário do bucket (padrão): as ACLs são desativadas e o proprietário do bucket automaticamente tem a propriedade e o controle total sobre todos os objetos do bucket. As ACLs não afetam mais as permissões aos dados no bucket do S3. O bucket usa políticas exclusivamente para definir o controle de acesso.

ACLs ativadas

- Bucket owner preferred (Preferencial do proprietário do bucket): o proprietário do bucket tem a propriedade e o controle total sobre novos objetos que outras contas gravam no bucket com a ACL `bucket-owner-full-control` pré-configurada.
- Object writer (Gravador de objetos): a Conta da AWS que carrega um objeto é a proprietária do objeto, tem controle total sobre ele e pode conceder acesso a outros usuários por meio de ACLs.

Melhores práticas adicionais

Considere o uso das seguintes ferramentas e configurações de bucket para ajudar a proteger os dados em trânsito e em repouso, ambas as quais são cruciais para manter a integridade e a acessibilidade dos dados.

- Bloquear acesso público: não desative a configuração padrão ao nível do bucket Bloquear acesso público. Essa configuração bloqueia o acesso público aos seus dados por padrão. Para obter mais informações sobre como bloquear o acesso público, consulte Bloquear o acesso público ao armazenamento do Amazon S3.
- Versionamento do S3: para manter a integridade dos dados, você pode implementar a configuração de bucket Versionamento do S3, que cria versões dos objetos à medida que você faz atualizações, em vez de substituí-los. O Versionamento do S3 pode ser usado para preservar, recuperar e restaurar uma versão anterior, se necessário. Para obter informações sobre o Versionamento do S3, consulte Reter várias versões de objetos com o Versionamento do S3.
- Bloqueio de Objetos do S3: a funcionalidade Bloqueio de Objetos do S3 é outra configuração que você pode implementar para alcançar a integridade dos dados. Esse recurso pode implementar um modelo de gravação única e várias leituras (WORM) para armazenar objetos de forma imutável. Para obter mais informações sobre Bloqueio de objetos, consulte Bloquear objetos com o Bloqueio de Objetos.
- Criptografia de objetos: o Amazon S3 oferece várias opções de criptografia de objetos que protegem os dados em trânsito e em repouso. A criptografia no lado do servidor criptografa o objeto antes de salvá-lo em discos em seus data centers e os descriptografa ao fazer download dos objetos. Se você autentica sua solicitação e tem permissões de acesso, não há diferença na forma de acesso aos objetos criptografados ou não criptografados. Para obter mais informações, consulte Proteger os dados usando criptografia do lado do servidor. O S3 criptografa objetos recém-carregados por padrão. Para obter mais informações, consulte Definir o comportamento padrão da criptografia para os buckets do Amazon S3. Criptografia no lado do cliente é o ato de criptografar os dados antes de enviá-los para o Amazon S3. Para obter mais informações, consulte Proteger dados usando a criptografia do lado do cliente.
- Métodos de assinatura: o Signature Version 4 é o processo para adicionar informações de autenticação às solicitações da AWS enviadas por HTTP. Por segurança, a maioria das solicitações para AWS deve ser assinada com uma chave de acesso, que consiste em um ID de chave de acesso e na chave de acesso secreta. Essas duas chaves são comumente conhecidas como suas credenciais de segurança. Para obter mais informações, consulte Autenticação de solicitações (AWS Signature Version 4) e Processo de assinatura do Signature Version 4.

Ações

Consulte uma lista completa de permissões e chaves de condição do S3 em Actions, resources, and condition keys for Amazon S3 na Referência de autorização do serviço.

Para ter mais informações sobre as permissões referentes a operações de API do S3 de acordo com os tipos de recurso do S3, consulte Permissões obrigatórias para operações de API do Amazon S3.

Ações

As ações do AWS Identity and Access Management (IAM) para o Amazon S3 são as ações possíveis que podem ser executadas em um bucket ou objeto do S3. Conceda essas ações às identidades para que elas possam agir em seus recursos do S3. Exemplos de ações do S3 são `s3:GetObject` para ler objetos em um bucket e `s3:PutObject` para gravar objetos em um bucket.

Chaves de condição

Além das ações, as chaves de condição do IAM se limitam a conceder acesso somente quando uma condição é atendida. As chaves de condição são opcionais.

> **Note**
>
> Em uma política de acesso baseada em recursos, como uma política de bucket, ou em uma política baseada em identidade, você pode especificar o seguinte:
>
> - Uma ação ou uma matriz de ações no elemento `Action` da declaração de política.
> - No elemento `Effect` da declaração de política, é possível especificar `Allow` para permitir as ações listadas ou especificar `Deny` para bloquear as ações listadas. Para aprimorar ainda mais a prática de privilégios mínimos, as instruções `Deny` no elemento `Effect` da política de acesso devem ser o mais amplas possíveis e as instruções `Allow` devem ser tão restritas quanto possível. O efeito de `Deny` combinado com a ação `s3:*` é outra boa maneira de implementar as práticas recomendadas de adesão para as identidades incluídas em instruções de condição da política.
> - Uma chave de condição no elemento `Condition` de uma declaração de política.

Casos de uso do gerenciamento de acesso

O Amazon S3 fornece aos proprietários de recursos uma variedade de ferramentas para conceder acesso. A ferramenta de gerenciamento de acesso do S3 utilizada dependerá dos recursos do S3 que você deseja compartilhar, das identidades às quais você está concedendo acesso e das ações que deseja permitir ou negar. Talvez você queira usar uma ferramenta ou uma combinação de ferramentas de gerenciamento de acesso do S3 para gerenciar o acesso aos recursos do S3.

Na maioria dos casos, é possível usar uma política de acesso para gerenciar as permissões. Uma política de acesso pode ser uma política baseada em recurso que é vinculada a um recurso, como um bucket ou outro recurso do Amazon S3 (Recursos do S3). Uma política de acesso também pode ser uma política baseada em identidade que é anexada a um usuário, grupo ou perfil do AWS Identity and Access Management (IAM) em sua conta. Talvez uma política de bucket funcione melhor para o seu caso de uso. Para obter mais informações, consulte Políticas de bucket para o Amazon S3. Como alternativa, o AWS Identity and Access Management (IAM) permite a criação de usuários, grupos e perfis do IAM em sua Conta da AWS e o gerenciamento do acesso dessas entidades a buckets e objetos por meio de políticas baseadas em identidade. Para obter mais informações, consulte Políticas baseadas em identidade do Amazon S3.

Para ajudar você a navegar por essas opções de gerenciamento de acesso, veja a seguir alguns casos de uso comuns de clientes do Amazon S3 e recomendações para cada uma das ferramentas de gerenciamento de acesso do S3.

A Conta da AWS proprietária deseja compartilhar buckets somente com usuários da mesma conta

Todas as ferramentas de gerenciamento de acesso podem atender a esse caso de uso básico. Recomendamos as seguintes ferramentas de gerenciamento de acesso para esse caso de uso:

- Política de bucket: se você quiser conceder acesso a um bucket ou a um pequeno número de buckets, ou se suas permissões de acesso ao bucket forem semelhantes entre buckets, utilize uma política de bucket. Com as políticas de bucket, você gerencia uma política para cada bucket. Para obter mais informações, consulte Políticas de bucket para o Amazon S3.
- Política baseada em identidade: se você tiver um número muito grande de buckets com permissões de acesso diferentes para cada bucket e apenas alguns perfis de usuário para gerenciar, poderá usar uma política do IAM para usuários, grupos ou perfis. As políticas do IAM também são uma boa opção quando você precisa gerenciar o acesso dos usuários a outros

recursos da AWS, bem como aos recursos do Amazon S3. Para obter mais informações, consulte Exemplo 1: Proprietário do bucket que concede permissões do bucket aos usuários.

- Concessões de Acesso do S3: você pode usar a funcionalidade Concessões de Acesso do S3 para conceder acesso a buckets, prefixos ou objetos do S3. A funcionalidade Concessões de Acesso do S3 permite que você especifique várias permissões ao nível do objeto em grande escala, enquanto as políticas de bucket são limitadas a 20 KB. Para obter mais informações, consulte Conceitos básicos da funcionalidade Concessões de Acesso do S3.
- Pontos de acesso: você pode usar os pontos de acesso, que são endpoints de rede nomeados e anexados a um bucket. Um bucket pode ter até 10.000 pontos de acesso anexados, e é possível impor permissões distintas e controles de rede a cada ponto de acesso para fornecer controle detalhado sobre o acesso aos objetos do S3. Para obter mais informações, consulte Gerenciar o acesso a conjuntos de dados compartilhados com pontos de acesso.

A Conta da AWS proprietária quer compartilhar buckets ou objetos com usuários de outra conta da AWS (entre contas)

Para conceder permissão a outra Conta da AWS, é necessário usar uma política de bucket ou uma das ferramentas de gerenciamento de acesso recomendadas a seguir. Você não pode usar uma política de acesso baseada em identidade para esse caso de uso. Para obter mais informações sobre a concessão de acesso entre contas, consulte Como oferecer acesso entre contas a objetos que estão em buckets do Amazon S3?

Recomendamos as seguintes ferramentas de gerenciamento de acesso para esse caso de uso:

- Política de bucket: com as políticas de bucket, você gerencia uma política para cada bucket. Para obter mais informações, consulte Políticas de bucket para o Amazon S3.
- Concessões de Acesso do S3: você pode usar a funcionalidade Concessões de Acesso do S3 para conceder permissões entre contas aos buckets, prefixos ou objetos do S3. Você pode usar a funcionalidade Concessões de Acesso do S3 para especificar várias permissões ao nível do objeto em grande escala, enquanto as políticas de bucket são limitadas a 20 KB. Para obter mais informações, consulte Conceitos básicos da funcionalidade Concessões de Acesso do S3.
- Pontos de acesso: você pode usar os pontos de acesso, que são endpoints de rede nomeados e anexados a um bucket. Um bucket pode ter até 10.000 pontos de acesso anexados, e é possível impor permissões distintas e controles de rede a cada ponto de acesso para fornecer controle detalhado sobre o acesso aos objetos do S3. Para obter mais informações, consulte Gerenciar o acesso a conjuntos de dados compartilhados com pontos de acesso.

A Conta da AWS proprietária ou o proprietário do bucket deve conceder permissões ao nível do objeto ou do prefixo, e essas permissões variam de objeto para objeto ou de prefixo para prefixo

Em uma política de bucket, por exemplo, é possível conceder acesso aos objetos dentro de um bucket que compartilham um prefixo de nome de chave específico ou que têm uma etiqueta específica. Você pode conceder permissão de leitura em objetos que começam com o prefixo de nome de chave `logs/`. Contudo, se as permissões de acesso variam por objeto, conceder permissões para objetos individuais usando uma política de bucket talvez não seja prático, principalmente porque as políticas de bucket têm limite de 20 KB.

Recomendamos as seguintes ferramentas de gerenciamento de acesso para esse caso de uso:

- Concessões de Acesso do S3: você pode usar a funcionalidade Concessões de Acesso do S3 para gerenciar permissões ao nível do objeto ou do prefixo. Ao contrário das políticas de bucket, você pode usar a funcionalidade Concessões de Acesso do S3 para especificar várias permissões ao nível do objeto em grande escala. As políticas de bucket são limitadas a 20 KB. Para obter mais informações, consulte Conceitos básicos da funcionalidade Concessões de Acesso do S3.
- Pontos de acesso: você pode usar os pontos de acesso para gerenciar permissões ao nível do objeto ou do prefixo. Os pontos de acesso são endpoints de rede nomeados que são anexados a um bucket. Um bucket pode ter até 10.000 pontos de acesso anexados, e é possível impor permissões distintas e controles de rede a cada ponto de acesso para fornecer controle detalhado sobre o acesso aos objetos do S3. Para obter mais informações, consulte Gerenciar o acesso a conjuntos de dados compartilhados com pontos de acesso.
- ACLs: não recomendamos o uso de listas de controle de acesso (ACLs), principalmente porque as ACLs têm limite de 100 concessões por objeto. No entanto, se você optar por ativar as ACLs, defina a Propriedade de Objeto como Proprietário do bucket preferido e ative as ACLs nas configurações do bucket. Com essa configuração, novos objetos que são escritos com a ACL `bucket-owner-full-control` pré-configurada são automaticamente de propriedade do proprietário do bucket, e não do gravador de objeto. Depois, você pode usar as ACLs de objeto, que são uma política de acesso em formato XML, para conceder acesso ao objeto para outros usuários. Para obter mais informações, consulte Visão geral da lista de controle de acesso (ACL).

A Conta da AWS proprietária ou o proprietário do bucket quer limitar o acesso ao bucket somente para IDs de conta específicos

Recomendamos as seguintes ferramentas de gerenciamento de acesso para esse caso de uso:

- Política de bucket: com as políticas de bucket, você gerencia uma política para cada bucket. Para obter mais informações, consulte Políticas de bucket para o Amazon S3.
- Pontos de acesso: os pontos de acesso são endpoints de rede nomeados que são anexados a um bucket. Um bucket pode ter até 10.000 pontos de acesso anexados, e é possível impor permissões distintas e controles de rede a cada ponto de acesso para fornecer controle detalhado sobre o acesso aos objetos do S3. Para obter mais informações, consulte Gerenciar o acesso a conjuntos de dados compartilhados com pontos de acesso.

A Conta da AWS proprietária ou o proprietário do bucket quer endpoints distintos para cada usuário ou aplicação que acessa os dados

Recomendamos a seguinte ferramenta de gerenciamento de acesso para esse caso de uso:

- Pontos de acesso: os pontos de acesso são endpoints de rede nomeados que são anexados a um bucket. Um bucket pode ter até 10.000 pontos de acesso anexados, e é possível impor permissões distintas e controles de rede a cada ponto de acesso para fornecer controle detalhado sobre o acesso aos objetos do S3. Cada ponto de acesso impõe uma política de ponto de acesso personalizada que funciona em conjunto com a política de bucket anexada ao bucket subjacente. Para obter mais informações, consulte Gerenciar o acesso a conjuntos de dados compartilhados com pontos de acesso.

A Conta da AWS proprietária ou o proprietário do bucket precisa gerenciar o acesso realizado por meio de endpoints da nuvem privada virtual (VPC) para o S3

Os endpoints de nuvem privada virtual (VPC) para o Amazon S3 são entidades lógicas dentro de uma VPC que só permitem conectividade com o S3. Recomendamos as seguintes ferramentas de gerenciamento de acesso para esse caso de uso:

- Buckets em uma configuração de VPC: você pode usar uma política de bucket para controlar quem tem permissão para acessar os buckets e quais endpoints de VPC podem ser acessados. Para obter mais informações, consulte Controlar o acesso a partir de VPC endpoints com políticas de bucket.
- Pontos de acesso: se você optar por configurar pontos de acesso, poderá usar uma política de pontos de acesso. Você pode configurar qualquer ponto de acesso para aceitar solicitações somente de uma Virtual Private Cloud (VPC) para restringir o acesso a dados do Amazon S3 a uma rede privada. Você também pode configurar definições personalizadas do Bloqueio de acesso

público para cada ponto de acesso. Para obter mais informações, consulte Gerenciar o acesso a conjuntos de dados compartilhados com pontos de acesso.

A Conta da AWS proprietária ou o proprietário do bucket precisa disponibilizar publicamente um site estático

Com o S3, é possível hospedar um site estático e permitir que qualquer pessoa visualize o conteúdo do site, que é hospedado em um bucket do S3.

Recomendamos as seguintes ferramentas de gerenciamento de acesso para esse caso de uso:

- Amazon CloudFront: esta solução permite que você hospede um site estático do Amazon S3 para o público e, ao mesmo tempo, continue bloqueando todo o acesso público ao conteúdo de um bucket. Se quiser manter todas as quatro configurações da funcionalidade Bloqueio de Acesso Público do S3 habilitadas e hospedar um site estático do S3, use o controle de acesso à origem (OAC) do Amazon CloudFront. O Amazon CloudFront fornece os recursos necessários para configurar um site estático seguro. Além disso, os sites estáticos do Amazon S3 que não usam essa solução só são compatíveis com endpoints HTTP. O CloudFront usa o armazenamento durável do Amazon S3 ao mesmo tempo que fornece cabeçalhos de segurança adicionais, como HTTPS. O HTTPS adiciona segurança criptografando uma solicitação HTTP normal e protegendo-a contra ataques cibernéticos comuns.

  Para obter mais informações, consulte Conceitos básicos de um site estático seguro no Guia do desenvolvedor do Amazon CloudFront.
- Tornar o bucket do Amazon S3 acessível ao público: você pode configurar um bucket para ser usado como um site estático com acesso público.

  > **Warning**
  >
  > Não recomendamos esse método. Em vez disso, recomendamos que você use sites estáticos do Amazon S3 como parte do Amazon CloudFront. Para obter mais informações, confira a opção anterior ou consulte Conceitos básicos de um site estático seguro.

  Para criar um site estático do Amazon S3 sem o Amazon CloudFront, primeiro é necessário desativar todas as configurações da funcionalidade Bloqueio de Acesso Público. Ao escrever a política de bucket para o site estático, aceite apenas ações `s3:GetObject` e não permissões `ListObject` e `PutObject`. Isso ajuda a garantir que os usuários não possam visualizar todos

os objetos no bucket nem adicionar seu próprio conteúdo. Para obter mais informações, consulte Configuração de permissões para acesso ao site.

A Conta da AWS proprietária ou o proprietário do bucket quer disponibilizar publicamente o conteúdo de um bucket

Ao criar um bucket do Amazon S3, a configuração Bloquear acesso público é habilitada por padrão. Para obter mais informações sobre como bloquear o acesso público, consulte Bloquear o acesso público ao armazenamento do Amazon S3.

Não recomendamos que você permita acesso público ao seu bucket. No entanto, se você precisar fazer isso para um caso de uso específico, recomendamos a seguinte ferramenta de gerenciamento de acesso:

- Desabilitar a configuração Bloquear acesso público: o proprietário de um bucket pode permitir solicitações não autenticadas para o bucket. Por exemplo, solicitações PUT Object não autenticadas são permitidas quando um bucket tem uma política de bucket pública ou quando uma ACL de bucket concede acesso público. Todas as solicitações não autenticadas são feitas por outros usuários arbitrários da AWS ou até mesmo por usuários anônimos não autenticados. Esse usuário é representado em ACLs pelo ID de usuário canônico específico `65a011a29cdf8ec533ec3d1ccaae921c`. Se um objeto for carregado em `WRITE` ou `FULL_CONTROL`, isso concederá, especificamente, acesso ao grupo Todos os usuários ou ao usuário anônimo. Para obter mais informações sobre políticas de bucket público e listas de controle de acesso (ACLs) públicas, consulte O significado de "público".

A Conta da AWS proprietária ou o proprietário do bucket excedeu os limites de tamanho da política de acesso

Tanto as políticas de bucket quanto as políticas baseadas em identidade têm um limite de 20 KB. Se seus requisitos de permissão de acesso forem complexos, você poderá exceder esse limite de tamanho.

Recomendamos as seguintes ferramentas de gerenciamento de acesso para esse caso de uso:

- Pontos de acesso: use os pontos de acesso caso eles funcionem para o seu caso de uso. Com os pontos de acesso, cada bucket tem vários endpoints de rede nomeados, cada um com sua própria política de ponto de acesso que funciona com a política de bucket subjacente. No entanto, os pontos de acesso só podem atuar em objetos, não em buckets, e não oferecem suporte à

replicação entre regiões. Para obter mais informações, consulte Gerenciar o acesso a conjuntos de dados compartilhados com pontos de acesso.

- Concessões de Acesso do S3: use a funcionalidade Concessões de Acesso do S3, que oferece suporte a um número muito grande de concessões que dão acesso a buckets, prefixos ou objetos. Para obter mais informações, consulte Conceitos básicos da funcionalidade Concessões de Acesso do S3.

A Conta da AWS proprietária ou o perfil de administrador quer conceder acesso a buckets, prefixos ou objetos diretamente para usuários ou grupos em um diretório corporativo

Em vez de gerenciar usuários, grupos e perfis por meio do AWS Identity and Access Management (IAM), você pode adicionar seu diretório corporativo ao AWS IAM Identity Center. Para obter mais informações, consulte What is IAM Identity Center?

Depois de adicionar seu diretório corporativo ao AWS IAM Identity Center, recomendamos que você use a seguinte ferramenta de gerenciamento de acesso para conceder às identidades do diretório corporativo acesso aos seus recursos do S3:

- Concessões de Acesso do S3: use a funcionalidade Concessões de Acesso do S3, que oferece suporte à concessão de acesso a usuários ou perfis em seu diretório corporativo. Para obter mais informações, consulte Conceitos básicos da funcionalidade Concessões de Acesso do S3.

A Conta da AWS proprietária ou o proprietário do bucket quer conceder ao serviço AWS CloudFront acesso para gravar logs do CloudFront em um bucket do S3

Recomendamos a seguinte ferramenta de gerenciamento de acesso para esse caso de uso:

- ACL de bucket: o único caso de uso recomendado para as ACLs de bucket é a concessão de permissões a determinados Serviços da AWS, como a conta `awslogsdelivery` do Amazon CloudFront. Ao criar ou atualizar uma distribuição e ativar o registro em log do CloudFront, o CloudFront atualiza a ACL do bucket para conceder à conta `awslogsdelivery` permissões `FULL_CONTROL` para gravar logs em seu bucket. Para obter mais informações, consulte Permissões necessárias para configurar o registro padrão e acessar seus arquivos de log no Guia do desenvolvedor do Amazon CloudFront. Se o bucket que armazena os logs usar a configuração Imposto pelo proprietário do bucket para a funcionalidade Propriedade de Objeto do S3 a fim de

desativar as ACLs, o CloudFront não poderá gravar logs no bucket. Para obter mais informações, consulte Controlar a propriedade de objetos e desabilitar ACLs para seu bucket.

Como proprietário do bucket, você quer manter o controle total dos objetos que são adicionados ao bucket por outros usuários

Você pode conceder acesso a outras contas para que façam upload de objetos no bucket usando uma política de bucket, um ponto de acesso ou a funcionalidade Concessões de Acesso do S3. Se você concedeu acesso entre contas ao seu bucket, pode garantir que todos os objetos enviados para o bucket permaneçam totalmente sob seu controle.

Recomendamos a seguinte ferramenta de gerenciamento de acesso para esse caso de uso:

- Propriedade de objeto: mantenha a configuração ao nível do bucket Propriedade de objeto definida com a opção padrão Imposto pelo proprietário do bucket.

Solução de problemas de gerenciamento de acesso

Os recursos a seguir podem ajudar você a solucionar problemas no gerenciamento de acesso do S3:

Solucionar erros de acesso negado (403 proibido)

Se você encontrar problemas de negação de acesso, verifique as configurações ao nível de conta e de bucket. Além disso, verifique o recurso de gerenciamento de acesso que você está usando para conceder acesso a fim de garantir que a política, a definição ou a configuração estejam corretas. Para receber mais informações sobre as causas comuns de erros de acesso negado (403 proibido) no Amazon S3, consulte Solucionar erros de acesso negado (403 Forbidden) no Amazon S3.

IAM Access Analyzer para S3

Se você não quiser disponibilizar publicamente nenhum dos seus recursos ou se quiser limitar o acesso público aos seus recursos, poderá usar o IAM Access Analyzer para S3. No console do Amazon S3, use o IAM Access Analyzer para S3 a fim de revisar todos os buckets que têm listas de controle de acesso (ACLs) de bucket, políticas de bucket ou políticas de ponto de acesso que concedem acesso público ou compartilhado. O IAM Access Analyzer para S3 alerta você sobre buckets que são configurados para permitir o acesso a qualquer pessoa na internet ou a outras Contas da AWS, incluindo Contas da AWS fora da organização. Para cada bucket público ou compartilhado, você recebe descobertas que relatam a origem e o nível de acesso público ou compartilhado.

No IAM Access Analyzer para S3, é possível bloquear todo o acesso público a um bucket com uma única ação. Recomendamos que você bloqueie todo o acesso público aos buckets, a menos que exija acesso público para oferecer suporte a um caso de uso específico. Antes de bloquear todo o acesso público, garanta que as aplicações continuarão funcionando corretamente sem acesso público. Para obter mais informações, consulte Bloquear o acesso público ao armazenamento do Amazon S3.

Você também pode conferir suas configurações de permissão ao nível do bucket para definir níveis detalhados de acesso. Para casos de uso específicos e verificados que exigem acesso público ou compartilhado, você pode confirmar e registrar sua intenção de que o bucket permaneça público ou compartilhado arquivando as descobertas do bucket. Você pode acessar novamente e modificar essas configurações de bucket a qualquer momento. Você também pode fazer download das descobertas como um relatório CSV para fins de auditoria.

O IAM Access Analyzer para S3 está disponível sem custo adicional no console do Amazon S3. O IAM Access Analyzer para S3 usa tecnologia do AWS Identity and Access Management (IAM) Access Analyzer. Para usar o IAM Access Analyzer para S3 no console do Amazon S3, acesse o console do IAM e crie um analisador ao nível da conta no IAM Access Analyzer para cada região.

Para obter mais informações sobre o IAM Access Analyzer para S3, consulte Revisar o acesso de bucket usando o IAM Access Analyzer para S3.

Registro em log e monitoramento

O monitoramento é uma parte importante da manutenção da confiabilidade, disponibilidade e performance das soluções do Amazon S3 para que você possa depurar mais facilmente uma falha de acesso. O registro em log pode fornecer insights sobre quaisquer erros que os usuários estejam recebendo, bem como quando e quais solicitações são feitas. A AWS fornece várias ferramentas para monitoramento dos recursos do Amazon S3, como as seguintes:

- AWS CloudTrail
- Logs de acesso do Amazon S3
- AWS Trusted Advisor
- Amazon CloudWatch

Para obter mais informações, consulte Registrar em log e monitorar no Amazon S3.

Gerenciamento de identidade e acesso para o Amazon S3

O AWS Identity and Access Management (IAM) é um serviço da AWS service (Serviço da AWS) que ajuda um administrador a controlar com segurança o acesso aos recursos da AWS. Os administradores do IAM controlam quem pode ser autenticado (fazer login) e autorizado (ter permissões) para usar os recursos do Amazon S3. O IAM é um AWS service (Serviço da AWS) que pode ser usado sem custo adicional.

Para ter mais informações sobre as permissões referentes a operações de API do S3 de acordo com os tipos de recurso do S3, consulte Permissões obrigatórias para operações de API do Amazon S3.

> **Note**
>
> Para obter mais informações sobre o uso da classe de armazenamento Amazon S3 Express One Zone com buckets de diretório, consulte S3 Express One Zone e Trabalhar com buckets de diretório.

Tópicos

- Público
- Autenticação com identidades
- Gerenciar o acesso usando políticas
- Como o Amazon S3 funciona com o IAM
- Como o Amazon S3 autoriza uma solicitação
- Permissões obrigatórias para operações de API do Amazon S3
- Políticas e permissões no Amazon S3
- Políticas de bucket para o Amazon S3
- Políticas baseadas em identidade do Amazon S3
- Demonstrações que usam políticas para gerenciar o acesso a recursos do Amazon S3
- Usar funções vinculadas a serviços para o Amazon S3 Storage Lens
- Solução de problemas de identidade e acesso do Amazon S3
- Políticas gerenciadas da AWS para o Amazon S3

Público

A forma de usar o AWS Identity and Access Management (IAM) varia em função do trabalho realizado no Amazon S3.

Usuário do serviço: se você usar o serviço do Amazon S3 para fazer seu trabalho, o administrador fornecerá as credenciais e as permissões necessárias. À medida que usar mais recursos do Amazon S3 para fazer trabalhar, você poderá precisar de permissões adicionais. Compreenda como o acesso é gerenciado pode ajudar a solicitar as permissões corretas ao administrador. Se você não puder acessar um recurso no Amazon S3, consulte Solução de problemas de identidade e acesso do Amazon S3.

Administrador do serviço: se estiver a cargo dos recursos do Amazon S3 em sua empresa, você provavelmente terá acesso total ao Amazon S3. Cabe a você determinar quais funcionalidades e recursos do Amazon S3 os usuários do seu serviço devem acessar. Envie as solicitações ao administrador do IAM para alterar as permissões dos usuários de serviço. Revise as informações nesta página para compreender os conceitos básicos do IAM. Para saber mais sobre como a empresa pode usar o IAM com o Amazon S3, consulte Como o Amazon S3 funciona com o IAM.

Administrador do IAM: se você for um administrador do IAM, talvez deseje saber detalhes sobre como pode escrever políticas para gerenciar o acesso ao Amazon S3. Consulte exemplos de políticas baseadas em identidade do Amazon S3 que podem ser usadas no IAM em Políticas baseadas em identidade do Amazon S3.

Autenticação com identidades

A autenticação é a forma como fazer login na AWS usando suas credenciais de identidade. É necessário ser autenticado (fazer login na AWS) como Usuário raiz da conta da AWS, como usuário do IAM, ou assumindo um perfil do IAM.

É possível fazer login na AWS como uma identidade federada usando credenciais fornecidas por uma fonte de identidades. AWS IAM Identity Center (Centro de Identidade do IAM), a autenticação única da empresa e as suas credenciais do Google ou do Facebook são exemplos de identidades federadas. Quando você faz login como identidade federada, o administrador já configurou anteriormente a federação de identidades usando perfis do IAM. Quando você acessa a AWS usando a federação, está indiretamente assumindo um perfil.

A depender do tipo de usuário, você pode fazer login no AWS Management Console ou no portal de acesso AWS. Para obter mais informações sobre como fazer login na AWS, consulte Como fazer login na contaConta da AWS no Início de Sessão da AWS Guia do usuário.

Se você acessar a AWS de forma programática, a AWS fornecerá um kit de desenvolvimento de software (SDK) e uma interface de linha de comandos (CLI) para você assinar de forma criptográfica as solicitações usando as suas credenciais. Se você não utilizar as ferramentas da AWS, deverá assinar as solicitações por conta própria. Para obter mais informações sobre como usar o método recomendado para designar solicitações por conta própria, consulte Versão 4 do AWS Signature para solicitações de API no Guia do usuário do IAM.

Independente do método de autenticação usado, também pode ser necessário fornecer informações adicionais de segurança. Por exemplo, a AWS recomenda o uso da autenticação multifator (MFA) para aumentar a segurança de sua conta. Para saber mais, consulte Autenticação multifator no Guia do usuário do AWS IAM Identity Center e Usar a autenticação multifator da AWS no IAM no Guia do usuário do IAM.

Usuário-raiz Conta da AWS

Ao criar uma Conta da AWS, você começa com uma identidade de login com acesso completo a todos os Serviços da AWS e recursos na conta. Essa identidade, chamada usuário-raiz da Conta da AWS, é acessada por login com o endereço de e-mail e a senha usada para criar a conta. É altamente recomendável não usar o usuário-raiz para tarefas diárias. Proteja as credenciais do usuário-raiz e use-as para executar as tarefas que somente ele puder executar. Para obter a lista completa das tarefas que exigem login como usuário-raiz, consulte Tarefas que exigem credenciais de usuário-raiz no Guia do Usuário do IAM.

Identidade federada

Como prática recomendada, exija que os usuários, inclusive os que precisam de acesso de administrador, usem a federação com um provedor de identidades para acessar os Serviços da AWS usando credenciais temporárias.

Uma identidade federada é um usuário de seu diretório de usuários corporativos, um provedor de identidades da web, o AWS Directory Service, o diretório do Centro de Identidade ou qualquer usuário que acesse os Serviços da AWS usando credenciais fornecidas por meio de uma fonte de identidade. Quando as identidades federadas acessam Contas da AWS, elas assumem perfis que fornecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, é recomendável usar o AWS IAM Identity Center. É possível criar usuários e grupos no IAM Identity Center ou conectar-se e sincronizar com um conjunto de usuários e grupos em sua própria fonte de identidade para uso em todas as suas Contas

da AWS e aplicações. Para obter mais informações sobre o Centro de Identidade do IAM, consulte O que é o Centro de Identidade do IAM? no Guia do Usuário do AWS IAM Identity Center.

Usuários e grupos do IAM

Um usuário do IAM é uma identidade dentro da Conta da AWS que tem permissões específicas para uma única pessoa ou aplicação. Sempre que possível, é recomendável contar com credenciais temporárias em vez de criar usuários do IAM com credenciais de longo prazo, como senhas e chaves de acesso. No entanto, se você tiver casos de uso específicos que exijam credenciais de longo prazo com usuários do IAM, é recomendável alternar as chaves de acesso. Para obter mais informações, consulte Alternar as chaves de acesso regularmente para casos de uso que exijam credenciais de longo prazo no Guia do Usuário do IAM.

Um grupo do IAM é uma identidade que especifica uma coleção de usuários do IAM. Não é possível fazer login como um grupo. É possível usar grupos para especificar permissões para vários usuários de uma vez. Os grupos facilitam o gerenciamento de permissões para grandes conjuntos de usuários. Por exemplo, você pode ter um grupo chamado IAMAdmins e conceder a esse grupo permissões para administrar recursos do IAM.

Usuários são diferentes de perfis. Um usuário é exclusivamente associado a uma pessoa ou a uma aplicação, mas um perfil pode ser assumido por qualquer pessoa que precisar dele. Os usuários têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte Casos de uso para usuários do IAM no Guia do usuário do IAM.

Perfis do IAM

Um perfil do IAM é uma identidade na Conta da AWS que tem permissões específicas. Ele é semelhante a um usuário do IAM, mas não está associado a uma pessoa específica. Para assumir temporariamente um perfil do IAM no AWS Management Console, você pode alternar de um usuário para um perfil do IAM (console). É possível presumir um perfil chamando uma operação de API da AWS CLI ou da AWS, ou usando um URL personalizado. Para obter mais informações sobre métodos para usar perfis, consulte Métodos para assumir um perfil no Guia do usuário do IAM.

Perfis do IAM com credenciais temporárias são úteis nas seguintes situações:

- Acesso de usuário federado: para atribuir permissões a identidades federadas, é possível criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas por ele. Para ter mais informações sobre perfis para federação, consulte Criar um perfil para um provedor de identidade de terceiros (federação) no Guia do usuário do IAM. Se usar o Centro de Identidade do IAM,

configure um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o Centro de Identidade do IAM correlaciona o conjunto de permissões a um perfil no IAM. Para obter informações sobre conjuntos de permissões, consulte Conjuntos de Permissões no Guia do Usuário do AWS IAM Identity Center.

- Permissões temporárias para usuários do IAM: um usuário ou um perfil do IAM pode presumir um perfil do IAM para obter temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas: é possível usar um perfil do IAM para permitir que alguém (uma entidade principal confiável) em outra conta acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto, alguns Serviços da AWS permitem anexar uma política diretamente a um recurso (em vez de usar um perfil como proxy). Para conhecer a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.
- Acesso entre serviços: alguns Serviços da AWS usam recursos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicações no Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões da entidade principal da chamada, usando um perfil de serviço ou um perfil vinculado ao serviço.
  - Sessões de acesso direto (FAS): qualquer pessoa que utilizar um perfil ou usuário do IAM para executar ações na AWS é considerada uma entidade principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O recurso FAS usa as permissões da entidade principal chamando um AWS service (Serviço da AWS), bem como o AWS service (Serviço da AWS) solicitante, para fazer solicitações para serviços subsequentes. As solicitações de FAS são feitas somente quando um serviço recebe uma solicitação que exige interações com outros Serviços da AWS ou com recursos para serem concluídas. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Sessões de acesso direto.
  - Perfil de serviço: um perfil de serviço é um perfil do IAM que um serviço assume para executar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.
  - Perfil vinculado a serviço: um perfil vinculado a serviço é um tipo de perfil de serviço vinculado a um AWS service (Serviço da AWS). O serviço pode presumir o perfil para executar uma ação em seu nome. Perfis vinculadas ao serviço aparecem em sua Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para perfis vinculados a serviço.

- Aplicações em execução no Amazon EC2: é possível usar um perfil do IAM para gerenciar credenciais temporárias para aplicações em execução em uma instância do EC2 e fazer solicitações da AWS CLI ou da API da AWS. É preferível fazer isso a armazenar chaves de acesso na instância do EC2. Para atribuir um perfil da AWS a uma instância do EC2 e disponibilizá-la para todas as suas aplicações, crie um perfil de instância que esteja anexado a ela. Um perfil de instância contém o perfil e permite que os programas em execução na instância do EC2 obtenham credenciais temporárias. Para mais informações, consulte Utilizar um perfil do IAM para conceder permissões a aplicações em execução nas instâncias do Amazon EC2 no Guia do usuário do IAM.

Gerenciar o acesso usando políticas

Você controla o acesso na AWS criando políticas e anexando-as a identidades ou recursos da AWS. Uma política é um objeto na AWS que, quando associado a uma identidade ou recurso, define suas permissões. A AWS avalia essas políticas quando uma entidade principal (usuário, usuário-raiz ou sessão de perfil) faz uma solicitação. As permissões nas políticas determinam se a solicitação será permitida ou negada. A maioria das políticas é armazenada na AWS como documentos JSON. Para obter mais informações sobre a estrutura e o conteúdo de documentos de políticas JSON, consulte Visão geral das políticas JSON no Guia do usuário do IAM.

Os administradores podem usar as políticas JSON da AWS para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

Por padrão, usuários e perfis não têm permissões. Para conceder permissão aos usuários para executar ações nos recursos que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM aos perfis e os usuários podem assumir os perfis.

As políticas do IAM definem permissões para uma ação independentemente do método usado para executar a operação. Por exemplo, suponha que você tenha uma política que permite a ação `iam:GetRole`. Um usuário com essa política pode obter informações de perfis do AWS Management Console, da AWS CLI ou da API AWS.

Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário, grupo de usuários ou perfil do IAM. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que

condições. Para saber como criar uma política baseada em identidade, consulte Definir permissões personalizadas do IAM com as políticas gerenciadas pelo cliente no Guia do Usuário do IAM.

As políticas baseadas em identidade podem ser categorizadas como políticas em linha ou políticas gerenciadas. As políticas em linha são anexadas diretamente a um único usuário, grupo ou perfil. As políticas gerenciadas são políticas independentes que podem ser anexadas a vários usuários, grupos e perfis na Conta da AWS. As políticas gerenciadas incluem políticas gerenciadas pela AWS e políticas gerenciadas pelo cliente. Para saber como escolher entre uma política gerenciada ou uma política em linha, consulte Escolher entre políticas gerenciadas e políticas em linha no Guia do usuário do IAM.

Políticas baseadas em recursos

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o atributo ao qual a política está anexada, a política define quais ações uma entidade principal especificado pode executar nesse atributo e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. As entidades principais podem incluir contas, usuários, funções, usuários federados ou Serviços da AWS.

Políticas baseadas em recursos são políticas em linha localizadas nesse serviço. Não é possível usar as políticas gerenciadas pela AWS do IAM em uma política baseada em atributos.

Listas de controle de acesso (ACLs)

As listas de controle de acesso (ACLs) controlam quais entidades principais (membros, usuários ou perfis da conta) têm permissões para acessar um recurso. As ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

O Amazon S3, o AWS WAF e a VPC são exemplos de serviços compatíveis com ACLs. Para saber mais sobre ACLs, consulte Visão geral da lista de controle de acesso (ACL) no Guia do Desenvolvedor do Amazon Simple Storage Service.

Outros tipos de política

A AWS oferece compatibilidade com tipos de política menos comuns. Esses tipos de política podem definir o máximo de permissões concedidas a você pelos tipos de política mais comuns.

- Limites de permissões: um limite de permissões é um recurso avançado no qual você define o máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM (usuário ou perfil do IAM). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade de uma entidade com seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou o perfil no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte Limites de permissões para identidades do IAM no Guia do usuário do IAM.
- Políticas de controle de serviço (SCPs): SCPs são políticas JSON que especificam as permissões máximas para uma organização ou unidade organizacional (UO) no AWS Organizations. O AWS Organizations é um serviço que agrupa e gerencia centralmente várias Contas da AWS pertencentes a sua empresa. Se você habilitar todos os recursos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as contas. A SCP limita as permissões para entidades em contas de membros, o que inclui cada Usuário raiz da conta da AWS. Para obter mais informações sobre o Organizations e SCPs, consulte Service control policies no Guia do usuário do AWS Organizations.
- Políticas de controle de recursos (RCPs): RCPs são políticas JSON que podem ser usadas para definir o máximo de permissões disponíveis para recursos em suas contas sem atualizar as políticas do IAM anexadas a cada recurso que você possui. A RCP limita as permissões para recursos nas contas-membro e pode afetar as permissões efetivas para identidades, incluindo o Usuário raiz da conta da AWS, independentemente de pertencerem a sua organização. Consulte mais informações sobre o Organizations e as RCPs, incluindo uma lista de Serviços da AWS compatível com RCPs em Resource control policies (RCPs) no Guia do usuário do AWS Organizations.
- Políticas de sessão: são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para um perfil ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou do perfil e das políticas de sessão. As permissões também podem ser provenientes de uma política baseada em recursos. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, consulte Políticas de sessão no Guia do usuário do IAM.

Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Para saber como a AWS determina se deve permitir ou não uma solicitação quando há vários tipos de política envolvidos, consulte Lógica da avaliação de políticas no Guia do usuário do IAM.

Como o Amazon S3 funciona com o IAM

Antes de usar o IAM para gerenciar o acesso ao Amazon S3, saiba quais recursos do IAM estão disponíveis para uso com o Amazon S3.

Recursos do IAM que você pode usar com o Amazon S3

Atributo do IAM	Suporte ao Amazon S3
Políticas baseadas em identidade	Sim
Políticas baseadas em atributos	Sim
Ações de políticas	Sim
Recursos de políticas	Sim
Chaves de condição de política (específicas do serviço)	Sim
ACLs	Sim
ABAC (tags em políticas)	Parcial
Credenciais temporárias	Sim
Sessões de acesso direto (FAS)	Sim
Perfis de serviço	Sim
Perfis vinculados a serviço	Parcial

Consulte uma visão geral de como o Amazon S3 e outros serviços da AWS funcionam com a maioria dos recursos do IAM em Serviços da AWS que funcionam com o IAM no Guia do usuário do IAM.

Para ter mais informações sobre as permissões referentes a operações de API do S3 de acordo com os tipos de recurso do S3, consulte Permissões obrigatórias para operações de API do Amazon S3.

Políticas baseadas em identidade do Amazon S3

Compatível com políticas baseadas em identidade: sim

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário do IAM, grupo de usuários ou perfil. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Definir permissões personalizadas do IAM com as políticas gerenciadas pelo cliente no Guia do Usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações e recursos permitidos ou negados, assim como as condições sob as quais as ações são permitidas ou negadas. Você não pode especificar a entidade principal em uma política baseada em identidade porque ela se aplica ao usuário ou perfil ao qual ela está anexada. Para saber mais sobre todos os elementos que podem ser usados em uma política JSON, consulte Referência de elemento de política JSON do IAM no Guia do usuário do IAM.

Exemplos de políticas baseadas em identidade para o Amazon S3

Consulte exemplos de políticas baseadas em identidade do Amazon S3 em Políticas baseadas em identidade do Amazon S3.

Políticas baseadas em recurso no Amazon S3

Compatível com políticas baseadas em recursos: sim

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o atributo ao qual a política está anexada, a política define quais ações uma entidade principal especificado pode executar nesse atributo e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. As entidades principais podem incluir contas, usuários, perfis, usuários federados ou Serviços da AWS.

Para permitir o acesso entre contas, você pode especificar uma conta inteira ou as entidades do IAM em outra conta como a entidade principal em uma política baseada em recursos. Adicionar uma entidade principal entre contas à política baseada em recurso é apenas metade da tarefa de estabelecimento da relação de confiança. Quando a entidade principal e o recurso estão em diferentes Contas da AWS, um administrador do IAM da conta confiável também deve conceder à entidade principal (usuário ou perfil) permissão para acessar o recurso. Eles concedem permissão ao anexar uma política baseada em identidade para a entidade. No entanto, se uma política baseada em recurso conceder acesso a uma entidade principal na mesma conta, nenhuma política baseada em identidade adicional será necessária. Consulte mais informações em Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

O serviço do Amazon S3 é compatível com políticas de bucket, políticas de pontos de acesso e concessões de acesso:

- Políticas de bucket são políticas baseadas em recursos que são anexadas a um bucket do Amazon S3. Uma política de bucket define quais entidades principais podem realizar ações no bucket.
- As políticas de ponto de acesso são políticas baseadas em recursos que são avaliadas em conjunto com a política de bucket correspondente.
- As concessões de acesso são um modelo simplificado para definir permissões de acesso aos dados no Amazon S3 por prefixo, bucket ou objeto. Consulte informações sobre a funcionalidade Concessões de Acesso do S3 em Gerenciar o acesso com a funcionalidade Concessões de Acesso do S3.

Entidades principais para políticas de bucket

O elemento `Principal` especifica o usuário, a conta, o serviço ou outra entidade que tem o acesso permitido ou negado a um recurso. Veja a seguir exemplos de especificação de `Principal`. Para obter mais informações, consulte Principal no Guia do usuário do IAM.

Conceder permissões a uma Conta da AWS

Para conceder permissões a uma Conta da AWS, identifique a conta usando o formato a seguir.

```
"AWS":"account-ARN"
```

Veja os exemplos a seguir.

```
"Principal":{"AWS":"arn:aws:iam::AccountIDWithoutHyphens:root"}
```

```
"Principal":{"AWS":
["arn:aws:iam::AccountID1WithoutHyphens:root","arn:aws:iam::AccountID2WithoutHyphens:root"]}
```

> **Note**
>
> Os exemplos acima concedem permissões ao usuário-raiz, que delega permissões em nível da conta. No entanto, as políticas do IAM ainda são necessárias para os perfis e usuários específicos da conta.

Conceder permissões a um usuário do IAM

Para conceder permissão para um usuário do IAM na sua conta, você deve fornecer um par de nome-valor `"AWS":"user-ARN"`.

```
"Principal":{"AWS":"arn:aws:iam::account-number-without-hyphens:user/username"}
```

Para obter exemplos detalhados que fornecem instruções passo a passo, consulte Exemplo 1: Proprietário do bucket que concede permissões do bucket aos usuários e Exemplo 3: O proprietário do bucket concede permissões para objetos que não possui.

> **Note**
>
> Se uma identidade do IAM for excluída depois que você atualizar a política de bucket, a política de bucket mostrará um identificador exclusivo no elemento da entidade principal em vez de um ARN. Esses IDs exclusivos nunca são reutilizados; portanto você pode remover com segurança entidades principais com identificadores exclusivos de todas as suas instruções de política. Para obter mais informações sobre identificadores exclusivos, consulte Identificadores do IAM no Guia do usuário do IAM.

Conceder permissões anônimas

> **Warning**
>
> Tenha cuidado ao conceder acesso anônimo ao bucket do Amazon S3. Quando você concede acesso anônimo, qualquer pessoa no mundo pode acessar seu bucket. É altamente recomendável que você nunca conceda nenhum tipo de acesso anônimo de gravação ao seu bucket do S3.

Para conceder permissão a todos, também denominada acesso anônimo, defina o curinga (`"*"`) como o valor `Principal`. Por exemplo, se você configura seu bucket como um site, quer que todos os objetos no bucket sejam publicamente acessíveis.

```
"Principal":"*"
```

```
"Principal":{"AWS":"*"}
```

Usar `"Principal": "*"` com um efeito `Allow` em uma política baseada em recursos permite que qualquer pessoa, mesmo que não esteja conectada à AWS, acesse seu recurso.

Usar `"Principal" : { "AWS" : "*" }` com um efeito `Allow` em uma política baseada em recursos permite que qualquer usuário raiz, usuário do IAM, sessão de função assumida ou usuário federado em qualquer conta na mesma partição acesse seu recurso.

Para usuários anônimos, esses dois métodos são equivalentes. Para obter mais informações, consulte Todas as entidades principais no Guia do usuário do IAM.

Não é possível usar um curinga para fazer a correspondência de parte de um nome de entidade principal ou ARN.

> **Important**
>
> Nas políticas de controle de acesso da AWS, as entidades principais “*” e {"AWS": "*"} se comportam de maneira idêntica.

Restringir permissões de recursos

Também é possível usar a política de recursos para restringir o acesso a recursos que, de outra forma, estariam disponíveis para entidades principais do IAM. Use uma instrução `Deny` para impedir o acesso.

O exemplo a seguir bloqueará o acesso se um protocolo de transporte seguro não for usado:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyBucketAccessIfSTPNotUsed",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
      "Condition": {
        "Bool": {
          "aws:SecureTransport": "false"
        }
      }
    }
  ]
}
```

Usar `"Principal": "*"` para que essa restrição se aplique a todos é uma prática recomendada para essa política, em vez de tentar negar acesso somente a contas ou entidades principais específicas usando esse método.

Exigir acesso por URLs do CloudFront

Você pode exigir que os usuários acessem seu conteúdo do Amazon S3 somente usando URLs do CloudFront em vez de URLs do Amazon S3. Para fazer isso, crie um controle de acesso de origem (OAC) do CloudFront. Depois, altere as permissões em seus dados do S3. Na política de bucket, é possível definir o CloudFront como entidade principal da seguinte forma:

```
"Principal":{"Service":"cloudfront.amazonaws.com"}
```

Use um elemento `Condition` na política para permitir que o CloudFront acesse o bucket somente quando a solicitação for em nome da distribuição do CloudFront que contém a origem do S3.

```
        "Condition": {
           "StringEquals": {
              "AWS:SourceArn":
"arn:aws:cloudfront::111122223333:distribution/CloudFront-distribution-ID"
           }
        }
```

Consulte mais informações sobre como solicitar acesso ao S3 por meio de URLs do CloudFront em Restringir o acesso ao conteúdo de uma origem do Amazon Simple Storage Service no Guia do desenvolvedor do Amazon CloudFront. Consulte mais informações sobre os benefícios de segurança e privacidade com o uso do Amazon CloudFront em Configurar o acesso seguro e restringir o acesso ao conteúdo.

Exemplos de política baseada em recursos para o Amazon S3

- Consulte exemplos de política para buckets do Amazon S3 em Políticas de bucket para o Amazon S3.
- Consulte exemplos de política para pontos de acesso em Configurar políticas do IAM para uso de pontos de acesso.

Ações de políticas para o Amazon S3

Compatível com ações de políticas: sim

Os administradores podem usar as políticas JSON da AWS para especificar quem tem acesso a quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento `Action` de uma política JSON descreve as ações que podem ser usadas para permitir ou negar acesso em uma política. As ações de políticas geralmente têm o mesmo nome que a operação de API da AWS associada. Existem algumas exceções, como ações somente de permissão, que não têm uma operação de API correspondente. Algumas operações também exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

Incluem ações em uma política para conceder permissões para executar a operação associada.

Veja a seguir diferentes tipos de relacionamento de mapeamento entre as operações de API do S3 e as ações de políticas necessárias.

- Mapeamento de um para um com o mesmo nome. Por exemplo, para usar a operação de API `PutBucketPolicy`, a ação de política `s3:PutBucketPolicy` é necessária.
- Mapeamento de um para um com nomes diferentes. Por exemplo, para usar a operação de API `ListObjectsV2`, a ação de política `s3:ListBucket` é necessária.
- Mapeamento de um para muitos. Por exemplo, para usar a operação de API `HeadObject`, a `s3:GetObject` é necessária. Além disso, quando você usa o Bloqueio de Objetos do S3 e deseja obter o status de retenção legal ou as configurações de retenção de um objeto, as ações de política `s3:GetObjectLegalHold` ou `s3:GetObjectRetention` correspondentes também são necessárias para que você possa usar a operação de API `HeadObject`.
- Mapeamento de muitos para um. Por exemplo, para usar as operações de API `ListObjectsV2` ou `HeadBucket`, a ação de política `s3:ListBucket` é necessária.

Consulte uma lista de ações do Amazon S3 para uso em políticas em Actions defined by Amazon S3 na Referência de autorização do serviço. Consulte uma lista completa de operações de API do Amazon S3 em Amazon S3 API Actions na Referência de API do Amazon Simple Storage Service.

Para ter mais informações sobre as permissões referentes a operações de API do S3 de acordo com os tipos de recurso do S3, consulte Permissões obrigatórias para operações de API do Amazon S3.

As ações da política no Amazon S3 usam o seguinte prefixo antes da ação:

```
s3
```

Para especificar várias ações em uma única declaração, separe-as com vírgulas.

```
"Action": [
      "s3:action1",
      "s3:action2"
         ]
```

Operações de buckets

As operações de bucket são operações de API do S3 que operam no tipo de recurso de bucket. Por exemplo, `CreateBucket`, `ListObjectsV2` e `PutBucketPolicy`. As ações de política do S3 para operações de bucket exigem que o elemento `Resource` nas políticas de bucket ou nas políticas

baseadas em identidade do IAM seja o identificador do nome do recurso da Amazon (ARN) do tipo de bucket do S3 no formato de exemplo a seguir.

```
"Resource": "arn:aws:s3:::amzn-s3-demo-bucket"
```

A política de bucket a seguir concede ao usuário *Akua* (conta *12345678901*) a permissão `s3:ListBucket` para realizar a operação de API ListObjectsV2 e listar objetos em um bucket do S3.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow Akua to list objects in the bucket",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::12345678901:user/Akua"
            },
            "Action": [
            "s3:ListBucket"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket"
        }
    ]
}
```

Operações de bucket em políticas de ponto de acesso para buckets de uso geral

As permissões concedidas em uma política de ponto de acesso para buckets de uso geral entrarão em vigor somente se o bucket subjacente conceder as mesmas permissões. Ao usar os pontos de acesso do S3, você deve delegar o controle de acesso do bucket ao ponto de acesso ou adicionar as mesmas permissões nas políticas de ponto de acesso à política do bucket subjacente. Para obter mais informações, consulte Configurar políticas do IAM para uso de pontos de acesso. Nas políticas de ponto de acesso, as ações de política do S3 para operações de bucket exigem que você use o ARN do ponto de acesso para o elemento `Resource` no formato a seguir.

```
"Resource": "arn:aws:s3:us-west-2:123456789012:accesspoint/example-access-point"
```

A política de ponto de acesso a seguir concede ao usuário *Akua* (conta *12345678901*) a permissão `s3:ListBucket` para realizar a operação de API ListObjectsV2 por meio do Ponto de Acesso S3

chamado *example-access-point*. Essa permissão autoriza *Akua* a indicar os objetos no bucket associado a *example-access-point*.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow Akua to list objects in the bucket through access point",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::12345678901:user/Akua"
            },
            "Action": [
            "s3:ListBucket"
            ],
            "Resource": "arn:aws:s3:us-west-2:123456789012:accesspoint/example-access-
point"
        }
    ]
}
```

> **Note**
>
> Nem todas as operações de bucket são compatíveis com pontos de acesso para buckets de uso geral. Para obter mais informações, consulte Compatibilidade de pontos de acesso com operações do S3.

Operações de bucket em políticas de ponto de acesso para buckets de diretório

As permissões concedidas em uma política de ponto de acesso para buckets de diretório entrarão em vigor somente se o bucket subjacente conceder as mesmas permissões. Ao usar os pontos de acesso do S3, você deve delegar o controle de acesso do bucket ao ponto de acesso ou adicionar as mesmas permissões nas políticas de ponto de acesso à política do bucket subjacente. Para obter mais informações, consulte Configurar políticas do IAM para usar pontos de acesso para buckets de diretório. Nas políticas de ponto de acesso, as ações de política do S3 para operações de bucket exigem que você use o ARN do ponto de acesso para o elemento `Resource` no formato a seguir.

```
"Resource": "arn:aws:s3:us-west-2:123456789012:accesspoint/example-access-point--usw2-
az1--xa-s3"
```

A política de ponto de acesso a seguir concede ao usuário *Akua* (conta *12345678901*) a permissão `s3:ListBucket` para realizar a operação de API ListObjectsV2 por meio do ponto de acesso chamado *example-access-point--usw2-az1--xa-s3*. Essa permissão autoriza *Akua* a indicar os objetos no bucket associado a *example-access-point--usw2-az1--xa-s3*.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow Akua to list objects in the bucket through access point",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::12345678901:user/Akua"
            },
            "Action": [
            "s3:ListBucket"
            ],
            "Resource": "arn:aws:s3express:us-west-2:123456789012:accesspoint/example-access-point--usw2-az1--xa-s3"
        }
    ]
}
```

> **Note**
>
> Nem todas as operações de bucket são compatíveis com pontos de acesso para buckets de diretório. Para obter mais informações, consulte Operações de objeto referentes a pontos de acesso para buckets de diretório.

Operações com objetos

As operações de objeto são operações de API do S3 que atuam sobre o tipo de recurso do objeto. Por exemplo, `GetObject`, `PutObject` e `DeleteObject`. As ações de política do S3 para operações de objeto exigem que o elemento `Resource` nas políticas seja o ARN do objeto do S3 nos formatos de exemplo a seguir.

```
"Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
```

```
"Resource": "arn:aws:s3:::amzn-s3-demo-bucket/prefix/*"
```

> **Note**
>
> O ARN do objeto deve conter uma barra após o nome do bucket, conforme mostrado nos exemplos anteriores.

A política de bucket a seguir concede ao usuário *Akua* (conta *12345678901*) a permissão `s3:PutObject`. Essa permissão autoriza *Akua* a usar a operação de API PutObject para fazer upload de objetos no bucket do S3 chamado *amzn-s3-demo-bucket*.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow Akua to upload objects",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::12345678901:user/Akua"
            },
            "Action": [
            "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
        }
    ]
}
```

Operações de objetos em políticas de ponto de acesso

Ao usar os pontos de acesso do S3 para controlar o acesso às operações de objetos, você pode usar políticas de ponto de acesso. Ao usar políticas de ponto de acesso, as ações de política do S3 para operações de objeto exigem que você use o ARN do ponto de acesso para o elemento `Resource` no seguinte formato: `arn:aws:s3:region:account-id:accesspoint/access-point-name/object/resource`. Para operações de objeto que usem pontos de acesso, é necessário incluir o valor `/object/` após o ARN completo do ponto de acesso no elemento `Resource`. Aqui estão alguns exemplos.

```
"Resource": "arn:aws:s3:us-west-2:123456789012:accesspoint/example-access-point/object/
*"
```

```
"Resource": "arn:aws:s3:us-west-2:123456789012:accesspoint/example-access-point/
object/prefix/*"
```

A política de ponto de acesso a seguir concede ao usuário *Akua* (conta *12345678901*) a permissão `s3:GetObject`. Essa permissão autoriza *Akua* a realizar a operação de API GetObject por meio do ponto de acesso denominado *example-access-point* em todos os objetos no bucket associado ao ponto de acesso.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow Akua to get objects through access point",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::12345678901:user/Akua"
            },
            "Action": [
            "s3:GetObject"
            ],
            "Resource": "arn:aws:s3:us-west-2:123456789012:accesspoint/example-access-
point/object/*"
        }
    ]
}
```

> **Note**
>
> Nem todas as operações de objeto são compatíveis com pontos de acesso. Para obter mais informações, consulte Compatibilidade de pontos de acesso com operações do S3.

Operações de objeto em políticas de ponto de acesso para buckets de diretório

Ao usar pontos de acesso para buckets de diretório com o objetivo de controlar o acesso a operações de objeto, é possível usar políticas de ponto de acesso. Ao usar políticas de ponto de acesso, as ações de política do S3 para operações de objeto exigem que você use o ARN do ponto de acesso para o elemento `Resource` no seguinte formato: `arn:aws:s3:region:account-id:accesspoint/access-point-name/object/resource`. Para operações de objeto que

usem pontos de acesso, é necessário incluir o valor `/object/` após o ARN completo do ponto de acesso no elemento `Resource`. Aqui estão alguns exemplos.

```
"Resource": "arn:aws:s3express:us-west-2:123456789012:accesspoint/example-access-point--usw2-az1--xa-s3/object/*"
```

```
"Resource": "arn:aws:s3express:us-west-2:123456789012:accesspoint/example-access-point--usw2-az1--xa-s3/object/prefix/*"
```

A política de ponto de acesso a seguir concede ao usuário *Akua* (conta *12345678901*) a permissão `s3:GetObject`. Essa permissão autoriza *Akua* a realizar a operação de API GetObject por meio do ponto de acesso denominado *example-access-point--usw2-az1--xa-s3* em todos os objetos no bucket associado ao ponto de acesso.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow Akua to get objects through access point",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::12345678901:user/Akua"
            },
            "Action": "s3express:CreateSession","s3:GetObject"
            "Resource": "arn:aws:s3:us-west-2:123456789012:accesspoint/example-access-point--usw2-az1--xa-s3/object/*"
        }
    ]
}
```

> **Note**
>
> Nem todas as operações de objeto são compatíveis com pontos de acesso para buckets de diretório. Para obter mais informações, consulte Operações de objeto referentes a pontos de acesso para buckets de diretório.

Operações de ponto de acesso para buckets de uso geral

As operações de ponto de acesso são operações de API do S3 que operam no tipo de recurso de `accesspoint`. Por exemplo, `CreateAccessPoint`, `DeleteAccessPoint` e `GetAccessPointPolicy`. As ações de política do S3 para operações de ponto de acesso só podem ser usadas em políticas baseadas em identidade do IAM, não em políticas de bucket ou políticas de ponto de acesso. As operações de ponto de acesso exigem que o elemento `Resource` seja o ARN do ponto de acesso no formato de exemplo a seguir.

```
"Resource": "arn:aws:s3:us-west-2:123456789012:accesspoint/example-access-point"
```

A política baseada em identidade do IAM a seguir concede a permissão `s3:GetAccessPointPolicy` para realizar a operação de API GetAccessPointPolicy no Ponto de Acesso S3 denominado *`example-access-point`*.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Grant permission to retrieve the access point policy of access
 point example-access-point",
            "Effect": "Allow",
            "Action": [
            "s3:GetAccessPointPolicy"
            ],
            "Resource": "arn:aws:s3:*:123456789012:accesspoint/example-access-point"
        }
    ]
}
```

Se você usa pontos de acesso, consulte Operações de bucket em políticas de ponto de acesso para buckets de uso geral para controlar o acesso às operações de bucket e Operações de objetos em políticas de ponto de acesso para controlar o acesso às operações de objetos. Consulte mais informações sobre como configurar políticas de ponto de acesso em Configurar políticas do IAM para uso de pontos de acesso.

Operações de ponto de acesso para buckets de diretório

As operações de ponto de acesso para buckets de diretório são operações de API do S3 que atuam no tipo de recurso de `accesspoint`. Por exemplo, `CreateAccessPoint`, `DeleteAccessPoint` e `GetAccessPointPolicy`. As ações de política do S3 para operações de ponto de acesso só

podem ser usadas em políticas baseadas em identidade do IAM, não em políticas de bucket ou políticas de ponto de acesso. As operações de ponto de acesso para buckets de diretório exigem que o elemento `Resource` seja o ARN do ponto de acesso no formato de exemplo a seguir.

```
"Resource": "arn:aws:s3:us-west-2:123456789012:accesspoint/example-access-point--usw2-az1--xa-s3"
```

A política baseada em identidade do IAM a seguir concede a permissão `s3express:GetAccessPointPolicy` para realizar a operação de API GetAccessPointPolicy no ponto de acesso denominado *example-access-point--usw2-az1--xa-s3*.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Grant permission to retrieve the access point policy of access
 point example-access-point--usw2-az1--xa-s3",
            "Effect": "Allow",
            "Action": [
            "s3express:CreateSession","s3express:GetAccessPointPolicy"
            ],
            "Resource": "arn:aws:s3:*:123456789012:accesspoint/example-access-point--
usw2-az1--xa-s3"
        }
    ]
}
```

A política baseada em identidade do IAM a seguir concede a permissão `s3express:CreateAccessPoint` para criar pontos de acesso para buckets de diretório.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Grant CreateAccessPoint.",
            "Principal": "*",
            "Action": "s3express:CreateSession",
            "s3express:CreateAccessPoint""Effect": "Allow",
            "Resource": "*"
        }
```

```
    ]
}
```

A política baseada em identidade do IAM a seguir concede a permissão `s3express:PutAccessPointScope` para criar um escopo de ponto de acesso para buckets de diretório.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Grant PutAccessPointScope",
            "Principal": "*",
            "Action": "s3express:CreateSession",
            "s3express:CreateAccessPoint",
            "S3Express:PutAccessPointScope""Effect": "Allow",
            "Resource": "*",
        }
    ]
}
```

Se você usa pontos de acesso para buckets de diretório, consulte Operações de bucket em políticas de ponto de acesso para buckets de diretório para controlar o acesso a operações de bucket e Operações de objeto em políticas de ponto de acesso para buckets de diretório para controlar o acesso a operações de objeto. Consulte mais informações sobre como configurar políticas de ponto de acesso para buckets de diretório em Configurar políticas do IAM para usar pontos de acesso para buckets de diretório.

Operações de ponto de acesso do Object Lambda

Com o Amazon S3 Object Lambda, você pode adicionar seu próprio código às solicitações `GET`, `LIST` e `HEAD` do Amazon S3 para modificar e processar dados, conforme eles são retornados para uma aplicação. É possível fazer solicitações por um ponto de acesso do Object Lambda, que funciona da mesma maneira que fazer solicitações por outros pontos de acesso. Para obter mais informações, consulte Transformar objetos com o S3 Object Lambda.

Consulte mais informações sobre como configurar políticas de operações de ponto de acesso do Object Lambda em Configurar políticas do IAM para pontos de acesso do Object Lambda.

Operações de ponto de acesso multirregionais

Um ponto de acesso multirregional fornece um endpoint global que as aplicações podem usar para atender a solicitações de buckets do S3 localizados em várias Região da AWS. É possível usar um ponto de acesso multirregional para criar aplicações de várias regiões com a mesma arquitetura usada em uma única região, depois executar essas aplicações em qualquer lugar do mundo. Para obter mais informações, consulte Gerenciar o tráfego multirregional com Pontos de Acesso Multirregionais.

Consulte mais informações sobre como configurar políticas de operações de ponto de acesso multirregionais em Exemplos de políticas de pontos de acesso multirregionais.

Operações de trabalho em lote

As operações de trabalho (operações em lote) são operações de API do S3 que operam no tipo de recurso de trabalho. Por exemplo, `DescribeJob` e `CreateJob`. As ações de política do S3 para operações de trabalho só podem ser usadas em políticas baseadas em identidade do IAM, não em políticas de buckets. Além disso, as operações de trabalho exigem que o elemento `Resource` nas políticas baseadas em identidade do IAM seja o ARN `job` no formato de exemplo a seguir.

```
"Resource": "arn:aws:s3:*:123456789012:job/*"
```

A política baseada em identidade do IAM a seguir concede a permissão `s3:DescribeJob` para realizar a operação de API DescribeJob no trabalho *`example-job`* de Operações em Lote do S3.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow describing the Batch operation job example-job",
            "Effect": "Allow",
            "Action": [
            "s3:DescribeJob"
            ],
            "Resource": "arn:aws:s3:*:123456789012:job/example-job"
        }
    ]
}
```

Operações de configuração da Lente de Armazenamento do S3

Consulte mais informações sobre como definir as operações de configuração do Lente de Armazenamento do S3 em Configurar permissões da Lente de Armazenamento do Amazon S3.

Operações de conta

As operações da conta são operações de API do S3 que operam no nível da conta. Por exemplo, `GetPublicAccessBlock` (para conta). A conta não é um tipo de recurso definido pelo Amazon S3. As ações de política do S3 para operações de conta só podem ser usadas em políticas baseadas em identidade do IAM, não em políticas de buckets. Além disso, as operações da conta exigem que o elemento `Resource` nas políticas baseadas em identidade do IAM seja `"*"`.

A política baseada em identidade do IAM a seguir concede a permissão `s3:GetAccountPublicAccessBlock` para realizar a operação de API GetPublicAccessBlock em nível de conta e recuperar as configurações do Bloqueio de Acesso Público em nível de conta.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"Allow retrieving the account-level Public Access Block settings",
         "Effect":"Allow",
         "Action":[
            "s3:GetAccountPublicAccessBlock"
         ],
         "Resource":[
            "*"
         ]
       }
    ]
}
```

Exemplos de políticas para o Amazon S3

- Consulte exemplos de políticas baseadas em identidade do Amazon S3 em Políticas baseadas em identidade do Amazon S3.
- Consulte exemplos de políticas baseadas em recursos do Amazon S3 em Políticas de bucket para o Amazon S3 e Configurar políticas do IAM para uso de pontos de acesso.

Recursos de políticas para o Amazon S3

Compatível com recursos de políticas: sim

Os administradores podem usar as políticas JSON da AWS para especificar quem tem acesso a quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento de política JSON `Resource` especifica o objeto ou os objetos aos quais a ação se aplica. As instruções devem incluir um elemento `Resource` ou `NotResource`. Como prática recomendada, especifique um recurso usando seu nome do recurso da Amazon (ARN). Isso pode ser feito para ações que oferecem compatibilidade com um tipo de recurso específico, conhecido como permissões em nível de recurso.

Para ações que não oferecem compatibilidade com permissões em nível de recurso, como operações de listagem, use um curinga (*) para indicar que a instrução se aplica a todos os recursos.

```
"Resource": "*"
```

Algumas ações de API do Amazon S3 são compatíveis com vários recursos. Por exemplo, `s3:GetObject` acessa *`example-resource-1`* e *`example-resource-2`*; portanto, uma entidade principal deve ter permissões para acessar os dois recursos. Para especificar vários recursos em uma única declaração, separe os ARNs com vírgula, como mostrado no exemplo a seguir.

```
"Resource": [
      "example-resource-1",
      "example-resource-2"
```

Os recursos no Amazon S3 são buckets, objetos, pontos de acesso ou trabalhos. Em uma política, use o nome do recurso da Amazon (ARN) do bucket, do objeto, do ponto de acesso ou do trabalho para identificar o recurso.

Consulte uma lista completa dos tipos de recurso do Amazon S3 e os respectivos ARNs em Resources defined by Amazon S3 na Referência de autorização do serviço. Para saber com quais ações você pode especificar o ARN de cada recurso, consulte Actions defined by Amazon S3.

Para ter mais informações sobre as permissões referentes a operações de API do S3 de acordo com os tipos de recurso do S3, consulte Permissões obrigatórias para operações de API do Amazon S3.

Caracteres curinga em ARNs de recursos

É possível usar caracteres curinga como parte do ARN do recurso. É possível usar caracteres curinga (* e ?) em qualquer segmento de ARN (as partes separadas por dois-pontos). Um asterisco (*) representa qualquer combinação de zero ou mais caracteres, e um ponto de interrogação (?) representa qualquer caractere único. Você pode usar vários caracteres * ou ? em cada segmento. No entanto, um caractere curinga não pode abranger segmentos.

- O ARN a seguir usa o caractere curinga * na parte `relative-ID` do ARN para identificar todos os objetos no bucket *amzn-s3-demo-bucket*.

```
arn:aws:s3:::amzn-s3-demo-bucket/*
```

- O ARN a seguir usa * para indicar todos os buckets e objetos do S3.

```
arn:aws:s3:::*
```

- O ARN a seguir usa caracteres curinga, * e ?, na parte de `relative-ID`. Esse ARN identifica todos os objetos em buckets, como *amzn-s3-demo-example1bucket*, *amzn-s3-demo-example2bucket*, *amzn-s3-demo-example3bucket* etc.

```
arn:aws:s3:::amzn-s3-demo-example?bucket/*
```

Variáveis de política para ARNs de recursos

Você pode usar variáveis de política em ARNs do Amazon S3. No momento da avaliação da política, essas variáveis predefinidas são substituídas pelos valores correspondentes. Vamos supor que você organize seu bucket como um conjunto de pastas, sendo uma pasta para cada um dos usuários. O nome da pasta é igual ao nome do usuário. Para conceder aos usuários permissão às pastas, você pode especificar uma variável de política no ARN do recurso:

```
arn:aws:s3:::bucket_name/developers/${aws:username}/
```

No tempo de execução, quando a política é avaliada, a variável `${aws:username}` no ARN do recurso é substituída pelo nome de usuário da pessoa que faz a solicitação.

Exemplos de políticas para o Amazon S3

- Consulte exemplos de políticas baseadas em identidade do Amazon S3 em Políticas baseadas em identidade do Amazon S3.
- Consulte exemplos de políticas baseadas em recursos do Amazon S3 em Políticas de bucket para o Amazon S3 e Configurar políticas do IAM para uso de pontos de acesso.

Chaves de condição de política para o Amazon S3

Compatível com chaves de condição de política específicas de serviço: sim

Os administradores podem usar as políticas JSON da AWS para especificar quem tem acesso a quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento `Condition` (ou bloco `Condition`) permite que você especifique condições nas quais uma instrução estiver em vigor. O elemento `Condition` é opcional. É possível criar expressões condicionais que usem agentes de condição, como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação.

Se você especificar vários elementos de `Condition` em uma declaração ou várias chaves em um único elemento de `Condition`, a AWS os avaliará usando uma operação lógica `AND`. Se você especificar vários valores para uma única chave de condição, a AWS avaliará a condição usando uma operação lógica `OR`. Todas as condições devem ser atendidas antes que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar condições. Por exemplo, é possível conceder a um usuário do IAM permissão para acessar um recurso somente se ele estiver marcado com seu nome de usuário do IAM. Para obter mais informações, consulte Elementos da política do IAM: variáveis e tags no Guia do usuário do IAM.

A AWS oferece compatibilidade com chaves de condição globais e chaves de condição específicas do serviço. Para ver todas as chaves de condição globais da AWS, consulte Chaves de contexto de condição globais da AWS no Guia do usuário do IAM.

Cada chave de condição do Amazon S3 é associada ao mesmo cabeçalho de solicitação de nome permitido pela API na qual a condição pode ser definida. As chaves de condição específicas do Amazon S3 ditam o comportamento dos cabeçalhos de solicitação de mesmo nome. Por exemplo, a chave de condição `s3:VersionId` usada para conceder permissão condicional à permissão `s3:GetObjectVersion`

define o comportamento do parâmetro de consulta `versionId` que você define em uma solicitação GET Object.

Consulte uma lista de chaves de condição do Amazon S3 em Condition keys for Amazon S3 na Referência de autorização do serviço. Para saber com quais ações e recursos é possível usar uma chave de condição, consulte Actions defined by Amazon S3.

Exemplo: restringir uploads aos objetos com uma classe de armazenamento específica

Suponha que a conta A, representada pelo ID da conta *123456789012*, tem um bucket. O administrador da conta A deseja restringir *Dave*, um usuário na conta A, para que *Dave* só possa fazer upload de objetos no bucket se o objeto estiver armazenado na classe de armazenamento `STANDARD_IA`. Para restringir uploads de objetos a uma classe de armazenamento específica, o administrador da Conta A pode usar a chave de condição `s3:x-amz-storage-class`, conforme mostrado no exemplo de política de bucket a seguir.

```
{
                "Version": "2012-10-17",
                "Statement": [
                  {
                    "Sid": "statement1",
                    "Effect": "Allow",
                    "Principal": {
                      "AWS": "arn:aws:iam::123456789012:user/Dave"
                    },
                    "Action": "s3:PutObject",
                    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*",
                    "Condition": {
                      "StringEquals": {
                        "s3:x-amz-storage-class": [
                          "STANDARD_IA"
                        ]
                      }
                    }
                  }
                ]
            }
```

No exemplo, o bloco `Condition` especifica a condição `StringEquals` que é aplicada ao par de chave-valor especificado, `"s3:x-amz-acl":["public-read"]`. Existe um conjunto de chaves predefinidas que pode ser usado para expressar uma condição. O exemplo usa a chave de condição

`s3:x-amz-acl`. Essa condição exige que o usuário inclua o cabeçalho `x-amz-acl` com o valor `public-read` em cada solicitação `PutObject`.

Exemplos de políticas para o Amazon S3

- Consulte exemplos de políticas baseadas em identidade do Amazon S3 em Políticas baseadas em identidade do Amazon S3.
- Consulte exemplos de políticas baseadas em recursos do Amazon S3 em Políticas de bucket para o Amazon S3 e Configurar políticas do IAM para uso de pontos de acesso.

ACLs no Amazon S3

Compatível com ACLs: sim

No Amazon S3, as listas de controle de acesso (ACLs) controlam quais Contas da AWS têm permissões para acessar um recurso. As ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

> **Important**
>
> A maioria dos casos de uso modernos no Amazon S3 não exige mais o uso de ACLs.

Consulte informações sobre como usar ACLs para controlar o acesso no Amazon S3 em Gerenciar o acesso com ACLs.

ABAC com o Amazon S3

Compatível com ABAC (tags em políticas): parcial

O controle de acesso por atributo (ABAC) é uma estratégia de autorização que define as permissões com base em atributos. Na AWS, esses atributos são chamados de tags. É possível anexar tags a entidades do IAM (usuários ou perfis) e a muitos recursos da AWS. Marcar de entidades e atributos é a primeira etapa do ABAC. Em seguida, você cria políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso que ela estiver tentando acessar.

O ABAC é útil em ambientes que estão crescendo rapidamente e ajuda em situações em que o gerenciamento de políticas se torna um problema.

Para controlar o acesso baseado em tags, forneça informações sobre as tags no elemento de condição de uma política usando as `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou chaves de condição `aws:TagKeys`.

Se um serviço for compatível com as três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço for compatível com as três chaves de condição somente para alguns tipos de recursos, o valor será Parcial

Para obter mais informações sobre o ABAC, consulte Definir permissões com autorização do ABAC no Guia do usuário do IAM. Para visualizar um tutorial com etapas para configurar o ABAC, consulte Usar controle de acesso baseado em atributos (ABAC) no Guia do usuário do IAM.

Consulte exemplos de políticas baseadas em identidade para limitar o acesso aos trabalhos de Operações em Lote do S3 com base em tags em Controlar permissões para o Operações em Lote usando tags de trabalho.

ABAC e tags de objetos

Nas políticas de ABAC, os objetos usam tags `s3:` em vez de tags `aws:`. Para controlar o acesso a objetos com base em tags, forneça informações sobre a tag no elemento Condition de uma política usando as seguintes tags:

- `s3:ExistingObjectTag/tag-key`
- `s3:RequestObjectTagKeys`
- `s3:RequestObjectTag/tag-key`

Consulte informações sobre como usar tags de objeto para controlar o acesso, incluindo exemplos de políticas de permissão, em Marcação e políticas de controle de acesso.

Usar credenciais temporárias com o Amazon S3

Compatível com credenciais temporárias: sim

Alguns Serviços da AWS não funcionam quando você faz login usando credenciais temporárias. Para obter informações adicionais, como quais Serviços da AWS funcionam com credenciais temporárias, consulte Serviços da AWS que funcionem com o IAM no Guia do usuário do IAM.

Você está usando credenciais temporárias se fizer login no AWS Management Console por qualquer método, exceto nome de usuário e uma senha. Por exemplo, quando você acessa a AWS usando o link de autenticação única (SSO) da sua empresa, esse processo cria credenciais temporárias

automaticamente. Você também cria automaticamente credenciais temporárias quando faz login no console como usuário e, em seguida, alterna perfis. Para obter mais informações sobre como alternar funções, consulte Alternar para um perfil do IAM (console) no Guia do usuário do IAM.

É possível criar credenciais temporárias manualmente usando a API AWS CLI ou AWS. Em seguida, você pode usar essas credenciais temporárias para acessar a AWS. A AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para obter mais informações, consulte Credenciais de segurança temporárias no IAM.

Sessões de acesso direto para o Amazon S3

Compatibilidade com o recurso de encaminhamento de sessões de acesso (FAS): sim

O usuário ou perfil do IAM usado para executar ações na AWS é considerado uma entidade principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O recurso FAS usa as permissões da entidade principal chamando um AWS service (Serviço da AWS), bem como o AWS service (Serviço da AWS) solicitante, para fazer solicitações para serviços subsequentes. As solicitações de FAS são feitas somente quando um serviço recebe uma solicitação que exige interações com outros Serviços da AWS ou com recursos para serem concluídas. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Sessões de acesso direto.

- O FAS é usado pelo Amazon S3 para fazer chamadas ao AWS KMS para descriptografar um objeto quando se usa a SSE-KMS para criptografá-lo. Para obter mais informações, consulte Usar criptografia do lado do servidor com o AWS KMS (SSE-KMS).
- A funcionalidade Concessões de Acesso do S3 também usa FAS. Depois de criar uma concessão de acesso aos seus dados do S3 para uma identidade específica, o beneficiário solicita uma credencial temporária da funcionalidade Concessões de Acesso do S3. A funcionalidade Concessões de Acesso do S3 obtém uma credencial temporária para o solicitante pelo AWS STS e vende a credencial a ele. Para obter mais informações, consulte Solicitar acesso aos dados do Amazon S3 por meio da funcionalidade Concessões de Acesso do S3.

Perfis de serviço para o Amazon S3

Compatível com perfis de serviço: sim

O perfil de serviço é um perfil do IAM que um serviço assume para executar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais

informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.

> **Warning**
>
> A alteração das permissões de um perfil de serviço pode interromper a funcionalidade do Amazon S3. Edite perfis de serviço somente quando o Amazon S3 instruir a fazer isso.

Perfis vinculados ao serviço para o Amazon S3

Compatível com perfis vinculados ao serviço: parcialmente

Um perfil vinculado a serviço é um tipo de perfil de serviço vinculado a um AWS service (Serviço da AWS). O serviço pode presumir o perfil de executar uma ação em seu nome. Perfis vinculadas ao serviço aparecem em sua Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para perfis vinculados a serviço.

O Amazon S3 é compatível com perfis vinculados a serviço da Lente de Armazenamento do Amazon S3. Consulte detalhes de como criar ou gerenciar perfis vinculados ao serviço do Amazon S3 em Usar funções vinculadas a serviços para o Amazon S3 Storage Lens.

Serviço do Amazon S3 como entidade principal

Nome do serviço na política	Recurso do S3	Mais informações
`s3.amazonaws.com`	Replicação do S3	Visão geral da configuração da replicação em tempo real
`s3.amazonaws.com`	Notificações de eventos do S3	Notificações de eventos do Amazon S3
`s3.amazonaws.com`	Inventário S3	Catalogar e analisar seus dados com o Inventário S3
`access-grants.s3.amazonaws.com`	Concessões de Acesso do S3	Registrar um local
`batchoperations.s3.amazonaws.com`	Operações em lote do S3	Conceder permissões para operações em lote

Nome do serviço na política	Recurso do S3	Mais informações
`logging.s3.amazonaws.com`	Registro em log de acesso ao servidor do S3	Habilitar o log de acesso ao servidor do Amazon S3
`storage-lens.s3.amazonaws.com`	Lente de Armazenamento do S3	Exibição de métricas de lente de armazenamento do Amazon S3 usando uma exportação de dados

Como o Amazon S3 autoriza uma solicitação

Quando o Amazon S3 recebe uma solicitação — por exemplo, uma operação de bucket ou de objeto — ele primeiro verifica se o solicitante tem as permissões necessárias. O Amazon S3 avalia todas as políticas de acesso relevantes, as políticas de usuário e as políticas baseadas em recursos (política de bucket, lista de controle de acesso (ACL) de bucket e ACL de objeto) para decidir se autoriza a solicitação.

> **Note**
>
> Se a verificação de permissão do Amazon S3 não conseguir encontrar permissões válidas, será retornado um erro de permissão negada “Acesso negado” (403 Proibido). Consulte mais informações em Solucionar erros de acesso negado (403 proibido) no Amazon S3.

Para determinar se o solicitante tem permissão para executar a operação específica, o Amazon S3 faz o seguinte, na ordem que se apresenta, quando recebe uma solicitação:

1. Converte todas as políticas de acesso relevantes (política de usuário, política de bucket e ACLs) no tempo de execução em um conjunto de políticas para avaliação.
2. Avalia o conjunto de políticas resultante nas seguintes etapas. Em cada etapa, o Amazon S3 avalia um subconjunto de políticas em um contexto específico, com base na autoridade contextual.
   a. Contexto de usuário: no contexto de usuário, a conta pai à qual o usuário pertence é a autoridade contextual.

      O Amazon S3 avalia um subconjunto de políticas de propriedade da conta pai. Esse subconjunto inclui a política de usuário que o pai anexa ao usuário. Se a conta principal também possuir o recurso na solicitação (bucket ou objeto), o Amazon S3 também avaliará as políticas de recursos correspondentes (política de bucket, ACL de bucket e ACL de objeto) ao mesmo tempo.

      Um usuário deve ter permissão da conta pai para executar uma operação.

      Essa etapa será aplicável somente se a solicitação for feita por um usuário em uma Conta da AWS. Se a solicitação for feita usando as credenciais do usuário raiz de uma Conta da AWS, o Amazon S3 ignorará essa etapa.

b. Contexto de bucket: no contexto de bucket, o Amazon S3 avalia as políticas de propriedade da Conta da AWS que possui o bucket.

   Se a solicitação for para uma operação de bucket, o solicitante deverá ter permissão do proprietário do bucket. Se a solicitação for para um objeto, o Amazon S3 avaliará todas as políticas de propriedade do proprietário do bucket para verificar se o proprietário do bucket não negou explicitamente o acesso ao objeto. Se houver uma negação explícita definida, o Amazon S3 não autorizará a solicitação.

c. Contexto de objeto: se a solicitação for para um objeto, o Amazon S3 avaliará o subconjunto de políticas de propriedade do proprietário do objeto.

Veja a seguir alguns exemplos de cenários que ilustram como o Amazon S3 autoriza uma solicitação.

Example – O solicitante é uma entidade principal do IAM

Se o solicitante for uma entidade principal do IAM, o Amazon S3 deverá determinar se a Conta da AWS pai à qual a entidade principal pertence concedeu a permissão necessária para ele executar a operação. Além disso, se a solicitação for para uma operação de bucket, como uma solicitação para listar o conteúdo do bucket, o Amazon S3 deverá verificar se o proprietário do bucket concedeu permissão para o solicitante executar a operação. Para executar uma operação específica em um recurso, uma entidade principal do IAM precisa de permissão da Conta da AWS pai à qual ele pertence e da Conta da AWS que é proprietária do recurso.

Example – O solicitante é uma entidade principal do IAM: se a solicitação for para uma operação ou um objeto que não pertence ao proprietário do bucket

Se a solicitação for para uma operação em um objeto que o proprietário do bucket não possui, além de verificar se o solicitante tem permissões do proprietário do objeto, o Amazon S3 também deverá verificar a política do bucket para garantir que o proprietário do bucket não definiu uma negação explícita no objeto. Um proprietário de bucket (que paga a fatura) pode negar explicitamente o acesso aos objetos do bucket independentemente de quem os possui. O proprietário do bucket também pode excluir qualquer objeto do bucket

Por padrão, quando outra Conta da AWS faz upload de um objeto no bucket de uso geral do S3, essa conta (que gravou o objeto) é a proprietária do objeto, tem acesso a ele e pode conceder acesso a outros usuários por meio de listas de controle de acesso (ACLs). É possível usar a

Propriedade de objetos para alterar esse comportamento padrão de modo que as ACLs sejam desabilitadas e o proprietário do bucket torne-se automaticamente proprietário de todos os objetos no bucket de uso geral. Como resultado, o controle de acesso para seus dados é baseado em políticas, como políticas de usuários do IAM, políticas de bucket do S3, políticas de endpoint da nuvem privada virtual (VPC) e políticas de controle de serviço (SCPs) do AWS Organizations. Para obter mais informações, consulte Controlar a propriedade de objetos e desabilitar ACLs para seu bucket.

Para obter mais informações sobre como o Amazon S3 avalia as políticas de acesso para autorizar ou negar solicitações para operações de bucket e operações de objeto, consulte os seguintes tópicos:

Tópicos

- Como o Amazon S3 autoriza uma solicitação para uma operação de bucket
- Como o Amazon S3 autoriza uma solicitação para uma operação de objeto

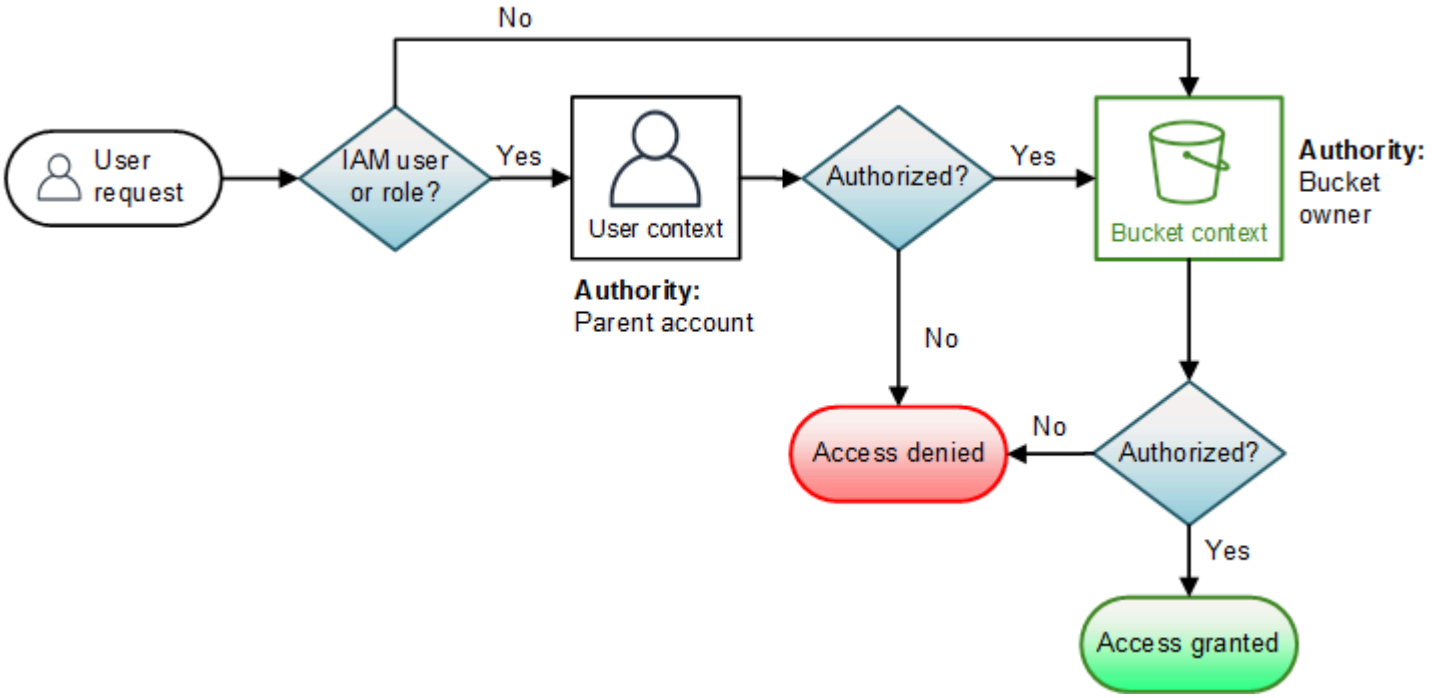
Como o Amazon S3 autoriza uma solicitação para uma operação de bucket

Quando o Amazon S3 recebe uma solicitação para uma operação de bucket, ele converte todas as permissões relevantes em um conjunto de políticas para avaliar em tempo de execução. As permissões relevantes incluem permissões baseadas em recursos (por exemplo, políticas de bucket e listas de controle de acesso de bucket) e políticas de usuário se a solicitação vier de uma entidade principal do IAM. Em seguida, o Amazon S3 avalia o conjunto de políticas resultante em uma série de etapas, de acordo com o contexto específico (contexto do usuário ou do bucket):

1. Contexto do usuário: se o solicitante for um principal do IAM, o principal deverá ter permissão da Conta da AWS pai à qual ele pertence. Nesta etapa, o Amazon S3 avalia um subconjunto de políticas de propriedade da conta pai (também conhecida como a autoridade de contexto). Esse subconjunto de políticas inclui a política de usuário que a conta pai anexa ao principal. Se o pai também possuir o recurso na solicitação (neste caso, o bucket), o Amazon S3 também avaliará as políticas dos recursos correspondentes (a política do bucket e a ACL do bucket) ao mesmo tempo. Sempre que uma solicitação para uma operação de bucket é feita, os logs de acesso ao servidor registram o ID canônico do solicitante. Para obter mais informações, consulte Registrar em log as solicitações com registro em log de acesso ao servidor.
2. Contexto de bucket: o solicitante deve ter permissões do proprietário do bucket para executar uma operação específica de bucket. Nesta etapa, o Amazon S3 avalia um subconjunto de políticas de propriedade da Conta da AWS que é proprietária do bucket.

O proprietário do bucket pode conceder permissão usando uma política do bucket ou a ACL do bucket. Se a Conta da AWS que é proprietária do bucket também for a conta principal de uma entidade principal do IAM, ela poderá configurar permissões de bucket em uma política de usuário.

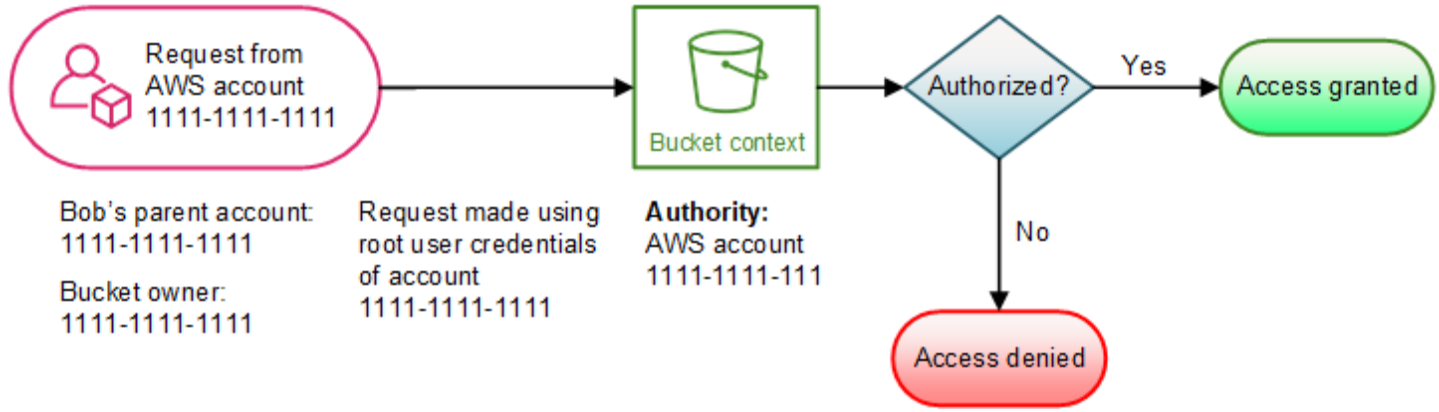
O seguinte é uma ilustração gráfica da avaliação baseada em contexto para a operação de bucket.



Os exemplos a seguir ilustram a lógica da avaliação.

Exemplo 1: operação de bucket solicitada pelo proprietário do bucket

Neste exemplo, o proprietário do bucket envia uma solicitação a uma operação de bucket usando as credenciais raiz da Conta da AWS.

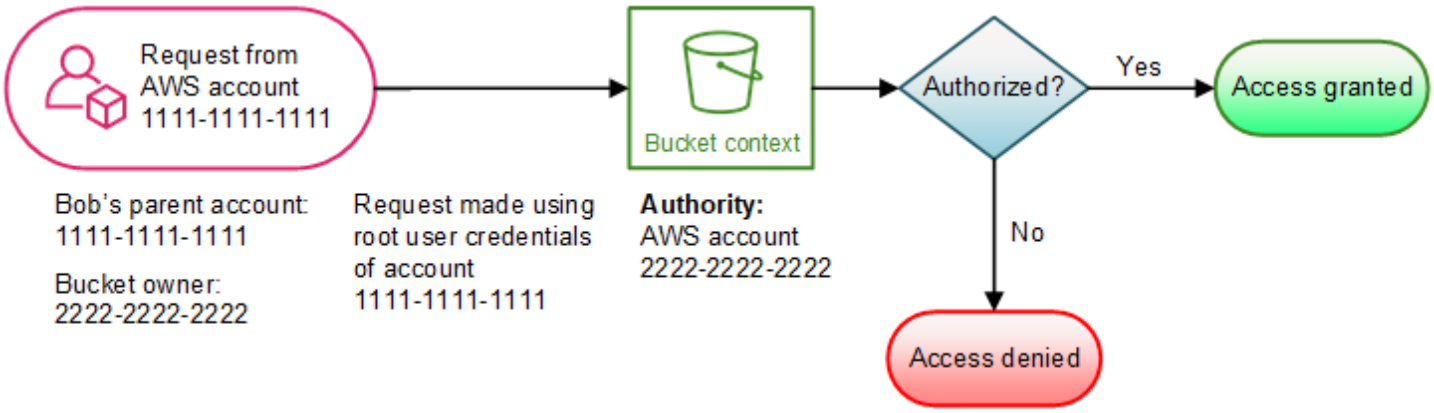


O Amazon S3 executa a avaliação de contexto da seguinte forma:

1. Como a solicitação é feita usando as credenciais do usuário raiz de uma Conta da AWS, o contexto do usuário não é avaliado.
2. No contexto de bucket, o Amazon S3 analisa a política de bucket para determinar se o solicitante tem permissão para executar a operação. O Amazon S3 autoriza a solicitação.

Exemplo 2: operação de bucket solicitada por uma Conta da AWS que não é a proprietária do bucket

Neste exemplo, uma solicitação é feita usando as credenciais do usuário raiz da Conta da AWS 1111-1111-1111 a uma operação de bucket pertencente à Conta da AWS 2222-2222-2222. Nenhum usuário do IAM está envolvido nessa solicitação.

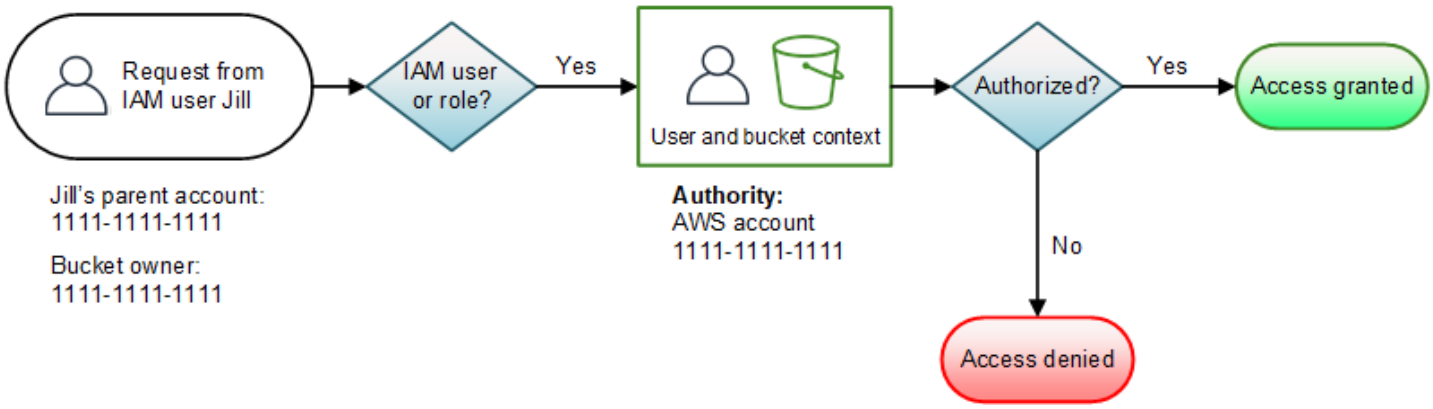


Nesse exemplo, o Amazon S3 avalia o contexto da seguinte forma:

1. Como a solicitação é feita usando as credenciais do usuário raiz de uma Conta da AWS, o contexto do usuário não é avaliado.
2. No contexto de bucket, o Amazon S3 examina a política de bucket. Se o proprietário do bucket (Conta da AWS 2222-2222-2222) não tiver autorizado a Conta da AWS 1111-1111-1111 a executar a operação solicitada, o Amazon S3 negará a solicitação. Caso contrário, o Amazon S3 concederá a solicitação e executará a operação.

Exemplo 3: operação de bucket solicitada por uma entidade principal do IAM cuja Conta da AWS pai também é a proprietária do bucket

No exemplo, a solicitação é enviada por Jill, uma usuária do IAM na Conta da AWS 1111-1111-1111, que também é proprietária do bucket.



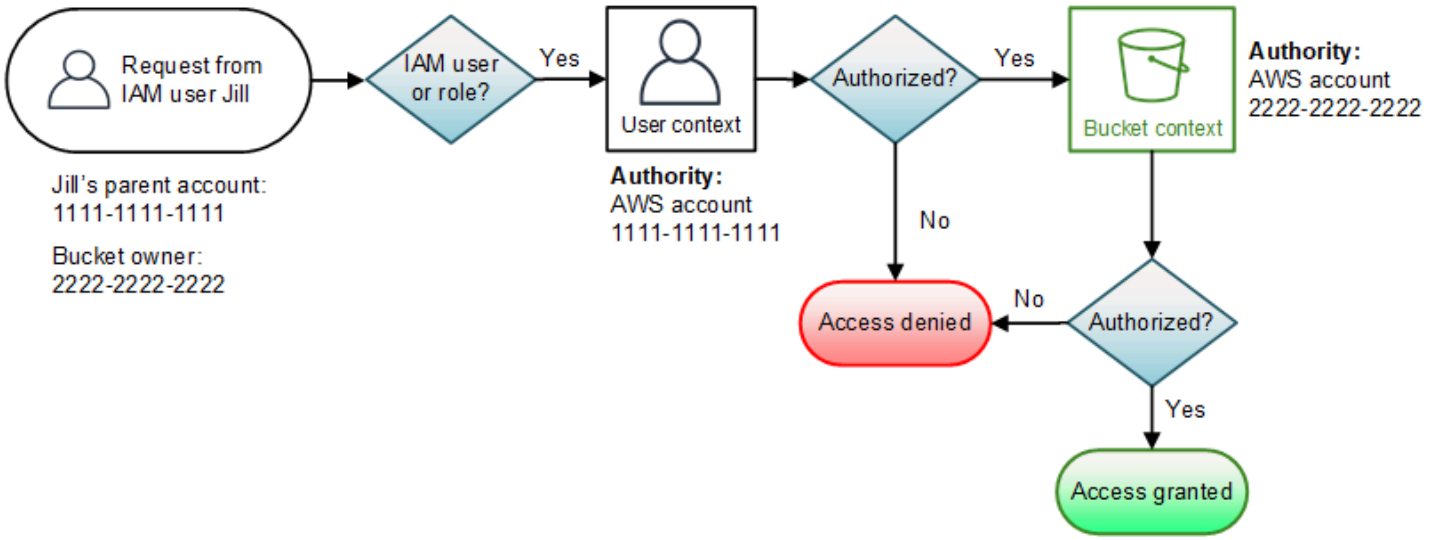
O Amazon S3 executa a seguinte avaliação de contexto:

1. Como a solicitação é de uma entidade principal do IAM, no contexto de usuário, o Amazon S3 avalia todas as políticas que pertencem à Conta da AWS pai para determinar se Jill tem permissão para executar a operação.

   Neste exemplo, a Conta da AWS pai 1111-1111-1111 à qual a entidade principal pertence também é a proprietária do bucket. Como resultado, além da política do usuário, o Amazon S3 também avalia a política e a ACL do bucket no mesmo contexto, já que pertencem à mesma conta.
2. Como o Amazon S3 avaliou a política do bucket e a ACL do bucket como parte do contexto de usuário, ele não avalia o contexto de bucket.

Exemplo 4: operação de bucket solicitada por uma entidade principal do IAM cuja Conta da AWS pai não é a proprietária do bucket

Neste exemplo, a solicitação é enviada por Jill, uma usuária do IAM cuja Conta da AWS pai é 1111-1111-1111, mas o bucket pertence a outra Conta da AWS, 2222-2222-2222.



Jill precisará de permissões da Conta da AWS pai e do proprietário do bucket. O Amazon S3 avalia o contexto da seguinte forma:

1. Como a solicitação é de um principal do IAM, o Amazon S3 avalia o contexto de usuário analisando as políticas criadas pela conta para verificar se Jill tem as permissões necessárias. Se Jill tiver permissão, o Amazon S3 avaliará o contexto de bucket. Se Jill não tiver permissão, a solicitação será negada.
2. No contexto de bucket, o Amazon S3 verifica se o proprietário do bucket 2222-2222-2222 concedeu a Jill (ou à Conta da AWS pai) permissão para executar a operação solicitada. Se ela tiver permissão, o Amazon S3 concederá a solicitação e executará a operação. Caso contrário, o Amazon S3 negará a solicitação.

Como o Amazon S3 autoriza uma solicitação para uma operação de objeto

Ao receber uma solicitação para uma operação de objeto, o Amazon S3 converterá todas as permissões relevantes, permissões baseadas em recursos (lista de controle de acesso [ACL] de objeto, política de bucket, ACL do bucket) e políticas de usuário do IAM, se a solicitação for de um usuário, em um conjunto de políticas a serem avaliadas no tempo de execução. Em seguida, ele avalia o conjunto de políticas resultante em uma série de etapas. Em cada etapa, ele avalia um subconjunto de políticas em três contextos específicos (contexto do usuário, do bucket e do objeto):

1. Contexto do usuário: se o solicitante for um principal do IAM, o principal deverá ter permissão da Conta da AWS pai à qual ele pertence. Nesta etapa, o Amazon S3 avalia um subconjunto de políticas de propriedade da conta pai (também conhecida como a autoridade de contexto). Esse subconjunto de políticas inclui a política de usuário que a pai anexa ao principal. Se a conta

principal também possuir o recurso na solicitação (bucket ou objeto), o Amazon S3 avaliará as políticas de recursos correspondentes (política de bucket, ACL de bucket e ACL de objeto) ao mesmo tempo.

> **Note**
>
> Se a Conta da AWS pai for a proprietária do recurso (bucket ou objeto), ela poderá conceder permissões de recurso à entidade principal do IAM usando a política de usuário ou a política de recurso.

2. Contexto do bucket: neste contexto, o Amazon S3 avalia as políticas de propriedade da Conta da AWS que possui o bucket.

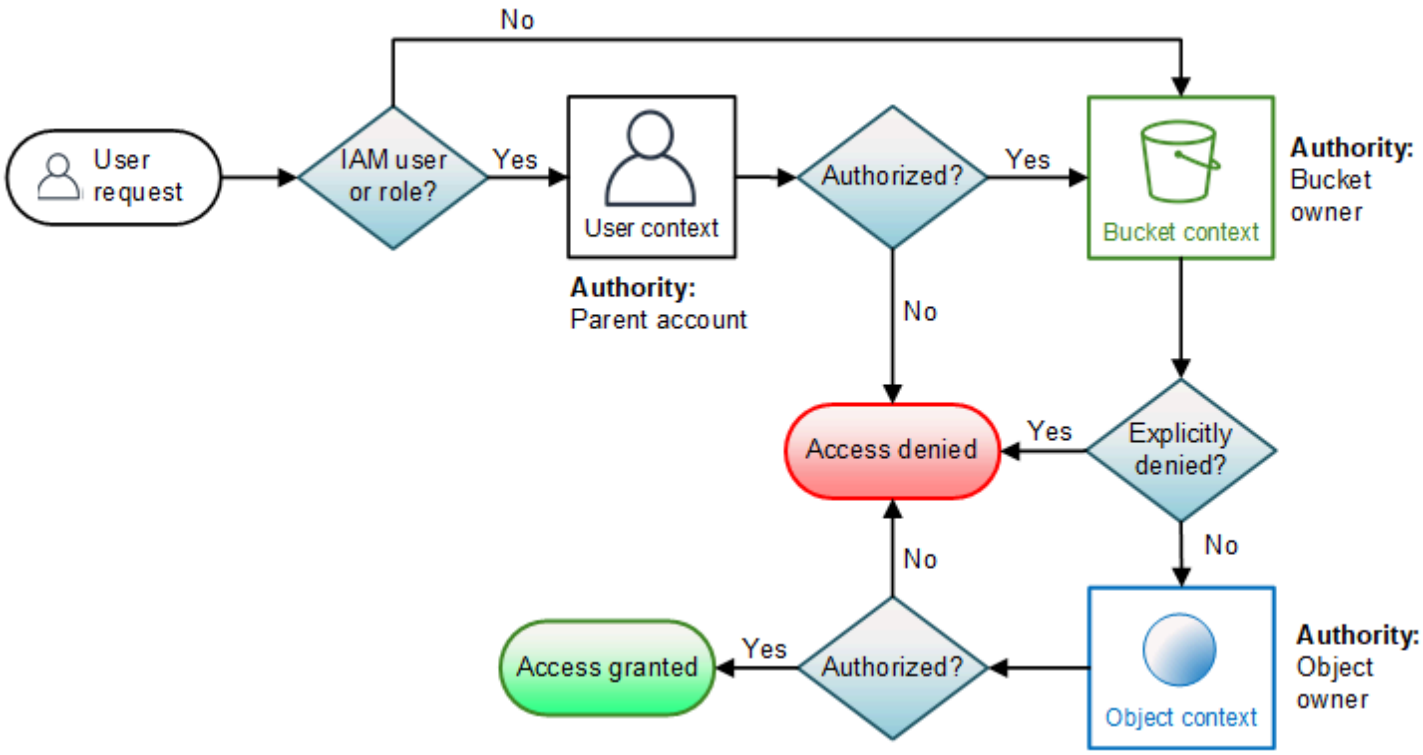
   Se a Conta da AWS que é proprietária do objeto na solicitação não for a mesma que é proprietária do bucket, o Amazon S3 verificará as políticas se o proprietário do bucket tiver negado explicitamente o acesso ao objeto. Se houver uma negação explícita definida no objeto, o Amazon S3 não autorizará a solicitação.

3. Contexto de objeto: o solicitante deve ter permissões do proprietário do objeto para executar uma operação específica de objeto. Nesta etapa, o Amazon S3 avalia a ACL do objeto.

> **Note**
>
> Se os proprietários do bucket e do objeto forem os mesmos, o acesso ao objeto poderá ser concedido na política de bucket, que é avaliada no contexto de bucket. Se os proprietários forem diferentes, os proprietários do objeto deverão usar uma ACL do objeto para conceder permissões. Se a Conta da AWS que é proprietária do objeto também for a conta pai à qual a entidade principal do IAM pertence, ela poderá configurar permissões de objeto em uma política de usuário, que é avaliada no contexto de usuário. Para obter mais informações sobre como usar essas alternativas de política de acesso, consulte Demonstrações que usam políticas para gerenciar o acesso a recursos do Amazon S3. Como proprietário do bucket, se você quiser ter propriedade de todos os objetos do bucket e usar políticas de bucket ou políticas baseadas no IAM para gerenciar o acesso a esses objetos, use a configuração aplicada pelo proprietário do bucket em Propriedade do objeto. Com essa configuração, você, como proprietário do bucket, automaticamente tem a propriedade e o controle total sobre todos os objetos de seu bucket. As ACLs de bucket e objeto não poderão ser editadas e não serão mais consideradas para acesso. Para obter

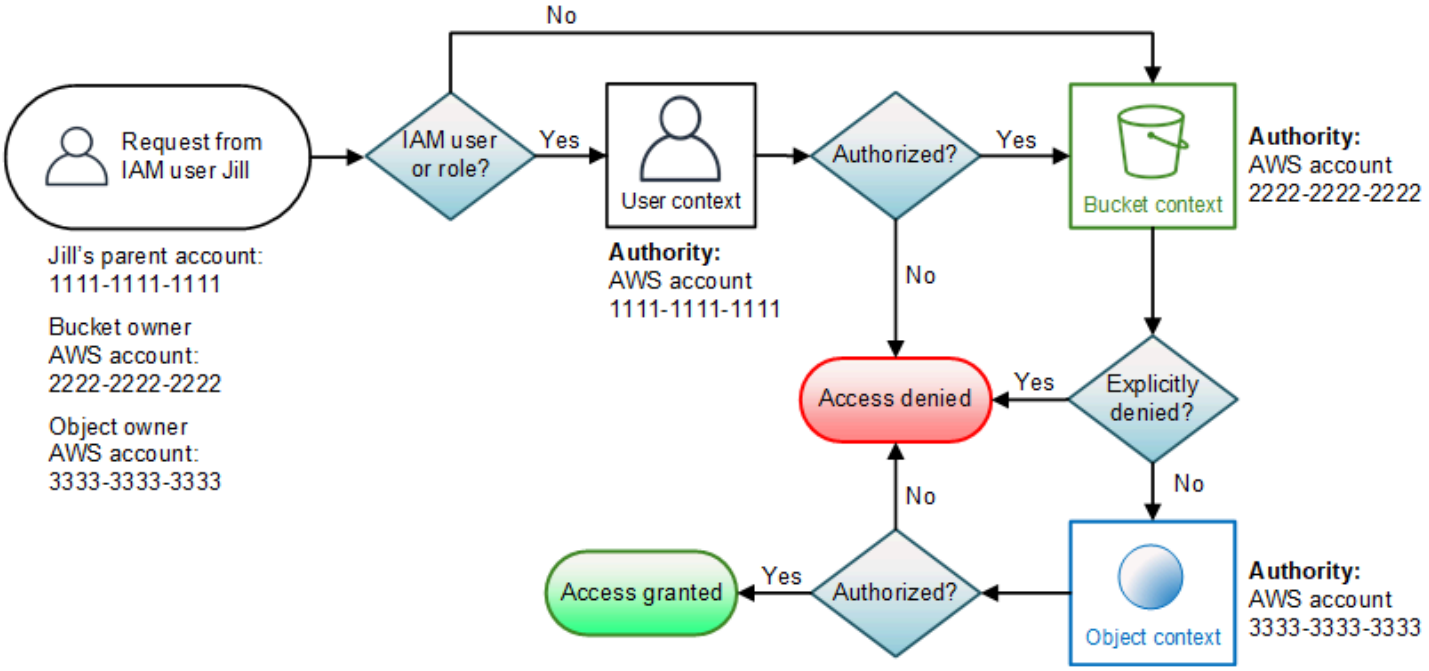
mais informações, consulte Controlar a propriedade de objetos e desabilitar ACLs para seu bucket.

O seguinte é uma ilustração gráfica da avaliação baseada em contexto para uma operação de objeto.



Exemplo de uma solicitação de operação de objeto

Neste exemplo, a usuária do IAM, Jill, cuja Conta da AWS pai é 1111-1111-1111, envia uma solicitação de operação de objeto (por exemplo, `GetObject`) a um objeto pertencente à Conta da AWS 3333-3333-3333 em um bucket pertencente à Conta da AWS 2222-2222-2222.



Jill precisará de permissões da Conta da AWS pai, do proprietário do bucket e do proprietário do objeto. O Amazon S3 avalia o contexto da seguinte forma:

1. Como a solicitação é de uma entidade principal do IAM, o Amazon S3 avalia o contexto de usuário para verificar se a Conta da AWS pai 1111-1111-1111 forneceu a Jill permissão para executar a operação solicitada. Se ela tiver essa permissão, o Amazon S3 avaliará o contexto de bucket. Caso contrário, o Amazon S3 negará a solicitação.
2. No contexto do bucket, o proprietário do bucket, a Conta da AWS 2222-2222-2222, é a autoridade de contexto. O Amazon S3 avalia a política de bucket para determinar se o proprietário do bucket negou explicitamente o acesso de Jill ao objeto.
3. No contexto do objeto, a autoridade de contexto é a Conta da AWS 3333-3333-3333, a proprietária do objeto. O Amazon S3 avalia a ACL do objeto para determinar se Jill tem permissão para acessar o objeto. Se tiver, o Amazon S3 autorizará a solicitação.

Permissões obrigatórias para operações de API do Amazon S3

> **Note**
>
> Esta página é sobre as ações de política do Amazon S3 para buckets de uso geral. Para saber mais sobre as ações de política do Amazon S3 para buckets de diretório, consulte Ações para buckets de diretório.

Para realizar uma operação de API do S3, é necessário ter as permissões corretas. Esta página associa as operações de API do S3 às permissões necessárias. Para conceder permissões para realizar uma operação de API do S3, você deve criar uma política válida (como uma política de bucket do S3 ou uma política baseada em identidade do IAM) e especificar as ações correspondentes no elemento `Action` da política. Essas ações são chamadas de ações de políticas. Nem toda operação de API do S3 é representada por uma única permissão (uma única ação de política), e algumas permissões (algumas ações de política) são necessárias para diferentes operações de API.

Ao criar políticas, você deve especificar o elemento `Resource` com base no tipo de recurso correto exigido pelas ações de política correspondentes do Amazon S3. Esta página categoriza as permissões para as operações de API do S3 de acordo com os tipos de recurso. Consulte mais informações sobre os tipos de recurso em Resource types defined by Amazon S3 na Referência de autorização do serviço. Consulte uma lista completa de ações, recursos e chaves de condição do Amazon S3 para uso em políticas em Actions, resources, and condition keys for Amazon S3 na Referência de autorização do serviço. Consulte uma lista completa de operações de API do Amazon S3 em Amazon S3 API Actions na Referência de API do Amazon Simple Storage Service.

Para ter mais informações sobre como resolver os erros HTTP `403 Forbidden` no S3, consulte Solucionar erros de acesso negado (403 Forbidden) no Amazon S3. Para ter mais informações sobre os recursos do IAM para usar com o S3, consulte Como o Amazon S3 funciona com o IAM. Para ter mais informações sobre as práticas recomendadas de segurança do S3, consulte Práticas recomendadas de segurança para o Amazon S3.

Tópicos

- Permissões e operações de bucket
- Permissões e operações do objeto
- Operações e permissões de ponto de acesso para buckets de uso geral

- Permissões e operações de ponto de acesso do Object Lambda
- Operações e permissões de ponto de acesso multirregional
- Operações e permissões de trabalho em lote
- Operações e permissões de configuração da Lente de Armazenamento do S3
- Operações e permissões de grupos da Lente de Armazenamento do S3
- Operações e permissões de instância da funcionalidade Concessão de Acesso do S3
- Operações e permissões de localização da Concessão de Acesso do S3
- Operações e permissões de concessão do recurso Concessão de Acesso do S3
- Permissões e operações de conta

Permissões e operações de bucket

As operações de bucket são operações de API do S3 que operam no tipo de recurso de bucket. É necessário especificar as ações de política do S3 para operações de bucket nas respectivas políticas ou em políticas baseadas em identidade do IAM.

Nas políticas, o elemento `Resource` deve ser o nome do recurso da Amazon (ARN) do bucket. Para ter mais informações sobre o formato do elemento `Resource` e políticas de exemplo, consulte Operações de buckets.

> **Note**
>
> Para conceder permissões a operações de bucket em políticas de pontos de acesso, observe o seguinte:
>
> - As permissões concedidas para operações de bucket em uma política de ponto de acesso entrarão em vigor somente se o bucket subjacente conceder as mesmas permissões. Ao usar um ponto de acesso, é necessário delegar o controle de acesso do bucket ao ponto de acesso ou adicionar as mesmas permissões nas políticas de ponto de acesso à política do bucket subjacente.
> - Nas políticas de pontos de acesso que concedem permissões às operações de bucket, o elemento `Resource` deve ser o ARN `accesspoint`. Para ter mais informações sobre o formato do elemento `Resource` e políticas de exemplo, consulte Operações de bucket em políticas de ponto de acesso para buckets de uso geral. Para ter mais informações sobre políticas de ponto de acesso, consulte Configurar políticas do IAM para uso de pontos de acesso.

- Nem todas as operações de bucket são compatíveis com pontos de acesso. Para obter mais informações, consulte Compatibilidade de pontos de acesso com operações do S3.

Veja a seguir a correlação entre as operações de bucket e as ações de política obrigatórias.

Operações de API	Ações de políticas	Descrição das ações de política
CreateBucket	(Obrigatória) `s3:CreateBucket`	Obrigatória para criar um bucket do S3.
	(Obrigatória em determinadas condições) `s3:PutBucketAcl`	Obrigatória se você quiser usar a lista de controle de acesso (ACL) para especificar permissões em um bucket ao fazer uma solicitação `CreateBucket` .
	(Obrigatória em determinadas condições) `s3:PutBucketObjectLockConfiguration` , `s3:PutBucketVersioning`	Obrigatória se você quiser habilitar o Bloqueio de Objetos ao criar um bucket.
	(Obrigatória em determinadas condições) `s3:PutBucketOwnershipControls`	Obrigatória se você quiser especificar a propriedade de objetos do S3 ao criar um bucket.
CreateBucketMetadataTableConfiguration	(Obrigatório) `s3:CreateBucketMetadataTableConfiguration` , `s3tables:CreateNamespace` , `s3tables:CreateTable` , `s3tables:GetTable` ,	Necessária para criar uma configuração de tabelas de metadados em um bucket de uso geral. Para criar a tabela de metadados no bucket de tabela especificado na

Operações de API	Ações de políticas	Descrição das ações de política
	`s3tables:PutTablePolicy`	configuração de tabelas de metadados, é necessário ter as permissões `s3tables` especificadas. Se você também quiser integrar o bucket de tabela com os serviços de analytics da AWS para poder consultar a tabela de metadados, precisará de permissões adicionais. Para ter mais informações, consulte Integrating Amazon S3 Tables with AWS analytics services.
DeleteBucket	(Obrigatória) `s3:DeleteBucket`	Obrigatória para excluir um bucket do S3.
DeleteBucketAnalyticsConfiguration	(Obrigatória) `s3:PutAnalyticsConfiguration`	Obrigatória para excluir uma configuração de analytics do S3 de um bucket do S3.
DeleteBucketCors	(Obrigatória) `s3:PutBucketCORS`	Obrigatória para excluir a configuração de compartilhamento de recursos entre origens (CORS) de um bucket.
DeleteBucketEncryption	(Obrigatória) `s3:PutEncryptionConfiguration`	Obrigatória para redefinir a configuração de criptografia padrão para um bucket do S3 como criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3).

Operações de API	Ações de políticas	Descrição das ações de política
DeleteBucketIntelligentTieringConfiguration	(Obrigatória) `s3:PutIntelligentTieringConfiguration`	Obrigatória para excluir a configuração existente do S3 Intelligent-Tiering de um bucket do S3.
DeleteBucketInventoryConfiguration	(Obrigatória) `s3:PutInventoryConfiguration`	Obrigatória para excluir uma configuração do Inventário S3 de um bucket do S3.
DeleteBucketLifecycle	(Obrigatória) `s3:PutLifecycleConfiguration`	Obrigatória para excluir a configuração de ciclo de vida do S3 para um bucket do S3.
DeleteBucketMetadataTableConfiguration	(Obrigatória) `s3:DeleteBucketMetadataTableConfiguration`	Necessária para excluir uma configuração de tabelas de metadados de um bucket de uso geral.
DeleteBucketMetricsConfiguration	(Obrigatória) `s3:PutMetricsConfiguration`	Obrigatória para excluir uma configuração de métricas de solicitação do Amazon CloudWatch de um bucket do S3.
DeleteBucketOwnershipControls	(Obrigatória) `s3:PutBucketOwnershipControls`	Obrigatória para remover a configuração de propriedade do objeto de um bucket do S3. Após a remoção, a configuração de propriedade do objeto torna-se `Object writer`.
DeleteBucketPolicy	(Obrigatória) `s3:DeleteBucketPolicy`	Obrigatória para excluir a política de um bucket do S3.

Operações de API	Ações de políticas	Descrição das ações de política
DeleteBucketReplication	(Obrigatória) `s3:PutReplicationConfiguration`	Obrigatória para excluir a configuração de replicação de um bucket do S3.
DeleteBucketTagging	(Obrigatória) `s3:PutBucketTagging`	Obrigatória para excluir tags de um bucket do S3.
DeleteBucketWebsite	(Obrigatória) `s3:DeleteBucketWebsite`	Obrigatória para remover a configuração do site de um bucket do S3.
DeletePublicAccessBlock (nível de bucket)	(Obrigatória) `s3:PutBucketPublicAccessBlock`	Obrigatória para remover a configuração do Bloqueio de Acesso Público de um bucket do S3.
GetBucketAccelerateConfiguration	(Obrigatória) `s3:GetAccelerateConfiguration`	Obrigatória para usar o sub-recurso de aceleração para exibir o estado da Aceleração de Transferências do Amazon S3 de um bucket, que é Habilitado ou Suspenso.
GetBucketAcl	(Obrigatória) `s3:GetBucketAcl`	Obrigatória para exibir uma lista de controle de acesso (ACL) de um bucket do S3.
GetBucketAnalyticsConfiguration	(Obrigatória) `s3:GetAnalyticsConfiguration`	Obrigatória para exibir uma configuração de analytics identificada pelo ID de configuração de analytics de um bucket do S3.

Operações de API	Ações de políticas	Descrição das ações de política
GetBucketCors	(Obrigatória) `s3:GetBucketCORS`	Obrigatória para exibir a configuração de compartilhamento de recursos entre origens (CORS) de um bucket do S3.
GetBucketEncryption	(Obrigatória) `s3:GetEncryptionConfiguration`	Obrigatória para exibir a configuração de criptografia padrão de um bucket do S3.
GetBucketIntelligentTieringConfiguration	(Obrigatória) `s3:GetIntelligentTieringConfiguration`	Obrigatória para obter a configuração existente do S3 Intelligent-Tiering de um bucket do S3.
GetBucketInventoryConfiguration	(Obrigatória) `s3:GetInventoryConfiguration`	Obrigatória para exibir uma configuração de inventário identificada pelo ID de configuração de inventário do bucket.
GetBucketLifecycle	(Obrigatória) `s3:GetLifecycleConfiguration`	Obrigatória para exibir a configuração de ciclo de vida do S3 do bucket.
GetBucketLocation	(Obrigatória) `s3:GetBucketLocation`	Obrigatória para exibir a Região da AWS onde reside um bucket do S3.
GetBucketLogging	(Obrigatória) `s3:GetBucketLogging`	Obrigatória para exibir o status do registro em log de um bucket do S3 e as permissões que os usuários têm para visualizar e modificar esse status.

Operações de API	Ações de políticas	Descrição das ações de política
GetBucketMetadataTableConfiguration	(Obrigatória) `s3:GetBucketMetadataTableConfiguration`	Necessária para recuperar uma configuração de tabelas de metadados para um bucket de uso geral.
GetBucketMetricsConfiguration	(Obrigatória) `s3:GetMetricsConfiguration`	Obrigatória para obter a configuração de uma métrica especificada pelo ID da configuração de métricas do bucket.
GetBucketNotificationConfiguration	(Obrigatória) `s3:GetBucketNotification`	Obrigatória para exibir a configuração de notificação de um bucket do S3.
GetBucketOwnershipControls	(Obrigatória) `s3:GetBucketOwnershipControls`	Obrigatória para recuperar a configuração de propriedade do objeto de um bucket do S3.
GetBucketPolicy	(Obrigatória) `s3:GetBucketPolicy`	Obrigatória para exibir a política de um bucket do S3.
GetBucketPolicyStatus	(Obrigatória) `s3:GetBucketPolicyStatus`	Obrigatória para recuperar o status da política de um bucket do S3 que indica se o bucket é público.
GetBucketReplication	(Obrigatória) `s3:GetReplicationConfiguration`	Obrigatória para exibir a configuração de replicação de um bucket do S3.
GetBucketRequestPayment	(Obrigatória) `s3:GetBucketRequestPayment`	Obrigatória para exibir a configuração de pagamento de solicitação de um bucket do S3.

Operações de API	Ações de políticas	Descrição das ações de política
GetBucketVersioning	(Obrigatória) `s3:GetBucketVersioning`	Obrigatória para exibir o estado de versionamento de um bucket do S3.
GetBucketTagging	(Obrigatória) `s3:GetBucketTagging`	Obrigatória para exibir o conjunto de tags associado a um bucket do S3.
GetBucketWebsite	(Obrigatória) `s3:GetBucketWebsite`	Obrigatória para exibir a configuração do site de um bucket do S3.
GetObjectLockConfiguration	(Obrigatória) `s3:GetBucketObjectLockConfiguration`	Obrigatória para obter a configuração do Bloqueio de Objetos de um bucket do S3.
GetPublicAccessBlock (nível de bucket)	(Obrigatória) `s3:GetBucketPublicAccessBlock`	Obrigatória para recuperar a configuração do Bloqueio de Acesso Público de um bucket do S3.
HeadBucket	(Obrigatória) `s3:ListBucket`	Obrigatória para determinar se existe um bucket e se você tem permissão para acessá-lo.
ListBucketAnalyticsConfigurations	(Obrigatória) `s3:GetAnalyticsConfiguration`	Obrigatória para listar as configurações de analytics de um bucket do S3.
ListBucketIntelligentTieringConfigurations	(Obrigatória) `s3:GetIntelligentTieringConfiguration`	Obrigatória para listar as configurações do S3 Intelligent-Tiering de um bucket do S3.

Operações de API	Ações de políticas	Descrição das ações de política
ListBucketInventoryConfigurations	(Obrigatória) `s3:GetInventoryConfiguration`	Obrigatória para exibir uma lista de configurações de inventário de um bucket do S3.
ListBucketMetricsConfigurations	(Obrigatória) `s3:GetMetricsConfiguration`	Obrigatória para listar as configurações de métricas de um bucket do S3.
ListObjects	(Obrigatória) `s3:ListBucket`	Obrigatória para listar alguns ou todos os objetos (até mil) de um bucket do S3.
	(Obrigatória em determinadas condições) `s3:GetObjectAcl`	Obrigatória se você quiser exibir informações do proprietário do objeto.
ListObjectsV2	(Obrigatória) `s3:ListBucket`	Obrigatória para listar alguns ou todos os objetos (até mil) de um bucket do S3.
	(Obrigatória em determinadas condições) `s3:GetObjectAcl`	Obrigatória se você quiser exibir informações do proprietário do objeto.
ListObjectVersions	(Obrigatória) `s3:ListBucketVersions`	Obrigatória para obter metadados sobre todas as versões de objetos em um bucket do S3.
PutBucketAccelerateConfiguration	(Obrigatória) `s3:PutAccelerateConfiguration`	Obrigatória para definir a configuração de aceleração de um bucket existente.

Operações de API	Ações de políticas	Descrição das ações de política
PutBucketAcl	(Obrigatória) `s3:PutBucketAcl`	Obrigatória para usar listas de controle de acesso (ACLs) e definir as permissões em um bucket existente.
PutBucketAnalyticsConfiguration	(Obrigatória) `s3:PutAnalyticsConfiguration`	Obrigatória para definir uma configuração de analytics de um bucket do S3.
PutBucketCors	(Obrigatória) `s3:PutBucketCORS`	Obrigatório para definir a configuração de compartilhamento de recursos entre origens (CORS) de um bucket do S3.
PutBucketEncryption	(Obrigatória) `s3:PutEncryptionConfiguration`	Obrigatória para configurar a criptografia padrão de um bucket do S3.
PutBucketIntelligentTieringConfiguration	(Obrigatória) `s3:PutIntelligentTieringConfiguration`	Obrigatória para obter a configuração do S3 Intelligent-Tiering de um bucket do S3.
PutBucketInventoryConfiguration	(Obrigatória) `s3:PutInventoryConfiguration`	Obrigatória para adicionar uma configuração de inventário a um bucket do S3.
PutBucketLifecycle	(Obrigatória) `s3:PutLifecycleConfiguration`	Obrigatória para criar uma configuração de ciclo de vida do S3 ou substituir uma configuração de ciclo de vida existente de um bucket do S3.

Operações de API	Ações de políticas	Descrição das ações de política
PutBucketLogging	(Obrigatória) `s3:PutBucketLogging`	Obrigatória para definir os parâmetros de registro em log de um bucket do S3 e especificar permissões para quem pode visualizar e modificar os parâmetros de registro em log.
PutBucketMetricsConfiguration	(Obrigatória) `s3:PutMetricsConfiguration`	Obrigatória para definir ou atualizar uma configuração de métricas de solicitação do Amazon CloudWatch de um bucket do S3.
PutBucketNotificationConfiguration	(Obrigatória) `s3:PutBucketNotification`	Obrigatória para habilitar notificações de eventos especificados para um bucket do S3.
PutBucketOwnershipControls	(Obrigatória) `s3:PutBucketOwnershipControls`	Obrigatória para criar ou modificar a configuração de propriedade do objeto de um bucket do S3.
PutBucketPolicy	(Obrigatória) `s3:PutBucketPolicy`	Obrigatória para aplicar uma política de bucket do S3 a um bucket.
PutBucketReplication	(Obrigatória) `s3:PutReplicationConfiguration`	Obrigatória para criar uma configuração de replicação ou substituir uma existente por um bucket do S3.

Operações de API	Ações de políticas	Descrição das ações de política
PutBucketRequestPayment	(Obrigatória) `s3:PutBucketRequestPayment`	Obrigatória para definir a configuração de pagamento de solicitação de um bucket.
PutBucketTagging	(Obrigatória) `s3:PutBucketTagging`	Obrigatória para adicionar um conjunto de tags a um bucket do S3.
PutBucketVersioning	(Obrigatória) `s3:PutBucketVersioning`	Obrigatória para definir o estado de versionamento de um bucket do S3.
PutBucketWebsite	(Obrigatória) `s3:PutBucketWebsite`	Obrigatória para configurar um bucket como um site e definir a configuração do site.
PutObjectLockConfiguration	(Obrigatória) `s3:PutBucketObjectLockConfiguration`	Obrigatória para aplicar a configuração do Bloqueio de Objetos de um bucket do S3.
PutPublicAccessBlock (nível de bucket)	(Obrigatória) `s3:PutBucketPublicAccessBlock`	Obrigatória para criar ou modificar a configuração do Bloqueio de Acesso Público de um bucket do S3.

Permissões e operações do objeto

As operações de objeto são operações de API do S3 que atuam no tipo de recurso do objeto. É necessário especificar ações de política do S3 para operações de objeto em políticas baseadas em recursos (como políticas de bucket, políticas de ponto de acesso, políticas de ponto de acesso multirregional, políticas de endpoint da VPC) ou políticas baseadas em identidade do IAM.

Nas políticas, o elemento `Resource` deve ser o ARN do objeto. Para ter mais informações sobre o formato do elemento `Resource` e políticas de exemplo, consulte Operações com objetos.

Note

- As ações de política do AWS KMS (`kms:GenerateDataKey` e `kms:Decrypt`) são aplicáveis somente ao tipo de recurso do AWS KMS e devem ser especificadas em políticas baseadas em identidade do IAM e nas políticas baseadas em recursos do AWS KMS (políticas de chave do AWS KMS). Não é possível especificar ações de política do AWS KMS em políticas baseadas em recursos do S3, como políticas de bucket do S3.
- Ao usar pontos de acesso para controlar o acesso a operações de objeto, é possível usar políticas de ponto de acesso. Para conceder permissões a operações de objeto em políticas de ponto de acesso, observe o seguinte:
  - Em políticas de ponto de acesso que concedem permissões a operações de objeto, o elemento `Resource` deve ser os ARNs para objetos acessados por meio de um ponto de acesso. Para ter mais informações sobre o formato do elemento `Resource` e políticas de exemplo, consulte Operações de objetos em políticas de ponto de acesso.
  - Nem todas as operações de objeto são compatíveis com pontos de acesso. Para obter mais informações, consulte Compatibilidade de pontos de acesso com operações do S3.
- Nem todas as operações de objeto são compatíveis com pontos de acesso multirregionais. Para obter mais informações, consulte Compatibilidade de pontos de acesso multirregionais com operações do S3.

Veja a seguir a correlação entre as operações de bucket e as ações de política obrigatórias.

Operações de API	Ações de políticas	Descrição das ações de política
AbortMultipartUpload	(Obrigatória) `s3:AbortMultipartUpload`	Obrigatória para interromper um carregamento fracionado.
CompleteMultipartUpload	(Obrigatória) `s3:PutObject`	Obrigatória para concluir o carregamento fracionado.
	(Obrigatória em determinadas condições) `kms:Decrypt`	Obrigatória se você quiser concluir um carregamento fracionado para um objeto criptografado com uma chave

Operações de API	Ações de políticas	Descrição das ações de política
		do AWS KMS gerenciada pelo cliente.
CopyObject	Para um objeto de origem:	Para um objeto de origem:
	(Obrigatória) `s3:GetObject` ou `s3:GetObjectVersion`	• `s3:GetObject` : obrigatória se você quiser copiar um objeto do bucket de origem sem especificar `versionId` na solicitação. • `s3:GetObjectVersion` : obrigatória se você quiser copiar uma versão específica de um objeto do bucket de origem sem especificar `versionId` na solicitação.
	(Obrigatória em determinadas condições) `kms:Decrypt`	Obrigatória se você quiser copiar um objeto do bucket de origem criptografado com uma chave do AWS KMS gerenciada pelo cliente.
	Para um objeto de destino:	Para um objeto de destino:
	(Obrigatória) `s3:PutObject`	Obrigatória para colocar o objeto copiado no bucket de destino.

Operações de API	Ações de políticas	Descrição das ações de política
	(Obrigatória em determina das condições) `s3:PutObjectAcl`	Obrigatória se você quiser colocar o objeto copiado com a lista de controle de acesso (ACL) do objeto no bucket de destino ao fazer uma solicitação `CopyObject` .
	(Obrigatória em determina das condições) `s3:PutObjectTagging`	Obrigatória se você quiser colocar o objeto copiado com marcação de objeto no bucket de destino ao fazer uma solicitação `CopyObject` .
	(Obrigatória em determina das condições) `kms:GenerateDataKey`	Obrigatória se você quiser criptografar o objeto copiado com uma chave do AWS KMS gerenciada pelo cliente e colocá-lo no bucket de destino.
	(Obrigatória em determina das condições) `s3:PutObjectRetention`	Obrigatória se você quiser definir uma configuração de retenção do Bloqueio de Objetos para o novo objeto.
	(Obrigatória em determina das condições) `s3:PutObjectLegalHold`	Obrigatória se quiser colocar uma retenção legal do Bloqueio de Objetos no novo objeto.
CreateMultipartUpload	(Obrigatória) `s3:PutObject`	Obrigatória para criar um carregamento fracionado.

Operações de API	Ações de políticas	Descrição das ações de política
	(Obrigatória em determina das condições) `s3:PutObjectAcl`	Obrigatória se você quiser definir as permissões de lista de controle de acesso (ACL) para objetos carregados.
	(Obrigatória em determina das condições) `s3:PutObjectTagging`	Obrigatória se você quiser adicionar marcações de objeto ao objeto carregado.
	(Obrigatória em determina das condições) `kms:GenerateDataKey`	Obrigatória se você quiser usar uma chave do AWS KMS gerenciada pelo cliente para criptografar um objeto ao iniciar um carregamento fracionado.
	(Obrigatória em determina das condições) `s3:PutObjectRetention`	Obrigatória se você quiser definir uma configuração de retenção do Bloqueio de Objetos para o objeto carregado.
	(Obrigatória em determina das condições) `s3:PutObjectLegalHold`	Obrigatória se você quiser aplicar uma retenção legal do Bloqueio de Objetos ao objeto carregado.

Operações de API	Ações de políticas	Descrição das ações de política
DeleteObject	(Obrigatória) `s3:DeleteObject` ou `s3:DeleteObjectVersion`	• `s3:DeleteObject` : obrigatória se você quiser remover um objeto sem especificar `versionId` na solicitação. • `s3:DeleteObjectVersion` : obrigatória se você quiser remover uma versão específica de um objeto determinando `versionId` na solicitação.
	(Obrigatória em determinadas condições) `s3:BypassGovernanceRetention`	Obrigatória se você quiser excluir um objeto protegido pelo modo de governança para retenção do Bloqueio de Objetos.
DeleteObjects	(Obrigatória) `s3:DeleteObject` ou `s3:DeleteObjectVersion`	• `s3:DeleteObject` : obrigatória se você quiser remover um objeto sem especificar `versionId` na solicitação. • `s3:DeleteObjectVersion` : obrigatória se você quiser remover uma versão específica de um objeto determinando `versionId` na solicitação.

Operações de API	Ações de políticas	Descrição das ações de política
	(Obrigatória em determina das condições) `s3:Bypass GovernanceRetention`	Obrigatória se você quiser excluir objetos protegidos pelo modo de governança para retenção do Bloqueio de Objetos.
DeleteObjectTagging	(Obrigatória) `s3:Delete ObjectTagging` ou `s3:DeleteObjectVer sionTagging`	• `s3:DeleteObjectTag ging` : obrigatória se você quiser remover todo um conjunto de tags de um objeto sem especificar `versionId` na solicitação. • `s3:DeleteObjectVer sionTagging` : obrigatór ia se você quiser excluir tags de uma versão específica de um objeto determinando `versionId` na solicitação.
GetObject	(Obrigatória) `s3:GetObject` ou `s3:GetObjectVersio n`	• `s3:GetObject` : obrigatór ia se você quiser obter um objeto sem especificar `versionId` na solicitação. • `s3:GetObjectVersio n` : obrigatória se você quiser obter uma versão específica de um objeto determinando `versionId` na solicitação.

Operações de API	Ações de políticas	Descrição das ações de política
	(Obrigatória em determinadas condições) `kms:Decrypt`	Obrigatória se você quiser obter e descriptografar um objeto criptografado com uma chave do AWS KMS gerenciada pelo cliente.
	(Obrigatória em determinadas condições) `s3:GetObjectTagging`	Obrigatória se você quiser obter o conjunto de tags de um objeto ao fazer uma solicitação `GetObject` .
	(Obrigatória em determinadas condições) `s3:GetObjectLegalHold`	Obrigatória se você quiser conhecer o status atual de retenção legal do Bloqueio de Objetos de um objeto.
	(Obrigatória em determinadas condições) `s3:GetObjectRetention`	Obrigatória se você quiser recuperar as configurações de retenção do Bloqueio de Objetos de um objeto.
GetObjectAcl	(Obrigatória) `s3:GetObjectAcl` ou `s3:GetObjectVersionAcl`	• `s3:GetObjectAcl` : obrigatória se quiser obter a lista de controle de acesso (ACL) de um objeto sem especificar `versionId` na solicitação. • `s3:GetObjectVersionAcl` : obrigatória se você quiser obter a lista de controle de acesso (ACL) de um objeto especificando `versionId` na solicitação.

Operações de API	Ações de políticas	Descrição das ações de política
GetObjectAttributes	(Obrigatória) `s3:GetObject` ou `s3:GetObjectVersion`	• `s3:GetObject` : obrigatória se você quiser recuperar atributos relacionados a um objeto sem especificar `versionId` na solicitação. • `s3:GetObjectVersion` : obrigatória se quiser recuperar atributos relacionados à versão de um objeto específico sem determinar `versionId` na solicitação.
	(Obrigatória em determinadas condições) `kms:Decrypt`	Obrigatória se quiser recuperar atributos relacionados a um objeto criptografado com uma chave do AWS KMS gerenciada pelo cliente.
GetObjectLegalHold	(Obrigatória) `s3:GetObjectLegalHold`	Obrigatória para obter o status atual de retenção legal do Bloqueio de Objetos de um objeto.
GetObjectRetention	(Obrigatória) `s3:GetObjectRetention`	Obrigatória para recuperar as configurações de retenção do Bloqueio de Objetos de um objeto.

Operações de API	Ações de políticas	Descrição das ações de política
GetObjectTagging	(Obrigatória) `s3:GetObjectTagging` ou `s3:GetObjectVersionTagging`	• `s3:GetObjectTagging` : obrigatória se você quiser receber o conjunto de tags de um objeto sem especificar `versionId` na solicitação. • `s3:GetObjectVersionTagging` : obrigatória se você quiser obter as tags da versão de um objeto específico determinando `versionId` na solicitação.
GetObjectTorrent	(Obrigatória) `s3:GetObject`	Obrigatória para exibir os arquivos torrent de um objeto.
HeadObject	(Obrigatória) `s3:GetObject`	Obrigatória para recuperar metadados de um objeto sem exibir o próprio objeto.
	(Obrigatória em determinadas condições) `s3:GetObjectLegalHold`	Obrigatória se você quiser conhecer o status atual de retenção legal do Bloqueio de Objetos de um objeto.
	(Obrigatória em determinadas condições) `s3:GetObjectRetention`	Obrigatória se você quiser recuperar as configurações de retenção do Bloqueio de Objetos de um objeto.
ListMultipartUploads	(Obrigatória) `s3:ListBucketMultipartUploads`	Obrigatória para listar carregamentos fracionados em um bucket.

Operações de API	Ações de políticas	Descrição das ações de política
ListParts	(Obrigatória) `s3:ListMultipartUploadParts`	Obrigatória para listar as partes carregadas de um carregamento fracionado específico.
	(Obrigatória em determinadas condições) `kms:Decrypt`	Obrigatória se você quiser listar partes de um carregamento fracionado criptografado com uma chave do AWS KMS gerenciada pelo cliente.
PutObject	(Obrigatória) `s3:PutObject`	Obrigatória para colocar um objeto.
	(Obrigatória em determinadas condições) `s3:PutObjectAcl`	Obrigatória se você quiser colocar a lista de controle de acesso (ACL) do objeto ao fazer uma solicitação `PutObject` .
	(Obrigatória em determinadas condições) `s3:PutObjectTagging`	Obrigatória se você quiser colocar a marcação de objetos ao fazer uma solicitação `PutObject` .
	(Obrigatória em determinadas condições) `kms:GenerateDataKey`	Obrigatória se você quiser criptografar um objeto com uma chave do AWS KMSgerenciada pelo cliente .
	(Obrigatória em determinadas condições) `s3:PutObjectRetention`	Obrigatória se você quiser definir uma configuração de retenção do Bloqueio de Objetos em um objeto.

Operações de API	Ações de políticas	Descrição das ações de política
	(Obrigatória em determina das condições) `s3:PutObjectLegalHold`	Obrigatória se quiser aplicar uma retenção legal do Bloqueio de Objetos a um objeto especificado.
PutObjectAcl	(Obrigatória) `s3:PutObjectAcl` ou `s3:PutObjectVersionAcl`	• `s3:PutObjectAcl` : obrigatória se você quiser definir as permissões da lista de controle de acesso (ACL) de um objeto novo ou existente sem especificar `versionId` na solicitação. • `s3:PutObjectVersionAcl` : obrigatória se você quiser definir as permissões da lista de controle de acesso (ACL) de um objeto novo ou existente especificando `versionId` na solicitação.
PutObjectLegalHold	(Obrigatória) `s3:PutObjectLegalHold`	Obrigatória para aplicar uma configuração de retenção legal do Bloqueio de Objetos a um objeto.
PutObjectRetention	(Obrigatória) `s3:PutObjectRetention`	Obrigatória para aplicar uma configuração de retenção do Bloqueio de Objetos a um objeto.

Operações de API	Ações de políticas	Descrição das ações de política
	(Obrigatória em determina das condições) `s3:Bypass GovernanceRetention`	Obrigatória se você quiser ignorar o modo de governanç a de uma configuração de retenção do Bloqueio de Objetos.
PutObjectTagging	(Obrigatória) `s3:PutObj ectTagging` ou `s3:PutObjectVersio nTagging`	• `s3:PutObjectTaggin g` : obrigatória se você quiser definir o conjunto de tags fornecido para um objeto que já exista em um bucket sem especificar `versionId` na solicitação. • `s3:PutObjectVersio nTagging` : obrigatória se você quiser definir o conjunto de tags fornecido para um objeto que já exista em um bucket especificando `versionId` na solicitação.
RestoreObject	(Obrigatória) `s3:Restor eObject`	Obrigatória para restaurar uma cópia de um objeto arquivado.
SelectObjectContent	(Obrigatória) `s3:GetObject`	Obrigatória para filtrar o conteúdo de um objeto do S3 com base em uma declaraçã o de linguagem de consulta estruturada (SQL) simples.

Operações de API	Ações de políticas	Descrição das ações de política
	(Obrigatória em determinadas condições) `kms:Decrypt`	Obrigatória se você quiser filtrar o conteúdo de um objeto do S3 criptografado com uma chave do AWS KMS gerenciada pelo cliente.
UploadPart	(Obrigatória) `s3:PutObject`	Obrigatória para fazer upload de uma parte em um carregamento fracionado.
	(Obrigatória em determina das condições) `kms:GenerateDataKey`	Obrigatória se você quiser colocar uma parte do upload e criptografá-la com uma chave do AWS KMS gerenciada pelo cliente.
UploadPartCopy	Para um objeto de origem:	Para um objeto de origem:
	(Obrigatória) `s3:GetObject` ou `s3:GetObjectVersion`	• `s3:GetObject` : obrigatória se você quiser copiar um objeto do bucket de origem sem especificar `versionId` na solicitação. • `s3:GetObjectVersion` : obrigatória se você quiser copiar uma versão específica de um objeto do bucket de origem sem especificar `versionId` na solicitação.

Operações de API	Ações de políticas	Descrição das ações de política
	(Obrigatória em determinadas condições) `kms:Decrypt`	Obrigatória se você quiser copiar um objeto do bucket de origem criptografado com uma chave do AWS KMS gerenciada pelo cliente.
	Para a parte de destino:	Para a parte de destino:
	(Obrigatória) `s3:PutObject`	Obrigatória para fazer upload de uma parte de um carregamento fracionado no bucket de destino.
	(Obrigatória em determina das condições) `kms:Gener ateDataKey`	Obrigatória se você quiser criptografar uma parte com uma chave do AWS KMS gerenciada pelo cliente ao fazer upload da parte no bucket de destino.

Operações e permissões de ponto de acesso para buckets de uso geral

As operações de ponto de acesso são operações de API do S3 que operam no tipo de recurso de `accesspoint`. É necessário especificar ações de política do S3 para operações de ponto de acesso em políticas baseadas em identidade do IAM, não em políticas de bucket ou políticas de ponto de acesso.

Nas políticas, o elemento `Resource` deve ser o ARN do `accesspoint`. Para ter mais informações sobre o formato do elemento `Resource` e políticas de exemplo, consulte Operações de ponto de acesso para buckets de uso geral.

> **Note**
>
> Se quiser usar pontos de acesso para controlar o acesso a operações de bucket ou de objeto, observe o seguinte:

- Quanto ao uso de pontos de acesso para controlar o acesso a operações de bucket, consulte Operações de bucket em políticas de ponto de acesso para buckets de uso geral.
- Quanto ao uso de pontos de acesso para controlar o acesso a operações de objeto, consulte Operações de objetos em políticas de ponto de acesso.
- Consulte mais informações sobre como configurar políticas de ponto de acesso em Configurar políticas do IAM para uso de pontos de acesso.

Veja a seguir a correlação entre as operações de ponto de acesso e as ações de política obrigatórias.

Operações de API	Ações de políticas	Descrição das ações de política
CreateAccessPoint	(Obrigatória) `s3:CreateAccessPoint`	Obrigatória para criar um ponto de acesso associado a um bucket do S3.
DeleteAccessPoint	(Obrigatória) `s3:DeleteAccessPoint`	Obrigatória para excluir um ponto de acesso.
DeleteAccessPointPolicy	(Obrigatória) `s3:DeleteAccessPointPolicy`	Obrigatória para excluir uma política de ponto de acesso.
GetAccessPointPolicy	(Obrigatória) `s3:GetAccessPointPolicy`	Obrigatória para recuperar uma política de ponto de acesso.
GetAccessPointPolicyStatus	(Obrigatória) `s3:GetAccessPointPolicyStatus`	Obrigatória para recuperar as informações sobre se o ponto de acesso especificado no momento tem uma política que permita o acesso público.
PutAccessPointPolicy	(Obrigatória) `s3:PutAccessPointPolicy`	Obrigatória para aplicar uma política de ponto de acesso.

Permissões e operações de ponto de acesso do Object Lambda

As operações de ponto de acesso do Object Lambda são operações de API do S3 que operam no tipo de recurso `objectlambdaaccesspoint`. Consulte mais informações sobre como configurar políticas de operações de ponto de acesso do Object Lambda em Configurar políticas do IAM para pontos de acesso do Object Lambda.

Veja a seguir a correlação entre as operações de ponto de acesso do Object Lambda e as ações de política obrigatórias.

Operações de API	Ações de políticas	Descrição das ações de política
CreateAccessPointForObjectLambda	(Obrigatória) `s3:CreateAccessPointForObjectLambda`	Obrigatória para criar um ponto de acesso do Object Lambda.
DeleteAccessPointForObjectLambda	(Obrigatória) `s3:DeleteAccessPointForObjectLambda`	Obrigatória para excluir um ponto de acesso do Object Lambda especificado.
DeleteAccessPointPolicyForObjectLambda	(Obrigatória) `s3:DeleteAccessPointPolicyForObjectLambda`	Obrigatória para excluir a política em um ponto de acesso do Object Lambda especificado.
GetAccessPointConfigurationForObjectLambda	(Obrigatória) `s3:GetAccessPointConfigurationForObjectLambda`	Obrigatória para recuperar a configuração do ponto de acesso do Object Lambda.
GetAccessPointForObjectLambda	(Obrigatória) `s3:GetAccessPointForObjectLambda`	Obrigatória para recuperar informações sobre o ponto de acesso do Object Lambda.
GetAccessPointPolicyForObjectLambda	(Obrigatória) `s3:GetAccessPointPolicyForObjectLambda`	Obrigatória para exibir a política associada ao ponto de acesso do Object Lambda especificado.

Operações de API	Ações de políticas	Descrição das ações de política
GetAccessPointPolicyStatusForObjectLambda	(Obrigatória) `s3:GetAccessPointPolicyStatusForObjectLambda`	Obrigatória para exibir o status de uma política de ponto de acesso específica do Object Lambda.
PutAccessPointConfigurationForObjectLambda	(Obrigatória) `s3:PutAccessPointConfigurationForObjectLambda`	Obrigatória para definir a configuração do ponto de acesso do Object Lambda.
PutAccessPointPolicyForObjectLambda	(Obrigatória) `s3:PutAccessPointPolicyForObjectLambda`	Obrigatória para associar uma política de acesso a um ponto de acesso especificado do Object Lambda.

Operações e permissões de ponto de acesso multirregional

As operações de ponto de acesso multirregional são operações de API do S3 que operam no tipo de recurso `multiregionaccesspoint`. Consulte mais informações sobre como configurar políticas de operações de ponto de acesso multirregionais em Exemplos de políticas de pontos de acesso multirregionais.

Veja a seguir a correlação entre as operações de ponto de acesso multirregional e as ações de política obrigatórias.

Operações de API	Ações de políticas	Descrição das ações de política
CreateMultiRegionAccessPoint	(Obrigatória) `s3:CreateMultiRegionAccessPoint`	Obrigatória para criar um ponto de acesso multirregional e associá-lo aos buckets do S3.

Operações de API	Ações de políticas	Descrição das ações de política
DeleteMultiRegionAccessPoint	(Obrigatória) `s3:DeleteMultiRegionAccessPoint`	Obrigatória para excluir um ponto de acesso multirregional.
DescribeMultiRegionAccessPointOperation	(Obrigatória) `s3:DescribeMultiRegionAccessPointOperation`	Obrigatória para recuperar o status de uma solicitação assíncrona e gerenciar um ponto de acesso multirregional.
GetMultiRegionAccessPoint	(Obrigatória) `s3:GetMultiRegionAccessPoint`	Obrigatória para exibir informações de configuração sobre o ponto de acesso multirregional especificado.
GetMultiRegionAccessPointPolicy	(Obrigatória) `s3:GetMultiRegionAccessPointPolicy`	Obrigatória para exibir a política de controle de acesso do ponto de acesso multirregional especificado.
GetMultiRegionAccessPointPolicyStatus	(Obrigatória) `s3:GetMultiRegionAccessPointPolicyStatus`	Obrigatória para exibir o status da política de um ponto de acesso multirregional específico, sobre se esse ponto de acesso tem uma política de controle de acesso que permita o acesso público.
GetMultiRegionAccessPointRoutes	(Obrigatória) `s3:GetMultiRegionAccessPointRoutes`	Obrigatória para exibir a configuração de roteamento de um ponto de acesso multirregional.

Operações de API	Ações de políticas	Descrição das ações de política
PutMultiRegionAccessPointPolicy	(Obrigatória) `s3:PutMultiRegionAccessPointPolicy`	Obrigatória para atualizar a política de controle de acesso do ponto de acesso multirregional especificado.
SubmitMultiRegionAccessPointRoutes	(Obrigatória) `s3:SubmitMultiRegionAccessPointRoutes`	Obrigatória para enviar uma configuração de rota atualizada de um ponto de acesso multirregional.

Operações e permissões de trabalho em lote

As operações de trabalho (operações em lote) são operações de API do S3 que operam no tipo de recurso `job`. É necessário especificar as ações de política do S3 para operações de trabalho em políticas baseadas em identidade do IAM, não em políticas de bucket.

Nas políticas, o elemento `Resource` deve ser o ARN do `job`. Para ter mais informações sobre o formato do elemento `Resource` e políticas de exemplo, consulte Operações de trabalho em lote.

Veja a seguir a correlação entre as operações de trabalho em lote e as ações de política obrigatórias.

Operações de API	Ações de políticas	Descrição das ações de política
DeleteJobTagging	(Obrigatória) `s3:DeleteJobTagging`	Obrigatória para remover tags de um trabalho existente de Operações em Lote do S3.
DescribeJob	(Obrigatória) `s3:DescribeJob`	Obrigatória para recuperar os parâmetros de configuração e o status de um trabalho de operações em lote.
GetJobTagging	(Obrigatória) `s3:GetJobTagging`	Obrigatória para exibir o conjunto de tags de

Operações de API	Ações de políticas	Descrição das ações de política
		um trabalho existente de Operações em Lote do S3.
PutJobTagging	(Obrigatória) `s3:PutJobTagging`	Obrigatória para aplicar ou substituir tags de um trabalho existente de Operações em Lote do S3.
UpdateJobPriority	(Obrigatória) `s3:UpdateJobPriority`	Obrigatória para atualizar a prioridade de um trabalho existente.
UpdateJobStatus	(Obrigatória) `s3:UpdateJobStatus`	Obrigatória para atualizar o status do trabalho especific ado.

Operações e permissões de configuração da Lente de Armazenamento do S3

As operações de configuração da Lente de Armazenamento do S3 são operações de API do S3 que operam no tipo de recurso `storagelensconfiguration`. Consulte mais informações sobre como definir as operações de configuração do Lente de Armazenamento do S3 em Configurar permissões da Lente de Armazenamento do Amazon S3.

Veja a seguir a correlação entre as operações de configuração da Lente de Armazenamento do S3 e as ações de política obrigatórias.

Operações de API	Ações de políticas	Descrição das ações de política
DeleteStorageLensConfiguration	(Obrigatória) `s3:DeleteStorageLensConfiguration`	Obrigatória para excluir a configuração da Lente de Armazenamento do S3.

Operações de API	Ações de políticas	Descrição das ações de política
DeleteStorageLensConfigurationTagging	(Obrigatória) `s3:DeleteStorageLensConfigurationTagging`	Obrigatória para excluir as tags de configuração da Lente de Armazenamento do S3.
GetStorageLensConfiguration	(Obrigatória) `s3:GetStorageLensConfiguration`	Obrigatória para obter a configuração da Lente de Armazenamento do S3.
GetStorageLensConfigurationTagging	(Obrigatória) `s3:GetStorageLensConfigurationTagging`	Obrigatória para obter a configuração da Lente de Armazenamento do S3.
PutStorageLensConfigurationTagging	(Obrigatória) `s3:PutStorageLensConfigurationTagging`	Obrigatória para aplicar ou substituir tags em uma configuração existente da Lente de Armazenamento do S3.

Operações e permissões de grupos da Lente de Armazenamento do S3

As operações de grupos da Lente de Armazenamento do S3 são operações de API do S3 que operam no tipo de recurso `storagelensgroup`. Para ter mais informações sobre como configurar as operações de grupos da Lente de Armazenamento do S3, consulte Permissões de grupos de Lente de Armazenamento.

Veja a seguir a correlação entre as operações de grupos da Lente de Armazenamento do S3 e as ações de política obrigatórias.

Operações de API	Ações de políticas	Descrição das ações de política
DeleteStorageLensGroup	(Obrigatória) `s3:DeleteStorageLensGroup`	Obrigatória para excluir um grupo existente da Lente de Armazenamento do S3.

Operações de API	Ações de políticas	Descrição das ações de política
GetStorageLensGroup	(Obrigatória) `s3:GetStorageLensGroup`	Obrigatória para recuperar os detalhes da configuração da Lente de Armazenamento do S3.
UpdateStorageLensGroup	(Obrigatória) `s3:UpdateStorageLensGroup`	Obrigatória para atualizar o grupo existente da Lente de Armazenamento do S3.
CreateStorageLensGroup	(Obrigatória) `s3:CreateStorageLensGroup`	Necessária para criar um grupo da Lente de Armazenamento.
CreateStorageLensGroup, TagResource	(Obrigatórias) `s3:CreateStorageLensGroup` e `s3:TagResource`	Necessária para criar um grupo da Lente de Armazenamento com tags.
ListStorageLensGroups	(Obrigatória) `s3:ListStorageLensGroups`	Necessária para listar todos os grupos da Lente de Armazenamento na região de origem.
ListTagsForResource	(Obrigatória) `s3:ListTagsForResource`	Necessária para listar as tags que foram adicionadas ao grupo da Lente de Armazenamento.
TagResource	(Obrigatória) `s3:TagResource`	Necessária para adicionar ou atualizar uma tag para um grupo da Lente de Armazenamento existente.
UntagResource	(Obrigatória) `s3:UntagResource`	Necessária para excluir uma tag de um grupo da Lente de Armazenamento.

Operações e permissões de instância da funcionalidade Concessão de Acesso do S3

As operações de instância da Concessão de Acesso do S3 são operações de API do S3 que operam no tipo de recurso `accessgrantsinstance`. Uma instância da Concessão de Acesso do S3 é um contêiner lógico para concessões de acesso. Consulte mais informações sobre como trabalhar com instâncias da Concessão de Acesso do S3 em Trabalhar com instâncias do recurso Concessão de Acesso do S3.

Veja a seguir o mapeamento das operações de configuração de instância da Concessão de Acesso do S3 e as ações de política obrigatórias.

Operações de API	Ações de políticas	Descrição das ações de política
AssociateAccessGrantsIdentityCenter	(Obrigatória) `s3:AssociateAccessGrantsIdentityCenter`	Necessário para associar uma instância do AWS IAM Identity Center à instância da Concessão de Acesso do S3 e permitir a criação de concessões de acesso para usuários e grupos no diretório de identidades corporativas. Você também deve ter as seguintes permissões: `sso:CreateApplication` , `sso:PutApplicationGrant` e `sso:PutApplicationAuthenticationMethod` .
CreateAccessGrantsInstance	(Obrigatória) `s3:CreateAccessGrantsInstance`	Necessário para criar uma instância da Concessão de Acesso do S3 (recurso `accessgrantsinstance`) que é um contêiner

Operações de API	Ações de políticas	Descrição das ações de política
		para concessões de acesso individuais. Para associar uma instância do AWS IAM Identity Center à instância da Concessão de Acesso do S3, você também deve ter as permissões `sso:DescribeInstance` , `sso:CreateApplication` , `sso:PutApplicationGrant` e `sso:PutApplicationAuthenticationMethod` .
DeleteAccessGrantsInstance	(Obrigatória) `s3:DeleteAccessGrantsInstance`	Necessário para excluir uma instância da Concessão de Acesso do S3 (recurso `accessgrantsinstance`) de uma Região da AWS na conta.
DeleteAccessGrantsInstanceResourcePolicy	(Obrigatória) `s3:DeleteAccessGrantsInstanceResourcePolicy`	Necessário para excluir uma política de recurso da instância da Concessão de Acesso do S3.

Operações de API	Ações de políticas	Descrição das ações de política
DissociateAccessGrantsIdentityCenter	(Obrigatória) `s3:DissociateAccessGrantsIdentityCenter`	Necessário para desassociar uma instância do AWS IAM Identity Center da instância da Concessão de Acesso do S3. Você também deve ter as seguintes permissões: `sso:DeleteApplication`
GetAccessGrantsInstance	(Obrigatória) `s3:GetAccessGrantsInstance`	Necessário para recuperar a instância da Concessão de Acesso do S3 para uma Região da AWS na conta.
GetAccessGrantsInstanceForPrefix	(Obrigatória) `s3:GetAccessGrantsInstanceForPrefix`	Necessário para recuperar a instância da Concessão de Acesso do S3 que contém um prefixo específico.
GetAccessGrantsInstanceResourcePolicy	(Obrigatória) `s3:GetAccessGrantsInstanceResourcePolicy`	Necessário para retornar a política de recursos da instância da Concessão de Acesso do S3.
ListAccessGrantsInstances	(Obrigatória) `s3:ListAccessGrantsInstances`	Necessário para retornar uma lista das instâncias da Concessão de Acesso do S3 na conta.
PutAccessGrantsInstanceResourcePolicy	(Obrigatória) `s3:PutAccessGrantsInstanceResourcePolicy`	Necessário para atualizar a política de recurso da instância da Concessão de Acesso do S3.

Operações e permissões de localização da Concessão de Acesso do S3

As operações de localização da Concessão de Acesso do S3 são operações de API do S3 que operam no tipo de recurso `accessgrantslocation`. Consulte mais informações sobre como trabalhar com localizações da Concessão de Acesso do S3 em Trabalhar com locais do recurso Concessão de Acesso do S3.

Veja a seguir o mapeamento das operações de configuração de localização da Concessão de Acesso do S3 e as ações de política obrigatórias.

Operações de API	Ações de políticas	Descrição das ações de política
CreateAccessGrantsLocation	(Obrigatória) `s3:CreateAccessGrantsLocation`	Necessário para registrar uma localização na instância da Concessão de Acesso do S3 (criar um recurso `accessgrantslocation`). Você também deve ter a seguinte permissão para o perfil do IAM especificado: `iam:PassRole`
DeleteAccessGrantsLocation	(Obrigatória) `s3:DeleteAccessGrantsLocation`	Necessário para remover uma localização registrada da instância da Concessão de Acesso do S3.
GetAccessGrantsLocation	(Obrigatória) `s3:GetAccessGrantsLocation`	Necessário para recuperar os detalhes de uma localização específica registrada na instância da Concessão de Acesso do S3.
ListAccessGrantsLocations	(Obrigatória) `s3:ListAccessGrantsLocations`	Necessário para retornar uma lista das localizações registrad

Operações de API	Ações de políticas	Descrição das ações de política
		as na instância da Concessão de Acesso do S3.
UpdateAccessGrantsLocation	(Obrigatória) `s3:UpdateAccessGrantsLocation`	Necessário para atualizar o perfil do IAM de um local registrado na instância da Concessão de Acesso do S3.

Operações e permissões de concessão do recurso Concessão de Acesso do S3

As operações de concessão da funcionalidade Concessão de Acesso do S3 são operações de API do S3 que operam no tipo de recurso `accessgrant`. Consulte mais informações sobre como trabalhar com concessões individuais usando a Concessão de Acesso do S3 em Trabalhar com concessões no recurso Concessão de Acesso do S3.

Veja a seguir o mapeamento das operações de configuração de concessão da funcionalidade Concessão de Acesso do S3 e as ações de política obrigatórias.

Operações de API	Ações de políticas	Descrição das ações de política
CreateAccessGrant	(Obrigatória) `s3:CreateAccessGrant`	Necessário para criar uma concessão individual (recurso `accessgrant`) para um usuário ou grupo na instância da Concessão de Acesso do S3. Você também deve ter as seguintes permissões: Para qualquer identidade de diretório: `sso:DescribeInstance` e `sso:DescribeApplication`

Operações de API	Ações de políticas	Descrição das ações de política
		Para usuários do diretório : `identitystore:DescribeUser`
DeleteAccessGrant	(Obrigatória) `s3:DeleteAccessGrant`	Necessário para excluir uma concessão de acesso individual (recurso `accessgrant`) da instância da Concessão de Acesso do S3.
GetAccessGrant	(Obrigatória) `s3:GetAccessGrant`	Necessário para obter os detalhes sobre uma concessão de acesso individual na instância da Concessão de Acesso do S3.
ListAccessGrants	(Obrigatória) `s3:ListAccessGrants`	Necessário para retornar uma lista de concessões de acesso individuais na instância da Concessão de Acesso do S3.
ListCallerAccessGrants	(Obrigatória) `s3:ListCallerAccessGrants`	Necessário para listar as concessões de acesso que concedem ao chamador acesso aos dados do Amazon S3 por meio da Concessão de Acesso do S3.

Permissões e operações de conta

As operações da conta são operações de API do S3 que operam no nível da conta. A conta não é um tipo de recurso definido pelo Amazon S3. É necessário especificar ações de política do S3 para operações de conta em políticas baseadas em identidade do IAM, não em políticas de bucket.

Nas políticas, o elemento `Resource` deve ser `"*"`. Para ter mais informações sobre políticas de exemplo, consulte Operações de conta.

Veja a seguir a correlação entre as operações de conta e as ações de política obrigatórias.

Operações de API	Ações de políticas	Descrição das ações de política
CreateJob	(Obrigatória) `s3:CreateJob`	Obrigatória para criar um trabalho de Operações em Lote do S3.
CreateStorageLensGroup	(Obrigatória) `s3:CreateStorageLensGroup`	Obrigatória para criar um grupo de lentes da Lente de Armazenamento do S3 e associá-lo ao ID da Conta da AWS especificado.
	(Obrigatória em determinadas condições) `s3:TagResource`	Obrigatória se você quiser criar um grupo da Lente de Armazenamento do S3 com tags de recursos da AWS.
DeletePublicAccessBlock (nível de conta)	(Obrigatória) `s3:PutAccountPublicAccessBlock`	Obrigatória para remover a configuração do Bloqueio de Acesso Público de uma Conta da AWS.
GetAccessPoint	(Obrigatória) `s3:GetAccessPoint`	Obrigatória para recuperar informações de configuração sobre o ponto de acesso especificado.
GetAccessPointPolicy (nível de conta)	(Obrigatória) `s3:GetAccountPublicAccessBlock`	Obrigatória para recuperar a configuração do Bloqueio de Acesso Público de uma Conta da AWS.

Operações de API	Ações de políticas	Descrição das ações de política
ListAccessPoints	(Obrigatória) `s3:ListAccessPoints`	Obrigatória para listar os pontos de acesso de um bucket do S3 que pertencem a uma Conta da AWS.
ListAccessPointsForObjectLambda	(Obrigatória) `s3:ListAccessPointsForObjectLambda`	Obrigatória para listar os pontos de acesso do Object Lambda.
ListBuckets	(Obrigatória) `s3:ListAllMyBuckets`	Obrigatória para exibir uma lista de todos os buckets pertencentes ao remetente autenticado da solicitação.
ListJobs	(Obrigatória) `s3:ListJobs`	Obrigatória para listar os trabalhos atuais e os trabalhos encerrados recentemente.
ListMultiRegionAccessPoints	(Obrigatória) `s3:ListMultiRegionAccessPoints`	Obrigatória para exibir uma lista dos pontos de acesso multirregionais atualmente associados ao Conta da AWS especificado.
ListStorageLensConfigurations	(Obrigatória) `s3:ListStorageLensConfigurations`	Obrigatória para obter as configurações da Lente de Armazenamento do S3 de uma Conta da AWS.
ListStorageLensGroups	(Obrigatória) `s3:ListStorageLensGroups`	Obrigatória para listar todos os grupos da Lente de Armazenamento do S3 na Região da AWS inicial especificada.

Operações de API	Ações de políticas	Descrição das ações de política
PutPublicAccessBlock (nível de conta)	(Obrigatória) `s3:PutAccountPublicAccessBlock`	Obrigatório para criar ou modificar a configuração do Bloqueio de Acesso Público de uma Conta da AWS.
PutStorageLensConfiguration	(Obrigatória) `s3:PutStorageLensConfiguration`	Obrigatória para aplicar uma configuração da Lente de Armazenamento do S3.

Políticas e permissões no Amazon S3

Esta página fornece uma visão geral do bucket e políticas de usuário no Amazon S3 e descreve os elementos básicos de uma política do AWS Identity and Access Management (IAM). Cada elemento listado vincula mais detalhes sobre esse elemento e exemplos de como usá-lo.

Consulte uma lista completa de ações, recursos e condições do Amazon S3 em Actions, resources, and condition keys for Amazon S3 na Referência de autorização do serviço.

Para ter mais informações sobre as permissões referentes a operações de API do S3 de acordo com os tipos de recurso do S3, consulte Permissões obrigatórias para operações de API do Amazon S3.

No sentido mais básico, uma política contém os seguintes elementos:

- Resource: o bucket, o objeto, o ponto de acesso ou o trabalho do Amazon S3 ao qual a política se aplica. Use o nome do recurso da Amazon (ARN) do bucket, do objeto, do ponto de acesso ou do trabalho para identificar o recurso.

  Um exemplo de operações em nível de bucket:

  `"Resource": "arn:aws:s3:::bucket_name"`

  Exemplos de operação em nível de objeto:

  - `"Resource": "arn:aws:s3:::bucket_name/*"` para todos os objetos no bucket.
  - `"Resource": "arn:aws:s3:::bucket_name/prefix/*"` para objetos com um prefixo específico no bucket.

Para obter mais informações, consulte Recursos de políticas para o Amazon S3.

- Actions: para cada recurso, o Amazon S3 comporta um conjunto de operações. Você identifica as operações de recursos que permitirão (ou negarão) usando palavras-chave de ação.

  Por exemplo, a permissão `s3:ListBucket` autoriza o usuário a usar a operação ListObjectsV2 do Amazon S3. (A permissão `s3:ListBucket` é um caso em que o nome da ação não é associado diretamente ao nome da operação.) Para obter mais informações sobre como usar ações do Amazon S3, consulte Ações de políticas para o Amazon S3. Para obter uma lista completa de ações do Amazon S3, consulte Ações na Referência de API do Amazon Simple Storage Service.

- Effect: qual será o efeito quando o usuário solicitar a ação específica: pode ser `Allow` ou `Deny`.

  Se você não conceder (permitir) explicitamente acesso a um recurso, o acesso estará implicitamente negado. Você também pode negar acesso explicitamente a um recurso. Você poderia fazer isso para garantir que um usuário não possa acessar o recurso, mesmo se uma política diferente conceder acesso. Para obter mais informações, consulte Elementos de política JSON do IAM: efeito no Guia do usuário do IAM.

- Principal: a conta ou o usuário que tem permissão de acesso a ações e recursos na declaração. Em uma política de bucket, o principal é o usuário, a conta, o serviço ou outra entidade que receba essa permissão. Para obter mais informações, consulte Entidades principais para políticas de bucket.

- Condition: condições para quando uma política está em vigor. Você pode usar chaves de toda a AWS e chaves específicas do Amazon S3 para especificar condições em uma política de acesso do Amazon S3. Para obter mais informações, consulte Exemplos de políticas de bucket usando chaves de condição.

O exemplo de política de bucket a seguir mostra os elementos `Effect`, `Principal`, `Action` e `Resource`. Essa política permite ao *`Akua`*, um usuário na conta *`123456789012`*, as permissões `s3:GetObject`, `s3:GetBucketLocation` e `s3:ListBucket` do Amazon S3 no bucket *`amzn-s3-demo-bucket1`*.

```
{
    "Version": "2012-10-17",
    "Id": "ExamplePolicy01",
    "Statement": [
        {
```

```
            "Sid": "ExampleStatement01",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::123456789012:user/Akua"
            },
            "Action": [
                "s3:GetObject",
                "s3:GetBucketLocation",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket1/*",
                "arn:aws:s3:::amzn-s3-demo-bucket1"
            ]
        }
    ]
}
```

Consulte informações completas sobre a linguagem de políticas em Políticas e permissões no IAM e em Referência de política JSON do IAM no Guia do usuário do IAM.

Delegação de permissão

Se uma Conta da AWS for proprietária de um recurso, ela poderá conceder essas permissões a outra Conta da AWS. Essa conta pode então delegar essas permissões, ou um subconjunto delas, para usuários da conta. Isso é chamado de delegação de permissão. No entanto, uma conta que recebe permissões de outra conta não pode delegar permissão entre contas para outra Conta da AWS.

Propriedade de bucket e objeto do Amazon S3

Buckets e objetos são recursos do Amazon S3. Por padrão, apenas o proprietário dos recursos pode acessá-los. O proprietário do recurso refere-se à Conta da AWS que criou o recurso. Por exemplo:

- A Conta da AWS que você usa para criar buckets e carregar objetos é a proprietária desses recursos.
- Se você carregar um objeto usando credenciais de função ou usuário do AWS Identity and Access Management (IAM), a Conta da AWS à qual o usuário ou a função pertence será proprietária do objeto.
- Um proprietário do bucket pode conceder permissões entre contas à outra Conta da AWS (ou aos usuários em outra conta) para carregar objetos. Nesse caso, a Conta da AWS que carregar

os objetos será proprietária deles. O proprietário do bucket não tem permissões nos objetos de propriedade de outras contas, com as seguintes exceções:

- O proprietário do bucket paga as faturas. O proprietário do bucket pode negar acesso a todos os objetos ou excluir objetos no bucket, independentemente de quem o possui.
- O proprietário do bucket pode arquivar todos os objetos ou restaurar os objetos arquivados, independentemente de quem os possui. Arquivo refere-se à classe de armazenamento usada para armazenar os objetos. Para obter mais informações, consulte Gerenciar o ciclo de vida dos objetos.

Autenticação de solicitação e propriedade

Todas as solicitações para um bucket são autenticadas ou não autenticadas. As solicitações autenticadas devem incluir um valor de assinatura que autentica o remetente da solicitação. Para solicitações não autenticadas, isso não é necessário. Consulte mais informações sobre a autenticação de solicitações em Making requests na Referência da API do Amazon S3.

Um proprietário do bucket pode permitir solicitações não autenticadas. Por exemplo, solicitações PutObject não autenticadas são permitidas quando um bucket tem uma política pública de bucket, ou quando uma ACL do bucket concede acesso `WRITE` ou `FULL_CONTROL` ao grupo `All Users` ou ao usuário anônimo especificamente. Para obter mais informações sobre políticas de bucket público e listas de controle de acesso (ACLs) públicas, consulte O significado de "público".

Todas as solicitações não autenticadas são feitas pelo usuário anônimo. Esse usuário é representado em ACLs pelo ID de usuário canônico específico `65a011a29cdf8ec533ec3d1ccaae921c`. Se for feito o upload de um objeto em um bucket por meio de uma solicitação não autenticada, o usuário anônimo será proprietário o objeto. A ACL padrão do objeto concede `FULL_CONTROL` ao usuário anônimo como o proprietário do objeto. Portanto, o Amazon S3 permite que solicitações não autenticadas recuperem o objeto ou modifiquem a ACL dele.

Para evitar que os objetos sejam modificados pelo usuário anônimo, recomendamos que você não implemente políticas de bucket que permitam gravações públicas anônimas em seu bucket ou use ACLs que concedam ao usuário anônimo acesso de gravação ao bucket. Você pode aplicar esse comportamento recomendado usando o Bloqueio de acesso público do Amazon S3.

Para obter mais informações sobre como bloquear o acesso público, consulte Bloquear o acesso público ao armazenamento do Amazon S3. Para obter mais informações sobre ACLs, consulte Visão geral da lista de controle de acesso (ACL).

> **Important**
>
> Recomendamos que você não use credenciais de usuário raiz da Conta da AWS para fazer solicitações autenticadas. Em vez disso, crie um perfil do IAM e conceda acesso total a ele. Usuários com esse perfil são conhecidos como usuários administradores. Em vez de usar credenciais de usuário raiz da Conta da AWS, você pode usar credenciais atribuídas ao perfil administrador para interagir com a AWS e realizar tarefas, como criar um bucket, criar usuários e conceder permissões a eles. Para ter mais informações, consulte Credenciais de segurança da AWS e Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.

Políticas de bucket para o Amazon S3

Uma política de bucket é uma política baseada em recursos que você pode usar para conceder permissões de acesso ao bucket do Amazon S3 e aos objetos contidos nele. Só o proprietário do bucket pode associar uma política a um bucket. As permissões anexadas ao bucket se aplicam a todos os objetos do bucket que pertencem ao proprietário do bucket. Essas permissões não se aplicam a objetos pertencentes a outras Contas da AWS.

A Propriedade de objeto do S3 é uma configuração no nível do bucket do Amazon S3 que você pode usar para controlar a propriedade de objetos carregados no bucket e desabilitar ou habilitar as listas de controle de acesso (ACLs). Por padrão, a Propriedade de objeto está definida com a configuração Aplicada pelo proprietário do bucket e todas as ACLs estão desabilitadas. O proprietário do bucket possui todos os objetos do bucket e gerencia o acesso aos dados exclusivamente usando políticas.

As políticas de bucket usam uma linguagem de política do AWS Identity and Access Management (IAM) baseada em JSON. Você pode usar políticas de bucket para adicionar ou negar permissões para os objetos em um bucket. As políticas de bucket permitem ou negam solicitações com base nos elementos da política. Esses elementos incluem o solicitante, ações do S3, recursos e aspectos ou condições da solicitação (como o endereço IP usado para fazer a solicitação).

Por exemplo, você pode criar uma política de bucket que faça o seguinte:

- Concede a outras contas permissões entre contas para fazer upload de objetos em seu bucket do S3
- Garante que você, o proprietário do bucket, tenha controle total dos objetos enviados

Para obter mais informações, consulte Exemplos de políticas de bucket do Amazon S3.

> **Important**
>
> Você não pode usar uma política de bucket para evitar exclusões ou transições por meio de uma regra de ciclo de vida do S3. Por exemplo, mesmo que a política de bucket negue todas as ações para todas as entidades principais, a configuração do ciclo de vida do S3 ainda funcionará normalmente.

Os tópicos nesta seção fornecem exemplos e mostram como adicionar uma política de bucket no console do S3. Consulte mais informações sobre políticas baseadas em identidade em Políticas baseadas em identidade do Amazon S3. Para obter informações sobre a linguagem da política de bucket, consulte Políticas e permissões no Amazon S3.

Para ter mais informações sobre as permissões referentes a operações de API do S3 de acordo com os tipos de recurso do S3, consulte Permissões obrigatórias para operações de API do Amazon S3.

Tópicos

- Adicionar uma política de bucket usando o console do Amazon S3
- Controlar o acesso a partir de VPC endpoints com políticas de bucket
- Exemplos de políticas de bucket do Amazon S3
- Exemplos de políticas de bucket usando chaves de condição

Adicionar uma política de bucket usando o console do Amazon S3

Use o Gerador de Políticas da AWS e o console do Amazon S3 para adicionar uma nova política de bucket ou editar uma política de bucket existente. Uma política de bucket é uma política do AWS Identity and Access Management (IAM) baseada em recursos. Você adiciona uma política de bucket a um bucket para conceder permissões de acesso ao bucket, e aos objetos contidos nele, a outras Contas da AWS ou usuários do IAM. As permissões de objeto aplicam-se somente aos objetos criados pela proprietário do bucket. Para obter mais informações sobre políticas de bucket, consulte Gerenciamento de identidade e acesso para o Amazon S3.

Solucione avisos de segurança, erros, avisos gerais e sugestões de AWS Identity and Access Management Access Analyzer antes de salvar a política. O IAM Access Analyzer executa verificações de política para validar sua política em relação à gramática das políticas e às práticas

recomendadas do IAM. Essas verificações geram descobertas e fornecem recomendações práticas que ajudam a criar políticas que sejam funcionais e estejam em conformidade com as práticas recomendadas de segurança. Para saber mais sobre a validação de políticas usando o IAM Access Analyzer, consulte Validação de políticas do IAM Access Analyzer no Guia do usuário do IAM. Para visualizar uma lista de avisos, erros e sugestões retornados pelo IAM Access Analyzer, consulte Referência de verificação de políticas do IAM Access Analyzer.

Para obter orientação sobre como solucionar erros com uma política, consulte Solucionar erros de acesso negado (403 Forbidden) no Amazon S3.

Para criar ou editar uma política de bucket

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets de uso geral ou Buckets de diretórios.
3. Na lista de buckets, escolha o nome do bucket para o qual você deseja criar uma política de bucket ou cuja política de bucket você queira editar.
4. Escolha a aba Permissões.
5. Em Bucket policy (Política de bucket), escolha Edit (Editar). A página Edit bucket policy (Editar política de bucket) é exibida.
6. Na página Edit bucket policy (Editar política de bucket), faça uma das seguintes ações:

   - Para ver exemplos de políticas de bucket, selecione Exemplos de política. Ou consulte Exemplos de políticas de bucket do Amazon S3 no Guia do usuário do Amazon S3.
   - Para gerar uma política automaticamente ou editar o JSON na seção Policy (Política), escolha Policy generator (Gerador de políticas).

   Se você escolher Policy generator (Gerador de políticas), o Gerador de Políticas da AWS será aberto em uma nova janela.

   a. Na página Gerador de Políticas da AWS, em Selecionar tipo de política, escolha Política de bucket do S3.

   b. Adicione uma instrução inserindo as informações nos campos fornecidos e escolha Add Statement (Adicionar instrução). Repita esta etapa para todas as instruções que deseja adicionar. Para ter mais informações sobre esses campos, consulte a Referência de elementos de política JSON do IAM no Guia do usuário do IAM.

> **Note**
>
> Por conveniência, a página Editar política de bucket exibe o ARN do bucket (nome do recurso da Amazon) do bucket atual acima do campo de texto Política. Você pode copiar este ARN para usá-lo nas instruções da página do AWS Policy Generator.

c. Depois de terminar de adicionar as instruções, escolha Generate Policy (Gerar política).

d. Copie o texto da política gerada, escolha Close (Fechar) e retorne à página Edit bucket policy (Editar política de bucket) no console do Amazon S3.

7. Na caixa Policy (Política), edite a política existente ou cole a política de bucket do Gerador de Políticas da AWS. Solucione avisos de segurança, erros, avisos gerais e sugestões antes de salvar a política.

> **Note**
>
> As políticas de bucket são limitadas a 20 KB.

8. (Opcional) Escolha Preview external access (Pré-visualizar o acesso externo) na canto inferior direito para pré-visualizar a forma como sua nova política afetará o acesso público e entre contas ao seu recurso. Antes de salvar sua política, você pode verificar se ela introduz novas descobertas do IAM Access Analyzer ou resolve as descobertas existentes. Se você não vir um analisador ativo, escolha Go to Access Analyzer (Acessar o Access Analyzer) para criar um analisador de contas no IAM Access Analyzer. Para obter mais informações, consulte Visualizar acesso no Guia do usuário do IAM.

9. Escolha Save changes (Salvar alterações), o que levará você de volta à guia Permissions (Permissões).

Controlar o acesso a partir de VPC endpoints com políticas de bucket

É possível usar políticas de bucket do Amazon S3 para controlar o acesso a buckets por endpoints específicos da nuvem privada virtual (VPC) ou por VPCs específicas. Esta seção contém exemplos de políticas de bucket que você pode usar para controlar o acesso de endpoints da VPC ao bucket do Amazon S3. Para saber como configurar VPC endpoints, consulte VPC Endpoints no Guia do usuário da VPC.

A VPC permite executar os recursos da AWS em uma rede virtual definida por você. Um endpoint da VPC permite criar uma conexão privada entre a VPC e outro AWS service (Serviço da AWS). Essa conexão privada não exige acesso pela internet, por meio de uma conexão de rede privada virtual (VPN), de uma instância NAT ou do AWS Direct Connect.

Um endpoint de VPC para Amazon S3 é uma entidade lógica em uma VPC que oferece conectividade apenas ao Amazon S3. O VPC endpoint roteia as solicitações para o Amazon S3 e roteia as respostas de rotas de volta para a VPC. Os VPC endpoints alteram somente a forma como as solicitações são roteadas. Os endpoints públicos do Amazon S3 e os nomes de DNS continuarão funcionando com VPC endpoints. Consulte informações importantes sobre o uso de endpoints da VPC com o Amazon S3 em Gateway endpoints e em Gateway endpoints for Amazon S3 no Guia do usuário da VPC.

Os VPC endpoints para Amazon S3 fornecem duas maneiras de controlar o acesso aos dados do Amazon S3:

- É possível controlar as solicitações, os usuários ou os grupos permitidos por um VPC endpoint específico. Consulte informações sobre esse tipo de controle de acesso em Controlling access to VPC endpoints using endpoint policies no Guia do usuário da VPC.
- É possível controlar quais VPCs ou VPC endpoints têm acesso aos seus buckets usando as políticas de bucket do Amazon S3. Para obter exemplos desse tipo de controle de acesso de política de bucket, consulte os seguintes tópicos sobre restrição de acesso.

Tópicos

- Restringir o acesso a um VPC endpoint específico
- Restringir o acesso a uma VPC específica

> **Important**
>
> Ao aplicar políticas de bucket do Amazon S3 para os endpoints da VPC descritos nesta seção, talvez você bloqueie o acesso ao bucket de maneira não intencional. As permissões de bucket destinadas especificamente a limitar o acesso do bucket às conexões originadas do seu VPC endpoint podem bloquear todas as conexões ao bucket. Consulte informações sobre como corrigir esse problema em Como corrigir uma política de bucket quando ela tem o ID da VPC ou do endpoint da VPC errado? no Centro de Conhecimento da AWS Support.

Restringir o acesso a um VPC endpoint específico

O seguinte é um exemplo de um política de bucket do Amazon S3 que restringe o acesso a um bucket específico, `awsexamplebucket1`, somente no VPC endpoint com o ID `vpce-1a2b3c4d`. Se o endpoint especificado não for usado, essa política negará todo acesso ao bucket. A condição `aws:SourceVpce` especifica o endpoint. A condição `aws:SourceVpce` não exige um nome do recurso da Amazon (ARN) para o recurso do endpoint da VPC, somente o ID correspondente. Para obter mais informações sobre o uso de condições em uma política, consulte Exemplos de políticas de bucket usando chaves de condição.

> **Important**
>
> - Antes de usar a política de exemplo a seguir, substitua o ID do VPC endpoint por um valor apropriado para o caso de uso. Caso contrário, não será possível acessar o bucket.
> - Essa política desabilita o acesso do console ao bucket especificado, pois as solicitações do console não se originam do endpoint da VPC especificado.

```
{
   "Version": "2012-10-17",
   "Id": "Policy1415115909152",
   "Statement": [
     {
       "Sid": "Access-to-specific-VPCE-only",
       "Principal": "*",
       "Action": "s3:*",
       "Effect": "Deny",
       "Resource": ["arn:aws:s3:::awsexamplebucket1",
                    "arn:aws:s3:::awsexamplebucket1/*"],
       "Condition": {
         "StringNotEquals": {
           "aws:SourceVpce": "vpce-1a2b3c4d"
         }
       }
     }
   ]
}
```

Restringir o acesso a uma VPC específica

Você pode criar uma política de bucket que restringe o acesso a uma VPC específica usando a condição `aws:SourceVpc`. Isso será útil se você tiver vários VPC endpoints configurados na mesma VPC e desejar gerenciar o acesso aos buckets do Amazon S3 para todos os endpoints. Veja a seguir um exemplo de política que nega acesso a `awsexamplebucket1` e seus objetos para qualquer pessoa de fora da VPC `vpc-111bbb22`. Se a VPC especificada não for usada, a política negará todo acesso ao bucket. Essa instrução não concede acesso ao bucket. Para conceder acesso, é necessário adicionar uma instrução `Allow` separada. A chave de condição `vpc-111bbb22` não exige um ARN para o recurso da VPC, somente o ID correspondente.

> **Important**
>
> - Antes de usar a política de exemplo a seguir, substitua o ID da VPC por um valor apropriado para o caso de uso. Caso contrário, não será possível acessar o bucket.
> - Essa política desabilita o acesso do console ao bucket especificado, pois as solicitações do console não se originam da VPC especificada.

```
{
   "Version": "2012-10-17",
   "Id": "Policy1415115909153",
   "Statement": [
     {
       "Sid": "Access-to-specific-VPC-only",
       "Principal": "*",
       "Action": "s3:*",
       "Effect": "Deny",
       "Resource": ["arn:aws:s3:::awsexamplebucket1",
                    "arn:aws:s3:::awsexamplebucket1/*"],
       "Condition": {
         "StringNotEquals": {
           "aws:SourceVpc": "vpc-111bbb22"
         }
       }
     }
   ]
}
```

Para ter informações sobre como restringir o acesso ao bucket com base em IPs ou VPCs específicos, consulte Como faço para permitir que somente endpoints ou endereços IP de VPC específicos acessem meu bucket do Amazon S3? no Centro de Conhecimento do AWS re:Post.

Exemplos de políticas de bucket do Amazon S3

Com as políticas de bucket do Amazon S3, você pode proteger o acesso a objetos em seus buckets, para que somente usuários com as permissões apropriadas possam acessá-los. Você pode até mesmo impedir que usuários autenticados sem as permissões apropriadas acessem seus recursos do Amazon S3.

Esta seção apresenta exemplos de casos de uso típicos de políticas de bucket. Essas políticas de exemplo usam *`amzn-s3-demo-bucket`* como valor do recurso. Para testar essas políticas, substitua *`user input placeholders`* por suas informações (como o nome do seu bucket).

Para conceder ou negar permissões para um conjunto de objetos, você pode usar caracteres curinga (*) em nomes de recursos da Amazon (ARNs) e outros valores. Por exemplo, é possível controlar o acesso a grupos de objetos que começam com um prefixo ou terminam com uma extensão específica, como `.html`.

Para obter mais informações sobre a linguagem da política do AWS Identity and Access Management (IAM), consulte Políticas e permissões no Amazon S3.

Para ter mais informações sobre as permissões referentes a operações de API do S3 de acordo com os tipos de recurso do S3, consulte Permissões obrigatórias para operações de API do Amazon S3.

> **Note**
>
> Ao testar as permissões usando o console do Amazon S3, você deve conceder as permissões adicionais que o console exige: `s3:ListAllMyBuckets`, `s3:GetBucketLocation` e `s3:ListBucket`. Para acessar um exemplo de demonstração que concede permissões aos usuários e testa essas permissões usando o console, consulte Controlar o acesso a um bucket com políticas de usuário.

Recursos adicionais para criar políticas de bucket incluem:

- Consulte uma lista de ações de políticas do IAM, recursos e chaves de condição que você pode usar ao criar uma política de bucket em Actions, resources, and condition keys for Amazon S3 na Referência de autorização do serviço.

- Para ter mais informações sobre as permissões referentes a operações de API do S3 de acordo com os tipos de recurso do S3, consulte Permissões obrigatórias para operações de API do Amazon S3.
- Para obter orientação sobre como criar uma política do S3, consulte Adicionar uma política de bucket usando o console do Amazon S3.
- Para solucionar erros com uma política, consulte Solucionar erros de acesso negado (403 Forbidden) no Amazon S3.

Se você estiver tendo problemas para adicionar ou atualizar uma política, consulte Por que recebo o erro “Invalid principal in policy” quando tento atualizar minha política de bucket do Amazon S3? no Centro de Conhecimento do AWS re:Post.

Tópicos

- Conceder permissão somente leitura a um usuário anônimo público
- Exigir criptografia
- Gerenciar buckets usando ACLs predefinidas
- Gerenciar o acesso a objetos com marcação de objetos
- Gerenciar o acesso a objetos usando chaves de condição globais
- Gerenciar o acesso com base em solicitações HTTP ou HTTPS
- Gerenciar o acesso de usuários a pastas específicas
- Gerenciar o acesso para logs de acesso
- Gerenciar o acesso para uma OAI do Amazon CloudFront
- Gerenciar o acesso para a Lente de Armazenamento do Amazon S3
- Gerenciar permissões para o Inventário do S3, análises do S3 e relatórios do Inventário do S3
- Exigir MFA
- Impedir que os usuários excluam objetos

Conceder permissão somente leitura a um usuário anônimo público

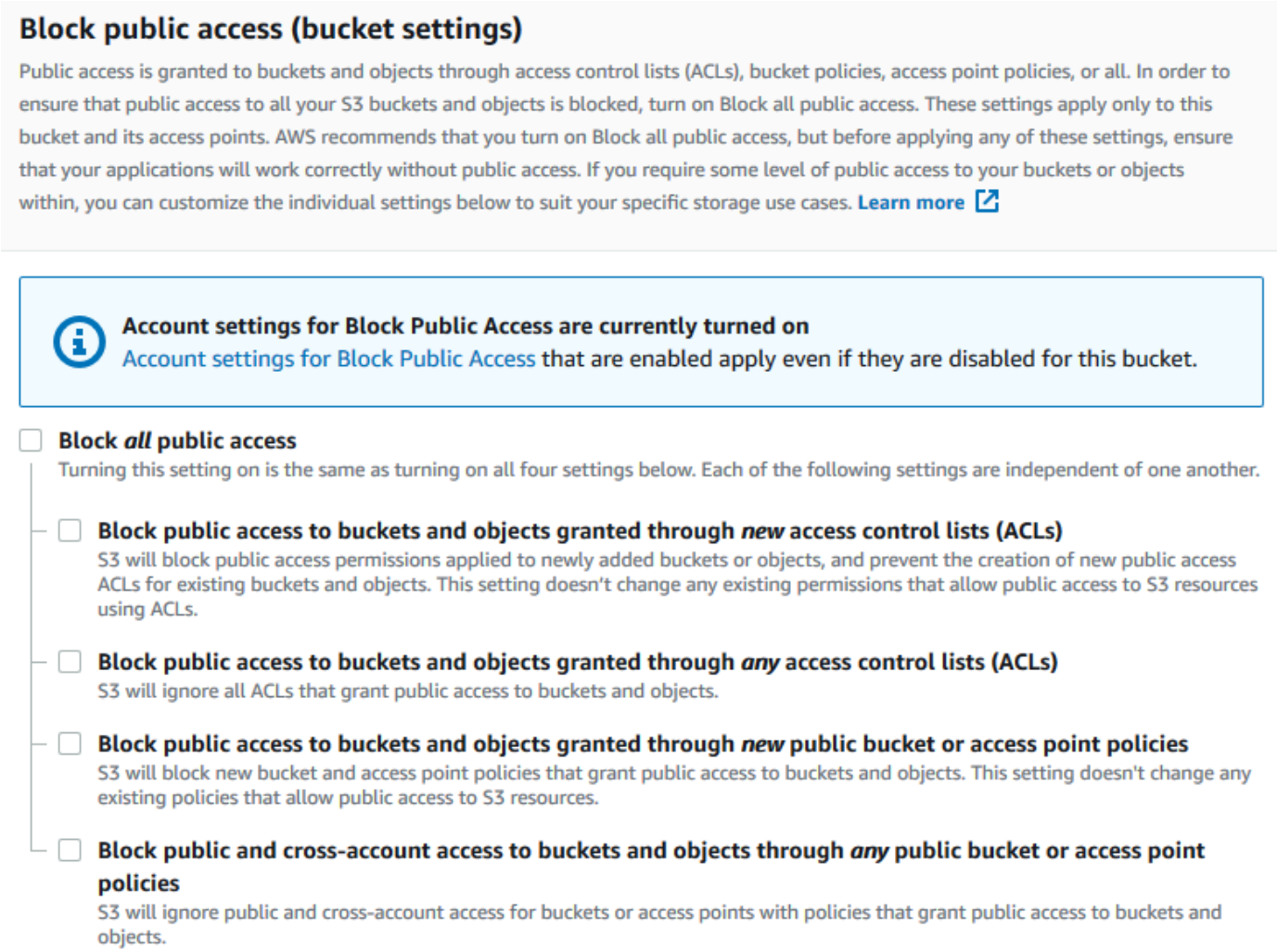
É possível usar as configurações de política para conceder acesso a usuários anônimos públicos, o que será útil se você estiver configurando o bucket como um site estático. A concessão de acesso a usuários anônimos públicos exige que você desative as configurações do Bloqueio de

Acesso Público do bucket. Consulte mais informações sobre como fazer isso e a política exigida em Configuração de permissões para acesso ao site. Para saber como configurar políticas mais restritivas para o mesmo propósito, consulte How can I grant public read access to some objects in my Amazon S3 bucket? no Centro de Conhecimento da AWS.

Por padrão, o Amazon S3 bloqueia o acesso público à sua conta e aos seus buckets. Se quiser usar um bucket para hospedar um site estático, use estas etapas para editar as configurações de bloqueio de acesso público.

> **Warning**
>
> Antes de concluir estas etapas, revise Bloquear o acesso público ao armazenamento do Amazon S3 para garantir que você entenda e aceite os riscos envolvidos em permitir o acesso público. Ao desativar as configurações de bloqueio de acesso público para tornar seu bucket público, qualquer pessoa na Internet pode acessá-lo. Recomendamos que você bloqueie todo o acesso público aos buckets.

1. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Escolha o nome do bucket configurado como um site estático.
3. Escolha Permissions (Permissões).
4. Em Block public access (bucket settings) (Bloqueio de acesso público (configurações de bucket), escolha Edit (Editar).
5. Desmarque Block all public access (Bloquear todo acesso público) e escolha Save changes (Salvar alterações).



O Amazon S3 desativa as configurações do Bloqueio de Acesso Público para o bucket. Para criar um site público estático, talvez também seja necessário editar as configurações do Bloqueio de Acesso Público para sua conta antes de adicionar uma política de bucket. Se as configurações do Bloqueio de Acesso Público da conta estiverem ativadas no momento, você verá uma observação em Bloquear acesso público (configurações de bucket).

Exigir criptografia

É possível exigir a criptografia do lado do servidor com chaves do AWS Key Management Service (AWS KMS) (SSE-KMS), conforme mostrado nos exemplos a seguir.

Exigir SSE-KMS para todos os objetos gravados em um bucket

O exemplo de política a seguir exige que cada objeto gravado no bucket seja criptografado com criptografia do lado do servidor usando chaves do AWS Key Management Service (AWS KMS) (SSE-KMS). Se o objeto não estiver criptografado com a SSE-KMS, a solicitação será negada.

```
{
"Version": "2012-10-17",
"Id": "PutObjPolicy",
"Statement": [{
  "Sid": "DenyObjectsThatAreNotSSEKMS",
  "Principal": "*",
  "Effect": "Deny",
  "Action": "s3:PutObject",
  "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
  "Condition": {
    "Null": {
      "s3:x-amz-server-side-encryption-aws-kms-key-id": "true"
    }
  }
}]
}
```

Exigir SSE-KMS com uma AWS KMS key específica para todos os objetos gravados em um bucket

O exemplo de política a seguir impede que objetos sejam gravados no bucket quando não estão criptografados com SSE-KMS usando um ID de chave do KMS específico. Mesmo que os objetos sejam criptografados com a SSE-KMS usando um cabeçalho por solicitação ou criptografia padrão de bucket, os objetos não serão gravados no bucket se não tiverem sido criptografados com a chave do KMS especificada. Substitua o ARN da chave do KMS usado neste exemplo pelo ARN da sua chave do KMS.

```
{
"Version": "2012-10-17",
"Id": "PutObjPolicy",
"Statement": [{
  "Sid": "DenyObjectsThatAreNotSSEKMSWithSpecificKey",
  "Principal": "*",
  "Effect": "Deny",
  "Action": "s3:PutObject",
  "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
  "Condition": {
```

```
    "ArnNotEqualsIfExists": {
      "s3:x-amz-server-side-encryption-aws-kms-key-id": "arn:aws:kms:us-
east-2:111122223333:key/01234567-89ab-cdef-0123-456789abcdef"
    }
  }
}]
}
```

Gerenciar buckets usando ACLs predefinidas

Conceder permissões a várias contas para fazer upload de objetos ou definir ACLs de objetos para acesso público

O exemplo de política a seguir concede as permissões `s3:PutObject` e `s3:PutObjectAcl` a várias Contas da AWS. Além disso, o exemplo de política exige que as solicitações para essas operações incluam a lista de controle de acesso (ACL) predefinida `public-read`. Para obter mais informações, consulte Ações de políticas para o Amazon S3 e Chaves de condição de política para o Amazon S3.

> **Warning**
>
> A ACL predefinida `public-read` permite que qualquer pessoa no mundo veja os objetos em seu bucket. Tenha cautela ao conceder acesso anônimo ao seu bucket do Amazon S3 ou ao desabilitar as configurações de bloqueio de acesso público. Quando você concede acesso anônimo, qualquer pessoa no mundo pode acessar seu bucket. Recomendamos nunca conceder acesso anônimo ao seu bucket do Amazon S3, a menos que seja especificamente necessário, como com a hospedagem de site estático. Se você quiser habilitar configurações de bloqueio de acesso público para hospedagem de sites estáticos, consulte Tutorial: Configurar um site estático no Amazon S3.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AddPublicReadCannedAcl",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::111122223333:root",
```

```
                "arn:aws:iam::444455556666:root"
            ]
        },
        "Action": [
            "s3:PutObject",
            "s3:PutObjectAcl"
        ],
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
        "Condition": {
            "StringEquals": {
                "s3:x-amz-acl": [
                    "public-read"
                ]
            }
        }
    }
  ]
}
```

Conceder permissões entre contas para fazer upload de objetos garantindo que o proprietário do bucket tenha controle total

O exemplo a seguir mostra como permitir que outra Conta da AWS faça upload de objetos no bucket e, ao mesmo tempo, garantir controle total sobre os objetos carregados. Essa política concede a uma Conta da AWS específica (*111122223333*) a capacidade de carregar objetos se essa conta incluir a ACL pré-configurada `bucket-owner-full-control` no carregamento. A condição `StringEquals` na política especifica a chave de condição `s3:x-amz-acl` para expressar o requisito de ACL predefinida. Para obter mais informações, consulte Chaves de condição de política para o Amazon S3.

```
{
   "Version":"2012-10-17",
   "Statement":[
     {
       "Sid":"PolicyForAllowUploadWithACL",
       "Effect":"Allow",
       "Principal":{"AWS":"111122223333"},
       "Action":"s3:PutObject",
       "Resource":"arn:aws:s3:::amzn-s3-demo-bucket/*",
       "Condition": {
         "StringEquals": {"s3:x-amz-acl":"bucket-owner-full-control"}
       }
```

```
      }
   ]
}
```

Gerenciar o acesso a objetos com marcação de objetos

Permitir que um usuário leia somente os objetos que têm a chave e o valor de uma etiqueta específica

A política de permissões a seguir limita a capacidade de leitura dos usuários para que leiam somente objetos que tenham a chave e o valor da tag `environment: production`. Essa política usa a chave de condição `s3:ExistingObjectTag` para especificar a chave e o valor da etiqueta.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Principal":{
            "AWS":"arn:aws:iam::111122223333:role/JohnDoe"
         },
         "Effect":"Allow",
         "Action":[
            "s3:GetObject",
            "s3:GetObjectVersion"
         ],
         "Resource":"arn:aws:s3:::amzn-s3-demo-bucket/*",
         "Condition":{
            "StringEquals":{
               "s3:ExistingObjectTag/environment":"production"
            }
         }
      }
   ]
}
```

Restringir quais chaves de etiqueta de objeto os usuários podem adicionar

O exemplo de política a seguir concede ao usuário permissão para executar a ação `s3:PutObjectTagging`, que permite que o usuário adicione etiquetas a um objeto existente. A condição usa a chave de condição `s3:RequestObjectTagKeys` para especificar as chaves de etiqueta permitidas, como `Owner` ou `CreationDate`. Para obter mais informações, consulte Criar uma condição que testa vários valores de chave no Guia do usuário do IAM.

A política garante que cada chave de etiqueta especificada na solicitação seja uma chave de etiqueta autorizada. O qualificador `ForAnyValue` na condição garante que pelo menos uma das chaves especificadas esteja presente na solicitação.

```
{
   "Version": "2012-10-17",
  "Statement": [
    {"Principal":{"AWS":[
            "arn:aws:iam::111122223333:role/JohnDoe"
         ]
       },
 "Effect": "Allow",
      "Action": [
        "s3:PutObjectTagging"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
      ],
      "Condition": {"ForAnyValue:StringEquals": {"s3:RequestObjectTagKeys": [
            "Owner",
            "CreationDate"
          ]
        }
      }
    }
  ]
}
```

Exigir a chave e o valor de uma etiqueta específica ao permitir que os usuários adicionem etiquetas de objeto

O exemplo de política a seguir concede ao usuário permissão para executar a ação `s3:PutObjectTagging`, que permite que o usuário adicione etiquetas a um objeto existente. A condição requer que o usuário inclua uma chave de etiqueta específica (como *`Project`*) com o valor definido como *`X`*.

```
{
   "Version": "2012-10-17",
  "Statement": [
    {"Principal":{"AWS":[
       "arn:aws:iam::111122223333:user/JohnDoe"
        ]
```

```
        },
      "Effect": "Allow",
      "Action": [
        "s3:PutObjectTagging"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
      ],
      "Condition": {"StringEquals": {"s3:RequestObjectTag/Project": "X"
        }
      }
    }
  ]
}
```

Permitir que um usuário adicione somente objetos com a chave e o valor de uma etiqueta específica

O exemplo de política a seguir concede ao usuário permissão para realizar a ação `s3:PutObject` para que possa adicionar objetos a um bucket. No entanto, a instrução `Condition` restringe as chaves e os valores de etiqueta permitidos nos objetos enviados. Neste exemplo, o usuário só pode adicionar objetos que tenham a chave de etiqueta específica (*`Department`*) com o valor definido como *`Finance`* no bucket.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Principal":{
            "AWS":[
                 "arn:aws:iam::111122223333:user/JohnDoe"
         ]
        },
        "Effect": "Allow",
        "Action": [
            "s3:PutObject"
        ],
        "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket/*"
        ],
        "Condition": {
            "StringEquals": {
                "s3:RequestObjectTag/Department": "Finance"
            }
        }
```

```
    }]
}
```

Gerenciar o acesso a objetos usando chaves de condição globais

As chaves de condição globais são chaves de condição com um prefixo `aws`. Os Serviços da AWS podem oferecer suporte a chaves de condição globais ou chaves específicas do serviço que incluem seu prefixo de serviço. É possível usar o elemento `Condition` de uma política JSON para comparar chaves em uma solicitação com os valores de chave especificados em sua política.

Restringir o acesso somente às entregas de logs de acesso ao servidor do Amazon S3

No exemplo de política de bucket a seguir, a chave de condição global aws:SourceArn é usada para comparar o nome do recurso da Amazon (ARN), fazendo uma solicitação de serviço a serviço com o ARN especificado na política. A chave de condição global `aws:SourceArn` é usada para impedir que o serviço Amazon S3 seja usado como um representante confuso durante transações entre os serviços. Somente o serviço Amazon S3 tem permissão para adicionar objetos ao bucket do Amazon S3.

Este exemplo de política de bucket concede permissões de `s3:PutObject` somente à entidade principal do serviço de registro em log (`logging.s3.amazonaws.com`).

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowPutObjectS3ServerAccessLogsPolicy",
            "Principal": {
                "Service": "logging.s3.amazonaws.com"
            },
            "Effect": "Allow",
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket-logs/*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111111111111"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:s3:::EXAMPLE-SOURCE-BUCKET"
                }
            }
```

```
        },
        {
            "Sid": "RestrictToS3ServerAccessLogs",
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket-logs/*",
            "Condition": {
                "ForAllValues:StringNotEquals": {
                    "aws:PrincipalServiceNamesList": "logging.s3.amazonaws.com"
                }
            }
        }
    ]
}
```

Permitir o acesso somente à sua organização

Se você quiser exigir que todas as entidades principais do IAM que acessam um recurso sejam de uma Conta da AWS em sua organização (incluindo a conta de gerenciamento do AWS Organizations), poderá usar a chave de condição global `aws:PrincipalOrgID`.

Para conceder ou restringir esse tipo de acesso, defina a condição `aws:PrincipalOrgID` e defina o valor como o ID da sua organização na política de bucket. O ID da organização é usado para controlar o acesso ao bucket. Quando você usa a condição `aws:PrincipalOrgID`, as permissões da política de bucket também são aplicadas a todas as novas contas adicionadas à organização.

Aqui está um exemplo de política de bucket baseada em recursos que você pode usar para conceder a entidades principais do IAM específicas em sua organização acesso direto ao bucket. Ao adicionar a chave de condição global `aws:PrincipalOrgID` à sua política de bucket, agora é necessário que a conta da entidade principal esteja em sua organização para obter acesso ao recurso. Mesmo que você acidentalmente especifique uma conta incorreta ao conceder acesso, a chave de condição global aws:PrincipalOrgID atuará como uma proteção adicional. Quando uma chave global é usada em uma política, ela impede que todas as entidades principais fora da organização especificada acessem o bucket do S3. Somente entidades principais de contas na organização listada podem obter acesso ao recurso.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "AllowGetObject",
```

```
        "Principal": {
            "AWS": "*"
        },
        "Effect": "Allow",
        "Action": "s3:GetObject",
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
        "Condition": {
            "StringEquals": {
                "aws:PrincipalOrgID": ["o-aa111bb222"]
            }
        }
    }]
}
```

Gerenciar o acesso com base em solicitações HTTP ou HTTPS

Restringir o acesso somente a solicitações HTTPS

Se você quiser evitar que possíveis invasores manipulem o tráfego de rede, poderá usar HTTPS (TLS) para permitir somente conexões criptografadas e, ao mesmo tempo, restringir o acesso de solicitações HTTP ao seu bucket. Para determinar se a solicitação é HTTP ou HTTPS, use a chave de condição global aws:SecureTransport em sua política de bucket do S3. A chave de condição `aws:SecureTransport` verifica se uma solicitação foi enviada usando HTTP.

Se uma solicitação retornar `true`, isso significa que ela foi enviada por HTTPS. Se a solicitação retornar `false`, isso significa que ela foi enviada por HTTP. Depois, você pode permitir ou negar acesso ao bucket com base no esquema de solicitação desejado.

No exemplo a seguir, a política de bucket nega explicitamente as solicitações HTTP.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "RestrictToTLSRequestsOnly",
        "Action": "s3:*",
        "Effect": "Deny",
        "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket",
            "arn:aws:s3:::amzn-s3-demo-bucket/*"
        ],
        "Condition": {
            "Bool": {
```

```
                "aws:SecureTransport": "false"
            }
        },
        "Principal": "*"
    }]
}
```

Restringir o acesso a um indicador HTTP específico

Suponha que você tenha um site com nome de domínio *www.example.com* ou *example.com* com links para fotos e vídeos armazenados em seu bucket chamado *amzn-s3-demo-bucket*. Por padrão, todos os recursos do Amazon S3 são privados e, portanto, somente a Conta da AWS que criou os recursos pode acessá-los.

Para permitir acesso de leitura a esses objetos em seu site, você pode adicionar uma política de bucket que conceda a permissão `s3:GetObject` com uma condição de que a solicitação GET deve se originar de páginas específicas da Web. A política a seguir restringe as solicitações usando a condição `StringLike` com a chave de condição `aws:Referer`.

```
{
  "Version":"2012-10-17",
  "Id":"HTTP referer policy example",
  "Statement":[
    {
      "Sid":"Allow only GET requests originating from www.example.com and
 example.com.",
      "Effect":"Allow",
      "Principal":"*",
      "Action":["s3:GetObject","s3:GetObjectVersion"],
      "Resource":"arn:aws:s3:::amzn-s3-demo-bucket/*",
      "Condition":{
        "StringLike":{"aws:Referer":["http://www.example.com/*","http://example.com/
*"]}
      }
    }
  ]
}
```

Certifique-se de que os navegadores que você usa incluam o cabeçalho HTTP `referer` na solicitação.

> **Warning**
>
> Recomendamos cuidado ao usar a chave de condição `aws:Referer`. É perigoso incluir um valor de cabeçalho do indicador HTTP conhecido publicamente. Partes não autorizadas podem usar navegadores personalizados ou modificados para fornecer qualquer valor de `aws:Referer` que escolherem. Assim sendo, não use `aws:Referer` para impedir que partes não autorizadas façam solicitações diretas à AWS.
> A chave de condição `aws:Referer` é oferecida apenas para permitir que os clientes protejam o conteúdo digital, como o conteúdo armazenado no Simple Storage Service (Amazon S3), evitando que seja referenciado em sites de terceiros não autorizados. Para obter mais informações, consulteaws:Referer no Guia do usuário do IAM.

Gerenciar o acesso de usuários a pastas específicas

Conceder acesso a pastas específicas para os usuários

Suponha que você esteja tentando conceder a uma pasta específica para os usuários. Se o usuário do IAM e o bucket do S3 pertencerem à mesma Conta da AWS, você poderá usar uma política do IAM para conceder acesso a uma pasta de bucket específica para os usuários. Com essa abordagem, você não precisa atualizar sua política de bucket para conceder acesso. Você pode adicionar a política do IAM a um perfil do IAM para o qual vários usuários podem mudar.

Se a identidade do IAM e o bucket do S3 pertencerem a Contas da AWS diferentes, você deverá conceder acesso entre contas tanto na política do IAM quanto na política de bucket. Para obter mais informações sobre como conceder acesso entre contas, consulte Proprietário do bucket concedendo permissões de bucket entre contas.

O exemplo de política de bucket a seguir concede a *JohnDoe* acesso total ao console somente na pasta dele (home/*JohnDoe*/). Ao criar uma pasta home e conceder as permissões apropriadas aos seus usuários, você pode fazer com que vários usuários compartilhem um único bucket. Essa política consiste em três instruções `Allow`:

- *AllowRootAndHomeListingOfCompanyBucket*: permite que o usuário (*JohnDoe*) liste objetos no nível raiz do bucket *amzn-s3-demo-bucket* e na pasta home. Essa instrução também permite que o usuário pesquise o prefixo home/ usando o console.
- *AllowListingOfUserFolder*: permite que o usuário (*JohnDoe*) liste todos os objetos na pasta home/*JohnDoe*/ e em quaisquer subpastas.

- *AllowAllS3ActionsInUserFolder*: permite que o usuário execute todas as ações do Amazon S3 ao conceder as permissões `Read`, `Write` e `Delete`. As permissões são limitadas à pasta inicial do proprietário do bucket.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRootAndHomeListingOfCompanyBucket",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::111122223333:user/JohnDoe"
                ]
            },
            "Effect": "Allow",
            "Action": ["s3:ListBucket"],
            "Resource": ["arn:aws:s3:::amzn-s3-demo-bucket"],
            "Condition": {
                "StringEquals": {
                    "s3:prefix": ["", "home/", "home/JohnDoe"],
                    "s3:delimiter": ["/"]
                }
            }
        },
        {
            "Sid": "AllowListingOfUserFolder",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::111122223333:user/JohnDoe"
                ]
            },
            "Action": ["s3:ListBucket"],
            "Effect": "Allow",
            "Resource": ["arn:aws:s3:::amzn-s3-demo-bucket"],
            "Condition": {
                "StringLike": {
                    "s3:prefix": ["home/JohnDoe/*"]
                }
            }
        },
        {
            "Sid": "AllowAllS3ActionsInUserFolder",
```

```
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::111122223333:user/JohnDoe"
                ]
            },
            "Action": ["s3:*"],
            "Resource": ["arn:aws:s3:::amzn-s3-demo-bucket/home/JohnDoe/*"]
        }
    ]
}
```

Gerenciar o acesso para logs de acesso

Conceder acesso ao Application Load Balancer para habilitar logs de acesso

Ao habilitar os logs de acesso para o Application Load Balancer, você deve especificar o nome do bucket do S3 em que o balanceador de carga armazenará os logs. O bucket deve ter uma política anexada que conceda ao Elastic Load Balancing permissão para gravar no bucket.

No exemplo a seguir, a política de bucket concede ao Elastic Load Balancing (ELB) permissão para gravar os logs de acesso no bucket:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Principal": {
        "AWS": "arn:aws:iam::elb-account-id:root"
      },
      "Effect": "Allow",
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/prefix/AWSLogs/111122223333/*"
    }
  ]
}
```

> **Note**
>
> Substitua *elb-account-id* pelo ID da Conta da AWS do Elastic Load Balancing para sua Região da AWS. Para ver a lista de regiões do Elastic Load Balancing, consulte Anexar uma política ao seu bucket do S3 no Guia do usuário do Elastic Load Balancing.

Se sua Região da AWS não aparecer na lista de regiões compatíveis do Elastic Load Balancing, use a política a seguir, que concede permissões ao serviço de entrega de logs especificado.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
       "Principal": {
         "Service": "logdelivery.elasticloadbalancing.amazonaws.com"
          },
      "Effect": "Allow",
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/prefix/AWSLogs/111122223333/*"
    }
  ]
}
```

Depois, configure os logs de acesso do Elastic Load Balancing habilitando-os. Você pode verificar as permissões de bucket criando um arquivo de teste.

Gerenciar o acesso para uma OAI do Amazon CloudFront

Conceder permissão para uma OAI do Amazon CloudFront

O exemplo de política de bucket a seguir concede uma permissão de identidade do acesso de origem (OAI) do CloudFront para obter (ler) todos os objetos em seu bucket do S3. Você pode usar uma OAI do CloudFront para permitir que os usuários acessem objetos em seu bucket por meio do CloudFront, mas não diretamente pelo Amazon S3. Para obter mais informações, consulte Restringir acesso ao conteúdo do Amazon S3 usando uma identidade do acesso de origem no Guia do desenvolvedor do Amazon CloudFront.

A política a seguir usa o ID da OAI como `Principal` da política. Para obter mais informações sobre como usar políticas de bucket do S3 para conceder acesso a uma OAI do CloudFront, consulte

Migrar da identidade do acesso de origem (OAI) para o controle de acesso à origem (OAC) no Guia do desenvolvedor do Amazon CloudFront.

Para usar este exemplo:

- Substitua *EH1HDMB1FH2TC* pelo ID da OAI. Para localizar o ID da OAI, consulte a página Origin Access Identity (Identidade do acesso de origem) no console do CloudFront ou use ListCloudFrontOriginAccessIdentities na API do CloudFront.
- Substitua *amzn-s3-demo-bucket* pelo nome do seu bucket.

```
{
    "Version": "2012-10-17",
    "Id": "PolicyForCloudFrontPrivateContent",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::cloudfront:user/CloudFront Origin Access
 Identity EH1HDMB1FH2TC"
            },
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
        }
    ]
}
```

Gerenciar o acesso para a Lente de Armazenamento do Amazon S3

Conceder permissões para a Lente de Armazenamento do Amazon S3

A Lente de Armazenamento do S3 agrega suas métricas e exibe as informações na seção Account snapshot (Snapshot da conta) na página Buckets do console do Amazon S3. A Lente de Armazenamento do S3 também oferece um painel interativo para visualizar insights e tendências, sinalizar discrepâncias e receber recomendações para otimizar os custos de armazenamento e aplicar as práticas recomendadas de proteção de dados. O painel tem opções de detalhamento para gerar e visualizar insights no nível da organização, conta, Região da AWS, classe de armazenamento, bucket, prefixo ou grupo de Lente de Armazenamento. Você também pode enviar uma exportação diária de métricas em CSV ou no formato Parquet para um bucket do S3.

A Lente de Armazenamento do S3 pode exportar as métricas de uso de armazenamento agregadas em um bucket do Amazon S3 para análise posterior. O bucket em que o S3 Storage Lens coloca as exportações de métricas dele é conhecido como bucket de destino. Ao configurar a exportação de métricas do S3 Storage Lens, você deve ter uma política para o bucket de destino. Para obter mais informações, consulte Avaliação de sua atividade de armazenamento e uso com a Lente de Armazenamento do Amazon S3.

O exemplo de política de bucket a seguir concede ao Amazon S3 permissão para gravar objetos (solicitações PUT) em um bucket de destino. Você usa uma política de bucket como essa no bucket de destino ao configurar uma exportação de métricas do S3 Storage Lens.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "S3StorageLensExamplePolicy",
            "Effect": "Allow",
            "Principal": {
                "Service": "storage-lens.s3.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-destination-bucket/destination-prefix/
StorageLens/111122223333/*"
            ],
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceAccount": "111122223333",
                    "aws:SourceArn": "arn:aws:s3:region-code:111122223333:storage-
lens/storage-lens-dashboard-configuration-id"
                }
            }
        }
    ]
}
```

Ao configurar uma exportação de métricas da organização da Lente de Armazenamento do S3, use a modificação a seguir na instrução `Resource` da política de bucket anterior.

```
"Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/destination-prefix/
StorageLens/your-organization-id/*",
```

Gerenciar permissões para o Inventário do S3, análises do S3 e relatórios do Inventário do S3

Conceder permissões para o Inventário do S3 e análises do S3

O Inventário do S3 cria listas dos objetos em um bucket do, e a exportação da análise da classe de armazenamento do S3 cria arquivos de saída dos dados usados na análise. O bucket para o qual o inventário lista objetos é chamado de bucket de origem. O bucket onde o arquivo de inventário ou arquivo de exportação da análise é gravado é chamado de bucket de destino. Ao configurar a exportação de um inventário ou uma análise, você deve criar uma política de bucket para o bucket de destino. Para obter mais informações, consulte Catalogar e analisar seus dados com o Inventário S3 e Análise do Amazon S3 – Análise de classe de armazenamento.

O exemplo da política de bucket a seguir concede permissão ao Amazon S3 para gravar objetos (solicitações PUT) da conta do bucket de origem para o bucket de destino. Use uma política de bucket como essa no bucket de destino ao configurar o Inventário do S3 e a exportação da análise do S3.

```
{
      "Version": "2012-10-17",
      "Statement": [
        {
            "Sid": "InventoryAndAnalyticsExamplePolicy",
            "Effect": "Allow",
            "Principal": {
                "Service": "s3.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": [
                "arn:aws:s3:::DOC-EXAMPLE-DESTINATION-BUCKET/*"
            ],
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:s3:::DOC-EXAMPLE-SOURCE-BUCKET"
                },
                "StringEquals": {
                    "aws:SourceAccount": "111122223333",
                    "s3:x-amz-acl": "bucket-owner-full-control"
                }
```

```
            }
        }
    ]
}
```

Controlar a criação da configuração de relatórios do Inventário S3

Catalogar e analisar seus dados com o Inventário S3 cria listas dos objetos em um bucket do S3 e dos metadados de cada objeto. Com a permissão `s3:PutInventoryConfiguration`, o usuário tem autorização para criar uma configuração de inventário que inclui todos os campos de metadados de objetos que estão disponíveis por padrão e especificar o bucket de destino para armazenar o inventário. Um usuário com acesso de leitura aos objetos no bucket de destino pode acessar todos os campos de metadados do objeto que estão disponíveis no relatório de inventário. Para obter mais informações sobre os campos de metadados que estão disponíveis no S3 Inventory, consulte Lista do Amazon S3 Inventory.

Para impedir que um usuário configure um relatório do Inventário S3, remova a permissão `s3:PutInventoryConfiguration` do usuário.

Alguns campos de metadados de objetos nas configurações de relatório do Inventário S3 são opcionais, o que significa que estão disponíveis por padrão, mas podem ser restritos quando você concede a permissão `s3:PutInventoryConfiguration` a um usuário. É possível controlar se os usuários podem incluir esses campos de metadados opcionais em seus relatórios usando a chave de condição `s3:InventoryAccessibleOptionalFields`. Consulte uma lista dos campos de metadados opcionais disponíveis no Inventário S3 em OptionalFields na Referência de API do Amazon Simple Storage Service.

Para conceder permissão ao usuário para criar uma configuração de inventário com campos de metadados opcionais específicos, use a chave de condição `s3:InventoryAccessibleOptionalFields` para refinar as condições na política de bucket.

O exemplo de política a seguir concede a um usuário (*Ana*) permissão para criar uma configuração de inventário condicionalmente. A condição `ForAllValues:StringEquals` na política usa a chave de condição `s3:InventoryAccessibleOptionalFields` para especificar os dois campos de metadados opcionais permitidos, a saber `Size` e `StorageClass`. Então, quando *Ana* está criando uma configuração de inventário, os únicos campos de metadados opcionais que ela pode incluir são `Size` e `StorageClass`.

```
{
```

```
 "Id": "InventoryConfigPolicy",
 "Version": "2012-10-17",
 "Statement": [{
   "Sid": "AllowInventoryCreationConditionally",
   "Effect": "Allow",
   "Principal": {
    "AWS": "arn:aws:iam::111122223333:user/Ana"
   },
   "Action":
    "s3:PutInventoryConfiguration",
   "Resource":
    "arn:aws:s3:::DOC-EXAMPLE-SOURCE-BUCKET",
   "Condition": {
    "ForAllValues:StringEquals": {
     "s3:InventoryAccessibleOptionalFields": [
        "Size",
        "StorageClass"
        ]
      }
    }
   }
 ]
}
```

Para impedir que um usuário configure um relatório do Inventário S3 que inclua campos de metadados opcionais específicos, adicione uma instrução `Deny` explícita à política do bucket de origem. O exemplo de política de bucket a seguir impede que a usuária *Ana* crie uma configuração de inventário no bucket de origem *DOC-EXAMPLE-SOURCE-BUCKET* que inclua os campos de metadados opcionais `ObjectAccessControlList` ou `ObjectOwner`. A usuária *Ana* ainda pode criar uma configuração de inventário com outros campos de metadados opcionais.

```
{
 "Id": "InventoryConfigSomeFields",
 "Version": "2012-10-17",
 "Statement": [{
   "Sid": "AllowInventoryCreation",
   "Effect": "Allow",
   "Principal": {
    "AWS": "arn:aws:iam::111122223333:user/Ana"
   },
   "Action": "s3:PutInventoryConfiguration",
   "Resource":
```

```
    "arn:aws:s3:::DOC-EXAMPLE-SOURCE-BUCKET",

  },
  {
   "Sid": "DenyCertainInventoryFieldCreation",
   "Effect": "Deny",
   "Principal": {
    "AWS": "arn:aws:iam::111122223333:user/Ana"
   },
   "Action": "s3:PutInventoryConfiguration",
   "Resource":
     "arn:aws:s3:::DOC-EXAMPLE-SOURCE-BUCKET",
   "Condition": {
    "ForAnyValue:StringEquals": {
     "s3:InventoryAccessibleOptionalFields": [
        "ObjectOwner",
        "ObjectAccessControlList"
        ]
      }
    }
   }
 ]
}
```

> **Note**
>
> O uso da chave de condição `s3:InventoryAccessibleOptionalFields` nas políticas de bucket não afeta a entrega de relatórios de inventário com base nas configurações de inventário existentes.

> **Important**
>
> Recomendamos usar `ForAllValues` com efeito `Allow` ou `ForAnyValue` com efeito `Deny`, conforme mostrado nos exemplos anteriores.
>
> Não use `ForAllValues` com efeito `Deny` nem `ForAnyValue` com efeito `Allow`, pois essas combinações podem ser excessivamente restritivas e bloquear a exclusão da configuração do inventário.
>
> Para saber mais sobre os operadores do conjunto de condições `ForAllValues` e `ForAnyValue`, consulte Multivalued context keys no Guia do usuário do IAM.

Exigir MFA

O Amazon S3 oferece suporte a acesso à API protegido por MFA, um recurso que pode impor a autenticação multifator para acessar os recursos do Amazon S3. A autenticação multifator fornece um nível extra de segurança que pode ser aplicado a seu ambiente da AWS. MFA é um recurso de segurança que exige que os usuários comprovem a posse física de um dispositivo MFA fornecendo um código válido de MFA. Para obter mais informações, consulte Autenticação multifator da AWS. É possível exigir a autenticação MFA para todas as solicitações de acesso a seus recursos do Amazon S3.

Para impor o requisito de MFA, use a chave de condição `aws:MultiFactorAuthAge` em uma política de bucket. Os usuários do IAM podem acessar os recursos do Amazon S3 usando credenciais temporárias emitidas pelo AWS Security Token Service (AWS STS). Forneça o código da MFA no momento da solicitação do AWS STS.

Quando o Amazon S3 recebe uma solicitação com autenticação multifator, a chave de condição `aws:MultiFactorAuthAge` fornece um valor numérico que indica há quanto tempo (em segundos) a credencial temporária foi criada. Se a credencial temporária fornecida na solicitação não foi criada usando um dispositivo MFA, esse valor de chave será nulo (ausente). Em uma política de bucket, você pode adicionar uma condição para verificar esse valor, conforme mostrado no exemplo a seguir.

O exemplo de política negará qualquer operação do Amazon S3 na pasta */taxdocuments* do bucket *amzn-s3-demo-bucket* se a solicitação não for autenticada usando MFA. Para saber mais sobre MFA, consulte Uso da autenticação multifator (MFA) na AWS no Guia do usuário do IAM.

```
{
    "Version": "2012-10-17",
    "Id": "123",
    "Statement": [
      {
        "Sid": "",
        "Effect": "Deny",
        "Principal": "*",
        "Action": "s3:*",
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/taxdocuments/*",
        "Condition": { "Null": { "aws:MultiFactorAuthAge": true }}
      }
    ]
 }
```

A condição `Null` no bloco `Condition` será avaliada como `true` se o valor da chave de condição `aws:MultiFactorAuthAge` for nulo, o que indica que as credenciais de segurança temporárias da solicitação foram criadas sem um dispositivo de MFA.

A política de bucket a seguir é uma extensão da política de bucket anterior. A política a seguir inclui duas declarações de política. Uma instrução concede a permissão `s3:GetObject` em um bucket (*amzn-s3-demo-bucket*) a todos. Outra instrução restringe ainda mais o acesso à pasta *amzn-s3-demo-bucket/taxdocuments* no bucket ao exigir MFA.

```
{
    "Version": "2012-10-17",
    "Id": "123",
    "Statement": [
      {
        "Sid": "",
        "Effect": "Deny",
        "Principal": "*",
        "Action": "s3:*",
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/taxdocuments/*",
        "Condition": { "Null": { "aws:MultiFactorAuthAge": true } }
      },
      {
        "Sid": "",
        "Effect": "Allow",
        "Principal": "*",
        "Action": ["s3:GetObject"],
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
      }
    ]
 }
```

Opcionalmente, você pode usar uma condição numérica para limitar a validade da chave `aws:MultiFactorAuthAge`. A duração que você especifica com a chave `aws:MultiFactorAuthAge` não depende do ciclo de vida da credencial de segurança temporária usada para autenticar a solicitação.

Por exemplo, a seguinte política de bucket, além de exigir autenticação MFA, também verifica há quanto tempo a sessão temporária foi criada. A política negará qualquer operação se o valor da chave `aws:MultiFactorAuthAge` indicar que a sessão temporária foi criada há mais de uma hora (3.600 segundos).

```
{
    "Version": "2012-10-17",
    "Id": "123",
    "Statement": [
      {
        "Sid": "",
        "Effect": "Deny",
        "Principal": "*",
        "Action": "s3:*",
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/taxdocuments/*",
        "Condition": {"Null": {"aws:MultiFactorAuthAge": true }}
      },
      {
        "Sid": "",
        "Effect": "Deny",
        "Principal": "*",
        "Action": "s3:*",
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/taxdocuments/*",
        "Condition": {"NumericGreaterThan": {"aws:MultiFactorAuthAge": 3600 }}
       },
       {
         "Sid": "",
         "Effect": "Allow",
         "Principal": "*",
         "Action": ["s3:GetObject"],
         "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
       }
    ]
 }
```

Impedir que os usuários excluam objetos

Por padrão, os usuários não têm nenhuma permissão. No entanto, ao criar políticas, você pode conceder permissões que não pretendia conceder. Para evitar essas brechas de permissão, você pode elaborar uma política de acesso mais estrita adicionando uma negação explícita.

Para impedir explicitamente que usuários ou contas excluam objetos, é necessário adicionar as seguintes ações a uma política de bucket: as permissões `s3:DeleteObject`, `s3:DeleteObjectVersion` e `s3:PutLifecycleConfiguration`. Todas as três ações são necessárias porque é possível excluir objetos chamando explicitamente a API `DELETE Object` ou configurando seu ciclo de vida (consulte Gerenciar o ciclo de vida dos objetos) de modo que o Amazon S3 possa remover os objetos quando o respectivo ciclo de vida expirar.

No exemplo de política a seguir, você nega explicitamente as permissões `DELETE Object` ao usuário *`MaryMajor`*. Uma declaração `Deny` explícita sempre se sobrepõe a qualquer outra permissão concedida.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "statement1",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:user/MaryMajor"
      },
      "Action": [
        "s3:GetObjectVersion",
        "s3:GetBucketAcl"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket1",
   "arn:aws:s3:::amzn-s3-demo-bucket1/*"
      ]
    },
    {
      "Sid": "statement2",
      "Effect": "Deny",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:user/MaryMajor"
      },
      "Action": [
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:PutLifecycleConfiguration"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket1",
     "arn:aws:s3:::amzn-s3-demo-bucket1/*"
      ]
    }
  ]
}
```

Exemplos de políticas de bucket usando chaves de condição

Você pode usar a linguagem de políticas de acesso para especificar condições ao conceder permissões. É possível usar o elemento `Condition` opcional ou o bloco `Condition` para especificar condições referentes a quando uma política está em vigor.

Para obter políticas que usam chaves de condição do Amazon S3 para operações de objeto e bucket, consulte os exemplos a seguir. Para obter mais informações sobre essas chaves de condição, consulte Chaves de condição de política para o Amazon S3. Consulte uma lista completa de ações, chaves de condição e recursos do Amazon S3 que você pode especificar em políticas em Actions, resources, and condition keys for Amazon S3 na Referência de autorização do serviço.

Para ter mais informações sobre as permissões referentes a operações de API do S3 de acordo com os tipos de recurso do S3, consulte Permissões obrigatórias para operações de API do Amazon S3.

Exemplos: chaves de condição do Amazon S3 para operações de objeto

Os exemplos a seguir mostram como usar chaves de condição específicas do Amazon S3 para operações de objeto. Consulte uma lista completa de ações, chaves de condição e recursos do Amazon S3 que você pode especificar em políticas em Actions, resources, and condition keys for Amazon S3 na Referência de autorização do serviço.

Para ter mais informações sobre as permissões referentes a operações de API do S3 de acordo com os tipos de recurso do S3, consulte Permissões obrigatórias para operações de API do Amazon S3.

Várias das políticas de exemplo mostram como você pode usar chaves de condições com operações de objeto PUT. As operações de objeto PUT permitem cabeçalhos específicos baseados em lista de controle de acesso (ACL) usados para conceder permissões baseadas em ACL. Usando essas chaves de condição, é possível definir uma condição para exigir permissões de acesso específicas quando o usuário faz upload de um objeto. Você também pode conceder permissões baseadas em ACL com a operação PutoObjectAcl. Para obter mais informações, consulte PutObjectAcl na Referência da API do Amazon S3 Amazon Simple Storage Service. Para obter mais informações sobre ACLs, consulte Visão geral da lista de controle de acesso (ACL).

Tópicos

- Exemplo 1: conceder a permissão s3:PutObject que exige que os objetos sejam armazenados usando criptografia do lado do servidor
- Exemplo 2: conceder a permissão s3:PutObject para copiar objetos com uma restrição na origem da cópia

- Exemplo 3: conceder acesso a uma versão específica de um objeto
- Exemplo 4: conceder permissões com base em tags de objetos
- Exemplo 5: restringir o acesso pelo ID da Conta da AWS do proprietário do bucket
- Exemplo 6: exigir uma versão mínima do TLS
- Exemplo 7: excluir determinadas entidades principais de uma declaração Deny
- Exemplo 8: forçar os clientes a fazer upload de objetos condicionalmente com base nos nomes de chave de objeto ou nas ETags

Exemplo 1: conceder a permissão **`s3:PutObject`** que exige que os objetos sejam armazenados usando criptografia do lado do servidor

Vamos supor que a conta A é proprietária de um bucket. O administrador da conta deseja conceder a Jane, uma usuária na conta A, permissão para fazer upload de objetos com a condição de que Jane sempre solicite a criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3). O administrador da conta A pode especificar esse requisito usando a chave de condição `s3:x-amz-server-side-encryption`, conforme exibido. O par de chave-valor no bloco `Condition` a seguir especifica a chave de condição `s3:x-amz-server-side-encryption` e SSE-S3 (`AES256`) como o tipo de criptografia:

```
"Condition": {
     "StringNotEquals": {
         "s3:x-amz-server-side-encryption": "AES256"
     }}
```

Ao testar essa permissão por meio da AWS CLI, você deve adicionar a criptografia necessária usando o parâmetro `--server-side-encryption`, conforme mostrado no exemplo a seguir. Para usar esse exemplo de comando, substitua os *`user input placeholders`* por suas próprias informações.

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key HappyFace.jpg --body c:
\HappyFace.jpg --server-side-encryption "AES256" --profile AccountAadmin
```

Exemplo 2: conceder a permissão **`s3:PutObject`** para copiar objetos com uma restrição na origem da cópia

Em uma solicitação de objeto PUT, quando se especifica o objeto de origem, a solicitação é uma operação de cópia (consulte CopyObject). De acordo com isso, o proprietário do bucket pode conceder ao usuário permissão para copiar objetos com restrições na origem; por exemplo:

- Permite copiar objetos somente do bucket de origem especificado (por exemplo, *amzn-s3-demo-source-bucket*).
- Permite copiar objetos do bucket de origem especificado e somente os objetos cujo nome de chave comece com um prefixo específico, como *public/* (por exemplo, *amzn-s3-demo-source-bucket/public/**).
- Permite copiar somente um objeto específico do bucket de origem (por exemplo, *amzn-s3-demo-source-bucket/example.jpg*).

A política de bucket a seguir concede a um usuário (*Dave*) a permissão `s3:PutObject`. Essa política permite que ele copie objetos apenas com a condição de que a solicitação inclua o cabeçalho `s3:x-amz-copy-source` e o valor do cabeçalho especifique o prefixo de nome de chave */amzn-s3-demo-source-bucket/public/**. Para usar esse exemplo de política, substitua os *user input placeholders* por suas próprias informações.

```
{
    "Version": "2012-10-17",
    "Statement": [
       {
            "Sid": "cross-account permission to user in your own account",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::123456789012:user/Dave"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
        },
        {
            "Sid": "Deny your user permission to upload object if copy source is not /
bucket/prefix",
            "Effect": "Deny",
            "Principal": {
                "AWS": "arn:aws:iam::123456789012:user/Dave"
            },
```

```
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-source-bucket/*",
            "Condition": {
                "StringNotLike": {
                    "s3:x-amz-copy-source": "amzn-s3-demo-source-bucket/public/*"
                }
            }
        }
    ]
}
```

Testar a política com a AWS CLI

Você pode testar a permissão usando o comando da AWS CLI `copy-object`. Você especifica a origem adicionando o parâmetro `--copy-source`; o prefixo de nome de chave que deve coincidir com o prefixo permitido na política. Você precisa inserir as credenciais do usuário de Dave usando o parâmetro `--profile`. Consulte mais informações sobre como configurar a AWS CLI em Developing with Amazon S3 using the AWS CLI na Referência de API do Amazon S3.

```
aws s3api copy-object --bucket amzn-s3-demo-source-bucket --key HappyFace.jpg
--copy-source amzn-s3-demo-source-bucket/public/PublicHappyFace1.jpg --
profile AccountADave
```

Conceder permissão para copiar somente um objeto específico

A política anterior usa a condição `StringNotLike`. Para conceder a permissão para copiar apenas um objeto específico, é necessário alterar a condição de `StringNotLike` para `StringNotEquals` e, depois, especificar a chave de objeto exata, conforme exibido no exemplo a seguir. Para usar esse exemplo de comando, substitua os *`user input placeholders`* por suas próprias informações.

```
"Condition": {
       "StringNotEquals": {
           "s3:x-amz-copy-source": "amzn-s3-demo-source-bucket/public/
PublicHappyFace1.jpg"
       }
}
```

Exemplo 3: conceder acesso a uma versão específica de um objeto

Vamos supor que a conta A seja proprietária de um bucket habilitado para versionamento. O bucket tem várias versões do objeto *`HappyFace.jpg`*. O administrador da conta A agora deseja conceder

ao usuário *Dave* permissão para receber apenas uma versão específica do objeto. O administrador da conta pode fazer isso concedendo ao usuário *Dave* a permissão `s3:GetObjectVersion` de modo condicional, conforme mostrado no exemplo a seguir. O par de chave-valor no bloco `Condition` especifica a chave de condição `s3:VersionId`. Neste caso, para recuperar o objeto do bucket específico habilitado para versionamento, *Dave* precisa conhecer o ID de versão do objeto exato. Para usar esse exemplo de política, substitua os *user input placeholders* por suas próprias informações.

Para obter mais informações, consulte GetObject na Referência da API do Amazon Simple Storage Service.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "statement1",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::123456789012:user/Dave"
            },
            "Action": "s3:GetObjectVersion",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/HappyFace.jpg"
        },
        {
            "Sid": "statement2",
            "Effect": "Deny",
            "Principal": {
                "AWS": "arn:aws:iam::123456789012:user/Dave"
            },
            "Action": "s3:GetObjectVersion",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/HappyFace.jpg",
            "Condition": {
                "StringNotEquals": {
                    "s3:VersionId": "AaaHbAQitwiL_h47_44lRO2DDfLlBO5e"
                }
            }
        }
    ]
}
```

Testar a política com a AWS CLI

É possível testar as permissões nessa política usando o comando `get-object` da AWS CLI com o parâmetro `--version-id` para identificar a versão específica do objeto a ser recuperada. O comando recupera a versão especificada do objeto e a salva no arquivo *`OutputFile.jpg`*.

```
aws s3api get-object --bucket amzn-s3-demo-bucket --key HappyFace.jpg OutputFile.jpg --
version-id AaaHbAQitwiL_h47_44lRO2DDfLlBO5e --profile AccountADave
```

Exemplo 4: conceder permissões com base em tags de objetos

Para ver exemplos de como usar chaves de condição de marcação de objetos com operações do Amazon S3, consulte Marcação e políticas de controle de acesso.

Exemplo 5: restringir o acesso pelo ID da Conta da AWS do proprietário do bucket

É possível usar a chave de condição `aws:ResourceAccount` ou `s3:ResourceAccount` para gravar políticas de endpoint da nuvem privada virtual (VPC) ou do IAM que restrinjam o acesso de usuários, perfis ou aplicações aos buckets do Amazon S3 pertencentes a um ID de Conta da AWS específico. É possível usar essas chaves de condição para restringir o acesso dos clientes dentro da VPC aos buckets que você não possui.

No entanto, saiba que os serviços da AWS dependem do acesso a buckets gerenciados pela AWS. Portanto, usar a chave `aws:ResourceAccount` ou `s3:ResourceAccount` em sua política do IAM também pode afetar o acesso a esses recursos. Para obter mais informações, consulte os seguintes recursos:

- Restringir o acesso a buckets em uma Conta da AWS especificada no Guia do usuário do AWS PrivateLink
- Restringir o acesso aos buckets que o Amazon ECR usa no Guia do Amazon ECR
- Fornecer acesso necessário ao Systems Manager para buckets do Amazon S3 gerenciados pela AWS no Guia do AWS Systems Manager

Para ter mais informações sobre as chaves de condição `aws:ResourceAccount` e `s3:ResourceAccount` e exemplos que mostram como usá-las, consulte Limit access to Amazon S3 buckets owned by specific Contas da AWS no Blog do AWS Storage.

Exemplo 6: exigir uma versão mínima do TLS

É possível usar a chave de condição `s3:TlsVersion` para gravar políticas do IAM, de endpoint de nuvem privada virtual (VPCE) ou de bucket que restrinjam o acesso de usuários ou de aplicações

aos buckets do Amazon S3 com base na versão de TLS usada pelo cliente. Você pode usar essa chave de condição para gravar políticas que exigem uma versão mínima do TLS.

> **Note**
>
> Quando os serviços da AWS fazem chamadas para outros serviços da AWS em seu nome (chamadas de serviço para serviço), determinado contexto de autorização específico da rede é editado, incluindo `s3:TlsVersion`, `aws:SecureTransport`, `aws:SourceIp` e `aws:VpcSourceIp`. Se sua política usar essas chaves de condição com instruções `Deny`, as entidades principais do serviço da AWS poderão ser bloqueadas acidentalmente. Para permitir que os serviços da AWS funcionem adequadamente, mantendo seus requisitos de segurança, exclua as entidades principais do serviço de suas instruções `Deny` adicionando a chave de condição `aws:PrincipalIsAWSService` com um valor `false`. Por exemplo:
>
> ```
> {
>   "Effect": "Deny",
>   "Action": "s3:*",
>   "Resource": "*",
>   "Condition": {
>     "Bool": {
>       "aws:SecureTransport": "false",
>       "aws:PrincipalIsAWSService": "false"
>     }
>   }
> }
> ```
>
> Essa política nega acesso às operações do S3 quando o HTTPS não é usado (`aws:SecureTransport` é falso), mas somente para entidades principais que não são de serviços da AWS. Isso garante que suas restrições condicionais se apliquem a todas as entidades principais, exceto às entidades principais de serviços da AWS.

Example

O exemplo de política de bucket a seguir nega solicitações `PutObject` de clientes que tenham uma versão de TLS inferior a 1.2; por exemplo, 1.1 ou 1.0. Para usar esse exemplo de política, substitua os *`user input placeholders`* por suas próprias informações.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:PutObject",
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket1",
                "arn:aws:s3:::amzn-s3-demo-bucket1/*"
            ],
            "Condition": {
                "NumericLessThan": {
                    "s3:TlsVersion": 1.2
                }
            }
        }
    ]
}
```

Example

O exemplo de política de bucket a seguir permite solicitações `PutObject` de clientes que têm uma versão de TLS posterior a 1.1; por exemplo, 1.2, 1.3 ou posterior:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:PutObject",
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket1",
                "arn:aws:s3:::amzn-s3-demo-bucket1/*"
            ],
            "Condition": {
                "NumericGreaterThan": {
                    "s3:TlsVersion": 1.1
                }
            }
        }
```

```
    ]
}
```

Exemplo 7: excluir determinadas entidades principais de uma declaração **Deny**

A política de bucket a seguir nega acesso `s3:GetObject` ao *amzn-s3-demo-bucket*, exceto às entidades principais com o número de conta *123456789012*. Para usar esse exemplo de política, substitua os *user input placeholders* por suas próprias informações.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyAccessFromPrincipalNotInSpecificAccount",
      "Principal": {
        "AWS": "*"
      },
      "Action": "s3:GetObject",
      "Effect": "Deny",
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
      ],
      "Condition": {
        "StringNotEquals": {
          "aws:PrincipalAccount": [
            "123456789012"
          ]
        }
      }
    }
  ]
}
```

Exemplo 8: forçar os clientes a fazer upload de objetos condicionalmente com base nos nomes de chave de objeto ou nas ETags

Com gravações condicionais, é possível adicionar outro cabeçalho às solicitações `WRITE` a fim de especificar condições prévias para a operação do S3. Esse cabeçalho especifica uma condição que, se não for atendida, provocará uma falha na operação do S3. Por exemplo, você pode evitar a substituição de dados existentes ao confirmar que não há nenhum objeto com o mesmo nome de

chave no bucket durante o upload do objeto. Você também pode verificar a tag de entidade (ETag) de um objeto no Amazon S3 antes de gravar um objeto.

Para conferir exemplos de políticas de bucket que usam condições para impor gravações condicionais, consulte the section called “Impor gravações condicionais”.

Exemplos: chaves de condição do Amazon S3 para operações de bucket

As políticas de exemplo a seguir mostram como usar chaves de condição específicas do Amazon S3 para operações de bucket.

Tópicos

- Exemplo 1: conceder a permissão s3:GetObject com uma condição em um endereço IP
- Exemplo 2: obter uma lista de objetos em um bucket com um prefixo específico
- Exemplo 3: definir o número máximo de chaves

Exemplo 1: conceder a permissão **`s3:GetObject`** com uma condição em um endereço IP

Será possível conceder a usuários autenticados permissão para usar a ação `s3:GetObject`, se a solicitação for proveniente de um intervalo específico de endereços IP (por exemplo, *`192.0.2.*`*), a menos que o endereço IP seja um dos que você queira excluir (por exemplo, *`192.0.2.188`*). No bloco `Condition`, `IpAddress` e `NotIpAddress` são condições, e cada uma recebe um par de chave-valor para avaliação. Os dois pares de chave-valor neste exemplo usam a chave `aws:SourceIp` em toda a AWS. Para usar esse exemplo de política, substitua os *`user input placeholders`* por suas próprias informações.

> **Note**
>
> Os valores de chave `IPAddress` e `NotIpAddress` especificados no bloco `Condition` usam notação CIDR conforme descrito na RFC 4632. Para obter mais informações,consulte http://www.rfc-editor.org/rfc/rfc4632.txt.

```
{
    "Version": "2012-10-17",
    "Id": "S3PolicyId1",
    "Statement": [
        {
```

```
            "Sid": "statement1",
            "Effect": "Allow",
            "Principal": "*",
            "Action":"s3:GetObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
            "Condition" : {
                "IpAddress" : {
                    "aws:SourceIp": "192.0.2.0/24"
                },
                "NotIpAddress" : {
                    "aws:SourceIp": "192.0.2.188/32"
                }
            }
        }
    ]
}
```

Você também pode usar outras chaves de condição de toda a AWS nas políticas do Amazon S3. Por exemplo, você pode especificar o `aws:SourceVpce` e as chaves de condição `aws:SourceVpc` em políticas de bucket para VPC endpoints. Para obter exemplos específicos, consulte Controlar o acesso a partir de VPC endpoints com políticas de bucket.

> **Note**
>
> Em relação a algumas chaves de condição globais da AWS, somente certos tipos de recurso são compatíveis. Portanto, confira se o Amazon S3 é compatível com a chave de condição global e o tipo de recurso que você deseja usar ou se você precisará usar uma chave de condição específica do Amazon S3. Consulte uma lista completa de chaves de condição e tipos de recurso compatíveis com o Amazon S3 em Actions, resources, and condition keys for Amazon S3 na Referência de autorização do serviço.
>
> Para ter mais informações sobre as permissões referentes a operações de API do S3 de acordo com os tipos de recurso do S3, consulte Permissões obrigatórias para operações de API do Amazon S3.

Exemplo 2: obter uma lista de objetos em um bucket com um prefixo específico

É possível usar a chave de condição `s3:prefix` para limitar a resposta da operação de API ListObjectsV2 a nomes de chave com um prefixo específico. Se o bucket pertencer a você, será possível usar essa chave de condição para impedir que um usuário liste o conteúdo de um prefixo

específico no bucket. A chave de condição `s3:prefix` será útil se os objetos no bucket forem organizados por prefixos de nome de chave.

O console do Amazon S3 usa prefixos de nomes de chaves para mostrar um conceito de pasta. Somente o console suporta o conceito de pastas; a API do Amazon S3 suporta somente buckets e objetos. Por exemplo, se você tiver dois objetos com nomes de chave *`public/object1.jpg`* e *`public/object2.jpg`*, o console mostrará os objetos na pasta *`public`*. Na API do Amazon S3, esses são objetos com prefixos, não objetos em pastas. Para obter mais informações sobre como usar prefixos e delimitadores para filtrar permissões de acesso, consulte Controlar o acesso a um bucket com políticas de usuário.

No caso a seguir, o proprietário do bucket e a conta principal à qual o usuário pertence são os mesmos. Assim, o proprietário do bucket pode usar uma política de bucket ou uma política de usuário para conceder acesso. Para ter mais informações sobre outras chaves de condição que você pode usar para chamar a operação de API `ListObjectsV2`, consulte ListObjectsV2.

> **Note**
>
> Se o bucket tiver o versionamento habilitado, para listar os objetos no bucket, você deverá conceder a permissão `s3:ListBucketVersions` nas políticas a seguir, em vez da permissão `s3:ListBucket`. A permissão `s3:ListBucketVersions` também comporta a chave de condição `s3:prefix`.

Política de usuário

A política de usuário a seguir concede a permissão `s3:ListBucket` (consulte ListObjectsV2) com uma declaração `Condition` que exige que o usuário especifique um prefixo na solicitação com um valor de *`projects`*. Para usar esse exemplo de política, substitua os *`user input placeholders`* por suas próprias informações.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"statement1",
         "Effect":"Allow",
         "Action": "s3:ListBucket",
         "Resource":"arn:aws:s3:::amzn-s3-demo-bucket",
         "Condition" : {
```

```
            "StringEquals" : {
                "s3:prefix": "projects"
            }
         }
      },
      {
         "Sid":"statement2",
         "Effect":"Deny",
         "Action": "s3:ListBucket",
         "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
         "Condition" : {
            "StringNotEquals" : {
                "s3:prefix": "projects"
            }
         }
      }
   ]
}
```

A declaração `Condition` determina que o usuário liste apenas as chaves de objeto com o prefixo *`projects`*. A declaração `Deny` explícita adicionada nega ao usuário a listagem de chaves com qualquer outro prefixo, independentemente de outras permissões que ele possa ter. Por exemplo, é possível que o usuário receba a permissão para listar chaves de objeto sem nenhuma restrição, tanto por meio de atualizações na política de usuário anterior quanto por meio de uma política de bucket. Como as declarações `Deny` explícitas sempre substituem as declarações `Allow`, se o usuário tentar indicar chaves que não tenham o prefixo *`projects`*, a solicitação será negada.

Política de bucket

Se você adicionar o elemento `Principal` à política de usuário acima, identificando o usuário, terá uma política de bucket conforme exibido no exemplo a seguir. Para usar esse exemplo de política, substitua os *`user input placeholders`* por suas próprias informações.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"statement1",
         "Effect":"Allow",
         "Principal": {
            "AWS": "arn:aws:iam::123456789012:user/bucket-owner"
         },
```

```
         "Action":  "s3:ListBucket",
         "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
         "Condition" : {
             "StringEquals" : {
                 "s3:prefix": "projects"
             }
          }
       },
      {
         "Sid":"statement2",
         "Effect":"Deny",
         "Principal": {
            "AWS": "arn:aws:iam::123456789012:user/bucket-owner"
         },
         "Action": "s3:ListBucket",
         "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
         "Condition" : {
             "StringNotEquals" : {
                 "s3:prefix": "projects"
             }
          }
       }
    ]
}
```

Testar a política com a AWS CLI

Você pode testar a política usando o seguinte comando `list-object` da AWS CLI. No comando, você fornece as credenciais do usuário usando o parâmetro `--profile`. Consulte mais informações sobre como configurar e usar a AWS CLI em Developing with Amazon S3 using the AWS CLI na Referência de API do Amazon S3.

```
aws s3api list-objects --bucket amzn-s3-demo-bucket --prefix projects --
profile AccountA
```

Exemplo 3: definir o número máximo de chaves

É possível usar a chave de condição `s3:max-keys` para definir o número máximo de chaves que um solicitante pode exibir em uma solicitação ListObjectsV2 ou ListObjectVersions. Por padrão, essas operações de API exibem até mil chaves. Para obter uma lista de operadores de condição numérica que você pode usar com `s3:max-keys` e exemplos associados, consulte Operadores de condição numérica no Guia do usuário do IAM.

Políticas baseadas em identidade do Amazon S3

Por padrão, usuários e perfis não têm permissão para criar ou modificar recursos do Amazon S3. Eles também não podem executar tarefas usando o AWS Management Console, a AWS Command Line Interface (AWS CLI) ou a API da AWS. Para conceder aos usuários permissões para executar ações nos recursos que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM aos perfis e os usuários podem assumir os perfis.

Para saber como criar uma política baseada em identidade do IAM usando esses exemplos de documento de política JSON, consulte Criar políticas do IAM (no console) no Guia do usuário do IAM.

Consulte detalhes sobre ações e tipos de recurso definidos pelo Amazon S3, incluindo o formato dos ARNs para cada tipo de recurso, em Actions, resources, and condition keys for Amazon S3 na Referência de autorização do serviço.

Para ter mais informações sobre as permissões referentes a operações de API do S3 de acordo com os tipos de recurso do S3, consulte Permissões obrigatórias para operações de API do Amazon S3.

Tópicos

- Práticas recomendadas de política
- Controlar o acesso a um bucket com políticas de usuário
- Exemplos de políticas baseadas em identidade para o Amazon S3

Práticas recomendadas de política

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir recursos do Amazon S3 em sua conta. Essas ações podem incorrer em custos para sua Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo: para começar a conceder permissões a seus usuários e workloads, use as políticas gerenciadas pela AWS, que concedem permissões para muitos casos de uso comuns. Elas estão disponíveis em seus Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo cliente da AWS que são específicas para seus casos de uso. Para obter mais informações, consulte Políticas gerenciadas pela AWS ou Políticas gerenciadas pela AWS para funções de trabalho no Guia do usuário do IAM.

- Aplique permissões de privilégio mínimo: ao definir permissões com as políticas do IAM, conceda apenas as permissões necessárias para executar uma tarefa. Você faz isso definindo as ações que podem ser executadas em recursos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para obter mais informações sobre como usar o IAM para aplicar permissões, consulte Políticas e permissões no IAM no Guia do usuário do IAM.
- Use condições nas políticas do IAM para restringir ainda mais o acesso: você pode adicionar uma condição às políticas para limitar o acesso a ações e recursos. Por exemplo, você pode escrever uma condição de política para especificar que todas as solicitações devem ser enviadas usando SSL. Também pode usar condições para conceder acesso a ações de serviço, se elas forem usadas por meio de um AWS service (Serviço da AWS) específico, como o AWS CloudFormation. Para obter mais informações, consulte Elementos da política JSON do IAM: condição no Guia do usuário do IAM.
- Use o IAM Access Analyzer para validar suas políticas do IAM a fim de garantir permissões seguras e funcionais: o IAM Access Analyzer valida as políticas novas e existentes para que elas sigam a linguagem de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access Analyzer oferece mais de cem verificações de política e recomendações práticas para ajudar a criar políticas seguras e funcionais. Para obter mais informações, consulte Validação de políticas do IAM Access Analyzer no Guia do Usuário do IAM.
- Exigir autenticação multifator (MFA): se houver um cenário que exija usuários do IAM ou um usuário raiz em sua Conta da AWS, ative a MFA para obter segurança adicional. Para exigir MFA quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para obter mais informações, consulte Configuração de acesso à API protegido por MFA no Guia do Usuário do IAM.

Para obter mais informações sobre as práticas recomendadas do IAM, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.

Controlar o acesso a um bucket com políticas de usuário

Esta demonstração explica como as permissões de usuário funcionam com o Amazon S3. Nesse exemplo, você cria um bucket com pastas. Depois, crie usuários do AWS Identity and Access Management (IAM) na sua Conta da AWS e conceda a eles permissões incrementais no bucket do Amazon S3 e nas pastas dele.

Tópicos

- Elementos básicos de buckets e pastas

- Resumo da demonstração
- Preparar para a demonstração
- Etapa 1: Criar um bucket
- Etapa 2: criar usuários do IAM e um grupo
- Etapa 3: verificar se os usuários do IAM não têm nenhuma permissão
- Etapa 4: Conceder permissões no nível do grupo
- Etapa 5: conceder permissões específicas do usuário do IAM Alice
- Etapa 6: conceder permissões específicas do usuário do IAM Bob
- Etapa 7: Proteger a pasta Private
- Etapa 8: Limpar
- Recursos relacionados

Elementos básicos de buckets e pastas

O modelo de dados do Amazon S3 é uma estrutura plana: você cria um bucket e o bucket armazena objetos. Não há hierarquia de buckets ou de subpastas, mas você pode emular uma hierarquia de pastas. Ferramentas como o console do Amazon S3 podem apresentar uma visualização dessas pastas e subpastas lógicas no bucket.

O console mostra que o bucket nomeado `companybucket` tem três pastas, `Private`, `Development` e `Finance`, e um objeto, `s3-dg.pdf`. O console usa os nomes de objeto (chaves) para criar uma hierarquia lógica com pastas e subpastas. Considere os seguintes exemplos:

- Ao criar a pasta `Development`, o console cria um objeto com a chave `Development/`. Observe delimitador (`/`) no final.
- Quando você faz upload de um objeto chamado `Projects1.xls` na pasta `Development`, o console sobe o objeto e concede a ele a chave `Development/Projects1.xls`.

  Na chave, `Development` é o prefixo e `/` é o delimitador. A API do Amazon S3 oferece suporte a prefixos e delimitadores em suas operações. Por exemplo, você pode obter uma lista de todos os objetos no bucket com um prefixo e um delimitador específicos. No console, quando você abre a pasta `Development`, o console lista os objetos nela. No exemplo a seguir, a pasta `Development` contém um objeto.

  Quando o console lista a pasta `Development` no bucket `companybucket`, ele envia uma solicitação para o Amazon S3 na qual especifica o prefixo `Development` e o delimitador `/` na

solicitação. A resposta do console parece uma lista de pastas no sistema de arquivos de seu computador. O exemplo anterior mostra que o bucket `companybucket` tem um objeto com a chave `Development/Projects1.xls`.

O console está usando chaves de objeto para inferir uma hierarquia lógica. O Amazon S3 não tem hierarquia física. O Amazon S3 só tem buckets que contêm objetos em uma estrutura de arquivos simples. Ao criar objetos usando a API do Amazon S3, você pode usar chaves de objeto que implicam uma hierarquia lógica. Ao criar uma hierarquia lógica de objetos, você pode gerenciar o acesso a pastas individuais, como este passo a passo ensina.

Antes de começar, você precisa conhecer o conceito de conteúdo no nível raiz do bucket. Suponha que seu bucket `companybucket` contenha os seguintes objetos:

- `Private/privDoc1.txt`
- `Private/privDoc2.zip`
- `Development/project1.xls`
- `Development/project2.xls`
- `Finance/Tax2011/document1.pdf`
- `Finance/Tax2011/document2.pdf`
- `s3-dg.pdf`

Essas chaves de objeto criam uma hierarquia lógica com `Private`, `Development` e `Finance` como pastas no nível raiz, e `s3-dg.pdf` como objeto no nível raiz. Quando você escolhe o nome do bucket no console do Amazon S3, os itens no nível raiz são exibidos. O console exibe os prefixos no nível superior (`Private/`, `Development/` e `Finance/`) como pastas no nível raiz. A chave de `s3-dg.pdf` não tem um prefixo, então, ela aparece como um item no nível raiz.

Resumo da demonstração

Neste passo a passo, você cria um bucket com três pastas (`Private`, `Development` e `Finance`).

Você tem dois usuários, Alice e Bob. Você quer que a Alice tenha acesso somente à pasta `Development`, e Bob tenha acesso à `Finance`. Você quer manter o conteúdo da pasta `Private` privado. Na demonstração, você gerencia o acesso criando usuários do IAM (o exemplo usa os mesmos nomes de usuário, Alice e Bob) e concede as permissões necessárias.

O IAM também permite criar grupos de usuários e conceder permissões no nível do grupo que se aplicam a todos os usuários no grupo. Isso ajuda a gerenciar melhor as permissões. Neste exercício, Alice e Bob precisam ter algumas permissões comuns. Então, você também cria um grupo chamado `Consultants` e adiciona Alice e Bob a ele. Primeiro, você concede permissões anexando uma política de grupo ao grupo. Depois, adiciona permissões específicas do usuário anexando políticas a usuários específicos.

> **Note**
>
> O passo a passo usa `companybucket` como o nome do bucket, Alice e Bob como os usuários do `Consultants`, e IAM como o nome do grupo. Como o Amazon S3 exige que os nomes de bucket sejam globalmente exclusivos, você precisará substituir o nome do bucket pelo nome que criar.

Preparar para a demonstração

Neste exemplo, use suas credenciais da Conta da AWS para criar usuários do IAM. Inicialmente, esses usuários não têm nenhuma permissão. Você concede gradualmente a esses usuários as permissões para executar ações específicas do Amazon S3. Para testar essas permissões, você entra no console com as credenciais de cada usuário. À medida que conceder gradualmente permissões como proprietário da Conta da AWS e testar permissões como um usuário do IAM, você precisará entrar e sair, sempre usando credenciais diferentes. Você pode fazer o teste em apenas um navegador, mas o processo é mais rápido se você usar dois navegadores diferentes. Use um navegador para se conectar ao AWS Management Console com as suas credenciais da Conta da AWS e outro para se conectar com as credenciais de usuário do IAM.

Para fazer login no AWS Management Console com as credenciais da sua Conta da AWS, acesse https://console.aws.amazon.com/. Um usuário do IAM não pode fazer login com o mesmo link. Um usuário do IAM deve usar uma página de login habilitada para o IAM. Como proprietário da conta, você pode fornecer este link para seus usuários.

Para obter mais informações sobre o IAM, consulte a página sobre login no AWS Management Console no Guia do usuário do IAM.

Para fornecer um link de login para usuários do IAM

1. Faça login no AWS Management Console e abra o console do IAM em https://console.aws.amazon.com/iam/.

2. No painel Navigation (Navegação), escolha IAM Dashboard (Painel do IAM).
3. Observe o URL em IAM users sign in link: (Link de login de usuários do IAM:). Você dará este link para usuários do IAM entrarem no console com seu nome de usuário e senha do IAM.

Etapa 1: Criar um bucket

Nesta etapa, você faz login no console do Amazon S3 com suas credenciais da Conta da AWS, cria um bucket, adiciona pastas a ele e carrega uma ou duas amostras de documentos em cada pasta.

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Crie um bucket.

   Para obter instruções detalhadas, consulte Criar um bucket de uso geral.
3. Faça upload de um documento no bucket.

   Este exercício pressupõe que você tem o documento `s3-dg.pdf` no nível raiz desse bucket. Se você carregar um documento diferente, substitua o nome de arquivo para `s3-dg.pdf`.
4. Adicione três pastas nomeadas `Private`, `Finance` e `Development` ao bucket.

   Para obter instruções detalhadas para criar uma pasta, consulte Organizar objetos no console do Amazon S3 usando pastas> no Manual do usuário do Amazon Simple Storage Service.
5. Faça upload de um ou dois documentos em cada pasta.

   Neste exercício, suponha que você tenha carregado alguns documentos em cada pasta, resultando que o bucket tenha objetos com as seguintes chaves:

   - `Private/privDoc1.txt`
   - `Private/privDoc2.zip`
   - `Development/project1.xls`
   - `Development/project2.xls`
   - `Finance/Tax2011/document1.pdf`
   - `Finance/Tax2011/document2.pdf`
   - `s3-dg.pdf`

Para obter instruções detalhadas, consulte Fazer upload de objetos.

Etapa 2: criar usuários do IAM e um grupo

Agora, use o console do IAM para adicionar dois usuários do IAM, Alice e Bob, à sua Conta da AWS. Para obter instruções passo a passo, consulte Criar um usuário do IAM na sua Conta da AWS no Guia do usuário do IAM.

Crie também um grupo administrativo chamado `Consultants`. Depois, adicione os dois usuários ao grupo. Para obter instruções passo a passo, consulte Criação de grupos de usuários do IAM.

> **Warning**
>
> Quando você adicionar usuários e um grupo, não anexe políticas que concedem permissões a esses usuários. No início, esses usuários não terão permissões. Nas próximas seções, você concederá permissões incrementalmente. Primeiro verifique se atribuiu senhas a esses usuários do IAM. Você utilizará essas credenciais de usuário para testar as ações do Amazon S3 e verificar se as permissões funcionam como esperado.

Consulte instruções detalhadas de como criar um usuário do IAM em Criar um usuário do IAM na sua Conta da AWS no Guia do usuário do IAM. Ao criar usuários seguindo este passo a passo, selecione Acesso ao AWS Management Console e desmarque Acesso programático.

Para obter instruções passo a passo para criar um grupo administrativo, consulte Criar seu primeiro usuário administrador e grupo do IAM no Guia do usuário do IAM.

Etapa 3: verificar se os usuários do IAM não têm nenhuma permissão

Se você estiver usando dois navegadores, agora poderá usar o segundo navegador para entrar no console usando uma das credenciais de usuário do IAM.

1. Usando o link de login de usuário do IAM (consulte Para fornecer um link de login para usuários do IAM), entre no AWS Management Console usando qualquer uma das credenciais de usuário do IAM.
2. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.

   Verifique a mensagem do console que informa que o acesso foi negado.

Agora, você pode começar a conceder permissões incrementais aos usuários. Antes, você anexará uma política de grupo concedendo as permissões de que os dois usuários precisam.

Etapa 4: Conceder permissões no nível do grupo

Você quer que os usuários possam fazer o seguinte:

- Listar todos os buckets de propriedade da conta pai. Para fazer isso, Bob e Alice devem ter permissão para a ação `s3:ListAllMyBuckets`.
- Listar itens, pastas e objetos no nível raiz no bucket `companybucket`. Para fazer isso, Bob e Alice devem ter permissão para a ação `s3:ListBucket` no bucket `companybucket`.

Primeiro, você cria uma política que concede essas permissões e, depois, anexa-a ao grupo `Consultants`.

Etapa 4.1: Conceder permissão para listar todos os buckets

Nesta etapa, você cria uma política gerenciada que concede aos usuários as permissões mínimas para listar todos os buckets de propriedade da conta pai. Depois, anexa a política ao grupo `Consultants`. Ao anexar a política gerenciada a um usuário ou um grupo, você concede ao usuário ou grupo a permissão para obter uma lista de buckets de propriedade da Conta da AWS pai.

1. Faça login no AWS Management Console e abra o console do IAM em https://console.aws.amazon.com/iam/.

   > **Note**
   >
   > Como você está concedendo permissões de usuário, faça login com suas credenciais da Conta da AWS, e não como um usuário do IAM.

2. Crie a política gerenciada.

   a. No painel de navegação à esquerda, escolha Policies (Políticas) e Create Policy (Criar política).

   b. Selecione a guia JSON.

   c. Copie a política de acesso a seguir e cole-a no campo de texto da política.

```
{
  "Version": "2012-10-17",
```

```
  "Statement": [
    {
      "Sid": "AllowGroupToSeeBucketListInTheConsole",
      "Action": ["s3:ListAllMyBuckets"],
      "Effect": "Allow",
      "Resource": ["arn:aws:s3:::*"]
    }
  ]
}
```

Uma política é um documento JSON. No documento, uma `Statement` é uma matriz de objetos, cada uma descrevendo uma permissão usando uma coleção de pares de valores de nome. A política anterior descreve uma permissão específica. A `Action` especifica o tipo de acesso. Na política, `s3:ListAllMyBuckets` é uma ação do Amazon S3 predefinida. Esta ação abrange a operação GET Service do Amazon S3, que retorna uma lista de todos os buckets pertencentes ao remetente autenticado. O valor do elemento `Effect` determina se a permissão específica é permitida ou negada.

d. Escolha Review Policy (Revisar política). Na próxima página, insira `AllowGroupToSeeBucketListInTheConsole` no campo Name (Nome) e escolha em Create policy (Criar política).

> **Note**
>
> A entrada Summary (Resumo) exibe uma mensagem afirmando que a política não concede permissão nenhuma. Para esta apresentação, você pode, de maneira segura, ignorar essa mensagem.

3. Anexe a política gerenciada `AllowGroupToSeeBucketListInTheConsole` que você criou para o grupo `Consultants`.

   Consulte instruções detalhadas de como anexar uma política gerenciada em Adicionar e remover permissões de identidade do IAM no Guia do usuário do IAM.

   Anexe documentos de política a usuários e grupos do IAM no console do IAM. Como você quer que os dois usuários possam listar os buckets, você anexa a política ao grupo.

4. Teste a permissão.

a. Usando o link de login de usuário do IAM (consulte Para fornecer um link de login para usuários do IAM), entre no console usando qualquer uma das credenciais de usuário do IAM.

b. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.

   O console agora deve listar todos os buckets, mas não os objetos dos buckets.

Etapa 4.2: Permitir que os usuários listem o conteúdo do nível raiz de um bucket

Agora, você permite que todos os usuários no grupo `Consultants` listem itens no nível raiz do bucket `companybucket`. Quando um usuário escolhe o bucket da empresa no console do Amazon S3, ele pode visualizar os itens no nível raiz do bucket.

> **Note**
>
> Esse exemplo usa `companybucket` como ilustração. Use o nome do bucket que você criou.

Para entender a solicitação que o console envia ao Amazon S3 quando você escolhe o nome de um bucket, a resposta que o Amazon S3 retorna e como o console a interpreta, examine o fluxo mais detalhadamente.

Quando você clica no nome de um bucket, o console envia a solicitação GET Bucket ao Amazon S3. Essa solicitação inclui os parâmetros a seguir:

- O parâmetro `prefix` com uma string vazia como valor.
- O parâmetro `delimiter` com `/` como valor.

Veja a seguir uma solicitação de exemplo.

```
GET ?prefix=&delimiter=/ HTTP/1.1
Host: companybucket.s3.amazonaws.com
Date: Wed, 01 Aug  2012 12:00:00 GMT
Authorization: AWS AKIAIOSFODNN7EXAMPLE:xQE0diMbLRepdf3YB+FIEXAMPLE=
```

O Amazon S3 retorna uma resposta que inclui o seguinte elemento `<ListBucketResult/>`.

```
<ListBucketResult xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
```

```
  <Name>companybucket</Name>
  <Prefix></Prefix>
  <Delimiter>/</Delimiter>
   ...
  <Contents>
    <Key>s3-dg.pdf</Key>
    ...
  </Contents>
  <CommonPrefixes>
    <Prefix>Development/</Prefix>
  </CommonPrefixes>
  <CommonPrefixes>
    <Prefix>Finance/</Prefix>
  </CommonPrefixes>
  <CommonPrefixes>
    <Prefix>Private/</Prefix>
  </CommonPrefixes>
</ListBucketResult>
```

O objeto `s3-dg.pdf` da chave não contém o delimitador `/`, e o Amazon S3 retorna a chave no elemento `<Contents>`. Contudo, todas as outras chaves no bucket de exemplo contêm o delimitador `/`. O Amazon S3 agrupa essas chaves e retorna um elemento `<CommonPrefixes>` para cada um dos valores distintos de prefixo `Development/`, `Finance/` e `Private/`, isto é, uma substring desde o início dessas chaves até a primeira ocorrência do delimitador `/` especificado.

O console interpreta este resultado e exibe os itens no nível raiz como três pastas e uma chave de objeto.

Se Bob ou Alice abrirem a pasta Development (Desenvolvimento), o console enviará a solicitação GET Bucket (Listar objetos) ao Amazon S3 com os parâmetros `prefix` e `delimiter` definidos como os seguintes valores:

- O parâmetro `prefix` com valor `Development/`.
- O parâmetro `delimiter` com valor "`/`".

Em resposta, o Amazon S3 retorna as chaves de objeto que começam com o prefixo especificado.

```
<ListBucketResult xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Name>companybucket</Name>
  <Prefix>Development</Prefix>
  <Delimiter>/</Delimiter>
```

```
   ...
  <Contents>
    <Key>Project1.xls</Key>
    ...
  </Contents>
  <Contents>
    <Key>Project2.xls</Key>
    ...
  </Contents>
</ListBucketResult>
```

O console mostra as chaves de objeto.

Agora, volte a conceder aos usuários a permissão para listar itens no nível raiz do bucket. Para listar conteúdo de bucket, os usuários precisam de permissão para chamar a ação `s3:ListBucket`, conforme exibido na seguinte declaração de política. Para garantir que eles vejam somente o conteúdo no nível raiz, você adiciona uma condição de que os usuários devem especificar um `prefix` vazio na solicitação, isto é, eles não podem clicar duas vezes em nenhuma das pastas no nível raiz. Finalmente, você adiciona uma condição para solicitar o acesso de pasta exigindo que as solicitações de usuário incluam o parâmetro `delimiter` com valor "/".

```
{
  "Sid": "AllowRootLevelListingOfCompanyBucket",
  "Action": ["s3:ListBucket"],
  "Effect": "Allow",
  "Resource": ["arn:aws:s3:::companybucket"],
  "Condition":{
         "StringEquals":{
             "s3:prefix":[""], "s3:delimiter":["/"]
                       }
              }
}
```

Quando você escolhe o bucket no console do Amazon S3, o console primeiro envia a solicitação GET Bucket location para encontrar a Região da AWS em que o bucket está implantado. Depois, o console usa o endpoint específico da região para o bucket enviar a solicitação GET Bucket (listar objetos). Como resultado, se os usuários forem usar o console, você deverá conceder permissão para a ação `s3:GetBucketLocation` conforme exibido na seguinte declaração de política.

```
{
   "Sid": "RequiredByS3Console",
```

```
   "Action": ["s3:GetBucketLocation"],
   "Effect": "Allow",
   "Resource": ["arn:aws:s3:::*"]
}
```

Para permitir que os usuários listem o conteúdo do nível raiz do bucket

1. Faça login no AWS Management Console e abra o console do IAM em https://console.aws.amazon.com/iam/.

   Use as credenciais da sua Conta da AWS, e não as credenciais de um usuário do IAM, para fazer login no console.

2. Substitua a política gerenciada existente `AllowGroupToSeeBucketListInTheConsole` que está anexada ao grupo `Consultants` pela política a seguir, que também permite a ação `s3:ListBucket`. Lembre-se de substituir *`companybucket`* na política `Resource` pelo nome do bucket.

   Consulte instruções detalhadas em Edição de políticas do IAM no Guia do usuário do IAM. Ao seguir as instruções detalhadas, siga as etapas para aplicar as alterações em todas as entidades principais às quais a política está anexada.

   ```
   {
     "Version": "2012-10-17",
     "Statement": [
        {
          "Sid":
    "AllowGroupToSeeBucketListAndAlsoAllowGetBucketLocationRequiredForListBucket",
          "Action": [ "s3:ListAllMyBuckets", "s3:GetBucketLocation" ],
          "Effect": "Allow",
          "Resource": [ "arn:aws:s3:::*"  ]
        },
        {
          "Sid": "AllowRootLevelListingOfCompanyBucket",
          "Action": ["s3:ListBucket"],
          "Effect": "Allow",
          "Resource": ["arn:aws:s3:::companybucket"],
          "Condition":{
                "StringEquals":{
                       "s3:prefix":[""], "s3:delimiter":["/"]
                              }
                    }
   ```

```
      }
    ]
}
```

3. Teste as permissões atualizadas.

   a. Usando o link de login de usuário do IAM (consulte Para fornecer um link de login para usuários do IAM), acesse o AWS Management Console.

      Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.

   b. Escolha o bucket que você criou, e o console mostrará os itens no nível raiz do bucket. Se você escolher alguma pasta no bucket, não verá o conteúdo dela, porque ainda não concedeu essas permissões.

Esse teste é bem-sucedido quando os usuários usam o console do Amazon S3. Ao escolher um bucket no console, a implementação do console envia uma solicitação que inclui o parâmetro `prefix` com uma string vazia como seu valor e o parâmetro `delimiter` com "`/`" como valor.

Etapa 4.3: Resumo da política de grupo

O efeito final da política de grupo que você adicionou é conceder aos usuários do IAM Alice e Bob as seguintes permissões mínimas:

- Listar todos os buckets de propriedade da conta pai.
- Ver itens no nível raiz no bucket `companybucket`.

Contudo, os usuários ainda não podem fazer muita coisa. Agora, conceda as permissões específicas do usuário da seguinte maneira:

- Permite que a Alice obtenha e coloque objetos na pasta `Development`.
- Permite que o Bob obtenha e coloque objetos na pasta `Finance`.

Para permissões específicas do usuário, anexe uma política ao usuário específico, não ao grupo. Na próxima seção, conceda permissão para a Alice trabalhar na pasta `Development`. Você pode repetir as etapas para conceder a Bob permissão semelhante para trabalhar na pasta `Finance`.

Etapa 5: conceder permissões específicas do usuário do IAM Alice

Agora você concede permissões adicionais a Alice para que ela possa ver o conteúdo da pasta `Development` e obter e colocar objetos nela.

Etapa 5.1: conceder permissão do usuário do IAM Alice para listar o conteúdo da pasta Development

Para que Alice possa listar o conteúdo da pasta `Development`, você deve aplicar uma política à usuária Alice concedendo permissão para a ação `s3:ListBucket` no bucket `companybucket`, contanto que a solicitação inclua o prefixo `Development/`. Você quer que essa política seja aplicada somente ao usuário Alice, então, usa uma política em linha. Para obter mais informações sobre políticas em linha, consulte Políticas gerenciadas e em linha no Guia do usuário do IAM.

1. Faça login no AWS Management Console e abra o console do IAM em https://console.aws.amazon.com/iam/.

   Use as credenciais da sua Conta da AWS, e não as credenciais de um usuário do IAM, para fazer login no console.
2. Crie uma política em linha para conceder ao usuário Alice permissão para listar o conteúdo da pasta `Development`.

   a. No painel de navegação à esquerda, escolha Uses (Usuários).
   b. Selecione o nome de usuário Alice.
   c. Na página de detalhes do usuário, selecione a guia Permissions (Permissões) e escolha Add inline policy (Adicionar política em linha).
   d. Selecione a guia JSON.
   e. Copie a política a seguir e cole-a no campo de texto da política.

```
{
    "Version": "2012-10-17",
    "Statement": [
    {
      "Sid": "AllowListBucketIfSpecificPrefixIsIncludedInRequest",
      "Action": ["s3:ListBucket"],
      "Effect": "Allow",
      "Resource": ["arn:aws:s3:::companybucket"],
      "Condition":{  "StringLike":{"s3:prefix":["Development/*"] }
       }
    }
  ]
```

```
}
```

f. Escolha Review Policy (Revisar política). Na próxima página, insira um nome no campo Name (Nome) e escolha Create policy (Criar política).

3. Teste a alteração nas permissões de Alice:

   a. Usando o link de login de usuário do IAM (consulte Para fornecer um link de login para usuários do IAM), acesse o AWS Management Console.

   b. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.

   c. No console do Amazon S3, verifique se Alice pode visualizar a lista de objetos na pasta `Development/` no bucket.

      Quando o usuário escolhe a pasta `/Development` para visualizar a lista de objetos nela, o console do Amazon S3 envia a solicitação `ListObjects` ao Amazon S3 com o prefixo `/Development`. Como o usuário recebe permissão para visualizar a lista de objetos com o prefixo `Development` e o delimitador `/`, o Amazon S3 retorna a lista de objetos com o prefixo de chave `Development/`, e o console exibe a lista.

Etapa 5.2: conceder permissões do usuário do IAM Alice para obter e colocar objetos na pasta Development

Para que a Alice possa obter e colocar objetos na pasta `Development`, ela precisa de permissão para chamar as ações `s3:GetObject` e `s3:PutObject`. As declarações de política a seguir concedem essas permissões, contanto que a solicitação inclua o parâmetro `prefix` com um valor de `Development/`.

```
{
    "Sid":"AllowUserToReadWriteObjectData",
    "Action":["s3:GetObject", "s3:PutObject"],
    "Effect":"Allow",
    "Resource":["arn:aws:s3:::companybucket/Development/*"]
 }
```

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.

   Use as credenciais da sua Conta da AWS, e não as credenciais de um usuário do IAM, para fazer login no console.

2. Edite a política em linha que você criou na etapa anterior.

   a. No painel de navegação à esquerda, escolha Uses (Usuários).

   b. Selecione o nome de usuário Alice.

   c. Na página de detalhes do usuário, selecione a guia Permissions (Permissões) e depois expanda a seção Inline Policies (Políticas em linha).

   d. Escolha Edit Policy (Editar política) ao lado do nome da política que você criou na etapa anterior.

   e. Copie a política a seguir e cole no campo do texto de política para substituir a política existente:

```
{
     "Version": "2012-10-17",
     "Statement":[
      {
         "Sid":"AllowListBucketIfSpecificPrefixIsIncludedInRequest",
         "Action":["s3:ListBucket"],
         "Effect":"Allow",
         "Resource":["arn:aws:s3:::companybucket"],
         "Condition":{
            "StringLike":{"s3:prefix":["Development/*"]
            }
         }
      },
      {
        "Sid":"AllowUserToReadWriteObjectDataInDevelopmentFolder",
        "Action":["s3:GetObject", "s3:PutObject"],
        "Effect":"Allow",
        "Resource":["arn:aws:s3:::companybucket/Development/*"]
      }
   ]
}
```

3. Teste a política atualizada:

   a. Usando o link de login de usuário do IAM (consulte Para fornecer um link de login para usuários do IAM), acesse o AWS Management Console.

   b. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.

   c. No console do Amazon S3, verifique se Alice agora pode adicionar um objeto e fazer download de um objeto na pasta `Development`.

Etapa 5.3: negar explicitamente permissões do usuário do IAM Alice a todas as outras pastas no bucket

O usuário Alice agora pode listar o conteúdo do nível raiz no bucket `companybucket`. Ela também pode obter e colocar objetos na pasta `Development`. Se você quiser realmente limitar as permissões de acesso, poderá negar explicitamente o acesso de Alice a todas as outras pastas no bucket. Se houver alguma outra política (política de bucket ou ACL) que concede a Alice acesso a outras pastas no bucket, essa negação explícita cancelará essas permissões.

É possível adicionar a seguinte declaração à política de usuário Alice que exige que todas as solicitações que Alice envia ao Amazon S3 incluam o parâmetro `prefix`, cujo valor pode ser `Development/*` ou uma string vazia.

```
{
   "Sid": "ExplicitlyDenyAnyRequestsForAllOtherFoldersExceptDevelopment",
   "Action": ["s3:ListBucket"],
   "Effect": "Deny",
   "Resource": ["arn:aws:s3:::companybucket"],
   "Condition":{  "StringNotLike": {"s3:prefix":["Development/*",""] },
                  "Null"         : {"s3:prefix":false }
    }
}
```

Há duas expressões condicionais no bloco `Condition`. O resultado dessas expressões condicionais é combinado usando o operador lógico `AND`. Se ambas as condições forem verdadeiras, o resultado da condição combinada será verdadeiro. Como o `Effect` nessa política é `Deny`, quando `Condition` é classificado como verdadeiro, os usuários não podem executar a `Action` especificada.

- A expressão condicional `Null` garante que as solicitações de Alice incluam o parâmetro `prefix`.

  O parâmetro `prefix` requer acesso de pasta. Se você enviar uma solicitação sem o parâmetro `prefix`, o Amazon S3 retornará todas as chaves de objeto.

  Se a solicitação incluir o parâmetro `prefix` com um valor nulo, a expressão será classificada como verdadeiro e, portanto, a `Condition` inteira será classificada como verdadeira. Você deve permitir uma string vazia como o valor do parâmetro `prefix`. Com a discussão anterior, lembre-se que a string nula permite que Alice recupere itens de bucket no nível raiz como o console faz

na discussão anterior. Para obter mais informações, consulte Etapa 4.2: Permitir que os usuários listem o conteúdo do nível raiz de um bucket.

- A expressão condicional `StringNotLike` garante que, se o valor do parâmetro `prefix` for especificado e não for `Development/*`, a solicitação falhará.

Siga as etapas na seção anterior e atualize novamente a política em linha que você criou para o usuário Alice.

Copie a política a seguir e cole no campo do texto de política para substituir a política existente:

```
{
   "Version": "2012-10-17",
   "Statement":[
      {
         "Sid":"AllowListBucketIfSpecificPrefixIsIncludedInRequest",
         "Action":["s3:ListBucket"],
         "Effect":"Allow",
         "Resource":["arn:aws:s3:::companybucket"],
         "Condition":{
            "StringLike":{"s3:prefix":["Development/*"]
            }
         }
      },
      {
        "Sid":"AllowUserToReadWriteObjectDataInDevelopmentFolder",
        "Action":["s3:GetObject", "s3:PutObject"],
        "Effect":"Allow",
        "Resource":["arn:aws:s3:::companybucket/Development/*"]
      },
      {
         "Sid": "ExplicitlyDenyAnyRequestsForAllOtherFoldersExceptDevelopment",
         "Action": ["s3:ListBucket"],
         "Effect": "Deny",
         "Resource": ["arn:aws:s3:::companybucket"],
         "Condition":{  "StringNotLike": {"s3:prefix":["Development/*",""] },
                        "Null"         : {"s3:prefix":false }
          }
      }
   ]
}
```

Etapa 6: conceder permissões específicas do usuário do IAM Bob

Agora você quer conceder ao Bob permissão para a pasta `Finance`. Siga as etapas que você usou anteriormente para conceder permissões a Alice, mas substitua a pasta `Development` pela pasta `Finance`. Para obter instruções detalhadas, consulte Etapa 5: conceder permissões específicas do usuário do IAM Alice.

Etapa 7: Proteger a pasta Private

Neste exemplo, você tem apenas dois usuários. Você concedeu todas as permissões mínimas necessárias no nível do grupo e concedeu permissões no nível do usuário somente quando realmente precisou de permissões no nível do usuário individual. Essa abordagem ajuda a minimizar o esforço de gerenciamento de permissões. Conforme o número de usuários aumenta, gerenciar permissões pode ser um problema. Por exemplo, você não quer que nenhum dos usuários neste exemplo acesse o conteúdo da pasta `Private`. Como garantir que você não vai conceder acidentalmente uma permissão ao usuário para a pasta `Private`? Adicione uma política que negue explicitamente acesso à pasta. Uma negação explícita substitui todas as outras permissões.

Para garantir que a pasta `Private` permaneça privada, você pode adicionar as duas declarações de negação a seguir à política de grupo:

- Adicione a seguinte declaração para negar explicitamente qualquer ação em recursos na pasta `Private` (`companybucket/Private/*`).

```
{
  "Sid": "ExplictDenyAccessToPrivateFolderToEveryoneInTheGroup",
  "Action": ["s3:*"],
  "Effect": "Deny",
  "Resource":["arn:aws:s3:::companybucket/Private/*"]
}
```

- Você também nega permissão para a ação de listar objetos quando a solicitação especifica o prefixo `Private/`. No console, se Bob ou Alice abrir a pasta `Private`, essa política fará o Amazon S3 retornar uma resposta de erro.

```
{
  "Sid": "DenyListBucketOnPrivateFolder",
  "Action": ["s3:ListBucket"],
  "Effect": "Deny",
  "Resource": ["arn:aws:s3:::*"],
  "Condition":{
```

```
      "StringLike":{"s3:prefix":["Private/"]}
    }
}
```

Substitua a política do grupo `Consultants` por uma política atualizada que inclua as declarações de negação anteriores. Após a política atualizada ser aplicada, nenhum usuário no grupo poderá acessar a pasta `Private` no seu bucket.

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.

   Use as credenciais da sua Conta da AWS, e não as credenciais de um usuário do IAM, para fazer login no console.

2. Substitua a política gerenciada `AllowGroupToSeeBucketListInTheConsole` existente que está anexada ao grupo `Consultants` pela política a seguir. Lembre-se de substituir *`companybucket`* na política pelo nome do bucket.

   Consulte instruções em Edição de políticas gerenciadas pelo cliente no Guia do usuário do IAM. Ao seguir as instruções, não se esqueça de seguir as orientações para aplicar alterações em todas as entidades principais às quais a política está anexada.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid":
 "AllowGroupToSeeBucketListAndAlsoAllowGetBucketLocationRequiredForListBucket",
      "Action": ["s3:ListAllMyBuckets", "s3:GetBucketLocation"],
      "Effect": "Allow",
      "Resource": ["arn:aws:s3:::*"]
    },
    {
      "Sid": "AllowRootLevelListingOfCompanyBucket",
      "Action": ["s3:ListBucket"],
      "Effect": "Allow",
      "Resource": ["arn:aws:s3:::companybucket"],
      "Condition":{
          "StringEquals":{"s3:prefix":[""]}
       }
    },
```

```
    {
      "Sid": "RequireFolderStyleList",
      "Action": ["s3:ListBucket"],
      "Effect": "Deny",
      "Resource": ["arn:aws:s3:::*"],
      "Condition":{
          "StringNotEquals":{"s3:delimiter":"/"}
       }
     },
    {
      "Sid": "ExplictDenyAccessToPrivateFolderToEveryoneInTheGroup",
      "Action": ["s3:*"],
      "Effect": "Deny",
      "Resource":["arn:aws:s3:::companybucket/Private/*"]
    },
    {
      "Sid": "DenyListBucketOnPrivateFolder",
      "Action": ["s3:ListBucket"],
      "Effect": "Deny",
      "Resource": ["arn:aws:s3:::*"],
      "Condition":{
          "StringLike":{"s3:prefix":["Private/"]}
       }
    }
  ]
}
```

Etapa 8: Limpar

Para limpar, abra o console do IAM e remova os usuários Alice e Bob. Consulte instruções detalhadas em Exclusão de um usuário do IAM no Guia do usuário do IAM.

Para garantir que você não seja mais cobrado pelo armazenamento, exclua também os objetos e o bucket que criou neste exercício.

Recursos relacionados

- Como gerenciar políticas do IAM no Guia do usuário do IAM

Exemplos de políticas baseadas em identidade para o Amazon S3

Esta seção mostra diversos exemplos de políticas baseadas em identidade do AWS Identity and Access Management (IAM) para controle de acesso ao Amazon S3. Consulte exemplos de políticas de bucket (políticas baseadas em recursos) em Políticas de bucket para o Amazon S3. Para obter informações sobre a linguagem de políticas do IAM, consulte Políticas e permissões no Amazon S3.

Os exemplos de política a seguir funcionarão se você testá-los de forma programática. No entanto, para usá-los com o console do Amazon S3, você precisará conceder permissões adicionais solicitadas pelo console. Para obter informações sobre o uso de políticas como essas com o console do Amazon S3, consulte Controlar o acesso a um bucket com políticas de usuário.

Para ter mais informações sobre as permissões referentes a operações de API do S3 de acordo com os tipos de recurso do S3, consulte Permissões obrigatórias para operações de API do Amazon S3.

Tópicos

- Permitir que um usuário do IAM acesse um dos seus buckets
- Permitir que cada usuário do IAM acesse uma pasta em um bucket
- Permitir que um grupo tenha uma pasta compartilhada no Amazon S3
- Permitir que todos os seus usuários leiam objetos em uma parte de um bucket
- Permitir que um parceiro solte arquivos em uma parte específica de um bucket
- Restringir o acesso a buckets do Amazon S3 em uma Conta da AWS específica
- Restringir o acesso a buckets do Amazon S3 em sua unidade organizacional
- Restringir o acesso a buckets do Amazon S3 em sua unidade organizacional
- Conceder permissão para recuperar a configuração PublicAccessBlock para uma Conta da AWS
- Restringir a criação de buckets a uma região

Permitir que um usuário do IAM acesse um dos seus buckets

Neste exemplo, um usuário do IAM na sua Conta da AWS recebe acesso a um dos seus buckets, *amzn-s3-demo-bucket1*, e você permite que ele adicione, atualize e exclua objetos.

Além de conceder as permissões `s3:PutObject`, `s3:GetObject` e `s3:DeleteObject` ao usuário, a política também concede as permissões `s3:ListAllMyBuckets`, `s3:GetBucketLocation` e `s3:ListBucket`. Estas são permissões adicionais, exigidas pelo console. As ações `s3:PutObjectAcl` e `s3:GetObjectAcl` também são necessárias para

copiar, recortar e colar objetos no console. Para obter um exemplo de passo a passo que concede permissões aos usuários e testa-as usando o console, consulte Controlar o acesso a um bucket com políticas de usuário.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action": "s3:ListAllMyBuckets",
         "Resource":"*"
      },
      {
         "Effect":"Allow",
         "Action":["s3:ListBucket","s3:GetBucketLocation"],
         "Resource":"arn:aws:s3:::amzn-s3-demo-bucket1"
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3:PutObject",
            "s3:PutObjectAcl",
            "s3:GetObject",
            "s3:GetObjectAcl",
            "s3:DeleteObject"
         ],
         "Resource":"arn:aws:s3:::amzn-s3-demo-bucket1/*"
      }
   ]
}
```

Permitir que cada usuário do IAM acesse uma pasta em um bucket

Neste exemplo, você deseja que dois usuários do IAM, Mary e Carlos, tenham acesso ao bucket, *amzn-s3-demo-bucket1*, para que possam adicionar, atualizar e excluir objetos. No entanto, você quer restringir o acesso de todos os usuários a um único prefixo (pasta) no bucket. Você pode criar pastas com nomes correspondentes aos seus nomes de usuário.

```
amzn-s3-demo-bucket1
   Mary/
   Carlos/
```

Para conceder a cada usuário acesso apenas à pasta dele, crie uma política para cada um deles e anexe-a individualmente. Por exemplo, você pode anexar a política a seguir ao usuário Alice para conceder a ela permissões específicas do Amazon S3 na pasta *amzn-s3-demo-bucket1*/*Mary*.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "s3:PutObject",
            "s3:GetObject",
            "s3:GetObjectVersion",
            "s3:DeleteObject",
            "s3:DeleteObjectVersion"
         ],
         "Resource":"arn:aws:s3:::amzn-s3-demo-bucket1/Mary/*"
      }
   ]
}
```

Você pode anexar uma política semelhante ao usuário Carlos, especificando a pasta *Carlos* no valor `Resource`.

Em vez de anexar políticas a usuários individuais, você pode criar uma única política que use uma variável de política e anexá-la a um grupo. Primeiro, você precisará criar um grupo e adicionar os usuários Alice e Carlos a ele. O exemplo de política a seguir concede um conjunto de permissões do Amazon S3 na pasta *amzn-s3-demo-bucket1*/`${aws:username}`. Quando a política é avaliada, a variável `${aws:username}` é substituída pelo nome do usuário do solicitante. Por exemplo, se Alice enviar uma solicitação para colocar um objeto, a operação será permitida apenas se Alice estiver fazendo upload do objeto na pasta *amzn-s3-demo-bucket1*/`Mary`.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "s3:PutObject",
            "s3:GetObject",
            "s3:GetObjectVersion",
```

```
            "s3:DeleteObject",
            "s3:DeleteObjectVersion"
         ],
         "Resource":"arn:aws:s3:::amzn-s3-demo-bucket1/${aws:username}/*"
      }
   ]
}
```

> **Note**
>
> Ao usar variáveis de política, você deve especificar explicitamente a versão `2012-10-17` na política. A versão padrão da linguagem da política do IAM, 2008-10-17, não é compatível com variáveis de política.

Se quiser testar a política anterior no console do Amazon S3, o console exigirá permissões adicionais, conforme exibido na política a seguir. Para obter informações sobre como o console usa essas permissões, consulte Controlar o acesso a um bucket com políticas de usuário.

```
{
 "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "AllowGroupToSeeBucketListInTheConsole",
      "Action": [
       "s3:ListAllMyBuckets",
       "s3:GetBucketLocation"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::*"
    },
    {
      "Sid": "AllowRootLevelListingOfTheBucket",
      "Action": "s3:ListBucket",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1",
      "Condition":{
            "StringEquals":{
                   "s3:prefix":[""], "s3:delimiter":["/"]
                         }
               }
    },
```

```
    {
      "Sid": "AllowListBucketOfASpecificUserPrefix",
      "Action": "s3:ListBucket",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1",
      "Condition":{  "StringLike":{"s3:prefix":["${aws:username}/*"] }
       }
    },
      {
     "Sid": "AllowUserSpecificActionsOnlyInTheSpecificUserPrefix",
         "Effect":"Allow",
         "Action":[
            "s3:PutObject",
            "s3:GetObject",
            "s3:GetObjectVersion",
            "s3:DeleteObject",
            "s3:DeleteObjectVersion"
         ],
         "Resource":"arn:aws:s3:::amzn-s3-demo-bucket1/${aws:username}/*"
      }
  ]
}
```

> **Note**
>
> Na versão 2012-10-17 da política, as variáveis de política começam com $. Essa mudança na sintaxe poderá criar um conflito se a chave de objeto (nome do objeto) incluir um $. Para evitar esse conflito, especifique o caractere $ usando `${$}`. Por exemplo, para incluir a chave de objeto `my$file` em uma política, especifique-a como `my${$}file`.

Embora os nomes de usuários do IAM sejam identificadores amigáveis e legíveis, eles não precisam ser globalmente exclusivos. Por exemplo, se o usuário Carlos deixar a empresa e outro Carlos ingressar, este poderá acessar as informações do Carlos anterior.

Em vez de usar nomes de usuário, você pode criar pastas baseadas nos IDs de usuário do IAM. O ID de cada usuário do IAM é exclusivo. Neste caso, você deve modificar a política anterior para usar a variável de política `${aws:userid}`. Para obter mais informações sobre identificadores de usuário, consulte Identificadores do IAM no Guia do usuário do IAM.

```
{
```

```
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "s3:PutObject",
            "s3:GetObject",
            "s3:GetObjectVersion",
            "s3:DeleteObject",
            "s3:DeleteObjectVersion"
         ],
         "Resource":"arn:aws:s3:::amzn-s3-demo-bucket1/home/${aws:userid}/*"
      }
   ]
}
```

Permitir que usuários que não são do IAM (usuários de aplicativos móveis) acessem pastas em um bucket

Vamos supor que você queira desenvolver um aplicativo móvel, um jogo que armazena dados dos usuários em um bucket do S3. Para cada usuário do aplicativo, você quer criar uma pasta em seu bucket. Também é desejável limitar o acesso de todos os usuários à própria pasta, mas não é possível criar pastas antes que alguém baixe sua aplicação e comece a jogar, pois você não tem o ID do usuário.

Neste caso, você pode exigir que os usuários criem uma conta em seu aplicativo usando provedores públicos de identidade, como Login with Amazon, Facebook ou Google. Depois que os usuários criarem uma conta em seu aplicativo por meio de um desses provedores, eles terão um ID de usuário que você poderá usar para criar pastas específicas de usuário no tempo de execução.

Você pode usar a federação de identidades da web no AWS Security Token Service para integrar informações do provedor de identidade com seu aplicativo e para obter credenciais de segurança temporárias para cada usuário. Você pode criar políticas do IAM que permitem que o aplicativo acesse seu bucket e execute operações como criação de pastas específicas de usuário e upload de dados. Para obter mais informações sobre federação de identidades da Web, consulte Sobre federação de identidades da Web no Guia do usuário do IAM.

Permitir que um grupo tenha uma pasta compartilhada no Amazon S3

Anexar a política a seguir ao grupo concede a todos no grupo acesso à seguinte pasta no Amazon S3: *amzn-s3-demo-bucket1*/share/marketing. Os membros do grupo têm permissão para

acessar apenas permissões específicas do Amazon S3 exibidas na política e apenas para objetos na pasta especificada.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "s3:PutObject",
            "s3:GetObject",
            "s3:GetObjectVersion",
            "s3:DeleteObject",
            "s3:DeleteObjectVersion"
         ],
         "Resource":"arn:aws:s3:::amzn-s3-demo-bucket1/share/marketing/*"
      }
   ]
}
```

Permitir que todos os seus usuários leiam objetos em uma parte de um bucket

Neste exemplo, você cria um grupo chamado *AllUsers*, que contém todos os usuários do IAM que pertencem à Conta da AWS. Em seguida, anexe uma política que concede ao grupo acesso a `GetObject` e `GetObjectVersion`, mas somente para objetos na pasta *amzn-s3-demo-bucket1*`/readonly`.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "s3:GetObject",
            "s3:GetObjectVersion"
         ],
         "Resource":"arn:aws:s3:::amzn-s3-demo-bucket1/readonly/*"
      }
   ]
}
```

Permitir que um parceiro solte arquivos em uma parte específica de um bucket

Neste exemplo, crie um grupo chamado *AnyCompany* que representa uma empresa parceira. Crie um usuário do IAM para a pessoa ou aplicação específica na empresa parceira que precisa de acesso. Depois, coloque o usuário no grupo.

Depois, anexe uma política que conceda ao grupo `PutObject` acesso à seguinte pasta em um bucket:

amzn-s3-demo-bucket1`/uploads/anycompany`

É preciso impedir que o grupo *AnyCompany* faça qualquer outra coisa no bucket e, portanto, você adiciona uma declaração negando explicitamente outras permissões a ações do Amazon S3, exceto `PutObject`, em qualquer recurso do Amazon S3 na Conta da AWS.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":"s3:PutObject",
         "Resource":"arn:aws:s3:::amzn-s3-demo-bucket1/uploads/anycompany/*"
      },
      {
         "Effect":"Deny",
         "Action":"s3:*",
         "NotResource":"arn:aws:s3:::amzn-s3-demo-bucket1/uploads/anycompany/*"
      }
   ]
}
```

Restringir o acesso a buckets do Amazon S3 em uma Conta da AWS específica

Se quiser garantir que suas entidades principais do Amazon S3 acessem apenas os recursos que estão em uma Conta da AWS confiável, você poderá restringir o acesso. Por exemplo, esta política do IAM baseada em identidade usa um efeito `Deny` para bloquear o acesso às ações do Amazon S3, a menos que o recurso do Amazon S3 que está sendo acessado esteja na conta *222222222222*. Para impedir que uma entidade principal do IAM em uma Conta da AWS acesse objetos do Amazon S3 fora da conta, anexe a seguinte política do IAM:

```
{
  "Version": "2012-10-17",
```

```
  "Statement": [
    {
      "Sid": "DenyS3AccessOutsideMyBoundary",
      "Effect": "Deny",
      "Action": [
        "s3:*"
      ],
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:ResourceAccount": [
            "222222222222"
          ]
        }
      }
    }
  ]
}
```

> **Note**
>
> Essa política não substitui os controles de acesso do IAM existentes, pois não concede nenhum acesso. Em vez disso, essa política funciona como uma barreira de proteção adicional para suas outras permissões do IAM, independentemente das permissões concedidas por meio de outras políticas do IAM.

Substitua o ID da conta *222222222222* na política pela sua própria Conta da AWS. Para aplicar uma política a várias contas e ainda manter essa restrição, substitua o ID da conta pela chave de condição `aws:PrincipalAccount`. Essa condição exige que a entidade principal e o recurso estejam na mesma conta.

Restringir o acesso a buckets do Amazon S3 em sua unidade organizacional

Se você tiver uma unidade organizacional (UO) configurada no AWS Organizations, é recomendável restringir o acesso ao bucket do Amazon S3 a uma parte específica de sua organização. Neste exemplo, usaremos a chave `aws:ResourceOrgPaths` para restringir o acesso ao bucket do Amazon S3 a uma UO em sua organização. Neste exemplo, o ID da UO é *ou-acroot-exampleou*. Substitua esse valor em sua própria política por seus próprios IDs de UO.

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowS3AccessOutsideMyBoundary",
      "Effect": "Allow",
      "Action": [
        "s3:*"
      ],
      "Resource": "*",
      "Condition": {
        "ForAllValues:StringNotLike": {
          "aws:ResourceOrgPaths": [
            "o-acorg/r-acroot/ou-acroot-exampleou/"
          ]
        }
      }
    }
  ]
}
```

> **Note**
>
> Essa política não concede nenhum acesso. Em vez disso, essa política funciona como uma barreira para suas outras permissões do IAM, impedindo que suas entidades principais acessem objetos do Amazon S3 fora de um limite definido pela UO.

A política nega acesso às ações do Amazon S3, a menos que o objeto do Amazon S3 que está sendo acessado esteja na UO *ou-acroot-exampleou* em sua organização. A condição da política do IAM exige `aws:ResourceOrgPaths`, uma chave de condição com vários valores, para conter qualquer um dos caminhos de UO listados. A política usa o operador `ForAllValues:StringNotLike` para comparar os valores de `aws:ResourceOrgPaths` com as UOs listadas sem distinção de maiúsculas e minúsculas.

Restringir o acesso a buckets do Amazon S3 em sua unidade organizacional

Para restringir o acesso a objetos do Amazon S3 em sua organização, anexe uma política do IAM à raiz da organização, aplicando-a a todas as contas. Para exigir que suas entidades principais do IAM sigam essa regra, use uma política de controle de serviços (SCP). Se você optar por usar uma SCP, teste-a antes de anexar a política à raiz da organização.

No exemplo de política a seguir, o acesso é negado às ações do Amazon S3, a menos que o objeto do Amazon S3 que está sendo acessado esteja na mesma organização que a entidade principal do IAM que o está acessando:

```
{
   "Version": "2012-10-17",
   "Statement": [
     {
       "Sid": "DenyS3AccessOutsideMyBoundary",
       "Effect": "Deny",
       "Action": [
         "s3:*"
       ],
       "Resource": "arn:aws:s3:::*/*",
       "Condition": {
         "StringNotEquals": {
           "aws:ResourceOrgID": "${aws:PrincipalOrgID}"
         }
       }
     }
   ]
 }
```

> **Note**
>
> Essa política não concede nenhum acesso. Essa política funciona como uma barreira para suas outras permissões do IAM, impedindo que suas entidades principais acessem quaisquer objetos do Amazon S3 de fora de sua organização. Essa política também se aplica aos recursos do Amazon S3 que são criados depois que a política é implementada.

Neste exemplo, a condição da política do IAM exige que `aws:ResourceOrgID` e `aws:PrincipalOrgID` sejam equivalentes. Com esse requisito, a entidade principal que faz a solicitação e o recurso que está sendo acessado devem estar na mesma organização.

Conceder permissão para recuperar a configuração PublicAccessBlock para uma Conta da AWS

O exemplo de política baseada em identidade a seguir concede a permissão `s3:GetAccountPublicAccessBlock` a um usuário. Para todas essas permissões, defina o valor `Resource` como `"*"`. Consulte mais informações sobre os ARNs de recursos em Recursos de políticas para o Amazon S3.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"statement1",
         "Effect":"Allow",
         "Action":[
            "s3:GetAccountPublicAccessBlock"
         ],
         "Resource":[
            "*"
         ]
       }
    ]
}
```

Restringir a criação de buckets a uma região

Suponha que um administrador de uma Conta da AWS queira conceder ao seu usuário (Dave) a permissão para criar um bucket somente na região América do Sul (São Paulo). O administrador da conta pode anexar a política de usuário a seguir que concede a permissão `s3:CreateBucket` com uma condição, conforme exibido. O par de chave-valor no bloco `Condition` especifica a chave `s3:LocationConstraint` e a região `sa-east-1` como valor.

> **Note**
>
> Neste exemplo, o proprietário do bucket concede permissão para um de seus usuários, de modo que tanto uma política de bucket quanto uma política de usuário podem ser usadas. Este exemplo mostra uma política de usuário.

Para conferir a lista de regiões do Amazon S3, consulte Regiões e endpoints na Referência geral da AWS.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"statement1",
         "Effect":"Allow",
         "Action": "s3:CreateBucket",
```

```
        "Resource": "arn:aws:s3:::*",
        "Condition": {
            "StringLike": {
                "s3:LocationConstraint": "sa-east-1"
            }
        }
      }
    ]
}
```

Adicionar negação explícita

A política acima impede que o usuário crie um bucket em qualquer outra Região, exceto `sa-east-1`. No entanto, alguma outra política pode conceder a esse usuário permissão para criar buckets em outra Região. Por exemplo, se ele pertencer a um grupo, o grupo pode ter uma política anexada que permita que todos os seus usuários tenham permissão para criar buckets em outra Região. Para garantir que o usuário não obtenha permissão para criar buckets em nenhuma outra região, adicione uma instrução de negação explícita à política acima.

A declaração `Deny` usa a condição `StringNotLike`. Isto é, uma solicitação de criação de bucket será negada se a restrição de localização não for `sa-east-1`. A negação explícita não permite que o usuário crie um bucket em nenhuma outra região, independentemente de outras permissões que ele receba. A política a seguir inclui uma instrução de negação explícita.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"statement1",
         "Effect":"Allow",
         "Action": "s3:CreateBucket",
         "Resource": "arn:aws:s3:::*",
         "Condition": {
             "StringLike": {
                 "s3:LocationConstraint": "sa-east-1"
             }
         }
       },
      {
         "Sid":"statement2",
         "Effect":"Deny",
         "Action": "s3:CreateBucket",
```

```
            "Resource": "arn:aws:s3:::*",
            "Condition": {
                "StringNotLike": {
                    "s3:LocationConstraint": "sa-east-1"
                }
            }
        }
    ]
}
```

Testar a política com a AWS CLI

Você pode testar a política usando o seguinte comando `create-bucket` da AWS CLI. Este exemplo usa o arquivo `bucketconfig.txt` para especificar a restrição de localização. Anote o caminho do arquivo do Windows. Você precisa atualizar o nome e o caminho do bucket conforme apropriado. Você deve fornecer as credenciais do usuário usando o parâmetro `--profile`. Consulte mais informações sobre como configurar e usar a AWS CLI em Developing with Amazon S3 using the AWS CLI na Referência de API do Amazon S3.

```
aws s3api create-bucket --bucket examplebucket --profile AccountADave --create-bucket-configuration file://c:/Users/someUser/bucketconfig.txt
```

O arquivo `bucketconfig.txt` especifica a configuração da seguinte maneira.

```
{"LocationConstraint": "sa-east-1"}
```

Demonstrações que usam políticas para gerenciar o acesso a recursos do Amazon S3

Este tópico fornece exemplos de demonstrações introdutórias para conceder acesso aos recursos do Amazon S3. Esses exemplos usam o AWS Management Console para criar recursos (buckets, objetos, usuários) e conceder permissões a eles. Em seguida, os exemplos mostram como verificar as permissões usando as ferramentas da linha de comando, para que nenhum código precise ser escrito. Fornecemos comandos usando tanto a AWS Command Line Interface (AWS CLI) quanto o AWS Tools for Windows PowerShell.

- Exemplo 1: Proprietário do bucket que concede permissões do bucket aos usuários

  Por padrão, os usuários do IAM criados na conta não têm permissões. Neste exercício, você concederá uma permissão de usuário para realizar operações no bucket e no objeto.

- Exemplo 2: Proprietário do bucket concedendo permissões de bucket entre contas

  Neste exercício, um proprietário do bucket, conta A, concede permissões entre contas a outra Conta da AWS, conta B. Em seguida, a conta B delega essas permissões aos usuários em sua conta.

- Gerenciar permissões de objeto quando os proprietários do bucket e do objeto são diferentes

  Nesse caso, os cenários do exemplo são um proprietário de bucket que concede permissões de objeto para outros, mas nem todos os objetos do bucket pertencem ao proprietário do bucket. De quais permissões o proprietário do bucket precisa e como ele pode delegar essas permissões?

  A Conta da AWS que cria um bucket é chamada de proprietária do bucket. O proprietário pode conceder permissões a outras Contas da AWS para carregar objetos, e os proprietários desses objetos são as Contas da AWS que os criaram. O proprietário do bucket não tem permissões sobre os objetos criados por outras Contas da AWS. Quando o proprietário do bucket escreve uma política de bucket concedendo acesso aos objetos, ela não se aplica aos objetos pertencentes a outras contas.

  Nesse caso, o proprietário do objeto deve, primeiro, conceder permissões ao proprietário do bucket usando uma ACL do objeto. Em seguida, o proprietário do bucket pode autorizar essas permissões de objeto para outros, para usuários em sua própria conta ou para outra Conta da AWS, conforme ilustrado pelos exemplos a seguir.

  - Exemplo 3: O proprietário do bucket concede permissões para objetos que não possui

Neste exercício, primeiro o proprietário do bucket obtém permissões do proprietário do objeto. Em seguida, o proprietário do bucket delega tais permissões para usuários em sua própria conta.

- Exemplo 4: proprietário do bucket concede permissão entre contas a objetos que não possui

  Após o recebimento das permissões do proprietário do objeto, o proprietário do bucket não pode delegar permissões a outras Contas da AWS, já que a delegação entre contas não é permitida (consulte Delegação de permissão). Em vez disso, o proprietário do bucket pode criar uma função do IAM com permissões para realizar determinadas operações (como obter objeto) e permitir que outra Conta da AWS assuma essa função. Qualquer um que assumir a função pode, então, acessar os objetos. Este exemplo mostra como um proprietário do bucket pode usar uma função do IAM para habilitar essa delegação de conta cruzada.

Antes de tentar as demonstrações de exemplo

Esses exemplos usam o AWS Management Console para criar recursos e conceder permissões. Para testar permissões, os exemplos usam ferramentas de linha de comando, a AWS CLI e o AWS Tools for Windows PowerShell para que não seja necessário escrever nenhum código. Para testar permissões, você deve configurar uma dessas ferramentas. Para obter mais informações, consulte Configurar as ferramentas para as demonstrações.

Além disso, ao criar recursos, esses exemplos não usam as credenciais de usuário-raiz de uma Conta da AWS. Em vez disso, crie um usuário administrador nessas contas para executar essas tarefas.

Sobre o uso de um usuário administrador para criar recursos e conceder permissões

O AWS Identity and Access Management (IAM) recomenda não usar as credenciais do usuário raiz da sua Conta da AWS para fazer solicitações. Em vez disso, crie um perfil ou usuário do IAM, conceda acesso total a esse perfil ou usuário, depois use as credenciais desse perfil ou usuário para fazer solicitações. Essa entidade é conhecida como perfil ou usuário administrador. Para obter mais informações, acesse Credenciais de Usuário raiz da conta da AWS e identidades do IAM na Referência geral da AWS e Práticas recomendadas do IAM no Guia do usuário do IAM.

Todos as demonstrações com exemplos nesta seção usam as credenciais do usuário administrador. Caso você não tenha criado um usuário administrador para sua Conta da AWS, os tópicos mostram como fazê-lo.

Para fazer login no AWS Management Console usando as credenciais de usuário, é necessário usar o URL de login do usuário do IAM. O console do IAM fornece esse URL para sua Conta da AWS. Os tópicos mostram como obter o URL.

Configurar as ferramentas para as demonstrações

Os exemplos introdutórios (consulte Demonstrações que usam políticas para gerenciar o acesso a recursos do Amazon S3) usam o AWS Management Console para criar recursos e conceder permissões. Para testar permissões, os exemplos usam ferramentas de linha de comando, a AWS Command Line Interface (AWS CLI) e o AWS Tools for Windows PowerShell para que não seja necessário escrever nenhum código. Para testar permissões, você deve configurar uma dessas ferramentas.

Para configurar a AWS CLI

1. Faça download e configure a AWS CLI. Para obter instruções, consulte os seguintes tópicos no Guia do usuário do AWS Command Line Interface:

   Install or update to the latest version of the AWS Command Line Interface

   Get started with the AWS Command Line Interface
2. Defina o perfil padrão.

   As credenciais de usuário são armazenadas no arquivo de configuração da AWS CLI. Crie um perfil padrão no arquivo de configuração usando as credenciais da sua Conta da AWS. Consulte instruções sobre como encontrar e editar o arquivo de configuração da AWS CLI em Configuration and credential file settings.

   ```
   [default]
   aws_access_key_id = access key ID
   aws_secret_access_key = secret access key
   region = us-west-2
   ```
3. Verifique a configuração inserindo o comando a seguir no prompt de comando. Ambos os comandos não fornecem as credenciais explicitamente, de modo que as credenciais do perfil padrão são usadas.

   - Experimente o comando `help`.

     ```
     aws help
     ```

- Para obter uma lista dos buckets na conta configurada, use o comando `aws s3 ls`.

```
aws s3 ls
```

À medida que você avançar nas demonstrações, criará usuários e salvará credenciais de usuários nos arquivos de configuração ao criar perfis, conforme mostra o exemplo a seguir. Esses perfis têm os nomes de `AccountAadmin` e `AccountBadmin`.

```
[profile AccountAadmin]
aws_access_key_id = User AccountAadmin access key ID
aws_secret_access_key = User AccountAadmin secret access key
region = us-west-2

[profile AccountBadmin]
aws_access_key_id = Account B access key ID
aws_secret_access_key = Account B secret access key
region = us-east-1
```

Para executar um comando usando essas credenciais de usuário, adicione o parâmetro `--profile` especificando o nome do perfil. O comando da AWS CLI a seguir recupera uma lista de objetos em *`examplebucket`* e especifica o perfil `AccountBadmin`.

```
aws s3 ls s3://examplebucket --profile AccountBadmin
```

Como alternativa, configure um conjunto de credenciais de usuário como perfil padrão alterando a variável de ambiente `AWS_DEFAULT_PROFILE` no prompt de comando. Depois que fizer isso, sempre que você executar comandos da AWS CLI sem o parâmetro `--profile`, a AWS CLI usará o perfil definido na variável de ambiente como o perfil padrão.

```
$ export AWS_DEFAULT_PROFILE=AccountAadmin
```

Como configurar o AWS Tools for Windows PowerShell

1. Faça download e configure a AWS Tools for Windows PowerShell. Consulte instruções em Installing the AWS Tools for Windows PowerShell no Guia do usuário do Ferramentas da AWS para PowerShell.

> **Note**
>
> Para carregar o módulo do AWS Tools for Windows PowerShell, é necessário habilitar a execução de script do PowerShell. Consulte mais informações em Enable Script Execution no Guia do usuário do Ferramentas da AWS para PowerShell.

2. Para essas demonstrações, especifique credenciais da AWS por sessão usando o comando `Set-AWSCredentials`. O comando salva as credenciais em um armazenamento persistente (`-StoreAs` parâmetro).

```
Set-AWSCredentials -AccessKey AccessKeyID -SecretKey SecretAccessKey -
storeas string
```

3. Verifique a configuração.

   - Para recuperar uma lista de comandos disponíveis que podem ser usados para operações do Amazon S3, execute o comando `Get-Command`.

```
Get-Command -module awspowershell -noun s3* -StoredCredentials string
```

   - Para recuperar uma lista de objetos em um bucket, execute o comando `Get-S3Object`.

```
Get-S3Object -BucketName bucketname -StoredCredentials string
```

Consulte uma lista de comandos em AWS Tools for PowerShell Cmdlet Reference.

Agora está tudo pronto para você testar as demonstrações. Siga os links fornecidos no início de cada seção.

Exemplo 1: Proprietário do bucket que concede permissões do bucket aos usuários

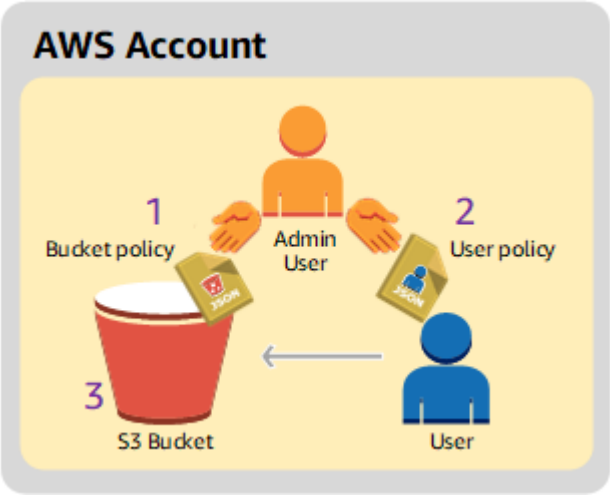
> **Important**
>
> Conceder permissões a perfis do IAM é uma prática mais adequada do que conceder permissões a usuários individuais. Consulte mais informações sobre como conceder permissões a perfis do IAM em Noções básicas de permissões entre contas e do uso de perfis do IAM.

Tópicos

- Preparar para a demonstração
- Etapa 1: criar recursos na Conta A e conceder permissões
- Etapa 2: Testar permissões

Nessa demonstração, uma Conta da AWS possui um bucket e a conta inclui um usuário do IAM. Por padrão, o usuário não tem permissões. Para que o usuário realize execute qualquer tarefa, a conta pai deve conceder permissão a ele. O proprietário do bucket e a conta pai são os mesmos. Portanto, para conceder ao usuário permissões no bucket, a Conta da AWS pode usar uma política de bucket, uma política de usuário ou ambas. O proprietário da conta concederá algumas permissões usando uma política de bucket e outras permissões usando uma política de usuário.

Os passos a seguir resumem as etapas de demonstração:



1. O administrador da conta cria uma política do bucket concedendo um conjunto de permissões ao usuário.

2. O administrador da conta anexa uma política de usuário ao usuário concedendo permissões adicionais.
3. O usuário então testa as permissões concedidas por política do bucket e por política de usuário.

Neste exemplo, você precisará de uma Conta da AWS. Em vez de usar as credenciais do usuário raiz da conta, você criará um usuário administrador (consulte Sobre o uso de um usuário administrador para criar recursos e conceder permissões). Fazemos referência à Conta da AWS e ao usuário administrador conforme indicado na tabela a seguir.

ID da conta	Conta referida como	Usuário administrador na conta
1111-1111-1111	Conta A	AccountAadmin

> **Note**
>
> O usuário administrador neste exemplo é AccountaAdmin, que se refere à conta A, e não à AccountAdmin.

Todas as tarefas de criar usuários e conceder permissões são feitas no AWS Management Console. Para verificar permissões, a demonstração usa as ferramentas de linha de comando, a AWS Command Line Interface (AWS CLI), e o AWS Tools for Windows PowerShell. Portanto, você não precisa escrever nenhum código.

Preparar para a demonstração

1. Verifique se você tem uma Conta da AWS que tenha um usuário com privilégios de administrador.

   a. Cadastre-se para obter uma Conta da AWS, se necessário. Nós nos referimos a essa conta como conta A.

      i. Acesse https://aws.amazon.com/s3 e selecione Criar uma conta da AWS.
      ii. Siga as instruções da tela.

      A AWS notificará você por e-mail quando sua conta estiver ativa e disponível para uso.

b. Na Conta A, crie um usuário administrador **`AccountAadmin`**. Usando as credenciais da conta A, faça login no console do IAM e faça o seguinte:

   i. Crie um usuário **`AccountAadmin`** e anote as credenciais de segurança do usuário.

      Consulte instruções em Criar um usuário do IAM na sua Conta da AWS no Guia do usuário do IAM.

   ii. Conceda privilégios de administrador a AccountAadmin anexando uma política de usuário com pleno acesso.

      Consulte instruções em Gerenciar políticas do IAM no Guia do usuário do IAM.

   iii. Anote o URL de login de usuário do IAM de AccountAadmin. Você precisará usar esse URL para fazer login no AWS Management Console. Consulte mais informações sobre onde encontrar o URL de login em Sign in to the AWS Management Console as an IAM user no Guia do usuário do IAM. Anote o URL de cada uma das contas.

2. Configure a AWS CLI ou o AWS Tools for Windows PowerShell. Salve as credenciais de usuário do administrador da seguinte maneira:

   - Se estiver usando a AWS CLI, crie um perfil, `AccountAadmin`, no arquivo de configuração.
   - Se estiver usando o AWS Tools for Windows PowerShell, armazene as credenciais da sessão como `AccountAadmin`.

   Para instruções, consulte Configurar as ferramentas para as demonstrações.

Etapa 1: criar recursos na Conta A e conceder permissões

Com as credenciais do usuário `AccountAadmin` na Conta A e o URL especial de login do usuário do IAM, faça login no AWS Management Console e execute o seguinte:

1. Crie recursos de um bucket e um usuário do IAM

   a. No console do Amazon S3, crie um bucket. Anote a Região da AWS na qual você criou o bucket. Para instruções, consulte Criar um bucket de uso geral.

   b. No console do IAM, faça o seguinte:

      i. Crie um usuário chamado Dave.

Para obter instruções passo a passo, consulte Criação de usuários do IAM (console) no Guia do usuário do IAM.

ii. Anote as credenciais de `UserDave`.

iii. Anote o nome do recurso da Amazon (ARN) do usuário Dave. No console do IAM, selecione o usuário para que a guia Resumo fornece o ARN do usuário.

2. Conceder permissões

Como o proprietário do bucket e a conta pai a que o usuário pertence são iguais, a Conta da AWS pode conceder permissões de usuário usando uma política do bucket, uma política de usuário ou ambas. Neste exemplo, você faz ambos. Se o objeto também for de propriedade da mesma conta, o proprietário do bucket pode conceder permissões de objeto na política do bucket (ou em uma política do IAM).

a. No console do Amazon S3, anexe a seguinte política do bucket a *`awsexamplebucket1`*.

A política tem duas instruções.

- A primeira instrução concede a Dave as permissões de operação dos buckets `s3:GetBucketLocation` e `s3:ListBucket`.
- A segunda instrução concede a permissão `s3:GetObject`. Como a Conta A também possui o objeto, o administrador da conta pode conceder a permissão `s3:GetObject`.

Na instrução `Principal`, Dave é identificado por seu ARN de usuário. Para obter mais informações sobre elementos de política, consulte Políticas e permissões no Amazon S3.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "statement1",
         "Effect": "Allow",
         "Principal": {
            "AWS": "arn:aws:iam::AccountA-ID:user/Dave"
         },
         "Action": [
            "s3:GetBucketLocation",
            "s3:ListBucket"
         ],
```

```
            "Resource": [
               "arn:aws:s3:::awsexamplebucket1"
            ]
         },
         {
            "Sid": "statement2",
            "Effect": "Allow",
            "Principal": {
               "AWS": "arn:aws:iam::AccountA-ID:user/Dave"
            },
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
               "arn:aws:s3:::awsexamplebucket1/*"
            ]
         }
      ]
}
```

b. Crie uma política inline para o usuário Dave usando as seguintes políticas. A política concede a Dave a permissão `s3:PutObject`. Você precisa atualizar a política, fornecendo o nome de seu bucket.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "PermissionForObjectOperations",
         "Effect": "Allow",
         "Action": [
            "s3:PutObject"
         ],
         "Resource": [
            "arn:aws:s3:::awsexamplebucket1/*"
         ]
      }
   ]
}
```

Consulte instruções em Gerenciamento de políticas do IAM no Guia do usuário do IAM. Observe que você precisa fazer login no console usando as credenciais da Conta A.

Etapa 2: Testar permissões

Com as credenciais de Dave, verifique se as permissões funcionam. Você pode usar um dos dois procedimentos a seguir.

Testar as permissões usando a AWS CLI

1. Atualize o arquivo de configuração da AWS CLI adicionando o perfil `UserDaveAccountA` a seguir. Para obter mais informações, consulte Configurar as ferramentas para as demonstrações.

   ```
   [profile UserDaveAccountA]
   aws_access_key_id = access-key
   aws_secret_access_key = secret-access-key
   region = us-east-1
   ```

2. Verifique se Dave pode executar as operações conforme concedido na política de usuário. Carregue um objeto de exemplo usando o comando `put-object` da AWS CLI a seguir.

   O parâmetro `--body` no comando identifica o arquivo de origem para fazer upload. Por exemplo, se o arquivo estiver na raiz da unidade C: de um computador Windows, você deve especificar `c:\HappyFace.jpg`. O parâmetro `--key` fornece o nome de chave para o objeto.

   ```
   aws s3api put-object --bucket awsexamplebucket1 --key HappyFace.jpg --
   body HappyFace.jpg --profile UserDaveAccountA
   ```

   Execute o comando da AWS CLI a seguir para obter o objeto.

   ```
   aws s3api get-object --bucket awsexamplebucket1 --key HappyFace.jpg OutputFile.jpg
    --profile UserDaveAccountA
   ```

Testar as permissões usando o AWS Tools for Windows PowerShell

1. Armazene as credenciais de Dave como `AccountADave`. Depois, use essas credenciais para PUT e GET um objeto.

   ```
   set-awscredentials -AccessKey AccessKeyID -SecretKey SecretAccessKey -storeas
    AccountADave
   ```

2. Carregue um objeto de exemplo usando o comando `Write-S3Object` do AWS Tools for Windows PowerShell com as credenciais armazenadas do usuário Dave.

```
Write-S3Object -bucketname awsexamplebucket1 -key HappyFace.jpg -file HappyFace.jpg
 -StoredCredentials AccountADave
```

Faça download do objeto anteriormente carregado.

```
Read-S3Object -bucketname awsexamplebucket1 -key HappyFace.jpg -file Output.jpg -
StoredCredentials AccountADave
```

Exemplo 2: Proprietário do bucket concedendo permissões de bucket entre contas

> **Important**
>
> Conceder permissões a perfis do IAM é uma prática melhor do que conceder permissões a usuários individuais. Para aprender a fazer isso, consulte Noções básicas de permissões entre contas e do uso de perfis do IAM.

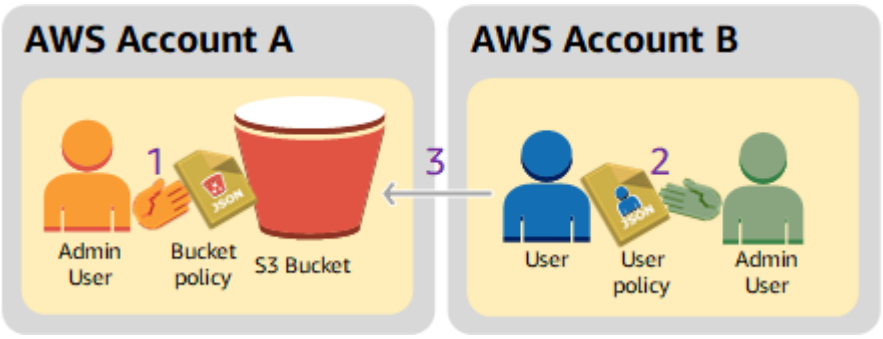
Tópicos

- Preparar para a demonstração
- Etapa 1: Fazer as tarefas da Conta A
- Etapa 2: Fazer as tarefas da Conta B
- Etapa 3: (opcional) tentar negação explícita
- Etapa 4: limpar

Uma Conta da AWS, por exemplo, a conta A, pode conceder a outra Conta da AWS, a conta B, permissão para acessar os respectivos recursos, como buckets e objetos. A Conta B pode então delegar essas permissões para usuários em sua conta. Neste cenário de exemplo, o proprietário do bucket concede a permissão entre contas a outra conta para executar operações específicas no bucket.

> **Note**
>
> A Conta A também pode conceder diretamente a um usuário na Conta B permissões usando uma política de bucket. No entanto, o usuário ainda precisará ter permissão da conta principal, a Conta B, à qual o usuário pertence, mesmo que a Conta B não tenha permissões da Conta A. Desde que o usuário tenha permissão do proprietário do recurso e da conta principal, o usuário poderá acessar o recurso.

Veja a seguir um resumo das etapas de demonstração:



1. O usuário administrador da Conta A anexa uma política de bucket concedendo permissões entre contas à Conta B para executar operações específicas no bucket.

   Observe que o usuário administrador da Conta B herdará automaticamente as permissões.
2. O usuário administrador da Conta B anexa uma política de usuário ao usuário delegando as permissões que recebeu da Conta A.
3. Em seguida, o usuário na Conta B verifica as permissões acessando um objeto no bucket de propriedade da Conta A.

Para este exemplo, você precisará de duas contas. A tabela a seguir mostra como nos referimos a essas contas e aos usuários administradores nessas contas. Conforme as diretrizes do IAM (consulte Sobre o uso de um usuário administrador para criar recursos e conceder permissões), não usamos as credenciais do usuário-raiz nessa demonstração. Em vez disso, você cria um usuário administrador em cada conta e usa essas credenciais para criar recursos e conceder permissões a eles.

ID da Conta da AWS	Conta referida como	Usuário administrador na conta
1111-1111-1111	Conta A	AccountAadmin
2222-2222-2222	Conta B	AccountBadmin

Todas as tarefas de criar usuários e conceder permissões são feitas no AWS Management Console. Para verificar permissões, a demonstração usa as ferramentas de linha de comando, a AWS Command Line Interface (CLI), e o AWS Tools for Windows PowerShell. Portanto, você não precisa escrever nenhum código.

Preparar para a demonstração

1. Você precisa ter duas Contas da AWS, e cada conta deverá ter um usuário administrador, conforme mostrado na tabela na seção anterior.

   a. Cadastre-se para obter uma Conta da AWS, se necessário.

   b. Usando as credenciais da Conta A, faça login no console do IAM para criar o usuário administrador:

      i. Crie um usuário **`AccountAadmin`** e anote as credenciais de segurança. Para obter instruções, consulte Criar um usuário do IAM na sua Conta da AWS no Guia do usuário do IAM.

      ii. Conceda privilégios de administrador a AccountAadmin anexando uma política de usuário com pleno acesso. Para instruções, consulte Como trabalhar com políticas no Guia do usuário do IAM.

   c. Enquanto estiver no console do IAM, anote o URL de login de usuário do IAM indicado no Painel. Todos os usuários nessa conta devem usar essa URL para fazer login no AWS Management Console.

      Para obter mais informações, consulte Como os usuários fazem login em sua conta no Guia do usuário do IAM.

   d. Repita a etapa anterior usando as credenciais da Conta B e crie um usuário administrador **`AccountBadmin`**.

2. Configure a AWS Command Line Interface (AWS CLI) ou o AWS Tools for Windows PowerShell. Salve as credenciais de usuário do administrador da seguinte maneira:

   - Se estiver usando a AWS CLI, crie dois perfis, `AccountAadmin` e `AccountBadmin`, no arquivo de configuração.
   - Se estiver usando o AWS Tools for Windows PowerShell, armazene as credenciais da sessão como `AccountAadmin` e `AccountBadmin`.

   Para instruções, consulte Configurar as ferramentas para as demonstrações.

3. Salve as credenciais do usuário administrador, também conhecidas como perfis. Você pode usar o nome do perfil em vez de especificar as credenciais para cada comando digitado. Para obter mais informações, consulte Configurar as ferramentas para as demonstrações.

a. Adicione perfis no arquivo de credenciais da AWS CLI para cada um dos usuários administradores, `AccountAadmin` e `AccountBadmin`, nas duas contas.

```
[AccountAadmin]
aws_access_key_id = access-key-ID
aws_secret_access_key = secret-access-key
region = us-east-1

[AccountBadmin]
aws_access_key_id = access-key-ID
aws_secret_access_key = secret-access-key
region = us-east-1
```

b. Se estiver usando o AWS Tools for Windows PowerShell, execute o comando a seguir.

```
set-awscredentials -AccessKey AcctA-access-key-ID -SecretKey AcctA-secret-
access-key -storeas AccountAadmin
set-awscredentials -AccessKey AcctB-access-key-ID -SecretKey AcctB-secret-
access-key -storeas AccountBadmin
```

Etapa 1: Fazer as tarefas da Conta A

Etapa 1.1: fazer login no AWS Management Console

Usando o URL de login do usuário do IAM da Conta A, primeiro faça login no AWS Management Console como o usuário AccountAadmin. Esse usuário criará um bucket e anexará uma política a ele.

Etapa 1.2: Criar um bucket

1. No console do Amazon S3, crie um bucket. Esse exercício supõe que o bucket é criado na Região da AWS Leste dos EUA (Norte da Virgínia) e que o nome dele é *amzn-s3-demo-bucket*.

   Para instruções, consulte Criar um bucket de uso geral.

2. Faça upload de um objeto de exemplo no bucket.

   Para obter instruções, vá para Etapa 2: fazer upload de um objeto para o seu bucket.

Etapa 1.3: anexar uma política de bucket para conceder permissões entre contas para a conta B

A política de bucket concede as permissões `s3:GetLifecycleConfiguration` e `s3:ListBucket` à Conta B, presumindo que você ainda está usando as credenciais do usuário AccountAadmin no console.

1. Anexe a política de bucket a seguir ao *amzn-s3-demo-bucket*. A política concede à Conta B permissão para as ações `s3:GetLifecycleConfiguration` e `s3:ListBucket`.

   Para instruções, consulte Adicionar uma política de bucket usando o console do Amazon S3.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "Example permissions",
         "Effect": "Allow",
         "Principal": {
            "AWS": "arn:aws:iam::AccountB-ID:root"
         },
         "Action": [
            "s3:GetLifecycleConfiguration",
            "s3:ListBucket"
         ],
         "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket"
         ]
      }
   ]
}
```

2. Verifique se a Conta B (ou seja, do usuário administrador) pode executar as operações.

   - Fazer a verificação usando a AWS CLI

```
aws s3 ls s3://amzn-s3-demo-bucket --profile AccountBadmin
aws s3api get-bucket-lifecycle-configuration --bucket amzn-s3-demo-bucket --
profile AccountBadmin
```

   - Fazer a verificação usando o AWS Tools for Windows PowerShell

```
get-s3object -BucketName amzn-s3-demo-bucket -StoredCredentials AccountBadmin
```

```
get-s3bucketlifecycleconfiguration -BucketName amzn-s3-demo-bucket -
StoredCredentials AccountBadmin
```

Etapa 2: Fazer as tarefas da Conta B

Agora o administrador da Conta B cria um usuário, Dave, e delega as permissões recebidas da Conta A.

Etapa 2.1: Fazer login no AWS Management Console

Usando o URL de login do usuário do IAM da Conta B, primeiro faça login no AWS Management Console como o usuário AccountBadmin.

Etapa 2.2: criar o usuário Dave na conta B

No console do IAM, crie um usuário chamado **`Dave`**.

Para obter instruções, consulte Criação de usuários do IAM (console) no Guia do usuário do IAM.

Etapa 2.3: delegar permissões para o usuário Dave

Crie uma política inline para o usuário Dave usando as seguintes políticas. Você precisará atualizar a política fornecendo o nome do bucket.

Presume-se que você fez login no console usando as credenciais do usuário AccountBadmin.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "Example",
         "Effect": "Allow",
         "Action": [
            "s3:ListBucket"
         ],
         "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket"
         ]
      }
   ]
}
```

Consulte instruções em Gerenciar políticas do IAM no Guia do usuário do IAM.

Etapa 2.4: Testar permissões

Agora Dave, na conta B, pode listar o conteúdo do *amzn-s3-demo-bucket* de propriedade da Conta A. Você pode verificar as permissões usando um dos seguintes procedimentos.

Testar as permissões usando a AWS CLI

1. Adicione o perfil `UserDave` ao arquivo de configuração da AWS CLI. Para obter mais informações sobre o arquivo de configuração, consulte Configurar as ferramentas para as demonstrações

   ```
   [profile UserDave]
   aws_access_key_id = access-key
   aws_secret_access_key = secret-access-key
   region = us-east-1
   ```

2. No prompt de comando, insira o comando da AWS CLI a seguir para verificar se agora Dave consegue obter uma lista de objetos do `UserDave` pertencente à Conta A. Observe que o comando especifica o perfil *amzn-s3-demo-bucket*.

   ```
   aws s3 ls s3://amzn-s3-demo-bucket --profile UserDave
   ```

   Dave não tem nenhuma outra permissão. Portanto, se ele tentar realizar qualquer outra operação (por exemplo, a configuração de `get-bucket-lifecycle` a seguir), o Amazon S3 retornará uma negação da permissão.

   ```
   aws s3api get-bucket-lifecycle-configuration --bucket amzn-s3-demo-bucket --profile
    UserDave
   ```

Testar as permissões usando o AWS Tools for Windows PowerShell

1. Armazene as credenciais de Dave como `AccountBDave`.

   ```
   set-awscredentials -AccessKey AccessKeyID -SecretKey SecretAccessKey -storeas
    AccountBDave
   ```

2. Teste o comando List Bucket.

   ```
   get-s3object -BucketName amzn-s3-demo-bucket -StoredCredentials AccountBDave
   ```

Dave não tem nenhuma outra permissão. Portanto, se ele tentar realizar qualquer outra operação (por exemplo, a `get-s3bucketlifecycleconfiguration` a seguir), o Amazon S3 retornará uma negação da permissão.

```
get-s3bucketlifecycleconfiguration -BucketName amzn-s3-demo-bucket -
StoredCredentials AccountBDave
```

Etapa 3: (opcional) tentar negação explícita

Você pode ter permissões concedidas usando uma lista de controle de acesso (ACL), uma política de bucket ou uma política de usuário. Entretanto, se houver uma negação explícita definida por uma política de bucket ou por uma política de usuário, ela terá precedência sobre qualquer outra permissão. Para testar, atualize a política de bucket e negue explicitamente a permissão `s3:ListBucket` para a Conta B. A política também concede a permissão `s3:ListBucket`. No entanto, a negação explícita tem precedência, e a Conta B ou os usuários da Conta B não poderão listar objetos no *amzn-s3-demo-bucket*.

1. Usando as credenciais do usuário `AccountAadmin` na Conta A, substitua a política de bucket pela seguinte:

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "Example permissions",
         "Effect": "Allow",
         "Principal": {
            "AWS": "arn:aws:iam::AccountB-ID:root"
         },
         "Action": [
            "s3:GetLifecycleConfiguration",
            "s3:ListBucket"
         ],
         "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket"
         ]
      },
      {
         "Sid": "Deny permission",
```

```
            "Effect": "Deny",
            "Principal": {
               "AWS": "arn:aws:iam::AccountB-ID:root"
            },
            "Action": [
               "s3:ListBucket"
            ],
            "Resource": [
               "arn:aws:s3:::amzn-s3-demo-bucket"
            ]
         }
      ]
}
```

2. Agora, se você tentar obter uma lista de bucket usando as credenciais de `AccountBadmin`, o acesso será negado.

   - Usando a AWS CLI, execute o seguinte comando:

     ```
     aws s3 ls s3://amzn-s3-demo-bucket --profile AccountBadmin
     ```

   - Usando o AWS Tools for Windows PowerShell, execute o seguinte comando:

     ```
     get-s3object -BucketName amzn-s3-demo-bucket -StoredCredentials AccountBDave
     ```

Etapa 4: limpar

1. Depois de terminar os testes, você pode fazer o seguinte para concluir a limpeza:

   - Faça login no AWS Management Console (AWS Management Console) usando as credenciais da Conta A e faça o seguinte:

     - No console do Amazon S3, remova a política de bucket anexada a *amzn-s3-demo-bucket*. Nas Propriedades do bucket, exclua a política na seção Permissions (Permissões).
     - Se o bucket foi criado para este exercício, no console do Amazon S3, exclua os objetos e, em seguida, exclua o bucket.
     - No console do IAM, remova o usuário `AccountAadmin`.

2. Faça login no console do IAM usando as credenciais da Conta B. Exclua o usuário `AccountBadmin`. Consulte instruções detalhadas em Exclusão de um usuário do IAM no Guia do usuário do IAM.

Exemplo 3: O proprietário do bucket concede permissões para objetos que não possui

> **Important**
>
> Conceder permissões a perfis do IAM é uma prática melhor do que conceder permissões a usuários individuais. Para aprender a fazer isso, consulte Noções básicas de permissões entre contas e do uso de perfis do IAM.

Tópicos

- Etapa 0: Preparar-se para a demonstração
- Etapa 1: Realizar as tarefas da Conta A
- Etapa 2: Realizar as tarefas da Conta B
- Etapa 3: Testar permissões
- Etapa 4: limpar

O cenário desse exemplo é que o proprietário do bucket deseja conceder permissão para acesso a objetos, mas o proprietário do bucket não possui todos os objetos do bucket. Para este exemplo, o proprietário do bucket está tentando conceder permissão aos usuários em sua própria conta.

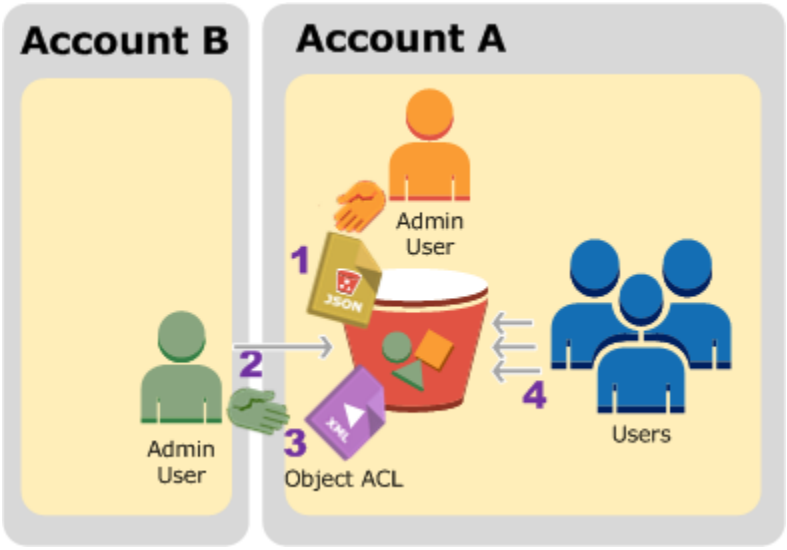
Um proprietário de bucket pode habilitar outras Contas da AWS a carregar objetos. Por padrão, o proprietário do bucket não possui objetos gravados em um bucket por outra Conta da AWS. Os objetos são de propriedade das contas que os gravam em um bucket do S3. Se o proprietário do bucket não for proprietário dos objetos no bucket, primeiro o proprietário dos objetos deverá conceder permissão ao proprietário do bucket usando uma lista de controle de acesso (ACL) de objetos. Depois, o proprietário do bucket poderá conceder permissões a um objeto que ele não possui. Para obter mais informações, consulte Propriedade de bucket e objeto do Amazon S3.

Se o proprietário do bucket adotar a configuração aplicada pelo proprietário do bucket em S3 Object Ownership para o bucket, o proprietário do bucket terá propriedade de todos os objetos do bucket, inclusive de objetos gravados por outra Conta da AWS. Essa abordagem resolve o problema de

objetos que não pertencem ao proprietário do bucket. Em seguida, é possível delegar permissão aos usuários em sua própria conta ou para outras Contas da AWS.

> **Note**
>
> A Propriedade de objetos do S3 é uma configuração no nível do bucket do Amazon S3 que você pode usar para controlar a propriedade de objetos carregados no bucket e para desabilitar ou habilitar as ACLs. Por padrão, a Propriedade de Objetos está definida com a configuração Imposto pelo proprietário do bucket e todas as ACLs estão desabilitadas. Quando as ACLs são desabilitadas, o proprietário do bucket possui todos os objetos do bucket e gerencia o acesso a eles exclusivamente usando políticas de gerenciamento de acesso.
>
> A maioria dos casos de uso modernos no Amazon S3 não exige mais o uso de ACLs. Recomendamos manter as ACLs desabilitadas, exceto em circunstâncias incomuns em que seja necessário controlar o acesso para cada objeto individualmente. Com as ACLs desabilitadas, é possível usar políticas para controlar o acesso a todos os objetos no bucket, independentemente de quem carregou os objetos para o bucket. Para obter mais informações, consulte Controlar a propriedade de objetos e desabilitar ACLs para seu bucket.

Neste exemplo, assumimos que o proprietário do bucket não aplicou a configuração aplicada pelo proprietário do bucket em Object Ownership. O proprietário do bucket delega permissão aos usuários em sua própria conta. Veja a seguir um resumo das etapas de demonstração:



1. O usuário administrador da Conta A anexa uma política de bucket com duas declarações.

- Habilitar permissão entre contas para a Conta B fazer upload de objetos.
- Permitir que um usuário em sua própria conta acesse objetos no bucket.

2. O usuário administrador da Conta B faz upload de objetos no bucket de propriedade da Conta A.
3. O administrador da Conta B atualiza a ACL do objeto adicionando uma concessão que dá ao proprietário do bucket permissão de controle total sobre o objeto.
4. O usuário na Conta A verifica acessando objetos no bucket, independentemente de quem os possui.

Para este exemplo, você precisará de duas contas. A tabela a seguir mostra como nos referimos a essas contas e aos usuários administradores nessas contas. Nesta demonstração, você não usa as credenciais do usuário raiz da conta, conforme as diretrizes recomendadas do IAM. Para obter mais informações, consulte Sobre o uso de um usuário administrador para criar recursos e conceder permissões. Em vez disso, você cria um administrador em cada conta e usa essas credenciais para criar recursos e conceder permissões a eles.

ID da Conta da AWS	Conta referida como	Administrador na conta
1111-1111-1111	Conta A	AccountAadmin
2222-2222-2222	Conta B	AccountBadmin

Todas as tarefas de criar usuários e conceder permissões são feitas no AWS Management Console. Para verificar permissões, a demonstração usa as ferramentas de linha de comando, a AWS Command Line Interface (AWS CLI), e o AWS Tools for Windows PowerShell. Portanto, você não precisa escrever nenhum código.

Etapa 0: Preparar-se para a demonstração

1. Você precisa ter duas Contas da AWS, e cada conta deverá ter um administrador, conforme mostrado na tabela na seção anterior.

   a. Cadastre-se para obter uma Conta da AWS, se necessário.

   b. Usando as credenciais da Conta A, faça login no console do IAM e faça o seguinte para criar um usuário administrador:

- Crie um usuário **`AccountAadmin`** e anote as credenciais de segurança do usuário. Para obter mais informações sobre como adicionar usuários, consulte Criar um usuário do IAM na sua Conta da AWS no Guia do usuário do IAM.
- Conceda permissões de administrador a AccountAadmin anexando uma política de usuário com pleno acesso. Consulte instruções em Gerenciar políticas do IAM no Guia do usuário do IAM.
- No console do IAM, anote o URL de login de usuário do IAM indicado no Painel. Os usuários nessa conta devem usar esse URL para fazer login no AWS Management Console. Para obter mais informações, consulte Como os usuários fazem login em sua conta no Guia do usuário do IAM.

c. Repita a etapa anterior usando as credenciais da Conta B e crie um usuário administrador **`AccountBadmin`**.

2. Configure a AWS CLI ou as Tools for Windows PowerShell. Salve as credenciais de administrador da seguinte forma:

   - Se estiver usando a AWS CLI, crie dois perfis, `AccountAadmin` e `AccountBadmin`, no arquivo de configuração.
   - Se estiver usando o Tools for Windows PowerShell, armazene as credenciais da sessão como `AccountAadmin` e `AccountBadmin`.

   Para instruções, consulte Configurar as ferramentas para as demonstrações.

Etapa 1: Realizar as tarefas da Conta A

Execute as seguintes etapas para a Conta A:

Etapa 1.1: Fazer login no console

Usando o URL de login do usuário do IAM da Conta A, faça login no AWS Management Console como o usuário **`AccountAadmin`**. Esse usuário criará um bucket e anexará uma política a ele.

Etapa 1.2: Criar um bucket e um usuário e adicionar uma política de bucket para conceder permissões ao usuário

1. No console do Amazon S3, crie um bucket. Esse exercício supõe que o bucket foi criado na Região da AWS Leste dos EUA (Norte da Virgínia) e que o nome dele é *`amzn-s3-demo-bucket1`*.

Para instruções, consulte Criar um bucket de uso geral.

2. No console do IAM, crie um usuário chamado **`Dave`**.

   Para obter instruções passo a passo, consulte Criação de usuários do IAM (console) no Guia do usuário do IAM.

3. Anote as credenciais do usuário Dave.

4. No console do Amazon S3, anexe a seguinte política do bucket ao bucket *`amzn-s3-demo-bucket1`*. Para instruções, consulte Adicionar uma política de bucket usando o console do Amazon S3. Siga as etapas para adicionar uma política de bucket. Para obter informações sobre como encontrar IDs de conta, consulte Como encontrar o ID da Conta da AWS.

   A política concede à Conta B as permissões `s3:PutObject` e `s3:ListBucket`. A política também concede ao usuário `Dave` a permissão `s3:GetObject`.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "Statement1",
         "Effect": "Allow",
         "Principal": {
            "AWS": "arn:aws:iam::AccountB-ID:root"
         },
         "Action": [
            "s3:PutObject",
            "s3:ListBucket"
         ],
         "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket1/*",
            "arn:aws:s3:::amzn-s3-demo-bucket1"
         ]
      },
      {
         "Sid": "Statement3",
         "Effect": "Allow",
         "Principal": {
            "AWS": "arn:aws:iam::AccountA-ID:user/Dave"
         },
         "Action": [
            "s3:GetObject"
```

```
            ],
            "Resource": [
               "arn:aws:s3:::amzn-s3-demo-bucket1/*"
            ]
         }
   ]
}
```

Etapa 2: Realizar as tarefas da Conta B

Agora que a Conta B tem permissões para executar operações no bucket da Conta A, o administrador da Conta B pode fazer o seguinte:

- Carregar um objeto no bucket da Conta A.
- Adicionar uma concessão à ACL do objeto para permitir que a Conta A, a proprietária do bucket, tenha controle total.

Como usar o AWS CLI

1. Usando o comando `put-object` da AWS CLI, carregue um objeto. O parâmetro `--body` no comando identifica o arquivo de origem para fazer upload. Por exemplo, se o arquivo estiver na unidade `C:` de um computador Windows, especifique `c:\HappyFace.jpg`. O parâmetro `--key` fornece o nome de chave para o objeto.

   ```
   aws s3api put-object --bucket amzn-s3-demo-bucket1 --key HappyFace.jpg --body
    HappyFace.jpg --profile AccountBadmin
   ```

2. Adicionar uma concessão à ACL do objeto para permitir controle total do objeto ao proprietário do bucket. Para obter informações sobre como encontrar um ID de usuário canônico, consulte Find the canonical user ID for your Conta da AWS no Guia de referência de gerenciamento de contas da AWS.

   ```
   aws s3api put-object-acl --bucket amzn-s3-demo-bucket1 --key HappyFace.jpg --grant-
   full-control id="AccountA-CanonicalUserID" --profile AccountBadmin
   ```

Usar o Tools for Windows PowerShell

1. Carregue um objeto usando o comando `Write-S3Object`.

```
Write-S3Object -BucketName amzn-s3-demo-bucket1 -key HappyFace.jpg -file
 HappyFace.jpg -StoredCredentials AccountBadmin
```

2. Adicionar uma concessão à ACL do objeto para permitir controle total do objeto ao proprietário do bucket.

```
Set-S3ACL -BucketName amzn-s3-demo-bucket1 -Key HappyFace.jpg -CannedACLName
 "bucket-owner-full-control" -StoredCreden
```

Etapa 3: Testar permissões

Agora verifique se o usuário Dave na conta A pode acessar o objeto de propriedade da conta B.

Como usar o AWS CLI

1. Adicione as credenciais do usuário Dave ao arquivo de configuração da AWS CLI e crie um novo perfil, `UserDaveAccountA`. Para obter mais informações, consulte Configurar as ferramentas para as demonstrações.

```
[profile UserDaveAccountA]
aws_access_key_id = access-key
aws_secret_access_key = secret-access-key
region = us-east-1
```

2. Execute o comando `get-object` da CLI para fazer download do arquivo `HappyFace.jpg` e salve-o localmente. Você fornece credenciais ao usuário Dave adicionando o parâmetro `--profile`.

```
aws s3api get-object --bucket amzn-s3-demo-bucket1 --key
 HappyFace.jpg Outputfile.jpg --profile UserDaveAccountA
```

Usar o Tools for Windows PowerShell

1. Armazene as credenciais da AWS do usuário Dave, como `UserDaveAccountA`, para armazenamento persistente.

```
Set-AWSCredentials -AccessKey UserDave-AccessKey -SecretKey UserDave-
SecretAccessKey -storeas UserDaveAccountA
```

2. Execute o comando `Read-S3Object` para fazer download do objeto `HappyFace.jpg` e salve-o localmente. Você fornece credenciais ao usuário Dave adicionando o parâmetro `-StoredCredentials`.

```
Read-S3Object -BucketName amzn-s3-demo-bucket1 -Key HappyFace.jpg -file
 HappyFace.jpg  -StoredCredentials UserDaveAccountA
```

Etapa 4: limpar

1. Depois de terminar os testes, você pode fazer o seguinte para concluir a limpeza:
   - Faça login no AWS Management Console usando as credenciais da Conta A e faça o seguinte:
     - No console do Amazon S3, remova a política de bucket anexada a *amzn-s3-demo-bucket1*. Nas Propriedades do bucket, exclua a política na seção Permissions (Permissões).
     - Se o bucket foi criado para este exercício, no console do Amazon S3, exclua os objetos e, em seguida, exclua o bucket.
     - No console do IAM, remova o usuário AccountAadmin. Consulte instruções detalhadas em Exclusão de um usuário do IAM no Guia do usuário do IAM.
2. Faça login no AWS Management Console usando as credenciais da Conta B. No console do IAM, exclua o usuário AccountBadmin.

Exemplo 4: proprietário do bucket concede permissão entre contas a objetos que não possui

Tópicos

- Noções básicas de permissões entre contas e do uso de perfis do IAM
- Etapa 0: Preparar-se para a demonstração
- Etapa 1: Realizar as tarefas da Conta A
- Etapa 2: Realizar as tarefas da Conta B

- Etapa 3: realizar as tarefas da Conta C
- Etapa 4: limpar
- Recursos relacionados

Neste cenário de exemplo, você é proprietário de um bucket e habilitou outras Contas da AWS para carregar objetos. Se você aplicou a configuração aplicada pelo proprietário do bucket em S3 Object Ownership para o bucket, terá propriedade de todos os objetos do bucket, inclusive de objetos gravados por outra Conta da AWS. Essa abordagem resolve o problema de objetos que não pertencem a você, o proprietário do bucket. Em seguida, é possível delegar permissão aos usuários em sua própria conta ou para outras Contas da AWS. Suponha que a configuração imposta pelo proprietário do bucket em S3 Object Ownership não esteja habilitada. Ou seja, seu bucket pode ter objetos pertencentes a outras Contas da AWS.

Agora, suponha que, como proprietário do bucket, você precise conceder permissão entre contas aos objetos, independentemente de quem seja o proprietário, a um usuário em outra conta. Por exemplo, esse usuário pode ser um aplicativo de faturamento que precise acessar metadados de objeto. Há dois problemas principais:

- O proprietário do bucket não tem permissões sobre os objetos criados por outras Contas da AWS. Para que o proprietário do bucket possa conceder permissões em objetos que não possui, o proprietário do objeto deve primeiro conceder permissão ao proprietário do bucket. O proprietário do objeto é a Conta da AWS que criou os objetos. Depois, o proprietário do bucket pode delegar essas permissões.
- O proprietário do bucket pode delegar permissões aos usuários em sua própria conta (consulte Exemplo 3: O proprietário do bucket concede permissões para objetos que não possui). No entanto, a conta do proprietário do bucket não pode delegar permissões a outras Contas da AWS porque a delegação entre contas não é permitida.

Nesse cenário, o proprietário do bucket pode criar um perfil do AWS Identity and Access Management (IAM) com permissão para acessar objetos e, depois, conceder permissão a outra Conta da AWS para assumir o perfil temporariamente, permitindo que ela acesse objetos no bucket.

> **Note**
>
> A Propriedade de objetos do S3 é uma configuração no nível do bucket do Amazon S3 que você pode usar para controlar a propriedade de objetos carregados no bucket e para desabilitar ou habilitar as ACLs. Por padrão, a Propriedade de Objetos está definida com

a configuração Imposto pelo proprietário do bucket e todas as ACLs estão desabilitadas. Quando as ACLs são desabilitadas, o proprietário do bucket possui todos os objetos do bucket e gerencia o acesso a eles exclusivamente usando políticas de gerenciamento de acesso.
A maioria dos casos de uso modernos no Amazon S3 não exige mais o uso de ACLs. Recomendamos manter as ACLs desabilitadas, exceto em circunstâncias incomuns em que seja necessário controlar o acesso para cada objeto individualmente. Com as ACLs desabilitadas, é possível usar políticas para controlar o acesso a todos os objetos no bucket, independentemente de quem carregou os objetos para o bucket. Para obter mais informações, consulte Controlar a propriedade de objetos e desabilitar ACLs para seu bucket.

Noções básicas de permissões entre contas e do uso de perfis do IAM

As funções do IAM permitem vários cenários para delegar acesso a seus recursos, e o acesso entre contas é um dos cenários principais. Neste exemplo, o proprietário do bucket, a Conta A, usa um perfil do IAM para delegar temporariamente o acesso entre contas a objetos aos usuários em uma outra Conta da AWS, a Conta C. Cada perfil do IAM que você cria tem estas duas políticas anexadas a ela:

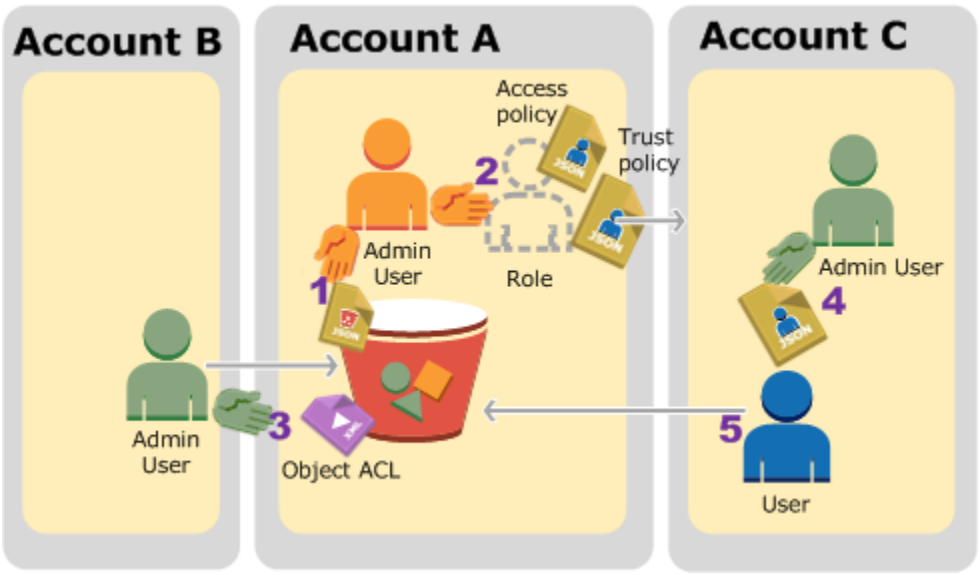
- Uma política de confiança que identifica outra Conta da AWS que pode assumir a função.
- Uma política de acesso que define quais permissões - por exemplo, `s3:GetObject` - são permitidas quando alguém assume a função. Para obter uma lista de permissões que você pode especificar em uma política, consulte Ações de políticas para o Amazon S3.

A Conta da AWS identificada na política de confiança concede ao respectivo usuário permissão para assumir a função. O usuário pode então fazer o seguinte para acessar os objetos:

- Assumir a função e, em resposta, obter credenciais de segurança temporárias.
- Usando as credenciais de segurança temporárias, acessar os objetos no bucket.

Para obter mais informações sobre funções do IAM, consulte Perfis do IAM no Guia do usuário do IAM.

Veja a seguir um resumo das etapas de demonstração:



1. O usuário administrador da Conta A anexa a política do bucket que concede à Conta B uma permissão condicional para fazer upload de objetos.
2. O administrador da Conta A cria uma função do IAM, estabelecendo a confiança com a Conta C, e assim os usuários dessa conta podem acessar a Conta. A. A política de acesso anexada à função limita o que o usuário na Conta C pode fazer quando acessa a Conta A.
3. O administrador da Conta B faz upload de um objeto no bucket de propriedade da Conta A, concedendo permissão de controle total ao proprietário do bucket.
4. O administrador da Conta C cria um usuário e anexa uma política de usuário que permite que o usuário assuma a função.
5. O usuário na Conta C primeiro assume a função, que retorna as credenciais de segurança temporárias ao usuário. Usando essas credenciais de segurança temporárias, o usuário então acessa os objetos no bucket.

Para este exemplo, você precisará de três contas. A tabela a seguir mostra como nos referimos a essas contas e aos usuários administradores nessas contas. Conforme as diretrizes do IAM (consulte Sobre o uso de um usuário administrador para criar recursos e conceder permissões), não usamos as credenciais do Usuário raiz da conta da AWS nesta demonstração. Em vez disso, você cria um usuário administrador em cada conta e usa essas credenciais para criar recursos e conceder permissões a eles.

ID da Conta da AWS	Conta referida como	Usuário administrador na conta
1111-1111-1111	Conta A	AccountAadmin
2222-2222-2222	Conta B	AccountBadmin
3333-3333-3333	Conta C	AccountCadmin

Etapa 0: Preparar-se para a demonstração

> **Note**
>
> É recomendado abrir um editor de texto e anotar algumas informações enquanto você passa pelas etapas. Especificamente, você vai precisar dos IDs de conta, IDs de usuários canônicos, URLs de login de usuário do IAM de cada conta para se conectar ao console e nomes de recurso da Amazon (ARNs) dos perfis e usuários do IAM.

1. Você precisa ter três Contas da AWS, e cada uma delas deve ter um usuário administrador, conforme exibido na tabela da seção anterior.

   a. Cadastre-se para Contas da AWS, se necessário. Nós nos referimos a essas contas como Conta A, Conta B e Conta C.

   b. Usando as credenciais da Conta A, faça login no console do IAM e faça o seguinte para criar um usuário administrador:

      - Crie o usuário **`AccountAadmin`** e anote as credenciais de segurança. Para obter mais informações sobre como adicionar usuários, consulte Criar um usuário do IAM na sua Conta da AWS no Guia do usuário do IAM.
      - Conceda privilégios de administrador a AccountAadmin anexando uma política de usuário com pleno acesso. Consulte instruções em Gerenciar políticas do IAM no Guia do usuário do IAM.
      - No console do IAM, anote o URL de login de usuário do IAM indicado no Painel. Os usuários nessa conta devem usar esse URL para fazer login no AWS Management

Console. Consulte mais informações em Sign in to the AWS Management Console as an IAM user no Guia do usuário do IAM.

c. Repita a etapa anterior para criar usuários administradores na Conta B e na Conta C.

2. Para a Conta C, anote o ID de usuário canônico.

   Quando criar uma função do IAM na Conta A, a política de confiança concederá à Conta C a permissão para assumir a função especificando o ID da conta. Você pode localizar as informações da conta da seguinte forma:

   a. Use o ID ou o alias da Conta da AWS, o nome de usuário do IAM e a senha para fazer login no console do Amazon S3.

   b. Selecione o nome de um bucket do Amazon S3 para visualizar os detalhes sobre esse bucket.

   c. Selecione a guia Permissions (Permissões) e selecione Access Control List (Lista de controle de acesso).

   d. Na seção Acesso à sua Conta da AWS, a coluna Conta inclui um identificador longo, como `c1daexampleaaf850ea79cf0430f33d72579fd1611c97f7ded193374c0b163b6`. Esse é seu ID de usuário canônico.

3. Ao criar uma política do bucket, você precisará das seguintes informações. Anote estes valores:

   - ID de usuário canônico da Conta A: quando o administrador da Conta A conceder permissão condicional para fazer upload de objeto ao administrador da Conta B, a condição especifica o ID de usuário canônico do usuário da Conta A que deverá ter pleno controle dos objetos.

     > **Note**
     >
     > O ID de usuário canônico é o único conceito do Amazon S3. Ele é a versão oculta de 64 caracteres do ID da conta.

   - ARN do usuário para o administrador da Conta B: é possível encontrar o ARN do usuário no console do IAM. Selecione o usuário e veja o respectivo ARN na guia Resumo.

     Na política do bucket, você concede permissão a `AccountBadmin` para carregar objetos e especifica o usuário com o ARN. Aqui está um exemplo de valor do Nome de recurso da Amazon (ARN):

     ```
     arn:aws:iam::AccountB-ID:user/AccountBadmin
     ```

4. Configure a AWS Command Line Interface (CLI) ou o AWS Tools for Windows PowerShell. Salve as credenciais de usuário do administrador da seguinte maneira:

   - Se estiver usando a AWS CLI, crie os perfis `AccountAadmin` e `AccountBadmin` no arquivo de configuração.
   - Se estiver usando o AWS Tools for Windows PowerShell, armazene as credenciais da sessão como `AccountAadmin` e `AccountBadmin`.

   Para instruções, consulte Configurar as ferramentas para as demonstrações.

Etapa 1: Realizar as tarefas da Conta A

Neste exemplo, a Conta A é o proprietário do bucket. Assim, o usuário AccountAadmin na Conta A realizará estas ações:

- Crie um bucket.
- Anexará uma política de bucket que conceda ao administrador da Conta B uma permissão para carregar objetos.
- Criará um perfil do IAM que conceda permissão à Conta C para assumir o perfil para que seja possível acessar os objetos no bucket.

Etapa 1.1: fazer login no AWS Management Console

Usando o URL de login do usuário do IAM da Conta A, primeiro faça login no AWS Management Console como o usuário **`AccountAadmin`**. Esse usuário criará um bucket e anexará uma política a ele.

Etapa 1.2: Criar um bucket e anexar uma política do bucket

No console do Amazon S3, faça o seguinte:

1. Crie um bucket. Este exercício supõe que o nome do bucket é *`amzn-s3-demo-bucket1`*.

   Para instruções, consulte Criar um bucket de uso geral.

2. Anexe a política de bucket a seguir. A política concede ao administrador da Conta B uma permissão condicional para carregar objetos.

Atualize a política fornecendo seus próprios valores para *amzn-s3-demo-bucket1*, *AccountB-ID* e *CanonicalUserId-of-AWSaccountA-BucketOwner*.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "111",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::AccountB-ID:user/AccountBadmin"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*"
        },
        {
            "Sid": "112",
            "Effect": "Deny",
            "Principal": {
                "AWS": "arn:aws:iam::AccountB-ID:user/AccountBadmin"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*",
            "Condition": {
                "StringNotEquals": {
                    "s3:x-amz-grant-full-control": "id=CanonicalUserId-of-
AWSaccountA-BucketOwner"
                }
            }
        }
    ]
}
```

Etapa 1.3: criar um perfil do IAM para conceder acesso entre contas na à Conta C na Conta A

No console do IAM, crie um perfil do IAM (**examplerole**) que conceda à Conta C permissão para assumir o perfil do IAM. Você deve manter a conexão como administrador da Conta A porque o perfil deve ser criado na Conta A.

1. Antes de criar a função, prepare as políticas gerenciadas que definem as permissões necessárias à função. Em uma etapa posterior, você anexará essa política à função.

a. No painel de navegação à esquerda, escolha Políticas e Criar política.

b. Próximo a Create Your Own Policy, escolha Select.

c. Insira **`access-accountA-bucket`** no campo Policy Name (Nome da política).

d. Copie a política de acesso a seguir e cole-a no campo Policy Document (Documento de políticas). A política de acesso concede permissão ao perfil `s3:GetObject`; assim, quando o usuário da Conta C assume o perfil, ele só pode executar a operação `s3:GetObject`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*"
    }
  ]
}
```

e. Escolha Create Policy.

As novas políticas aparecem na lista de políticas gerenciadas.

2. No painel de navegação à esquerda, escolha Perfis e Criar novo perfil.

3. Em Selecionar tipo de função, selecione Função para acesso entre contas e o botão Selecionar ao lado de Fornecer acesso entre as Contas da AWS que você possui.

4. Insira o ID de conta da Conta C.

Para esta demonstração, não é necessário exigir que os usuários tenham a autenticação multifator (MFA) para assumir o perfil; portanto, deixe essa opção desmarcada.

5. Escolha Próxima etapa para definir as permissões que serão associadas à função.

6. Marque a caixa de seleção ao lado da política access-accountA-bucket que você criou e escolha Próxima etapa.

A página Revisar será exibida para que você possa confirmar as configurações para a função antes de criá-la. Um item muito importante a observar nesta página é o link que você pode enviar aos usuários que precisem usar essa função. Os usuários que usam o link vão diretamente para a página Trocar perfil com os campos “ID da conta” e “Nome do perfil” já

preenchidos. Você também pode ver esse link mais tarde na página Resumo da função de qualquer função entre contas.

7. Insira `examplerole` para o nome do perfil e selecione Próxima etapa.
8. Depois de revisar o perfil, escolha Criar perfil.

   A função `examplerole` é exibida na lista de funções.
9. Selecione o nome de perfil `examplerole`.
10. Selecione a guia Trust Relationships (Relacionamentos de confiança).
11. Clique em Mostrar documento de política e verifique se a política de confiança mostrada corresponde à indicada a seguir.

    A política de confiança a seguir estabelece a confiança com a Conta C, permitindo-lhe a ação `sts:AssumeRole`. Para obter mais informações, consulte AssumeRole na Referência de APIs do AWS Security Token Service.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::AccountC-ID:root"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

12. Anote o nome do recurso da Amazon (ARN) do perfil `examplerole` que você criou.

    Depois, nas etapas a seguir, você anexará um política de usuário para permitir que um usuário do IAM assuma essa função e identificará a função com o valor de Nome de recurso da Amazon (ARN).

Etapa 2: Realizar as tarefas da Conta B

O exemplo de bucket de propriedade da Conta A precisa de objetos de propriedade de outras contas. Nessa etapa, o administrador da Conta B faz upload de um objeto usando as ferramentas da linha de comando.

- Usando o comando `put-object` da AWS CLI, faça upload de um objeto em *amzn-s3-demo-bucket1*.

  ```
  aws s3api put-object --bucket amzn-s3-demo-bucket1 --key HappyFace.jpg --
  body HappyFace.jpg --grant-full-control id="canonicalUserId-ofTheBucketOwner" --
  profile AccountBadmin
  ```

  Observe o seguinte:

  - O parâmetro `--Profile` especifica o perfil `AccountBadmin`; portanto, o objeto é de propriedade da Conta B.
  - O parâmetro `grant-full-control` concede ao proprietário do bucket permissão de pleno controle sobre o objeto conforme exigido pela política do bucket.
  - O parâmetro `--body` identifica o arquivo de origem para fazer upload. Por exemplo, se o arquivo estiver na unidade C: de um computador Windows, você especifica `c:\HappyFace.jpg`.

Etapa 3: realizar as tarefas da Conta C

Nas etapas anteriores, a Conta A já criou um perfil, `examplerole`, estabelecendo a confiança com a Conta C. Esse perfil permite que os usuários na Conta C acessem a Conta A. Nessa etapa, o administrador da Conta C cria um usuário (Dave) e delega para ele a permissão `sts:AssumeRole`, recebida da Conta A. Essa abordagem permite que Dave assuma o `examplerole` e tenha acesso temporário à Conta A. A política de acesso que a Conta A anexou ao perfil limita o que Dave pode fazer ao acessar a Conta A (especificamente, obter objetos no *amzn-s3-demo-bucket1*).

Etapa 3.1: criar um usuário na Conta C e delegar permissão para assumir examplerole

1. Usando o URL de login de usuário do IAM para a Conta C, primeiro faça login no AWS Management Console como o usuário **`AccountCadmin`**.

2. No console do IAM, crie um usuário chamado Dave.

Para obter instruções passo a passo, consulte Criação de usuários do IAM (AWS Management Console) no Guia do usuário do IAM.

3. Anote as credenciais de Dave. Dave precisará dessas credenciais para assumir a função `examplerole`.
4. Crie uma política em linha para o usuário do IAM Dave para delegar a ele a permissão `sts:AssumeRole` no perfil `examplerole` da conta A.

   a. No painel de navegação à esquerda, escolha Uses (Usuários).

   b. Selecione o nome de usuário Dave.

   c. Na página detalhes do usuário, selecione a guia Permissions (Permissões) e, em seguida, expanda a seção Inline Policies (Políticas em linha).

   d. Escolha clique aqui (ou Create User Policy [Criar política de usuário]).

   e. Escolha Custom Policy e depois Select.

   f. Insira um nome para a política no campo Policy Name (Nome da política).

   g. Cole a seguinte política no campo Policy Document (Documento da política).

   Você deve atualizar a política fornecendo o *AccountA-ID*.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["sts:AssumeRole"],
      "Resource": "arn:aws:iam::AccountA-ID:role/examplerole"
    }
  ]
}
```

   h. Selecione Aplicar política.

5. Salve as credenciais de Dave no arquivo de configuração da AWS CLI adicionando outro perfil, `AccountCDave`.

```
[profile AccountCDave]
aws_access_key_id = UserDaveAccessKeyID
aws_secret_access_key = UserDaveSecretAccessKey
region = us-west-2
```

Etapa 3.2: assumir o perfil (examplerole) e acessar objetos

Agora Dave pode acessar objetos no bucket de propriedade da Conta A, desta forma:

- Dave primeiro assume a `examplerole` usando suas próprias credenciais. Isso retornará credenciais temporárias.
- Usando as credenciais temporárias, Dave então acessará os objetos no bucket da Conta A.

1. No prompt de comando, execute o comando `assume-role` da AWS CLI usando o perfil `AccountCDave`.

   É necessário atualizar o valor do ARN no comando fornecendo o *`AccountA-ID`* em que `examplerole` foi definido.

   ```
   aws sts assume-role --role-arn arn:aws:iam::AccountA-ID:role/examplerole --profile
    AccountCDave --role-session-name test
   ```

   Em resposta, o AWS Security Token Service (AWS STS) retorna credenciais de segurança temporárias (ID da chave de acesso, chave de acesso secreta e um token de sessão).
2. Salve as credenciais de segurança temporárias no arquivo de configuração da AWS CLI no perfil `TempCred`.

   ```
   [profile TempCred]
   aws_access_key_id = temp-access-key-ID
   aws_secret_access_key = temp-secret-access-key
   aws_session_token = session-token
   region = us-west-2
   ```
3. No prompt de comando, execute o comando da AWS CLI a seguir para acessar objetos usando as credenciais temporárias. Por exemplo, o comando especifica a API do objeto head para recuperar os metadados do objeto para o objeto `HappyFace.jpg`.

   ```
   aws s3api get-object --bucket amzn-s3-demo-bucket1 --
   key HappyFace.jpg SaveFileAs.jpg --profile TempCred
   ```

   Como a política de acesso anexada a `examplerole` permite as ações, o Amazon S3 processa a solicitação. Você pode tentar qualquer outra ação em qualquer outro objeto no bucket.

Se tentar qualquer outra ação, como `get-object-acl`, você terá a permissão negada porque o perfil não tem permissão para realizar essa ação.

```
aws s3api get-object-acl --bucket amzn-s3-demo-bucket1 --key HappyFace.jpg --
profile TempCred
```

Usamos o usuário Dave para assumir a função e acessar o objeto usando credenciais temporárias. Também poderia ser um aplicativo na Conta C que acessa objetos em *amzn-s3-demo-bucket1*. O aplicativo pode obter credenciais de segurança temporárias, e a Conta C pode delegar permissão de aplicativo para assumir `examplerole`.

Etapa 4: limpar

1. Depois de terminar os testes, você pode fazer o seguinte para concluir a limpeza:
   - Faça login no AWS Management Console usando as credenciais da Conta A e faça o seguinte:
     - No console do Amazon S3, remova a política de bucket anexada a *amzn-s3-demo-bucket1*. Nas Propriedades do bucket, exclua a política na seção Permissions (Permissões).
     - Se o bucket foi criado para este exercício, no console do Amazon S3, exclua os objetos e, em seguida, exclua o bucket.
     - No console do IAM, remova o `examplerole` que você criou na Conta A. Consulte instruções detalhadas em Exclusão de um usuário do IAM no Guia do usuário do IAM.
     - No console do IAM, remova o usuário AccountAadmin.
2. Faça login no console do IAM usando as credenciais da Conta B. Exclua o usuário AccountBadmin.
3. Faça login no console do IAM usando as credenciais da Conta C. Exclua AccountCadmin e o usuário Dave.

Recursos relacionados

Consulte mais informações relacionadas a essa demonstração nos seguintes recursos do Guia do usuário do IAM:

- Criação de uma função para delegar permissões a um usuário do IAM
- Tutorial: delegar acesso entre Contas da AWS usando perfis do IAM
- Gerenciamento de políticas do IAM

Usar funções vinculadas a serviços para o Amazon S3 Storage Lens

Para usar o Amazon S3 Storage Lens para coletar e agregar métricas em todas as suas contas no AWS Organizations, primeiro você deve garantir que o S3 Storage Lens tenha acesso confiável habilitado pela conta de gerenciamento em sua organização. A Lente de Armazenamento do S3 cria um perfil vinculado ao serviço (SLR) para permitir que ele obtenha a lista de Contas da AWS pertencentes à sua organização. Essa lista de contas é usada pelo S3 Storage Lens para coletar métricas de recursos do S3 em todas as contas membro quando o painel ou as configurações do S3 Storage Lens são criadas ou atualizadas.

O Amazon S3 Storage Lens usa funções vinculadas a serviços do AWS Identity and Access Management (IAM). Uma função vinculada a serviço é um tipo exclusivo de função do IAM vinculada diretamente ao S3 Storage Lens. Os perfis vinculados ao serviço são predefinidos pela Lente de Armazenamento do S3 e incluem todas as permissões que o serviço exige para chamar outros Serviços da AWS em seu nome.

Uma função vinculada a serviços facilita a configuração do S3 Storage Lens porque você não precisa adicionar as permissões necessárias manualmente. O S3 Storage Lens define as permissões da função vinculada a serviços e, salvo outra definição, somente o S3 Storage Lens pode assumir suas funções. As permissões definidas incluem a política de confiança e a política de permissões, e essa política de permissões não pode ser anexada a nenhuma outra entidade do IAM.

Você pode excluir essa função vinculada a serviços somente após a exclusão dos recursos relacionados. Isso protege seus recursos do S3 Storage Lens, porque você não consegue remover por engano a permissão para acessar os recursos.

Para obter informações sobre outros serviços compatíveis com funções vinculadas a serviços, consulte Serviços da AWS que funcionam com o IAM e procure serviços que tenham Yes (Sim) na coluna Service-Linked Role (Função vinculada a serviço). Escolha um Sim com um link para visualizar a documentação sobre funções vinculadas ao serviço para esse serviço.

Permissões de funções vinculadas a serviços para o Amazon S3 Storage Lens

O S3 Storage Lens usa a função vinculada a serviços chamada AWSServiceRoleForS3StorageLens. Ela permite o acesso a serviços e recursos da AWS usados ou gerenciados pelo S3 Storage Lens. Isso permite que o S3 Storage Lens acesse recursos da AWS Organizations em seu nome.

A função vinculada a serviços do S3 Storage Lens confia no seguinte serviço no armazenamento da sua organização:

- `storage-lens.s3.amazonaws.com`

A política de permissões da função permite que o S3 Storage Lens execute as seguintes ações:

- `organizations:DescribeOrganization`

  `organizations:ListAccounts`

  `organizations:ListAWSServiceAccessForOrganization`

  `organizations:ListDelegatedAdministrators`

Você deve configurar permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua uma função vinculada ao serviço. Para obter mais informações, consulte Service-linked role permissions (Permissões de função vinculada a serviços) no Guia do usuário do IAM.

Criar uma função vinculada a serviços para o S3 Storage Lens

Você não precisa criar manualmente uma função vinculada a serviço. Quando você conclui uma das seguintes tarefas enquanto faz login no gerenciamento do AWS Organizations ou nas contas de administrador delegado, o S3 Storage Lens cria a função vinculada a serviços para você:

- Crie uma configuração de painel do S3 Storage Lens para sua organização no console do Amazon S3.
- Executar o comando PUT de uma configuração do S3 Storage Lens para sua organização usando a API REST, a AWS CLI e os SDKs.

> **Note**
>
> A Lente de Armazenamento do S3 permite no máximo cinco administradores delegados por organização.

Se você excluir essa função vinculada a serviços, as ações anteriores a recriarão conforme necessário.

Exemplo de política para função vinculada a serviços do S3 Storage Lens

Example Política de permissões para a função vinculada a serviços do S3 Storage Lens

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AwsOrgsAccess",
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:ListAccounts",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListDelegatedAdministrators"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

Editar uma função vinculada a serviços para o Amazon S3 Storage Lens

A Lente de Armazenamento do S3 não permite que você edite o perfil vinculado ao serviço AWSServiceRoleForS3StorageLens. Depois que você criar um perfil vinculado ao serviço, não poderá alterar o nome do perfil, pois várias entidades podem fazer referência ao perfil. No entanto, você poderá editar a descrição do perfil usando o IAM. Para obter mais informações, consulte Editar uma função vinculada a serviço no Guia do usuário do IAM.

Excluir uma função vinculada a serviços para o Amazon S3 Storage Lens

Se você não precisa mais usar a função vinculada a serviços, recomendamos que a exclua. Dessa forma, você não tem uma entidade não utilizada que não seja monitorada ativamente ou mantida. No entanto, você deve limpar os recursos de sua função vinculada ao serviço antes de excluí-la manualmente.

> **Note**
>
> Se o serviço Amazon S3 Storage Lens estiver usando a função quando você tentar excluir os recursos, a exclusão poderá falhar. Se isso acontecer, espere alguns minutos e tente a operação novamente.

Para excluir o AWSServiceRoleForS3StorageLens, você deve excluir todas as configurações da Lente de Armazenamento do S3 no nível da organização presentes em todas as Regiões da AWS usando o gerenciamento do AWS Organizations ou as contas de administrador delegadas.

Os recursos são configurações do S3 Storage Lens no nível da organização. Use a Lente de Armazenamento do S3 para limpar os recursos e, depois, use o console do IAM, a CLI, a API REST ou o SDK da AWS para excluir o perfil.

Na API REST, na AWS CLI e nos SDKs, as configurações da Lente de Armazenamento do S3 podem ser descobertas usando `ListStorageLensConfigurations` em todas as regiões onde sua organização tiver criado configurações da Lente de Armazenamento do S3. Use a ação `DeleteStorageLensConfiguration` a fim de excluir essas configurações para que você possa excluir a função.

> **Note**
>
> Para excluir a função vinculada a serviços, você deve excluir todas as configurações do S3 Storage Lens no nível da organização em todas as regiões em que elas existem.

Como excluir recursos da Lente de Armazenamento do Amazon S3 usados pelo SLR AWSServiceRoleForS3StorageLens

1. Para obter uma lista de configurações de nível de organização, é necessário usar `ListStorageLensConfigurations` em todas as regiões em que você tem configurações da

Lente de Armazenamento do S3. Essa lista também pode ser encontrada no console do Amazon S3.

2. Exclua essas configurações dos endpoints regionais apropriados invocando a chamada de API `DeleteStorageLensConfiguration` ou usando o console do Amazon S3.

Como excluir manualmente o perfil vinculado ao serviço usando o IAM

Depois de excluir as configurações, exclua o SLR AWSServiceRoleForS3StorageLens no console do IAM, invocando a API `DeleteServiceLinkedRole` do IAM ou usando a AWS CLI ou o SDK da AWS. Para obter mais informações, consulte Excluir uma função vinculada ao serviço no Guia do usuário do IAM.

Regiões com suporte para funções vinculadas a serviços do S3 Storage Lens

O S3 Storage Lens é compatível com as funções vinculadas a serviços em todas as Regiões da AWS em que o serviço está disponível. Para obter mais informações, consulte Regiões e endpoints do Amazon S3.

Solução de problemas de identidade e acesso do Amazon S3

Use as informações a seguir para ajudar a diagnosticar e corrigir problemas comuns que você possa encontrar ao trabalhar com o Amazon S3 e o IAM.

Tópicos

- Recebi um erro de acesso negado
- Não tenho autorização para executar uma ação no Amazon S3
- Não estou autorizado a executar iam:PassRole
- Quero permitir que as pessoas fora da minha Conta da AWS acessem meus recursos do Amazon S3
- Solucionar erros de acesso negado (403 Forbidden) no Amazon S3

Recebi um erro de acesso negado

Verifique se não há uma instrução `Deny` explícita contra o solicitante ao qual você está tentando conceder permissões, seja na política de bucket ou na política baseada em identidade.

Consulte informações detalhadas sobre a solução de problemas de erros de acesso negado em Solucionar erros de acesso negado (403 Forbidden) no Amazon S3.

Não tenho autorização para executar uma ação no Amazon S3

Se você receber uma mensagem de erro informando que não tem autorização para executar uma ação, suas políticas deverão ser atualizadas para permitir que você realize a ação.

O erro do exemplo a seguir ocorre quando o usuário do IAM `mateojackson` tenta usar o console para visualizar detalhes sobre um atributo *`my-example-widget`* fictício, mas não tem as permissões `s3:`*`GetWidget`* fictícias.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 s3:GetWidget on resource: my-example-widget
```

Nesse caso, a política do usuário `mateojackson` deve ser atualizada para permitir o acesso ao recurso *`my-example-widget`* usando a ação `s3:`*`GetWidget`*.

Se você precisar de ajuda, entre em contato com seu administrador AWS. Seu administrador é a pessoa que forneceu suas credenciais de login.

Não estou autorizado a executar iam:PassRole

Se receber uma mensagem de erro informando que você não tem autorização para executar a ação `iam:PassRole`, atualize suas políticas para permitir a transmissão de um perfil ao Amazon S3.

Alguns Serviços da AWS permitem que você passe um perfil existente para o serviço, em vez de criar um perfil de serviço ou perfil vinculado ao serviço. Para fazer isso, é preciso ter permissões para passar o perfil para o serviço.

O exemplo de erro a seguir ocorre quando uma usuária do IAM chamada `marymajor` tenta usar o console para executar uma ação no Amazon S3. No entanto, a ação exige que o serviço tenha permissões concedidas por um perfil de serviço. Mary não tem permissões para passar o perfil para o serviço.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Nesse caso, as políticas de Mary devem ser atualizadas para permitir que ela realize a ação `iam:PassRole`.

Se você precisar de ajuda, entre em contato com seu administrador AWS. Seu administrador é a pessoa que forneceu suas credenciais de login.

Quero permitir que as pessoas fora da minha Conta da AWS acessem meus recursos do Amazon S3

Você pode criar um perfil que os usuários de outras contas ou pessoas fora da organização podem usar para acessar seus recursos. É possível especificar quem é confiável para assumir o perfil. Para serviços que oferecem compatibilidade com políticas baseadas em recursos ou listas de controle de acesso (ACLs), você pode usar essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte:

- Para saber se o Amazon S3 é compatível com esses recursos, consulte Como o Amazon S3 funciona com o IAM.
- Para saber como conceder acesso a seus recursos em todas as Contas da AWS pertencentes a você, consulte Fornecimento de acesso a um usuário do IAM em outra Conta da AWS pertencente a você no Guia de usuário do IAM.
- Para saber como conceder acesso a seus recursos para Contas da AWS de terceiros, consulte Fornecimento de acesso a Contas da AWS pertencentes a terceiros no Guia do usuário do IAM.
- Para saber como conceder acesso por meio da federação de identidades, consulte Conceder acesso a usuários autenticados externamente (federação de identidades) no Guia do usuário do IAM.
- Para saber a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Solucionar erros de acesso negado (403 Forbidden) no Amazon S3

Erros de acesso negado (HTTP `403 Forbidden`) são exibidos quando a AWS nega explícita ou implicitamente uma solicitação de autorização.

- Uma negação explícita ocorre quando uma política contém uma instrução `Deny` para a ação específica da AWS.
- Uma negação implícita ocorre quando não há nenhuma instrução `Deny` aplicável e também nenhuma instrução `Allow` aplicável.

Como uma política do AWS Identity and Access Management (IAM) nega implicitamente uma entidade principal do IAM por padrão, a política deve permitir explicitamente que a entidade principal realize uma ação. Caso contrário, a política nega acesso implicitamente. Para ter mais informações,

consulte A diferença entre negações explícitas e implícitas no Guia do usuário do IAM. Para ter informações sobre a lógica de avaliação de políticas que determina se uma solicitação de acesso é permitida ou negada, consulte Lógica da avaliação de política no Guia do usuário do IAM.

Para ter mais informações sobre as permissões referentes a operações de API do S3 de acordo com os tipos de recurso do S3, consulte Permissões obrigatórias para operações de API do Amazon S3.

Os tópicos a seguir abordam as causas mais comuns dos erros de acesso negado no Amazon S3.

> **Note**
>
> Em relação a erros de acesso negado (HTTP `403 Forbidden`), o Amazon S3 não cobra do proprietário do bucket quando a solicitação é iniciada fora da conta da AWS individual dele ou da organização da AWS à qual ele pertence.

Tópicos

- Exemplos de mensagens de acesso negado e como solucioná-las
- Políticas de bucket e políticas do IAM
- Configurações de ACL do Amazon S3
- Configurações do bloqueio de acesso público do S3
- Configurações de criptografia do Amazon S3
- Configurações do bloqueio de objetos do S3
- Políticas de VPC endpoint
- Políticas do AWS Organizations
- Acesso à distribuição do CloudFront
- Configurações do ponto de acesso
- Recursos adicionais

> **Note**
>
> Se você estiver tentando solucionar um problema de permissões, comece com a seção the section called “Exemplos de mensagens de acesso negado e como solucioná-las” e acesse a seção ???. Lembre-se também de seguir as orientações em the section called “Dicas para verificar permissões”.

Exemplos de mensagens de acesso negado e como solucioná-las

> **Important**
>
> Em 16 de junho de 2025, o Amazon S3 começou a apresentar mensagens de erro aprimoradas de acesso negado para solicitações feitas a recursos em contas dentro da mesma organização no AWS Organizations. Essas mensagens estarão disponíveis em todas as Regiões da AWS, incluindo as AWS GovCloud (US) Regions e as regiões da China.

O Amazon S3 agora inclui contexto adicional em erros de acesso negado (HTTP `403 Forbidden`) para solicitações feitas a recursos dentro da mesma conta da Conta da AWS ou da mesma organização no AWS Organizations. Esse novo contexto inclui o tipo de política que negou o acesso, o motivo da negação e informações sobre o usuário ou o perfil do IAM que solicitou acesso ao recurso.

Esse contexto adicional ajuda você a solucionar problemas de acesso, identificar a causa-raiz dos erros de acesso negado e corrigir controles de acesso incorretos por meio da atualização das políticas pertinentes. Esse contexto adicional também está disponível nos logs do AWS CloudTrail. As mensagens de erro aprimoradas de acesso negado para solicitações da mesma conta ou da mesma organização agora estão disponíveis em todas as Regiões da AWS, incluindo as AWS GovCloud (US) Regions e as da China.

A maioria das mensagens de erro de acesso negado está no formato `User` *`user-arn`* `is not authorized to perform` *`action`* `on "`*`resource-arn`*`" because` *`context`*. Neste exemplo, *`user-arn`* é o nome do recurso da Amazon (ARN) do usuário que não recebe acesso, *`action`* é a ação de serviço que a política nega e *`resource-arn`* é o ARN do recurso no qual a política atua. O campo *`context`* representa contexto adicional sobre o tipo de política que explica por que o acesso é negado.

Quando uma política nega explicitamente o acesso porque ela contém uma declaração `Deny`, a mensagem de erro de acesso negado inclui a frase `with an explicit deny in a` *`type`* `policy`. Quando a política nega acesso implicitamente, a mensagem de erro de acesso negado inclui a frase `because no` *`type`* `policy allows the` *`action`* `action`.

Important

- As mensagens aprimoradas de acesso negado são exibidas somente para solicitações da mesma conta ou para solicitações dentro da mesma organização no AWS Organizations. As solicitações entre contas fora da mesma organização exibem uma mensagem `Access Denied` genérica.

  Para ter informações sobre a lógica de avaliação de políticas que determina se uma solicitação de acesso entre contas é permitida ou negada, consulte Lógica de avaliação de política entre contas no Guia do usuário do IAM. Para ter uma explicação detalhada que mostra como conceder acesso entre contas, consulte the section called “Conceder permissões entre contas”.
- Para solicitações dentro da mesma organização no AWS Organizations:
  - Não serão exibidas mensagens aprimoradas de acesso negado se uma negação ocorrer devido a uma política de endpoint de nuvem privada virtual (VPC).
  - Mensagens aprimoradas de acesso negado são apresentadas sempre que o proprietário do bucket e a conta do chamador pertencem à mesma organização no AWS Organizations. Embora os buckets configurado com as definições Proprietário do bucket preferido ou Autor do objeto da funcionalidade Propriedade de Objetos do S3 possam conter objetos pertencentes a contas diferentes, a propriedade do objeto não afeta as mensagens aprimoradas de acesso negado. As mensagens aprimoradas de acesso negado são exibidas para todas as solicitações de objeto desde que o proprietário do bucket e o chamador estejam na mesma organização, independentemente de quem seja o proprietário do objeto específico. Para ter informações sobre as configurações e definições de propriedade de objeto, consulte the section called “Controlar a propriedade do objeto”.
- Mensagens de erro aprimoradas de acesso negado não são exibidas para solicitações feitas aos buckets de diretório. Solicitações de bucket de diretório exibem uma mensagem `Access Denied` genérica.
- Se várias políticas do mesmo tipo negarem uma solicitação de autorização, a mensagem de erro de acesso negado não especificará o número de políticas.
- Se vários tipos de política negarem uma solicitação de autorização, a mensagem de erro incluirá somente um dos tipos de política.

- Se uma solicitação de acesso for negada por vários motivos, a mensagem de erro incluirá apenas um dos motivos da negação.

Os exemplos a seguir mostram o formato de diferentes tipos de mensagem de acesso negado e como solucionar problemas de cada tipo de mensagem.

Acesso negado devido a uma política de controle de recurso: negação explícita

1. Verifique se há uma instrução `Deny` para a ação em suas políticas de controle de recursos (RCPs). No exemplo a seguir, a ação é `s3:GetObject`.
2. Atualize sua RCP removendo a instrução `Deny`. Para obter mais informações, consulte Atualização de uma política de controle de recursos (RCP) no Guia do usuário do AWS Organizations.

```
An error occurred (AccessDenied) when calling the GetObject operation:
User: arn:aws:iam::777788889999:user/MaryMajor is not authorized to perform:
s3:GetObject on resource: "arn:aws:s3:::amzn-s3-demo-bucket1/object-name"
with an explicit deny in a resource control policy
```

Acesso negado devido a uma política de controle de serviço: negação implícita

1. Verifique se falta uma instrução `Allow` para a ação em suas políticas de controle de serviços (SCPs). No exemplo a seguir, a ação é `s3:GetObject`.
2. Atualize a SCP adicionando a instrução `Allow`. Para obter mais informações, consulte Atualizar uma SCP no Guia do usuário do AWS Organizations.

```
User: arn:aws:iam::777788889999:user/MaryMajor is not authorized to perform:
s3:GetObject because no service control policy allows the s3:GetObject action
```

Acesso negado devido a uma política de controle de serviço: negação explícita

1. Verifique se há uma instrução `Deny` para a ação em suas políticas de controle de serviços (SCPs). No exemplo a seguir, a ação é `s3:GetObject`.
2. Atualize a SCP alterando a declaração `Deny` para permitir que o usuário tenha o acesso necessário. Para ver um exemplo de como fazer isso, consulte Prevent IAM users and roles from making specified changes, with an exception for a specified admin role no Guia do usuário do

AWS Organizations. Para ter mais informações sobre a atualização da SCP, consulte Updating an SCP no Guia do usuário do AWS Organizations.

```
User: arn:aws:iam::777788889999:user/MaryMajor is not authorized to perform:
s3:GetObject with an explicit deny in a service control policy
```

Acesso negado devido a uma política de endpoint da VPC: negação implícita

1. Confira se falta uma declaração `Allow` para a ação nas políticas de endpoint da nuvem privada virtual (VPC). No exemplo a seguir, a ação é `s3:GetObject`.
2. Atualize sua política de endpoint da VPC adicionando a instrução `Allow`. Para obter mais informações, consulte Atualizar uma política de endpoint da VPC no Guia do AWS PrivateLink.

```
User: arn:aws:iam::123456789012:user/MaryMajor is not authorized to perform:
s3:GetObject because no VPC endpoint policy allows the s3:GetObject action
```

Acesso negado devido a uma política de endpoint da VPC: negação explícita

1. Confira se há uma declaração `Deny` explícita para a ação nas políticas de endpoint da nuvem privada virtual (VPC). No exemplo a seguir, a ação é `s3:GetObject`.
2. Atualize a política de endpoint da VPC alterando a declaração `Deny` para permitir que o usuário tenha o acesso necessário. Por exemplo, é possível atualizar a declaração `Deny` para usar a chave de condição `aws:PrincipalAccount` com o operador de condição `StringNotEquals` e permitir o acesso da entidade principal específica, conforme mostrado em the section called "Exemplo 7: excluir entidades principais de declarações Deny". Para ter mais informações sobre como atualizar a política de endpoint da VPC, consulte Update a VPC endpoint policy no Guia do AWS PrivateLink.

```
User: arn:aws:iam::123456789012:user/MaryMajor is not authorized to perform:
s3:GetObject on resource: "arn:aws:s3:::amzn-s3-demo-bucket1/object-name" with
an explicit deny in a VPC endpoint policy
```

Acesso negado devido a um limite de permissões: negação implícita

1. Verifique se falta uma instrução `Allow` para a ação em seu limite de permissões. No exemplo a seguir, a ação é `s3:GetObject`.

2. Atualize seu limite de permissões adicionando a instrução `Allow` à política do IAM. Para ter mais informações, consulte Limites de permissões para entidades do IAM e Edição de políticas do IAM no Guia do usuário do IAM.

```
User: arn:aws:iam::123456789012:user/MaryMajor is not authorized to perform:
s3:GetObject on resource: "arn:aws:s3:::amzn-s3-demo-bucket1/object-name"
because no permissions boundary allows the s3:GetObject action
```

Acesso negado devido a um limite de permissões: negação explícita

1. Verifique se há uma instrução `Deny` explícita para a ação em seu limite de permissões. No exemplo a seguir, a ação é `s3:GetObject`.
2. Atualize o limite de permissões alterando a declaração `Deny` em sua política do IAM para permitir que o usuário tenha o acesso necessário. Por exemplo, é possível atualizar a declaração `Deny` para usar a chave de condição `aws:PrincipalAccount` com o operador de condição `StringNotEquals` e permitir o acesso da entidade principal específica, conforme mostrado em aws:PrincipalAccount no Guia do usuário do IAM. Para ter mais informações, consulte Limites de permissões para entidades do IAM e Edição de políticas do IAM no Guia do usuário do IAM.

```
User: arn:aws:iam::777788889999:user/MaryMajor is not authorized to perform:
s3:GetObject with an explicit deny in a permissions boundary
```

Acesso negado devido às políticas de sessão: negação implícita

1. Verifique se falta uma instrução `Allow` para a ação em suas políticas de sessão. No exemplo a seguir, a ação é `s3:GetObject`.
2. Atualize a política de sessão adicionando a instrução `Allow`. Para ter mais informações, consulte Políticas de sessão e Edição de políticas do IAM no Guia do usuário do IAM.

```
User: arn:aws:iam::123456789012:user/MaryMajor is not authorized to perform:
s3:GetObject because no session policy allows the s3:GetObject action
```

Acesso negado devido às políticas de sessão: negação explícita

1. Verifique se há uma instrução `Deny` explícita para a ação em suas políticas de sessão. No exemplo a seguir, a ação é `s3:GetObject`.

2. Atualize a política de sessão alterando a declaração `Deny` para permitir que o usuário tenha o acesso necessário. Por exemplo, é possível atualizar a declaração `Deny` para usar a chave de condição `aws:PrincipalAccount` com o operador de condição `StringNotEquals` e permitir o acesso da entidade principal específica, conforme mostrado em the section called “Exemplo 7: excluir entidades principais de declarações Deny”. Para ter mais informações sobre como atualizar a política de sessão, consulte Políticas de sessão e Editar políticas do IAM no Guia do usuário do IAM.

```
User: arn:aws:iam::123456789012:user/MaryMajor is not authorized to perform:
s3:GetObject on resource: "arn:aws:s3:::amzn-s3-demo-bucket1/object-name" with
an explicit deny in a session policy
```

Acesso negado devido às políticas baseadas em recursos: negação implícita

> **Note**
>
> Políticas baseadas em recursos são, por exemplo, políticas de bucket e de ponto de acesso.

1. Verifique se falta uma instrução `Allow` para a ação em sua política baseada em recursos. Confira também se a configuração `IgnorePublicAcls` do Bloqueio de Acesso Público do S3 é aplicada em nível de bucket, de ponto de acesso ou de conta. No exemplo a seguir, a ação é `s3:GetObject`.
2. Atualize a política adicionando a instrução `Allow`. Para ter mais informações, consulte Políticas baseadas em recursos e Edição de políticas do IAM no Guia do usuário do IAM.

   Talvez você também precise ajustar a configuração `IgnorePublicAcls` do Bloqueio de Acesso Público para o bucket, o ponto de acesso ou a conta. Para obter mais informações, consulte the section called “Acesso negado devido a configurações do Bloqueio de Acesso Público” e the section called “Definir configurações de bucket e ponto de acesso”.

```
User: arn:aws:iam::123456789012:user/MaryMajor is not authorized to perform:
s3:GetObject because no resource-based policy allows the s3:GetObject action
```

Acesso negado devido às políticas baseadas em recursos: negação explícita

> **Note**
>
> Políticas baseadas em recursos são, por exemplo, políticas de bucket e de ponto de acesso.

1. Verifique se há uma instrução `Deny` explícita para a ação em sua política baseada em recursos. Confira também se a configuração `RestrictPublicBuckets` do Bloqueio de Acesso Público do S3 é aplicada em nível de bucket, de ponto de acesso ou de conta. No exemplo a seguir, a ação é `s3:GetObject`.
2. Atualize a política alterando a declaração `Deny` para permitir que o usuário tenha o acesso necessário. Por exemplo, é possível atualizar a declaração `Deny` para usar a chave de condição `aws:PrincipalAccount` com o operador de condição `StringNotEquals` e permitir o acesso da entidade principal específica, conforme mostrado em the section called “Exemplo 7: excluir entidades principais de declarações Deny”. Para ter mais informações sobre como atualizar a política baseada em recursos, consulte Políticas baseadas no recurso e Editar políticas do IAM no Guia do usuário do IAM.

   Talvez você também precise ajustar a configuração `RestrictPublicBuckets` do Bloqueio de Acesso Público para o bucket, o ponto de acesso ou a conta. Para obter mais informações, consulte the section called “Acesso negado devido a configurações do Bloqueio de Acesso Público” e the section called “Definir configurações de bucket e ponto de acesso”.

```
User: arn:aws:iam::123456789012:user/MaryMajor is not authorized to perform:
s3:GetObject on resource: "arn:aws:s3:::amzn-s3-demo-bucket1/object-name" with
an explicit deny in a resource-based policy
```

Acesso negado devido a políticas baseadas em identidade: negação implícita

1. Verifique se falta uma instrução `Allow` para a ação em políticas baseadas em identidade anexadas à identidade. Para o exemplo a seguir, a ação é `s3:GetObject` anexada ao usuário `MaryMajor`.
2. Atualize a política adicionando a instrução `Allow`. Para ter mais informações, consulte Políticas baseadas em identidade e Edição de políticas do IAM no Guia do usuário do IAM.

```
User: arn:aws:iam::123456789012:user/MaryMajor is not authorized to perform:
s3:GetObject because no identity-based policy allows the s3:GetObject action
```

Acesso negado devido às políticas baseadas em identidade: negação explícita

1. Verifique se há uma instrução `Deny` explícita para a ação em políticas baseadas em identidade anexadas à identidade. Para o exemplo a seguir, a ação é `s3:GetObject` anexada ao usuário `MaryMajor`.
2. Atualize a política alterando a declaração `Deny` para permitir que o usuário tenha o acesso necessário. Por exemplo, é possível atualizar a declaração `Deny` para usar a chave de condição `aws:PrincipalAccount` com o operador de condição `StringNotEquals` e permitir o acesso da entidade principal específica, conforme mostrado em aws:PrincipalAccount no Guia do usuário do IAM. Para ter mais informações, consulte Políticas baseadas em identidade e Edição de políticas do IAM no Guia do usuário do IAM.

```
User: arn:aws:iam::123456789012:user/MaryMajor is not authorized to perform:
s3:GetObject on resource: "arn:aws:s3:::amzn-s3-demo-bucket1/object-name" with
an explicit deny in an identity-based policy
```

Acesso negado devido a configurações do Bloqueio de Acesso Público

O recurso Bloqueio de acesso público do Amazon S3 fornece configurações para pontos de acesso, buckets e contas para ajudar você a gerenciar o acesso público aos recursos do Amazon S3. Para obter mais informações sobre como o Amazon S3 define “público”, consulte O significado de "público".

Por padrão, novos buckets, pontos de acesso e objetos não permitem acesso público. No entanto, os usuários podem modificar políticas de bucket, políticas de ponto de acesso, políticas do usuário do IAM, permissões de objeto ou listas de controle de acesso (ACLs) para permitir acesso público. As configurações do Bloqueio de Acesso Público do S3 substituem essas políticas, permissões e ACLs. Desde abril de 2023, todas as configurações do Bloqueio de Acesso Público estão habilitadas por padrão para novos buckets.

Ao receber uma solicitação para acessar um bucket ou um objeto, o Amazon S3 determina se o bucket ou a conta do proprietário do bucket tem uma configuração do Bloqueio de acesso público aplicada. Se a solicitação foi feita por meio de um ponto de acesso, o Amazon S3 também verificará se há configurações do Bloqueio de acesso público para o ponto de acesso. Caso haja uma

configuração do Bloqueio de acesso público que proíba o acesso solicitado, o Amazon S3 rejeitará a solicitação.

O Bloqueio de acesso público do Amazon S3 fornece quatro configurações. Essas configurações são independentes e podem ser usadas em qualquer combinação. Cada configuração pode ser aplicada a um ponto de acesso, a um bucket ou a uma conta inteira da AWS. Se as configurações do Bloqueio de acesso público para o ponto de acesso, o bucket ou a conta forem diferentes, o Amazon S3 aplicará a combinação mais restritiva das configurações de ponto de acesso, bucket e conta.

Quando o Amazon S3 avalia se uma operação é proibida por uma configuração do Bloqueio de acesso público, ela rejeita qualquer solicitação que viole uma configuração de ponto de acesso, bucket ou conta.

As quatro configurações fornecidas pelo Bloqueio de acesso público do Amazon S3 são as seguintes:

- `BlockPublicAcls`: essa configuração se aplica às solicitações `PutBucketAcl`, `PutObjectAcl`, `PutObject`, `CreateBucket`, `CopyObject` e `POST Object`. A configuração `BlockPublicAcls` causa o seguinte comportamento:
  - As chamadas `PutBucketAcl` e `PutObjectAcl` falharão se a lista de controle de acesso (ACL) especificada for pública.
  - As chamadas `PutObject` falharão se a solicitação incluir uma ACL pública.
  - Se essa configuração for aplicada a uma conta, as chamadas `CreateBucket` falharão com uma resposta HTTP `400` (`Bad Request`) se a solicitação incluir uma ACL pública.

  Por exemplo, quando o acesso é negado para uma solicitação `CopyObject` devido à configuração `BlockPublicAcls`, você recebe a seguinte mensagem:

  ```
  An error occurred (AccessDenied) when calling the CopyObject operation:
  User: arn:aws:sts::123456789012:user/MaryMajor is not authorized to
  perform: s3:CopyObject on resource: "arn:aws:s3:::amzn-s3-demo-bucket1/object-name"
  because public access control lists (ACLs) are blocked by the BlockPublicAcls block
  public access setting.
  ```

- `IgnorePublicAcls`: a configuração `IgnorePublicAcls` faz o Amazon S3 ignorar todas as ACLs públicas em um bucket e todos os objetos contidos. Se a permissão da solicitação for concedida somente por uma ACL pública, a configuração `IgnorePublicAcls` rejeitará a solicitação.

Qualquer negação resultante da configuração `IgnorePublicAcls` é implícita. Por exemplo, se `IgnorePublicAcls` negar uma solicitação `GetObject` devido a uma ACL pública, você receberá a seguinte mensagem:

```
User: arn:aws:iam::123456789012:user/MaryMajor is not authorized to perform:
s3:GetObject because no resource-based policy allows the s3:GetObject action
```

- `BlockPublicPolicy`: essa configuração se aplica às solicitações `PutBucketPolicy` e `PutAccessPointPolicy`.

  A configuração `BlockPublicPolicy` para um bucket faz com que o Amazon S3 rejeite chamadas para `PutBucketPolicy` caso a política de bucket especificada permita acesso público. A configuração também faz com que o Amazon S3 rejeite chamadas a `PutAccessPointPolicy` para todos os pontos de acesso na mesma conta do bucket caso a política especificada permita acesso público.

  A configuração `BlockPublicPolicy` para um ponto de acesso faz com que o Amazon S3 rejeite chamadas para `PutAccessPointPolicy` e `PutBucketPolicy` feitas por meio do ponto de acesso caso a política especificada (para o ponto de acesso ou o bucket subjacente) permita acesso público.

  Por exemplo, quando o acesso é negado em uma solicitação `PutBucketPolicy` devido à configuração `BlockPublicPolicy`, você recebe a seguinte mensagem:

  ```
  An error occurred (AccessDenied) when calling the PutBucketPolicy operation:
  User: arn:aws:sts::123456789012:user/MaryMajor is not authorized to
  perform: s3:PutBucketPolicy on resource: "arn:aws:s3:::amzn-s3-demo-bucket1/object-
  name"
  because public policies are blocked by the BlockPublicPolicy block public
  access setting.
  ```

- `RestrictPublicBuckets`: a configuração `RestrictPublicBuckets` restringe o acesso a um ponto de acesso ou a um bucket com uma política pública apenas a entidades principais do AWS service (Serviço da AWS) e a usuários autorizados dentro da conta do proprietário do bucket e da conta do proprietário do ponto de acesso. Essa configuração bloqueia todo acesso entre contas ao ponto de acesso ou ao bucket (exceto entidades principais do AWS service (Serviço da AWS)), mas continua permitindo que usuários na conta gerenciem o ponto de acesso ou o bucket. Essa configuração também rejeita todas as chamadas anônimas (ou não assinadas).

Qualquer negação resultante da configuração `RestrictPublicBuckets` é explícita. Por exemplo, se `RestrictPublicBuckets` negar uma solicitação `GetObject` devido a uma política de acesso público ou bucket público, você receberá a seguinte mensagem:

```
User: arn:aws:iam::123456789012:user/MaryMajor is not authorized to perform:
s3:GetObject on resource: "arn:aws:s3:::amzn-s3-demo-bucket1/object-name" with
an explicit deny in a resource-based policy
```

Para ter mais informações sobre essas configurações, consulte the section called “Configurações do bloqueio de acesso público”. Para revisar e atualizar essas configurações, consulte the section called “Configurar o bloqueio de acesso público”.

Políticas de bucket e políticas do IAM

Operações no nível do bucket

Se não houver uma política de bucket em vigor, o bucket permitirá implicitamente solicitações de qualquer identidade do AWS Identity and Access Management (IAM) na conta do proprietário do bucket. O bucket também nega implicitamente solicitações de qualquer outra identidade do IAM de qualquer outra conta e solicitações anônimas (não assinadas). No entanto, se não houver uma política do usuário do IAM em vigor, o solicitante (a menos que seja o usuário-raiz da Conta da AWS) será implicitamente impedido de fazer qualquer solicitação. Para obter mais informações sobre essa lógica de avaliação, consulte Determinar se uma solicitação é negada ou permitida em uma conta no Guia do usuário do IAM.

Operações no nível do objeto

Se o objeto pertencer à conta proprietária do bucket, a política de bucket e a política de usuário do IAM funcionarão da mesma forma para operações no nível do objeto e para operações no nível do bucket. Por exemplo, se não houver uma política de bucket em vigor, o bucket permitirá implicitamente solicitações de objeto de qualquer identidade do IAM na conta do proprietário do bucket. O bucket também nega implicitamente solicitações de objeto de qualquer outra identidade do IAM de qualquer outra conta e solicitações anônimas (não assinadas). No entanto, se não houver uma política de usuário do IAM em vigor, o solicitante (a menos que seja o usuário-raiz da Conta da AWS) será implicitamente impedido de fazer qualquer solicitação de objeto.

Se o objeto pertencer a uma conta externa, o acesso ao objeto só poderá ser concedido por meio de listas de controle de acesso (ACLs) do objeto. A política de bucket e a política de usuário do IAM ainda podem ser usadas para negar solicitações de objeto.

Portanto, para garantir que a política de bucket ou a política de usuário do IAM não esteja causando um erro de Acesso negado (403 Proibido), verifique se os seguintes requisitos são atendidos:

- Para acesso à mesma conta, não deve haver uma declaração `Deny` explícita contra o solicitante ao qual você está tentando conceder permissões, seja na política de bucket ou na política de usuário do IAM. Se você quiser conceder permissões usando somente a política de bucket e a política de usuário do IAM, deve haver pelo menos uma declaração `Allow` explícita em uma dessas políticas.
- Para acesso entre contas, não deve haver uma declaração `Deny` explícita ao solicitante ao qual você está tentando conceder permissões, seja na política de bucket ou na política do usuário do IAM. Para conceder permissões entre contas usando somente a política de bucket e a política do usuário do IAM, a política do bucket e a política do usuário do IAM do solicitante devem incluir uma declaração `Allow` explícita.

> **Note**
>
> As declarações `Allow` em uma política de bucket se aplicam somente a objetos que pertencem à mesma conta proprietária do bucket. No entanto, as declarações `Deny` em uma política de bucket se aplicam a todos os objetos, independentemente da propriedade dele.

Para revisar ou editar a política de bucket

> **Note**
>
> Para visualizar ou editar uma política de bucket, é necessário ter a permissão `s3:GetBucketPolicy`.

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets.

3. Na lista Buckets, escolha o nome do bucket para o qual você deseja visualizar ou editar uma política de bucket.
4. Escolha a aba Permissões.
5. Em Bucket policy (Política de bucket), escolha Edit (Editar). A página Edit bucket policy (Editar política de bucket) é exibida.

Para revisar ou editar a política de bucket usando a AWS Command Line Interface (AWS CLI), use o comando get-bucket-policy.

> **Note**
>
> Se seu acesso a um bucket for bloqueado devido a uma política de bucket incorreta, faça login no AWS Management Console usando as credenciais de usuário-raiz da Conta da AWS. Para recuperar o acesso ao bucket, exclua a política de bucket incorreta usando as credenciais de usuário-raiz da Conta da AWS.

Dicas para verificar permissões

Para verificar se o solicitante tem as permissões adequadas para realizar uma operação do Amazon S3, tente o seguinte:

- Identifique o solicitante. Se for uma solicitação não assinada, será uma solicitação anônima sem uma política de usuário do IAM. Se for uma solicitação que use um URL pré-assinado, a política do usuário será a mesma do perfil ou do usuário do IAM que assinou a solicitação.
- Verifique se você está usando o perfil ou usuário do IAM correto. É possível verificar o perfil ou usuário do IAM no canto superior direito doAWS Management Console ou usando o comando aws sts get-caller-identity.
- Verifique as políticas do IAM relacionadas ao perfil ou usuário do IAM. É possível usar um dos seguintes métodos:
  - Testar as políticas do IAM com o simulador de políticas do IAM
  - Analise os diferentes tipos de política do IAM.
- Se necessário, edite a política de usuário do IAM.
- Veja os seguintes exemplos de políticas que negam ou permitem explicitamente o acesso:
  - Política de usuário do IAM de permissão explícita: IAM: permite e nega acesso a vários serviços de forma programática e no console

- Política de bucket de permissão explícita: Conceder permissões a várias contas para fazer upload de objetos ou definir ACLs de objetos para acesso público
- Política de usuário do IAM de negação explícita: AWS: negar acesso àAWS com base na Região da AWS solicitada
- Política de bucket de negação explícita: Exigir SSE-KMS para todos os objetos gravados em um bucket

Configurações de ACL do Amazon S3

Ao verificar as configurações de ACL, primeiro revise a configuração de propriedade de objetos para verificar se as ACLs estão ativadas no bucket. Esteja ciente de que as permissões de ACL podem ser usadas somente para conceder permissões e não podem ser usadas para rejeitar solicitações. Também não é possível usar ACLs para conceder acesso a solicitantes que são rejeitados por negações explícitas nas políticas de bucket ou nas políticas do usuário do IAM.

A configuração de propriedade de objeto está definida como “Imposto pelo proprietário do bucket”

Se a configuração Imposto pelo proprietário do bucket estiver habilitada, é improvável que as configurações de ACL causem um erro de acesso negado (403 proibido), pois essa configuração desabilita todas as ACLs que se aplicam ao bucket e aos objetos. Imposto pelo proprietário do bucket é a configuração padrão (e recomendada) para os buckets do Amazon S3.

A configuração de propriedade de objeto está definida como “Proprietário do bucket preferido” ou “Autor do objeto”

As permissões de ACL ainda são válidas com a configuração Proprietário do objeto preferido ou a configuração Autor do objeto. Há dois tipos de ACLs: ACLs de bucket e ACLs de objeto. Para ver as diferenças entre esses dois tipos de ACLs, consulte Mapeamento das permissões da ACL e das permissões da política de acesso.

Dependendo da ação da solicitação rejeitada, verifique as permissões de ACL para o bucket ou objeto:

- Se o Amazon S3 rejeitou uma `LIST`, um objeto `PUT`, `GetBucketAcl` ou uma solicitação `PutBucketAcl`, revise as permissões de ACL para o bucket.

> **Note**
>
> Não é possível conceder permissões de objeto `GET` com as configurações de ACL do bucket.

- Se o Amazon S3 rejeitou uma solicitação `GET` em um objeto do S3 ou uma solicitação PutObjectAcl, revise as permissões de ACL para o objeto.

> **Important**
>
> Se a conta da que possui o objeto for diferente da conta da que possui o bucket, o acesso ao objeto não será controlado pela política de bucket.

Solução de problemas de um erro de acesso negado (403 proibido) de uma solicitação de objeto **`GET`** durante a propriedade de objetos entre contas

Examine as configurações de propriedade de objetos do bucket para determinar o proprietário do objeto. Se você tiver acesso às ACLs do objeto, também poderá verificar a conta do proprietário do objeto. (Para visualizar a conta do proprietário do objeto, revise a configuração da ACL do objeto no console do Amazon S3.) Como alternativa, você também pode fazer uma solicitação `GetObjectAcl` a fim de encontrar a ID canônica do proprietário do objeto para verificar a conta do proprietário do objeto. Por padrão, as ACLs concedem permissões explícitas para solicitações `GET` à conta do proprietário do objeto.

Depois de confirmar que o proprietário do objeto é diferente do proprietário do bucket, dependendo do caso de uso e nível de acesso, escolha um dos seguintes métodos para ajudar a resolver o erro Acesso negado (403 proibido):

- Desative as ACLs (recomendado): esse método se aplicará a todos os objetos e poderá ser executado pelo proprietário do bucket. Esse método concede automaticamente ao proprietário do bucket propriedade e controle total de todos os objetos do bucket. Antes de implementar esse método, verifique os pré-requisitos para desativar as ACLs. Para ter informações sobre como configurar o bucket no modo Imposto pelo proprietário do bucket (recomendado), consulte Configurar propriedade de objeto em um bucket existente.

> **Important**
>
> Para evitar um erro de acesso negado (403 proibido), migre as permissões da ACL para uma política de bucket antes de desativar as ACLs. Para obter mais informações, consulte Exemplos de políticas de bucket para migrar de permissões de ACL.

- Altere o proprietário do objeto para o proprietário do bucket: esse método pode ser aplicado a objetos individuais, mas somente o proprietário do objeto (ou um usuário com as permissões apropriadas) pode alterar a propriedade de um objeto. Custos adicionais de PUT podem ser aplicados. (Para obter mais informações, consulte Preço do Amazon S3.) Esse método concede ao proprietário do bucket a propriedade total do objeto, permitindo que ele controle o acesso ao objeto por meio de uma política de bucket.

  Para alterar a propriedade do objeto, siga um destes procedimentos:

  - Você (o proprietário do bucket) pode copiar o objeto de volta para o bucket.
  - É possível alterar a configuração de propriedade de objeto do bucket para a configuração Proprietário do bucket preferido. Se o versionamento estiver desativado, os objetos no bucket serão substituídos. Se o versionamento estiver ativado, versões duplicadas do mesmo objeto aparecerão no bucket, e o proprietário do bucket poderá definir uma regra de ciclo de vida para expirar. Para obter instruções sobre como alterar a configuração de propriedade de objetos, consulte Configurar propriedade de objeto em um bucket existente.

    > **Note**
    >
    > Quando você atualiza a configuração de propriedade de objeto para Proprietário do bucket preferido, a configuração só é aplicada a novos objetos que são enviados ao bucket.

  - É possível fazer com que o proprietário do objeto carregue o objeto novamente com a ACL `bucket-owner-full-control` do objeto predefinido.

    > **Note**
    >
    > Para uploads entre contas, você também pode exigir a ACL `bucket-owner-full-control` do objeto predefinido na política de bucket. Para obter um exemplo de política

de bucket, consulte Conceder permissões entre contas para fazer upload de objetos garantindo que o proprietário do bucket tenha controle total.

- Mantenha o gravador do objeto como proprietário do objeto: esse método não altera o proprietário do objeto, mas permite que você conceda acesso aos objetos individualmente. Para conceder acesso a um objeto, você deve ter a permissão `PutObjectAcl` para o objeto. Depois, para corrigir o erro Acesso negado (403 proibido), adicione o solicitante como beneficiário para acessar o objeto nas ACLs do objeto. Para obter mais informações, consulte Configurar ACLs.

Configurações do bloqueio de acesso público do S3

Se a solicitação com falha envolver acesso público ou políticas públicas, confira as configurações do Bloqueio de Acesso Público do S3 na conta, no bucket ou no ponto de acesso. Para ter mais informações sobre como solucionar erros de acesso negado relacionados a configurações do Bloqueio de Acesso Público do S3, consulte the section called “Acesso negado devido a configurações do Bloqueio de Acesso Público”.

Configurações de criptografia do Amazon S3

O Amazon S3 é compatível com a criptografia do lado do servidor no bucket. A criptografia do lado do servidor é a criptografia de dados em seu destino pela aplicação ou serviço que os recebe. O Amazon S3 criptografa os dados no nível do objeto no momento em que os grava em discos nos datacenters da AWS e descriptografa-os quando você os acessa.

Por padrão, o Amazon S3 agora aplica a criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3) como nível básico de criptografia para cada bucket no Amazon S3. O Amazon S3 também permite que você especifique o método de criptografia do lado do servidor ao fazer upload de objetos.

Para revisar as configurações de criptografia e o status da criptografia do lado do servidor do bucket

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets.
3. Na lista Buckets, escolha o bucket para o qual você deseja verificar as configurações de criptografia.
4. Escolha a guia Properties (Propriedades).
5. Role para baixo até a seção Criptografia padrão e veja as configurações de Tipo de criptografia.

Para verificar as configurações de criptografia usando a AWS CLI, use o comando get-bucket-encryption.

Para verificar o status de criptografia de um objeto

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets.
3. Na lista Buckets, escolha o nome do bucket que contém o objeto.
4. Na lista Objetos, escolha o nome do objeto ao qual você deseja adicionar ou no qual deseja alterar a criptografia.

   A página de detalhes do objeto é exibida.
5. Role para baixo até a seção Configurações de criptografia do lado do servidor para ver as configurações de criptografia do lado do servidor do objeto.

Para verificar o status de criptografia do objeto usando a AWS CLI, use o comando head-object.

Requisitos de permissões e criptografia

O Amazon S3 agora é compatível com três tipos de criptografia do lado do servidor.

- Criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3)
- Criptografia no lado do servidor com chaves do AWS Key Management Service (AWS KMS) (SSE-KMS)
- Criptografia do lado do servidor com chaves fornecidas pelo cliente (SSE-C)

Com base nas configurações de criptografia, verifique se os seguintes requisitos de permissões são atendidos:

- SSE-S3: nenhuma permissão extra é necessária.
- SSE-KMS (com uma chave gerenciada pelo cliente): para fazer upload de objetos, é necessária a permissão `kms:GenerateDataKey` no AWS KMS key. Para baixar objetos e fazer uploads de objetos em várias partes, é necessária a permissão `kms:Decrypt` na chave do KMS.
- SSE-KMS (com um Chave gerenciada pela AWS): o solicitante deve ser da mesma conta que possui a chave do KMS `aws/s3`. O solicitante também deve ter as permissões corretas do Amazon S3 para acessar o objeto.

- SSE-C (com uma chave fornecida pelo cliente): nenhuma permissão adicional é necessária. É possível configurar a política de bucket para exigir e restringir a criptografia do lado do servidor com chaves de criptografia fornecidas pelo cliente para objetos no bucket.

Se o objeto estiver criptografado com uma chave gerenciada pelo cliente, certifique-se de que a política de chaves do KMS permita que você realize as ações `kms:GenerateDataKey` ou `kms:Decrypt`. Para obter instruções sobre como verificar a política de chaves do KMS, consulte Visualizar uma política de chaves no Guia do desenvolvedor do AWS Key Management Service.

Configurações do bloqueio de objetos do S3

Se o bucket tiver o bloqueio de objetos do S3 ativado e o objeto estiver protegido por um período de retenção ou uma retenção legal, o Amazon S3 retornará um erro de acesso negado (403 proibido) quando você tentar excluir o objeto.

Para verificar se o bucket tem o bloqueio de objetos ativado

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets.
3. Na lista Buckets, escolha o nome do bucket que deseja revisar.
4. Escolha a guia Properties (Propriedades).
5. Role para baixo até a seção Bloqueio de objetos. Verifique se a configuração de Bloqueio de objetos está Ativada ou Desativada.

Para determinar se o objeto está protegido por um período de retenção ou uma retenção legal, veja as informações de bloqueio do objeto.

Se o objeto estiver protegido por um período de retenção ou uma retenção legal, verifique o seguinte:

- Se a versão do objeto estiver protegida pelo modo de retenção de conformidade, não há como excluí-lo permanentemente. Uma solicitação `DELETE` permanente de qualquer solicitante, incluindo o usuário-raiz da Conta da AWS, vai gerar um erro de Acesso negado (403 Proibido). Além disso, lembre-se de que quando você envia uma solicitação `DELETE` para um objeto protegido pelo modo de retenção de conformidade, o Amazon S3 cria um marcador de exclusão para o objeto.

- Se a versão do objeto estiver protegida com o modo de retenção de governança e você tiver a permissão `s3:BypassGovernanceRetention`, poderá ignorar a proteção e excluir permanentemente a versão. Para obter mais informações, consulte Ignorar modo de governança.
- Se a versão do objeto estiver protegida por uma retenção legal, uma solicitação `DELETE` permanente poderá resultar em um erro de Acesso negado (403 proibido). Para excluir permanentemente a versão do objeto, é necessário remover a retenção legal da versão do objeto. Para remover uma retenção legal, você deve ter a permissão `s3:PutObjectLegalHold`. Para obter mais informações como remover uma retenção legal, consulte Configurar a funcionalidade Bloqueio de Objetos do S3.

Políticas de VPC endpoint

Se você estiver acessando o Amazon S3 por meio de um endpoint da nuvem privada virtual (VPC), verifique se a política de endpoint da VPC não está impedindo o acesso aos recursos do Amazon S3. Por padrão, a política de endpoint da VPC permite todas as solicitações ao Amazon S3. Também é possível configurar a política de endpoint da VPC para restringir determinadas solicitações. Para ter informações sobre como conferir a política de endpoint da VPC, consulte os seguintes recursos:

- the section called “Acesso negado devido a uma política de endpoint da VPC: negação implícita”
- the section called “Acesso negado devido a uma política de endpoint da VPC: negação explícita”
- Control access to VPC endpoints by using endpoint policies no Guia do AWS PrivateLink

Políticas do AWS Organizations

Se a sua Conta da AWS pertence a uma organização, as políticas do AWS Organizations podem impedir que você acesse os recursos do Amazon S3. Por padrão, as políticas do AWS Organizations não bloqueiam nenhuma solicitação ao Amazon S3. No entanto, verifique se as suas políticas do AWS Organizations não foram configuradas para bloquear o acesso aos buckets do S3. Para ter instruções sobre como conferir as políticas do AWS Organizations, consulte os seguintes recursos:

- the section called “Acesso negado devido a uma política de controle de serviço: negação implícita”
- the section called “Acesso negado devido a uma política de controle de serviço: negação explícita”
- the section called “Acesso negado devido a uma política de controle de recurso: negação explícita”
- Listing all policies no Guia do usuário do AWS Organizations

Além disso, se você configurou incorretamente a política de bucket para uma conta-membro a fim de negar a todos os usuários o acesso ao bucket do S3, é possível desbloquear o bucket iniciando uma sessão privilegiada para a conta-membro no IAM. Depois de iniciar uma sessão privilegiada, você pode excluir a política de bucket configurada incorretamente para recuperar o acesso ao bucket. Consulte mais informações em Perform a privileged task on an AWS Organizations member account no Guia do usuário do AWS Identity and Access Management.

Acesso à distribuição do CloudFront

Se você receber um erro Access Denied (403 Forbidden) ao tentar acessar seu site estático do S3 por meio do CloudFront, verifique estes problemas comuns:

- Você tem o formato correto de nome de domínio de origem?
  - Você deve usar o formato de endpoint do site do S3 (bucket-name.s3-website-region.amazonaws.com) em vez do endpoint da API REST.
  - Verifique se a hospedagem do site estático está habilitada em seu bucket.
- Sua política de bucket permite acesso ao CloudFront?
  - Garanta que sua política de bucket inclua permissões para a identidade de acesso de origem (OAI) ou controle de acesso de origem (OAC) da sua distribuição do CloudFront.
  - Verifique se a política inclui as permissões s3:GetObject necessárias.

Para etapas e configurações adicionais de solução de problemas, incluindo configurações de página de erro e configurações de protocolo, consulte Estou usando um endpoint do site do S3 como origem de minha distribuição do CloudFront. Por que estou recebendo erros 403 Access Denied (Acesso negado)? no Centro de Conhecimento do AWS re:Post.

> **Note**
>
> Esse erro é diferente dos erros 403 que você pode receber ao acessar o S3 diretamente. Para problemas específicos do CloudFront, verifique as configurações de distribuição do CloudFront e as configurações do S3.

Configurações do ponto de acesso

Se você receber um erro de acesso negado (403 proibido) ao fazer solicitações por meio de Pontos de Acesso Amazon S3, talvez seja necessário verificar o seguinte:

- As configurações dos pontos de acesso
- A política de usuário do IAM usada para os pontos de acesso
- A política de bucket usada para gerenciar ou configurar os pontos de acesso entre contas

Políticas e configurações de pontos de acesso

- Ao criar um ponto de acesso, é possível designar Internet ou VPC como a origem da rede. Se a origem da rede for definida somente como VPC, o Amazon S3 rejeitará todas as solicitações feitas ao ponto de acesso que não sejam originadas da VPC especificada. Para verificar a origem da rede do ponto de acesso, consulte Criar pontos de acesso restritos a uma nuvem privada virtual.
- Com os pontos de acesso, você também pode definir configurações personalizadas do bloqueio de acesso público, que funcionam de forma semelhante às configurações desse recurso no nível do bucket ou da conta. Para verificar as configurações personalizadas do bloqueio de acesso público, consulte Gerenciar o acesso público a pontos de acesso para buckets de uso geral.
- Para fazer solicitações bem-sucedidas ao Amazon S3 usando pontos de acesso, o solicitante deve ter as permissões necessárias do IAM. Para obter mais informações, consulte Configurar políticas do IAM para uso de pontos de acesso.
- Se a solicitação envolver pontos de acesso entre contas, o proprietário do bucket deve ter atualizado a política do bucket para autorizar solicitações do ponto de acesso. Para obter mais informações, consulte Conceder permissões para pontos de acesso entre contas.

Se o erro Acesso negado (403 proibido) persistir depois de verificar todos os itens neste tópico, recupere seu ID de solicitação do Amazon S3 e entre em contato com o Suporte para obter mais orientações.

Recursos adicionais

Para obter orientação adicional sobre os erros Access Denied (403 Forbidden), você pode conferir os seguintes recursos:

- Como solucionar erros 403 Acesso Negado do Amazon S3? no Centro de Conhecimento do AWS re:Post.
- Por que estou recebendo um erro “403 Forbidden” (Proibido) quando tento acessar um bucket ou objeto do Amazon S3? no Centro de Conhecimento do AWS re:Post.
- Como soluciono os erros 403 Acesso negado do meu bucket do Amazon S3 em que todos os recursos são da mesma Conta da AWS? no Centro de Conhecimento do AWS re:Post.

- Como solucionar problemas de erros 403 Acesso negado em um bucket do Amazon S3 com acesso de leitura pública? no Centro de Conhecimento do AWS re:Post.
- Como soluciono os erros “SignatureDoesNotMatch” ou “403 Forbidden” nas solicitações de URL pré-assinadas do Amazon S3? no Centro de Conhecimento do AWS re:Post.
- Por que recebo um erro de acesso negado para ListObjectsV2 quando executo o comando de sincronização no meu bucket do Amazon S3? no Centro de Conhecimento do AWS re:Post.
- Estou usando um endpoint do site do S3 como origem de minha distribuição do CloudFront. Por que estou recebendo erros 403 Access Denied (Acesso negado)? no Centro de Conhecimento do AWS re:Post.

Políticas gerenciadas da AWS para o Amazon S3

Uma política gerenciada pela AWS é uma política independente criada e administrada pela AWS. As políticas gerenciadas pela AWS são criadas para fornecer permissões a vários casos de uso comuns a fim de que você possa começar a atribuir permissões a usuários, grupos e perfis.

Lembre-se de que as políticas gerenciadas pela AWS podem não conceder permissões de privilégio mínimo para casos de uso específicos, por estarem disponíveis para uso por todos os clientes da AWS. Recomendamos que você reduza ainda mais as permissões definindo as políticas gerenciadas pelo cliente que são específicas para seus casos de uso.

Você não pode alterar as permissões definidas em políticas gerenciadas pela AWS. Se a AWS atualiza as permissões definidas em um política gerenciada por AWS, a atualização afeta todas as identidades de entidades principais (usuários, grupos e perfis) às quais a política estiver vinculada. É provável que a AWS atualize uma política gerenciada por AWS quando um novo AWS service (Serviço da AWS) for lançado, ou novas operações de API forem disponibilizadas para os serviços existentes.

Para obter mais informações, consulte Políticas gerenciadas pela AWS no Guia do usuário do IAM.

Política gerenciada da AWS: AmazonS3FullAccess

É possível anexar a política `AmazonS3FullAccess` às identidades do IAM. Essa política concede permissões que possibilitam acesso total ao Amazon S3.

Para visualizar as permissões para esta política, consulte AmazonS3FullAccess no AWS Management Console.

Política gerenciada da AWS: AmazonS3ReadOnlyAccess

É possível anexar a política `AmazonS3ReadOnlyAccess` às identidades do IAM. Esta política concede permissões que oferecem acesso somente leitura ao Amazon S3.

Para visualizar as permissões para esta política, consulte AmazonS3ReadOnlyAccess no AWS Management Console.

Política gerenciada da AWS: AmazonS3ObjectLambdaExecutionRolePolicy

Fornece às funções do AWS Lambda as permissões necessárias para enviar dados para o S3 Object Lambda quando solicitações são feitas para um ponto de acesso do S3 Object Lambda. Também concede permissões do Lambda para gravar nos logs do Amazon CloudWatch.

Para visualizar as permissões para esta política, consulte AmazonS3ObjectLambdaExecutionRolePolicy no AWS Management Console.

Política gerenciada da AWS: S3UnlockBucketPolicy

Se você configurou incorretamente a política de bucket para uma conta-membro a fim de negar a todos os usuários o acesso ao bucket do S3, você pode usar essa política gerenciada pela AWS (`S3UnlockBucketPolicy`) para desbloquear o bucket. Consulte mais informações sobre como remover uma política de bucket configurada incorretamente que impede que todas as entidades principais acessem um bucket do Amazon S3 em Perform a privileged task on an AWS Organizations member account no Guia do usuário do AWS Identity and Access Management.

Atualizações do Amazon S3 para políticas gerenciadas pela AWS

Visualize detalhes sobre atualizações em políticas gerenciadas pela AWS para o Amazon S3 desde que esse serviço começou a rastrear essas alterações.

Alteração	Descrição	Data
O Amazon S3 adicionou `S3UnlockBucketPolicy`	O Amazon S3 adicionou uma nova política gerenciada pela AWS chamada `S3UnlockBucketPolicy` para desbloquear um bucket e remover uma política de bucket configurada incorreta	1.º de novembro de 2024

Alteração	Descrição	Data
	mente que nega a todas as entidades principais acesso a um bucket do Amazon S3.	
O Amazon S3 adicionou permissões de descrição a `AmazonS3ReadOnlyAccess` .	O Amazon S3 adicionou permissões `s3:Describe*` a `AmazonS3ReadOnlyAccess` .	11 de agosto de 2023
O Amazon S3 adicionou permissões do Lambda para objetos do S3 a `AmazonS3FullAccess` e `AmazonS3ReadOnlyAccess`	O Amazon S3 atualizou as políticas `AmazonS3FullAccess` e `AmazonS3ReadOnlyAccess` para incluir do Lambda para objetos do S3.	27 de setembro de 2021
O Amazon S3 adicionou `AmazonS3ObjectLambdaExecutionRolePolicy`	O Amazon S3 adicionou uma nova política gerenciada pela AWSchamada `AmazonS3ObjectLambdaExecutionRolePolicy` que fornece permissões de funções Lambda para interagir com o S3 Object Lambda e gravar em logs do CloudWatch.	18 de agosto de 2021
O Amazon S3 começou a monitorar as alterações	O Amazon S3 passou a controlar as alterações para as políticas gerenciadas pela AWS.	18 de agosto de 2021

Gerenciar o acesso a conjuntos de dados compartilhados com pontos de acesso

Os pontos de acesso do Amazon S3 simplificam o acesso a dados para qualquer produto da AWS ou aplicação de clientes que armazene dados no S3. Pontos de acesso são endpoints de rede nomeados que são anexados a uma fonte de dados, como um bucket ou um volume do Amazon FSx para OpenZFS. Para obter informações sobre como trabalhar com buckets, consulte Visão geral dos buckets de uso geral. Para ter informações sobre como trabalhar com o FSx para OpenZFS, consulte What is Amazon FSx for OpenZFS? no Guia do usuário do OpenZFS.

É possível usar pontos de acesso para executar operações de objeto do S3, como `GetObject` e `PutObject`. Cada ponto de acesso tem permissões distintas e controles de rede que o S3 aplica para qualquer solicitação feita por meio desse ponto de acesso. Cada endpoint impõe uma política de ponto de acesso personalizada que permite controlar o uso por recurso, usuário ou outras condições. Se o seu ponto de acesso estiver anexado a um bucket, a política de ponto de acesso funcionará em conjunto com a política de bucket subjacente. Você pode configurar qualquer ponto de acesso para aceitar solicitações somente de uma Virtual Private Cloud (VPC) para restringir o acesso a dados do Amazon S3 a uma rede privada. Você também pode configurar definições personalizadas do Bloqueio de acesso público para cada ponto de acesso.

> **Note**
>
> Você só pode usar pontos de acesso para executar operações em objetos. Não é possível usar pontos de acesso para executar outras operações do Amazon S3, como excluir buckets ou criar configurações do recurso Replicação do S3. Para obter uma lista completa das operações do S3 que oferecem suporte a pontos de acesso, consulte Compatibilidade dos pontos de acesso.

Os tópicos desta seção explicam como trabalhar com os Pontos de Acesso Amazon S3. Com relação a tópicos sobre como usar pontos de acesso com buckets de diretório, consulte Gerenciar o acesso a conjuntos de dados compartilhados em buckets de diretório por meio de pontos de acesso.

Tópicos

- Regras de nomenclatura, restrições e limitações dos pontos de acesso
- Fazer referência a pontos de acesso com ARNs, aliases de ponto de acesso ou URIs de estilo de hospedagem virtual

- Compatibilidade dos pontos de acesso
- Configurar políticas do IAM para uso de pontos de acesso
- Monitorar e registrar de pontos de acesso
- Criar um ponto de acesso
- Gerenciar o recurso Pontos de Acesso Amazon S3 para buckets de uso geral
- Usar o recurso Pontos de Acesso Amazon S3 para buckets de uso geral

Regras de nomenclatura, restrições e limitações dos pontos de acesso

Pontos de acesso são endpoints de rede nomeados anexados a um bucket ou a um volume em um sistema de arquivos do Amazon FSx que simplificam o gerenciamento de dados. Ao criar um ponto de acesso, escolha um nome e a Região da AWS onde deseja criá-lo. Os tópicos a seguir fornecem informações sobre regras de nomenclatura, restrições e limitações dos pontos de acesso.

Tópicos

- Regras de nomenclatura para pontos de acesso
- Restrições e limitações para os pontos de acesso
- Restrições e limitações para pontos de acesso anexados a um volume em um sistema de arquivos do Amazon FSx

Regras de nomenclatura para pontos de acesso

Ao criar um ponto de acesso, escolha um nome e a Região da AWS onde deseja criá-lo. Ao contrário dos buckets de uso geral, os nomes de pontos de acesso não precisam ser exclusivos entre Contas da AWS ou Regiões da AWS. A mesma Conta da AWS pode criar pontos de acesso com o mesmo nome em diferentes Regiões da AWS ou duas Contas da AWS diferentes podem usar o mesmo nome de ponto de acesso. No entanto, dentro de uma Região da AWS, a mesma Conta da AWS não pode ter dois pontos de acesso com nomes idênticos.

> **Note**
>
> Se você optar por divulgar o nome do ponto de acesso, evite incluir informações confidenciais no nome. Os nomes de ponto de acesso são publicados em um banco de dados acessível ao público conhecido como Sistema de Nome de Domínio (DNS).

Os nomes de pontos de acesso devem ser compatíveis com DNS e atender às seguintes condições:

- Devem ser exclusivos em cada Conta da AWS e Região da AWS.
- Devem começar com um número ou uma letra minúscula
- Devem conter entre 3 e 50 caracteres
- Não pode começar nem terminar com hífen (`-`)
- Não podem conter sublinhados (_), letras maiúsculas, espaços ou pontos (`.`).
- Não é possível terminar o nome com o sufixo `-s3alias` ou `-ext-s3alias`. Esses sufixos são reservados para nomes de alias de ponto de acesso. Para obter mais informações, consulte Alias de ponto de acesso.

Restrições e limitações para os pontos de acesso

Os pontos de acesso do Amazon S3 têm as seguintes restrições e limitações:

- Cada ponto de acesso está associado a exatamente um bucket ou volume do FSx para OpenZFS. Você deve especificar isso ao criar o ponto de acesso. Depois de criar um ponto de acesso, não é possível associá-lo a um bucket diferente ou a um volume diferente do FSx para OpenZFS. No entanto, é possível excluir um ponto de acesso e criar outro com o mesmo nome associado.
- Depois de criar um ponto de acesso, não é possível alterar sua configuração de nuvem privada virtual (VPC).
- As políticas de ponto de acesso estão limitadas a 20 KB.
- É possível criar até 10 mil pontos de acesso por Conta da AWS por Região da AWS. Se você precisar de mais de 10 mil pontos de acesso para uma única conta em uma única região, poderá solicitar um aumento de cota de serviço. Para obter mais informações sobre cotas de serviço e como solicitar um aumento, consulte AWS Service Quotas na Referência geral da AWS.
- Não é possível usar um ponto de acesso como destino para a replicação do S3. Para obter mais informações sobre a replicação, consulte Replicar objetos dentro de uma região e entre regiões.
- No console do Amazon S3, não é possível usar aliases de ponto de acesso do S3 como origem ou destino para operações Mover.
- Só é possível endereçar pontos de acesso usando URLs em estilo de host virtual. Para obter mais informações sobre o endereçamento no estilo de hospedagem virtual, consulte Acessar um bucket de uso geral do Amazon S3.
- As operações de API que controlam a funcionalidade do ponto de acesso (por exemplo, `PutAccessPoint` e `GetAccessPointPolicy`) não oferecem suporte a chamadas entre contas.

- É necessário usar o AWS Signature Version 4 ao fazer solicitações a um ponto de acesso usando as APIs REST. Para obter mais informações sobre como autenticar solicitações, consulte Autenticação de solicitações (AWS Signature Version 4) na Referência de APIs do Amazon Simple Storage Service.
- Os pontos de acesso permitem solicitações apenas por HTTPS. O Amazon S3 responderá automaticamente com um redirecionamento HTTP em todas as solicitações feitas por HTTP, para atualizar a solicitação para HTTPS.
- Os pontos de acesso não oferecem suporte ao acesso anônimo.
- Depois de criar um ponto de acesso, não será possível alterar as configurações de bloqueio de acesso público.
- Os pontos de acesso entre contas não concederão acesso aos dados no bucket até que você receba as permissões do proprietário do bucket. O proprietário do bucket sempre mantém o controle total sobre o acesso aos dados e deve atualizar a política do bucket para autorizar solicitações do ponto de acesso entre contas. Para ver um exemplo de política de bucket, consulte Configurar políticas do IAM para uso de pontos de acesso.
- Nas Regiões da AWS onde você tem mais de mil pontos de acesso, não é possível pesquisar um ponto de acesso pelo nome no console do Amazon S3.
- Quando você está visualizando um ponto de acesso entre contas no console Amazon S3, a coluna Acesso exibe Desconhecido. O console do Amazon S3 não pode determinar se o acesso público é concedido para o bucket e os objetos associados. A menos que você exija uma configuração pública para um caso de uso específico, recomendamos que você e o proprietário do bucket bloqueiem todo acesso público ao ponto de acesso e ao bucket. Para obter mais informações, consulte Bloquear o acesso público ao armazenamento do Amazon S3.

Restrições e limitações para pontos de acesso anexados a um volume em um sistema de arquivos do Amazon FSx

Abaixo são apresentadas as limitações específicas ao usar pontos de acesso anexados a um volume em um sistema de arquivos do Amazon FSx:

- Ao criar um ponto de acesso, você só pode anexá-lo a um volume em sistemas de arquivos do Amazon FSx que você possui. Não é possível anexá-lo a um volume de propriedade de outra Conta da AWS.

- Também não é possível usar a API `CreateAccessPoint` ao criar e anexar um ponto de acesso a um volume em um sistema de arquivos do Amazon FSx. Você deve usar a API `CreateAndAttachS3AccessPoint`.
- Não é possível desativar nenhuma configuração de bloqueio de acesso público ao criar ou usar um ponto de acesso anexado a um volume em um sistema de arquivos do Amazon FSx.
- Também não é possível listar objetos nem usar operações de cópia ou movimentação no console do S3 com pontos de acesso conectados a um volume em um sistema de arquivos do Amazon FSx.
- A operação `CopyObject` é permitida para pontos de acesso anexados a um volume do FSx para OpenZFS somente quando a origem e o destino são o mesmo ponto de acesso. Para ter mais informações sobre compatibilidade de ponto de acesso, consulte Compatibilidade dos pontos de acesso.
- Os uploads de várias partes estão limitados a 5 GB.
- O tipo de implantação do FSx para OpenZFS e a compatibilidade com a classe de armazenamento variam de acordo com a Região da AWS. Para ter mais informações, consulte Availability by Região da AWS no Guia do usuário do OpenZFS.

Fazer referência a pontos de acesso com ARNs, aliases de ponto de acesso ou URIs de estilo de hospedagem virtual

Depois de criar um ponto de acesso, você pode usar esses endpoints para realizar várias operações. Ao fazer referência a um ponto de acesso, você pode usar os nomes de recurso da Amazon (ARNs), o alias do ponto de acesso ou o URI de estilo de hospedagem virtual.

Tópicos

- ARNs de ponto de acesso
- Alias de ponto de acesso
- URI de estilo de hospedagem virtual

ARNs de ponto de acesso

Os pontos de acesso têm nomes de recurso da Amazon (ARNS). Os ARNs de ponto de acesso são semelhantes aos ARNs de bucket, mas são explicitamente digitados e codificam a Região da AWS do ponto de acesso e o ID da Conta da AWS do proprietário do ponto de acesso. Para ter mais

informações sobre ARNs, consulte Identifique recursos da AWS com nomes do recurso da Amazon (ARNs) no Guia do usuário do IAM.

Os ARNs de ponto de acesso usam o seguinte formato:

```
arn:aws:s3:region:account-id:accesspoint/resource
```

- `arn:aws:s3:us-west-2:123456789012:accesspoint/test` representa o ponto de acesso denominado *test*, pertencente à conta *123456789012* na região *us-west-2*.
- `arn:aws:s3:us-west-2:123456789012:accesspoint/*` representa todos os pontos de acesso na conta *123456789012* na região *us-west-2*.

Os ARNs para objetos acessados por meio de um ponto de acesso usam o seguinte formato:

```
arn:aws:s3:region:account-id:accesspoint/access-point-name/object/resource
```

- `arn:aws:s3:us-west-2:123456789012:accesspoint/test/object/unit-01` representa o objeto *unit-01*, acessado por meio do ponto de acesso denominado *test*, pertencente à conta *123456789012* na região *us-west-2*.
- `arn:aws:s3:us-west-2:123456789012:accesspoint/test/object/*` representa todos os objetos do ponto de acesso denominado *test*, na conta *123456789012* na região *us-west-2*.
- `arn:aws:s3:us-west-2:123456789012:accesspoint/test/object/unit-01/finance/*` representa todos os objetos com o prefixo *unit-01/finance/* para o ponto de acesso denominado *test*, na conta *123456789012* na região *us-west-2*.

Alias de ponto de acesso

Quando você cria um ponto de acesso, o Amazon S3 gera automaticamente um alias que poderá ser usado no lugar de um nome de bucket do Amazon S3 para acesso a dados. É possível usar esse alias de ponto de acesso em vez de um nome do recurso da Amazon (ARN) para operações de plano de dados do ponto de acesso. Para obter uma lista dessas operações, consulte Compatibilidade dos pontos de acesso.

Cria-se um nome de alias de ponto de acesso dentro do mesmo namespace de um bucket do Amazon S3. Esse nome de alias é gerado automaticamente, e não é possível alterá-lo. O nome de

alias de ponto de acesso atende a todos os requisitos de um nome de bucket válido do Amazon S3 e consiste nas seguintes partes:

ACCESS POINT NAME-METADATA-s3alias (para pontos de acesso anexados a um bucket do Amazon S3)

ACCESS POINT NAME-METADATA-ext-s3alias (para pontos de acesso anexados a uma fonte de dados de bucket que não seja do S3)

> **Note**
>
> Os sufixos -s3alias e -ext-s3alias são reservados para nomes de alias de ponto de acesso e não podem ser usados para nomes de bucket ou de ponto de acesso. Para obter mais informações sobre as regras para nomes de bucket do Amazon S3, consulte Regras de nomenclatura de buckets de uso geral.

Casos de uso e limitações de alias de ponto de acesso

Ao adotar pontos de acesso, é possível usar nomes de alias de ponto de acesso sem exigir alterações extensas de código.

Quando você cria um ponto de acesso, o Amazon S3 gera automaticamente um nome de alias de ponto de acesso, conforme o exemplo a seguir. Para executar esse comando, substitua os *user input placeholders* por suas próprias informações.

```
aws s3control create-access-point --bucket amzn-s3-demo-bucket1 --name my-access-point
 --account-id 111122223333
{
    "AccessPointArn": "arn:aws:s3:region:111122223333:accesspoint/my-access-point",
    "Alias": "my-access-point-aqfqprnstn7aefdfbarligizwgyfouse1a-s3alias"
}
```

É possível usar esse alias de ponto de acesso em vez de um nome de bucket do Amazon S3 para qualquer operação de plano de dados. Para obter uma lista dessas operações, consulte Compatibilidade dos pontos de acesso.

O exemplo a seguir da AWS CLI para o comando get-object usa o alias do ponto de acesso do bucket para retornar informações sobre o objeto especificado. Para executar esse comando, substitua os *user input placeholders* por suas próprias informações.

```
aws s3api get-object --bucket my-access-point-aqfqprnstn7aefdfbarligizwgyfouse1a-
s3alias --key dir/my_data.rtf my_data.rtf

{
    "AcceptRanges": "bytes",
    "LastModified": "2020-01-08T22:16:28+00:00",
    "ContentLength": 910,
    "ETag": "\"00751974dc146b76404bb7290f8f51bb\"",
    "VersionId": "null",
    "ContentType": "text/rtf",
    "Metadata": {}
}
```

Limitações dos alias de ponto de acesso

- Os aliases não podem ser configurados por clientes.
- Não é possível excluir, modificar ou desabilitar aliases de um ponto de acesso.
- É possível usar esse alias de ponto de acesso em vez de um nome de bucket do Amazon S3 em algumas operações de plano de dados. Para obter uma lista dessas operações, consulte Compatibilidade de pontos de acesso com operações do S3.
- Não é possível usar um nome de alias de ponto de acesso para operações do plano de controle do Amazon S3. Para obter uma lista de operações do plano de controle do Amazon S3, consulte Controle do Amazon S3 na Referência de APIs do Amazon Simple Storage Service.
- No console do Amazon S3, não é possível usar aliases de ponto de acesso do S3 como origem ou destino para operações Mover.
- Não é possível usar alias em políticas do AWS Identity and Access Management (IAM).
- Não é possível usar aliases como destino de log para logs de acesso do servidor S3.
- Não é possível usar aliases como destino de log para logs do AWS CloudTrail.
- O Amazon SageMaker AI GroundTruth não permite alias de ponto de acesso.

URI de estilo de hospedagem virtual

Os pontos de acesso são compatíveis apenas com o endereçamento em estilo de host virtual. Em um URI de estilo de hospedagem virtual, o nome do ponto de acesso, a Conta da AWS e a Região da AWS fazem parte do nome de domínio no URL. Para ter mais informações sobre a hospedagem virtual, consulte Hospedagem virtual de buckets de uso geral.

O URI de estilo de hospedagem virtual para pontos de acesso usa o seguinte formato:

```
https://access-point-name-account-id.s3-accesspoint.region.amazonaws.com
```

> **Note**
>
> - Se o nome do ponto de acesso incluir caracteres de traço (-), inclua os traços no URL e insira outro traço antes do ID da conta. Por exemplo, para usar um ponto de acesso chamado *finance-docs*, pertencente à conta *123456789012* na região *us-west-2*, o URL apropriado seria `https://finance-docs-123456789012.s3-accesspoint.us-west-2.amazonaws.com`.
> - Os Pontos de Acesso S3 não comportam acesso por HTTP. Eles comportam apenas o acesso seguro por HTTPS.

Compatibilidade dos pontos de acesso

Você pode usar pontos de acesso para acessar objetos usando o subconjunto de APIs do Amazon S3 a seguir. Todas as operações listadas abaixo podem aceitar ARNs de ponto de acesso ou aliases de ponto de acesso.

Para conferir exemplos de uso de pontos de acesso para executar operações em objetos, consulte Usar o recurso Pontos de Acesso Amazon S3 para buckets de uso geral.

Compatibilidade de pontos de acesso com operações do S3

A tabela a seguir é uma lista parcial das operações do Amazon S3 e mostra se elas são compatíveis com pontos de acesso. Todas as operações abaixo podem ser usadas em pontos de acesso que usam um bucket do S3 como fonte de dados, enquanto apenas algumas operações podem ser usadas em pontos de acesso que usam um volume do FSx para OpenZFS como fonte de dados.

Para ter mais informações, consulte Access point compatibility no Guia do usuário do FSx para OpenZFS.

Operação do S3	Ponto de acesso anexado a um bucket do S3	Ponto de acesso anexado a um volume do FSx para OpenZFS
AbortMultipartUpload	Compatível	Compatível
CompleteMultipartUpload	Compatível	Compatível
CopyObject (somente cópias da mesma região)	Compatível	Compatível, se a origem e o destino forem o mesmo ponto de acesso
CreateMultipartUpload	Compatível	Compatível
DeleteObject	Compatível	Compatível
DeleteObjects	Compatível	Compatível
DeleteObjectTagging	Compatível	Compatível
GetBucketAcl	Compatível	Não compatível
GetBucketCors	Compatível	Não compatível
GetBucketLocation	Compatível	Compatível
GetBucketNotificationConfiguration	Compatível	Não compatível
GetBucketPolicy	Compatível	Não compatível
GetObject	Compatível	Compatível
GetObjectAcl	Compatível	Não compatível
GetObjectAttributes	Compatível	Compatível
GetObjectLegalHold	Compatível	Não compatível

Operação do S3	Ponto de acesso anexado a um bucket do S3	Ponto de acesso anexado a um volume do FSx para OpenZFS
GetObjectRetention	Compatível	Não compatível
GetObjectTagging	Compatível	Compatível
HeadBucket	Compatível	Compatível
HeadObject	Compatível	Compatível
ListMultipartUploads	Compatível	Compatível
ListObjects	Compatível	Compatível
ListObjectsV2	Compatível	Compatível
ListObjectVersions	Compatível	Não compatível
ListParts	Compatível	Compatível
Presign	Compatível	Compatível
PutObject	Compatível	Compatível
PutObjectAcl	Compatível	Não compatível
PutObjectLegalHold	Compatível	Não compatível
PutObjectRetention	Compatível	Não compatível
PutObjectTagging	Compatível	Compatível
RestoreObject	Compatível	Não compatível
UploadPart	Compatível	Compatível
UploadPartCopy (somente cópias da mesma região)	Compatível	Compatível, se a origem e o destino forem o mesmo ponto de acesso

Configurar políticas do IAM para uso de pontos de acesso

Os pontos de acesso do Amazon S3 são compatíveis com as políticas de recursos do AWS Identity and Access Management (IAM) que permitem controlar o uso do ponto de acesso por recurso, usuário ou por outras condições. Para que uma aplicação ou um usuário possa acessar objetos por meio de um ponto de acesso, tanto o ponto de acesso quanto o bucket subjacente ou o sistema de arquivos do Amazon FSx devem permitir a solicitação.

> **Important**
>
> As restrições que você incluir em uma política de ponto de acesso se aplicam somente a solicitações feitas por meio desse ponto de acesso. Anexar um ponto de acesso a um bucket não altera o comportamento do recurso subjacente. Todas as operações existentes no bucket que não forem executadas por meio do seu ponto de acesso continuarão a funcionar como antes.

Ao usar políticas de recursos do IAM, solucione avisos de segurança, erros, avisos gerais e sugestões de AWS Identity and Access Management Access Analyzer antes de salvar a política. O IAM Access Analyzer executa verificações de política para validar sua política em relação à gramática das políticas e às práticas recomendadas do IAM. Essas verificações geram descobertas e fornecem recomendações que ajudam a criar políticas que sejam funcionais e estejam em conformidade com as práticas recomendadas de segurança.

Para saber mais sobre a validação de políticas usando o IAM Access Analyzer, consulte Validação de políticas do IAM Access Analyzer no Guia do usuário do IAM. Para visualizar uma lista de avisos, erros e sugestões retornados pelo IAM Access Analyzer, consulte Referência de verificação de políticas do IAM Access Analyzer.

Exemplos de política para pontos de acesso

Os exemplos a seguir demonstram como criar políticas do IAM para controlar solicitações feitas por meio de um ponto de acesso.

> **Note**
>
> As permissões concedidas em uma política de ponto de acesso entram em vigor somente se o bucket subjacente também permitir o mesmo acesso. É possível fazer isso de duas maneiras:

1. (Recomendado) Delegue o controle de acesso do bucket para o ponto de acesso conforme descrito em Delegar controle de acesso a pontos de acesso.
2. Adicione as mesmas permissões contidas na política de ponto de acesso à política do bucket subjacente. O Exemplo 1 de política de ponto de acesso demonstra como modificar a política de bucket subjacente para permitir o acesso necessário.

Example 1: Concessão da política de ponto de acesso

A política de ponto de acesso a seguir concede ao usuário do IAM *Jane* na conta *123456789012* permissões para objetos GET e PUT com o prefixo *Jane/* por meio do ponto de acesso *my-access-point* na conta *123456789012*.

```
{
    "Version":"2012-10-17",
    "Statement": [
    {
        "Effect": "Allow",
        "Principal": {
            "AWS": "arn:aws:iam::123456789012:user/Jane"
        },
        "Action": ["s3:GetObject", "s3:PutObject"],
        "Resource": "arn:aws:s3:us-west-2:123456789012:accesspoint/my-access-point/
object/Jane/*"
    }]
}
```

Note

Para que a política de ponto de acesso conceda efetivamente acesso ao usuário *Jane*, o bucket subjacente também deve permitir o mesmo acesso a *Jane*. É possível delegar o controle de acesso do bucket para o ponto de acesso conforme descrito em Delegar controle de acesso a pontos de acesso. Como alternativa, é possível adicionar a seguinte política ao bucket subjacente para conceder as permissões necessárias à Jane. Observe que a entrada `Resource` é diferente entre as políticas de ponto de acesso e bucket.

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
    {
        "Effect": "Allow",
        "Principal": {
            "AWS": "arn:aws:iam::123456789012:user/Jane"
        },
        "Action": ["s3:GetObject", "s3:PutObject"],
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/Jane/*"
    }]
}
```

Example 2: Política de ponto de acesso com condição de etiqueta

A política de ponto de acesso a seguir concede ao usuário do IAM *Mateo* na conta *123456789012* permissões para objetos GET por meio do ponto de acesso *my-access-point* na conta *123456789012* que possui a chave de etiqueta *data* definida com um valor *finance*.

```
{
    "Version":"2012-10-17",
    "Statement": [
    {
        "Effect":"Allow",
        "Principal" : {
            "AWS": "arn:aws:iam::123456789012:user/Mateo"
        },
        "Action":"s3:GetObject",
        "Resource" : "arn:aws:s3:us-west-2:123456789012:accesspoint/my-access-point/
object/*",
        "Condition" : {
            "StringEquals": {
                "s3:ExistingObjectTag/data": "finance"
            }
        }
    }]
}
```

Example 3: Política de ponto de acesso que permite a listagem de buckets

A política de ponto de acesso a seguir permite que o usuário do IAM `Arnav` na conta *123456789012* visualize os objetos contidos no bucket subjacente ao ponto de acesso *my-access-point* na conta *123456789012*.

```
{
    "Version":"2012-10-17",
    "Statement": [
    {
        "Effect": "Allow",
        "Principal": {
            "AWS": "arn:aws:iam::123456789012:user/Arnav"
        },
        "Action": "s3:ListBucket",
        "Resource": "arn:aws:s3:us-west-2:123456789012:accesspoint/my-access-point"
    }]
}
```

Example 4: Política de controle de serviço

A política de controle de serviço a seguir requer que todos os novos pontos de acesso sejam criados com uma origem de rede de nuvem privada virtual (VPC). Com essa política em vigor, os usuários da sua organização não podem criar novos pontos de acesso acessíveis da Internet.

```
{
    "Version": "2012-10-17",
    "Statement": [
    {
        "Effect": "Deny",
        "Action": "s3:CreateAccessPoint",
        "Resource": "*",
        "Condition": {
            "StringNotEquals": {
                "s3:AccessPointNetworkOrigin": "VPC"
            }
        }
    }]
}
```

Example 5: Política de bucket para limitar operações do S3 às origens de rede de VPC

A política de bucket a seguir limita o acesso a todas as operações de objeto do S3 para o bucket *amzn-s3-demo-bucket* para pontos de acesso com uma origem de rede de VPC.

> **Important**
>
> Antes de usar uma instrução como essa do exemplo, certifique-se de que você não precisa usar recursos que não são compatíveis com pontos de acesso, como replicação entre regiões.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Principal": "*",
            "Action": [
                "s3:AbortMultipartUpload",
                "s3:BypassGovernanceRetention",
                "s3:DeleteObject",
                "s3:DeleteObjectTagging",
                "s3:DeleteObjectVersion",
                "s3:DeleteObjectVersionTagging",
                "s3:GetObject",
                "s3:GetObjectAcl",
                "s3:GetObjectLegalHold",
                "s3:GetObjectRetention",
                "s3:GetObjectTagging",
                "s3:GetObjectVersion",
                "s3:GetObjectVersionAcl",
                "s3:GetObjectVersionTagging",
                "s3:ListMultipartUploadParts",
                "s3:PutObject",
                "s3:PutObjectAcl",
                "s3:PutObjectLegalHold",
                "s3:PutObjectRetention",
                "s3:PutObjectTagging",
                "s3:PutObjectVersionAcl",
                "s3:PutObjectVersionTagging",
                "s3:RestoreObject"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
            "Condition": {
                "StringNotEquals": {
                    "s3:AccessPointNetworkOrigin": "VPC"
```

```
                }
            }
        }
    ]
}
```

Chaves de condição

Os pontos de acesso do S3 têm chaves de condição que podem ser usadas em políticas do IAM para controlar o acesso aos recursos. As chaves de condição a seguir representam somente parte de uma política do IAM. Para obter exemplos de políticas completas, consulte Exemplos de política para pontos de acesso, the section called “Delegar controle de acesso a pontos de acesso” e the section called “Conceder permissões para pontos de acesso entre contas”.

`s3:DataAccessPointArn`

Este exemplo mostra uma string que você pode usar para estabelecer correspondência em um ARN de ponto de acesso. O exemplo a seguir estabelece a correspondência de todos os pontos de acesso da Conta da AWS *123456789012* na região *us-west-2*:

```
"Condition" : {
    "StringLike": {
        "s3:DataAccessPointArn": "arn:aws:s3:us-west-2:123456789012:accesspoint/*"
    }
}
```

`s3:DataAccessPointAccount`

Este exemplo mostra um operador de string que você pode utilizar para estabelecer correspondência com o ID da conta do proprietário de um ponto de acesso. O exemplo a seguir estabelece correspondência com todos os pontos de acesso pertencentes à Conta da AWS *123456789012*.

```
"Condition" : {
    "StringEquals": {
        "s3:DataAccessPointAccount": "123456789012"
    }
}
```

`s3:AccessPointNetworkOrigin`

Este exemplo mostra um operador de string que você pode utilizar para estabelecer correspondência com a origem da rede, `Internet` ou VPC. O exemplo a seguir corresponde apenas a pontos de acesso com uma origem de VPC.

```
"Condition" : {
    "StringEquals": {
        "s3:AccessPointNetworkOrigin": "VPC"
    }
}
```

Consulte mais informações sobre como usar chaves de condição com o Amazon S3 em Actions, resources, and condition keys for Amazon S3 na Referência de autorização do serviço.

Para ter mais informações sobre as permissões referentes a operações de API do S3 de acordo com os tipos de recurso do S3, consulte Permissões obrigatórias para operações de API do Amazon S3.

Delegar controle de acesso a pontos de acesso

Você pode delegar o controle de acesso de um bucket aos pontos de acesso do bucket. O exemplo de política de bucket a seguir permite acesso total a todos os pontos de acesso pertencentes à conta do proprietário do bucket. Assim, todo o acesso a esse bucket é controlado pelas políticas anexadas aos seus pontos de acesso. Recomendamos configurar seus buckets dessa maneira para todos os casos de uso que não exigem acesso direto ao bucket.

Example 6: Política de bucket que delega controle de acesso a pontos de acesso

```
{
    "Version": "2012-10-17",
    "Statement" : [
    {
        "Effect": "Allow",
        "Principal" : { "AWS": "*" },
        "Action" : "*",
        "Resource" : [ "Bucket ARN", "Bucket ARN/*"],
        "Condition": {
            "StringEquals" : { "s3:DataAccessPointAccount" : "Bucket owner's account
 ID" }
        }
```

```
    }]
}
```

Conceder permissões para pontos de acesso entre contas

Para criar um ponto de acesso para um bucket pertencente a outra conta, primeiro você deve criar o ponto de acesso especificando o nome do bucket e o ID do proprietário da conta. Depois, o proprietário do bucket deve atualizar a política do bucket para autorizar solicitações do ponto de acesso. Criar um ponto de acesso é semelhante à criação de um DNS CNAME, pois o ponto de acesso não fornece acesso ao conteúdo do bucket. Todo acesso ao bucket é controlado pela política de bucket. O exemplo de política de bucket a seguir permite solicitações `GET` e `LIST` no bucket de um ponto de acesso pertencente a uma Conta da AWS confiável.

Substitua *`Bucket ARN`* pelo ARN do bucket.

Example 7: Política de bucket que delega permissões a outra Conta da AWS

```
{
    "Version": "2012-10-17",
    "Statement" : [
    {
        "Effect": "Allow",
        "Principal" : { "AWS": "*" },
        "Action" : ["s3:GetObject","s3:ListBucket"],
        "Resource" : [ "Bucket ARN", "Bucket ARN/*"],
        "Condition": {
            "StringEquals" : { "s3:DataAccessPointAccount" : "Access point owner's
 account ID" }
        }
    }]
}
```

> **Note**
>
> Os pontos de acesso entre contas estão disponíveis somente para pontos de acesso anexados aos buckets do S3. Não é possível anexar um ponto de acesso a um volume em um sistema de arquivos do Amazon FSx de propriedade de outra Conta da AWS.

Monitorar e registrar de pontos de acesso

O Amazon S3 registra em log as solicitações feitas por meio de pontos de acesso e as solicitações feitas às operações de API que gerenciam pontos de acesso, como `CreateAccessPoint` e `GetAccessPointPolicy`. Para monitorar e gerenciar padrões de uso, você também pode configurar métricas de solicitação do Amazon CloudWatch Logs para pontos de acesso.

Tópicos

- Métricas de solicitação do CloudWatch
- Logs do AWS CloudTrail para solicitações feitas por meio de pontos de acesso

Métricas de solicitação do CloudWatch

Para entender e melhorar o desempenho das aplicações que estão usando pontos de acesso, você pode usar as métricas de solicitação do CloudWatch para Amazon S3. Métricas de solicitação ajudam a monitorar as solicitações do Amazon S3 para identificar e atuar rapidamente em problemas operacionais.

Por padrão, as métricas de solicitação estão disponíveis em nível de bucket. Porém, também é possível definir um filtro para as métricas de solicitação usando um prefixo compartilhado, etiquetas de objeto ou um ponto de acesso. Quando você cria um filtro de ponto de acesso, a configuração de métricas de solicitação inclui solicitações para o ponto de acesso especificado. Você pode receber métricas, definir alarmes e acessar painéis para ver operações em tempo real executadas por meio desse ponto de acesso.

Você deve aceitar métricas de solicitação configurando-as no console ou usando a API do Amazon S3. As métricas de solicitação estão disponíveis em intervalos de um minuto após alguma latência para processamento. As métricas de solicitação são cobradas usando a mesma taxa das métricas personalizadas do CloudWatch. Para obter mais informações, consulte Preço do Amazon CloudWatch.

Para criar uma configuração de métricas de solicitação que filtre por ponto de acesso, consulte Criação de uma configuração de métricas que filtre por prefixo, etiqueta de objeto ou ponto de acesso.

Logs do AWS CloudTrail para solicitações feitas por meio de pontos de acesso

Você pode registrar em log as solicitações feitas por meio de pontos de acesso e as solicitações feitas às APIs que gerenciam os pontos de acesso, como `CreateAccessPoint` e `GetAccessPointPolicy`, usando o registro de acesso ao servidor e o AWS CloudTrail.

As entradas de log do CloudTrail para solicitações feitas por meio de pontos de acesso incluirão o ARN do ponto de acesso na seção `resources` do log.

Por exemplo, suponha que você tenha a seguinte configuração:

- Um bucket nomeado *`amzn-s3-demo-bucket1`* na região *`us-west-2`* que contém o objeto nomeado *`my-image.jpg`*
- Um ponto de acesso chamado *`my-bucket-ap`* que está associado a *`amzn-s3-demo-bucket1`*
- O ID de Conta da AWS *`123456789012`*

O exemplo a seguir mostra a seção `resources` de uma entrada de log do CloudTrail da configuração anterior:

```
"resources": [
        {"type": "AWS::S3::Object",
            "ARN": "arn:aws:s3:::amzn-s3-demo-bucket1/my-image.jpg"
        },
        {"accountId": "123456789012",
            "type": "AWS::S3::Bucket",
            "ARN": "arn:aws:s3:::amzn-s3-demo-bucket1"
        },
        {"accountId": "123456789012",
            "type": "AWS::S3::AccessPoint",
            "ARN": "arn:aws:s3:us-west-2:123456789012:accesspoint/my-bucket-ap"
        }
    ]
```

Se você estiver usando um ponto de acesso anexado a um volume em um sistema de arquivos do Amazon FSx, a seção `resources` de uma entrada de log do CloudTrail terá uma aparência diferente. Por exemplo:

```
"resources": [
        {
```

```
            "accountId": "123456789012",
            "type": "AWS::FSx::Volume",
            "ARN": "arn:aws:fsx:us-east-1:123456789012:volume/fs-0123456789abcdef9/
fsvol-01234567891112223"
        }
    ]
```

Para obter mais informações sobre logs de acesso do servidor do S3, consulte Registrar em log as solicitações com registro em log de acesso ao servidor. Para obter mais informações sobre o AWS CloudTrail, consulte What is AWS CloudTrail? (O que é?) no AWS CloudTrail Guia do usuário.

Criar um ponto de acesso

Você pode criar pontos de acesso do S3 usando o AWS Management Console, a AWS Command Line Interface (AWS CLI), os AWS SDKs ou a API REST do Amazon S3. Pontos de acesso são endpoints de rede nomeados que são anexados a uma fonte de dados, como um bucket ou um volume do Amazon FSx para OpenZFS.

Por padrão, você pode criar até 10 mil pontos de acesso por região para cada uma das suas Contas da AWS. Se você precisar de mais de 10 mil pontos de acesso para uma única conta em uma única região, poderá solicitar um aumento de cota de serviço. Para obter mais informações sobre cotas de serviço e como solicitar um aumento, consulte AWS Service Quotas na Referência geral da AWS.

Tópicos

- Criar pontos de acesso com buckets do S3
- Criar pontos de acesso com o Amazon FSx
- Criar pontos de acesso restritos a uma nuvem privada virtual
- Gerenciar o acesso público a pontos de acesso para buckets de uso geral

Criar pontos de acesso com buckets do S3

Um ponto de acesso está associado a exatamente um bucket de uso geral do Amazon S3. Para usar um bucket em sua Conta da AWS, primeiro crie um bucket. Para obter mais informações sobre a criação de buckets, consulte Criar, configurar e trabalhar com buckets de uso geral do Amazon S3.

Você também pode criar um ponto de acesso entre contas associado a um bucket em outra Conta da AWS, desde que você saiba o nome do bucket e o ID da conta do proprietário do bucket. No entanto, a criação de pontos de acesso entre contas não concederá acesso aos dados no bucket até

que você receba as permissões do proprietário do bucket. O proprietário do bucket deve conceder à conta do proprietário do ponto de acesso (sua conta) acesso ao bucket por meio da política do bucket. Para obter mais informações, consulte Conceder permissões para pontos de acesso entre contas.

Usar o console do S3

Para criar um ponto de acesso

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Na barra de navegação na parte superior da página, escolha o nome da Região da AWS exibida no momento. Em seguida, escolha a região na qual você deseja criar um ponto de acesso. O ponto de acesso deve ser criado na mesma região em que o bucket associado.
3. No painel de navegação, escolha Access Points (Pontos de acesso).
4. Na página Access Points (Pontos de acesso), escolha Create access point (Criar ponto de acesso).
5. No campo Nome do ponto de acesso, insira o nome do ponto de acesso. Para obter mais informações sobre nomenclatura de pontos de acesso, consulte Regras de nomenclatura para pontos de acesso.
6. Em Fonte de dados, especifique o bucket do S3 que você deseja usar com o ponto de acesso.

   Para usar um bucket em sua conta, selecione Escolha um bucket nesta conta e insira ou pesquise o nome do bucket.

   Para usar um bucket em outra Conta da AWS, escolha Especificar um bucket em outra conta e insira o ID da Conta da AWS e o nome do bucket. Se você estiver usando um bucket em outra Conta da AWS, o proprietário do bucket deverá atualizar a política do bucket para autorizar solicitações do ponto de acesso. Para ver um exemplo de política de bucket, consulte Conceder permissões para pontos de acesso entre contas.

   > **Note**
   >
   > Para ter informações sobre como usar um volume do FSx para OpenZFS como fonte de dados, consulte Criar pontos de acesso com o Amazon FSx.

7. Escolha uma Origem da rede, seja Internet ou Nuvem privada virtual (VPC). Se você escolher Nuvem privada virtual (VPC), insira o ID da VPC que deseja usar com o ponto de acesso.

Para obter mais informações sobre origens de rede para pontos de acesso, consulte Criar pontos de acesso restritos a uma nuvem privada virtual.

8. Em Access point settings for Block Public Access (Configurações do ponto de acesso para o Bloqueio de acesso público), selecione as configurações de bloqueio de acesso público que você deseja aplicar ao ponto de acesso. Todas as configurações do bloqueio de acesso público são habilitadas por padrão para novos pontos de acesso. Recomendamos que você mantenha todas as configurações ativadas, a menos que saiba que tem uma necessidade específica de desativar qualquer uma delas.

   > **Note**
   >
   > Depois de criar um ponto de acesso, não será possível alterar as configurações de bloqueio de acesso público.

   Para obter mais informações sobre como usar o Bloqueio de acesso público do Amazon S3 com pontos de acesso, consulte Gerenciar o acesso público a pontos de acesso para buckets de uso geral.

9. (Opcional) Em Access point policy - optional (Política de ponto de acesso - opcional), especifique a política de ponto de acesso. Antes de salvar a política, solucione todos os avisos de segurança, os erros, os avisos gerais e as sugestões. Para obter mais informações sobre como especificar uma política de ponto de acesso, consulte Exemplos de política para pontos de acesso.
10. Selecione Criar ponto de acesso.

Como usar o AWS CLI

O exemplo de comando a seguir cria um ponto de acesso chamado *example-ap* para o bucket *amzn-s3-demo-bucket* na conta *111122223333*. Para criar o ponto de acesso, envie uma solicitação ao Amazon S3 que especifica o seguinte:

- O nome do ponto de acesso. Para obter informações sobre regras de nomeação, consulte the section called “Regras de nomenclatura para pontos de acesso”.
- O nome do bucket ao qual você deseja associar o ponto de acesso.
- O ID da Conta da AWS à qual o ponto de acesso pertence.

```
aws s3control create-access-point --name example-ap --account-id 111122223333 --
bucket amzn-s3-demo-bucket
```

Ao criar um ponto de acesso usando um bucket em outra Conta da AWS, inclua o parâmetro `--bucket-account-id`. O exemplo de comando a seguir cria um ponto de acesso na Conta da AWS *111122223333*, usando o bucket *amzn-s3-demo-bucket2*, que está na Conta da AWS *444455556666*.

```
aws s3control create-access-point --name example-ap --account-id 111122223333 --
bucket amzn-s3-demo-bucket --bucket-account-id 444455556666
```

Uso da API REST

É possível usar a API REST para criar um ponto de acesso. Para obter mais informações, consulte CreateAccessPoint na Referência da API do Amazon Simple Storage Service.

Criar pontos de acesso com o Amazon FSx

Você pode criar e anexar um ponto de acesso a um volume do FSx para OpenZFS usando o console do Amazon FSx, a AWS CLI ou a API. Depois de anexado, você pode usar as APIs de objeto do S3 para acessar seus dados de arquivo. Seus dados continuam residindo no sistema de arquivos do Amazon FSx e continuam diretamente acessíveis para suas workloads existentes. Você continua gerenciando seu armazenamento por meio de todos os recursos de gerenciamento de armazenamento do FSx para OpenZFS, como backups, snapshots, cotas de usuário e grupo e compressão.

Para ter instruções sobre como criar um ponto de acesso e anexá-lo a um volume do FSx para OpenZFS, consulte Creating access point no Guia do usuário FSx para OpenZFS.

Criar pontos de acesso restritos a uma nuvem privada virtual

Ao criar um ponto de acesso, você pode optar por tornar o ponto de acesso acessível pela internet ou pode especificar que todas as solicitações feitas por meio desse ponto de acesso devem ser originadas de uma nuvem privada virtual (VPC) específica. Considera-se que um ponto de acesso acessível da Internet tem uma origem de rede da `Internet`. Ele pode ser usado de qualquer lugar na internet e está sujeito a quaisquer outras restrições de acesso em vigor para o ponto de acesso, a fonte de dados subjacente e os recursos relacionados, como os objetos solicitados. Um ponto de acesso acessível apenas de uma VPC especificada tem uma origem de rede de `VPC`, e o Amazon S3 rejeita qualquer solicitação feita ao ponto de acesso que não tenha origem nessa VPC.

> **Important**
>
> Você só pode especificar a origem da rede de um ponto de acesso ao criá-lo. Depois de criar o ponto de acesso, não é possível alterar a origem da rede.

Para restringir um ponto de acesso ao acesso somente VPC, inclua o parâmetro `VpcConfiguration` com a solicitação para criar o ponto de acesso. No parâmetro `VpcConfiguration`, você especifica o ID da VPC que deseja usar o ponto de acesso. Se uma solicitação for feita por meio do ponto de acesso, ela deverá ser originada da VPC. Do contrário, o Amazon S3 a rejeitará.

Você pode recuperar a origem da rede de um ponto de acesso usando a AWS CLI, os AWS SDKs ou as APIs REST. Se um ponto de acesso tiver uma configuração de VPC especificada, sua origem de rede será `VPC`. Caso contrário, a origem da rede do ponto de acesso será `Internet`.

Exemplo: criar e restringir um ponto de acesso a um ID de VPC

O exemplo a seguir cria um ponto de acesso chamado `example-vpc-ap` para o bucket *amzn-s3-demo-bucket* na conta `123456789012` que permite acesso somente da VPC `vpc-1a2b3c`. O exemplo verifica se o novo ponto de acesso tem uma origem de rede da `VPC`.

AWS CLI

```
aws s3control create-access-point --name example-vpc-ap --account-id 123456789012 --
bucket amzn-s3-demo-bucket --vpc-configuration VpcId=vpc-1a2b3c
```

```
aws s3control get-access-point --name example-vpc-ap --account-id 123456789012

{
    "Name": "example-vpc-ap",
    "Bucket": "amzn-s3-demo-bucket",
    "NetworkOrigin": "VPC",
    "VpcConfiguration": {
        "VpcId": "vpc-1a2b3c"
    },
    "PublicAccessBlockConfiguration": {
        "BlockPublicAcls": true,
        "IgnorePublicAcls": true,
        "BlockPublicPolicy": true,
```

```
        "RestrictPublicBuckets": true
    },
    "CreationDate": "2019-11-27T00:00:00Z"
}
```

Para usar um ponto de acesso com uma VPC, é necessário modificar a política de acesso do endpoint da VPC especificado. Os VPC endpoints permitem que o tráfego flua da VPC para o Amazon S3. Os pontos de acesso têm políticas de controle de acesso que regulam como os recursos na VPC podem interagir com o Amazon S3. As solicitações da VPC ao Amazon S3 serão bem-sucedidas por meio de um ponto de acesso somente se a política do endpoint da VPC conceder acesso ao ponto de acesso e ao bucket subjacente.

> **Note**
>
> Para tornar os recursos acessíveis apenas em uma VPC, crie uma zona hospedada privada para o endpoint da VPC. Para usar uma zona hospedada privada, modifique suas configurações da VPC para que os atributos da rede de VPC `enableDnsHostnames` e `enableDnsSupport` sejam definidos como `true`.

O exemplo de instrução de política a seguir configura um VPC endpoint para permitir chamadas ao `GetObject` de um bucket denominado `awsexamplebucket1` e um ponto de acesso chamado `example-vpc-ap`.

```
{
    "Version": "2012-10-17",
    "Statement": [
    {
        "Principal": "*",
        "Action": [
            "s3:GetObject"
        ],
        "Effect": "Allow",
        "Resource": [
            "arn:aws:s3:::awsexamplebucket1/*",
            "arn:aws:s3:us-west-2:123456789012:accesspoint/example-vpc-ap/object/*"
        ]
    }]
}
```

> **Note**
>
> A declaração `"Resource"` neste exemplo usa um nome de recurso da Amazon (ARN) para especificar o ponto de acesso. Para obter mais informações sobre ARNs de ponto de acesso, consulte Fazer referência a pontos de acesso com ARNs, aliases de ponto de acesso ou URIs de estilo de hospedagem virtual.

Para obter mais informações sobre políticas do endpoint da VPC, consulte Políticas de endpoint para o Amazon S3 no Guia do usuário da VPC.

Para ver um tutorial sobre como criar pontos de acesso com endpoints da VPC, consulte Managing Amazon S3 access with VPC endpoints and access points.

Exemplo: criar e restringir um ponto de acesso anexado a um volume do FSx para OpenZFS a um ID de VPC

É possível criar um ponto de acesso que é anexado a um volume do FSx para OpenZFS usando o console do Amazon FSx, a AWS CLI ou a API. Depois de anexado, você pode usar as APIs de objeto do S3 para acessar seus dados de arquivo de uma VPC especificada.

Para ter instruções sobre como criar e restringir um ponto de acesso anexado a um volume do FSx para OpenZFS, consulte Creating access points restricted to a virtual private cloud (VPC) no Guia do usuário do FSx para OpenZFS.

Gerenciar o acesso público a pontos de acesso para buckets de uso geral

Os pontos de acesso do Amazon S3 oferecem suporte a configurações independentes do bloqueio de acesso público para cada ponto de acesso. Ao criar um ponto de acesso, você pode especificar configurações do Bloqueio de acesso público que se aplicam a esse ponto de acesso. Para qualquer solicitação feita por meio de um ponto de acesso, o Amazon S3 avalia as configurações de bloqueio de acesso público para esse ponto de acesso, o bucket subjacente e a conta do proprietário do bucket. Se qualquer uma dessas configurações indicar que a solicitação deve ser bloqueada, o Amazon S3 rejeitará a solicitação.

Para obter mais informações sobre o recurso de bloqueio de acesso público do S3, consulte Bloquear o acesso público ao armazenamento do Amazon S3.

Important

- Todas as configurações do Bloqueio de acesso público são habilitadas por padrão para pontos de acesso. Você deve desabilitar explicitamente todas as configurações que não deseja aplicar durante a criação de um ponto de acesso.
- Não é possível desativar nenhuma configuração de bloqueio de acesso público ao criar ou usar um ponto de acesso anexado a um sistema de arquivos do Amazon FSx.
- Depois de criar um ponto de acesso, não será possível alterar as configurações de bloqueio de acesso público.

Example

Exemplo: criar um ponto de acesso com configurações personalizadas do Bloqueio de acesso público

Este exemplo cria um ponto de acesso chamado `example-ap` para o bucket *amzn-s3-demo-bucket* na conta `123456789012` com configurações não padrão do Bloqueio de acesso público. O exemplo recupera a configuração do novo ponto de acesso para verificar as configurações do Bloqueio de acesso público.

AWS CLI

```
aws s3control create-access-point --name example-ap --account-id
 123456789012 --bucket amzn-s3-demo-bucket--public-access-block-configuration
 BlockPublicAcls=false,IgnorePublicAcls=false,BlockPublicPolicy=true,RestrictPublicBuckets=t
```

```
aws s3control get-access-point --name example-ap --account-id 123456789012

{
    "Name": "example-ap",
    "Bucket": "amzn-s3-demo-bucket",
    "NetworkOrigin": "Internet",
    "PublicAccessBlockConfiguration": {
        "BlockPublicAcls": false,
        "IgnorePublicAcls": false,
        "BlockPublicPolicy": true,
        "RestrictPublicBuckets": true
    },
```

```
    "CreationDate": "2019-11-27T00:00:00Z"
}
```

Gerenciar o recurso Pontos de Acesso Amazon S3 para buckets de uso geral

Esta seção explica como gerenciar o recurso Pontos de Acesso Amazon S3 para buckets de uso geral usando o AWS Management Console, a AWS Command Line Interface ou a API REST. Para ter informações sobre o gerenciamento de pontos de acesso anexados a um volume do FSx para OpenZFS, consulte Managing your Amazon S3 access points no Guia do usuário do FSx para OpenZFS.

> **Note**
>
> Você só pode usar pontos de acesso para executar operações em objetos. Não é possível usar pontos de acesso para executar outras operações do Amazon S3, como excluir buckets ou criar configurações do recurso Replicação do S3. Para obter uma lista completa das operações do S3 que oferecem suporte a pontos de acesso, consulte Compatibilidade dos pontos de acesso.

Tópicos

- Listar os pontos de acesso para buckets de uso geral
- Visualizar detalhes dos pontos de acesso para buckets de uso geral
- Excluir um ponto de acesso para um bucket de uso geral

Listar os pontos de acesso para buckets de uso geral

Esta seção explica como listar os pontos de acesso para buckets de uso geral usando o AWS Management Console, a AWS Command Line Interface ou a API REST.

Usar o console do S3

Como listar os pontos de acesso na Conta da AWS

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.

2. Na barra de navegação na parte superior da página, escolha o nome da Região da AWS exibida no momento. Em seguida, escolha a região para a qual você deseja listar os pontos de acesso.
3. No painel de navegação, no lado esquerdo do console, escolha Pontos de acesso.
4. (Opcional) Pesquise pontos de acesso pelo nome. Somente os pontos de acesso na Região da AWS selecionada aparecerão aqui.
5. Escolha o nome do ponto de acesso que você deseja gerenciar ou usar.

Como usar o AWS CLI

O exemplo de comando `list-access-points` a seguir mostra como você pode usar a AWS CLI para listar os pontos de acesso.

O comando a seguir lista os pontos de acesso para a Conta da AWS *111122223333*.

```
aws s3control list-access-points --account-id 111122223333
```

O comando a seguir lista os pontos de acesso para a Conta da AWS *111122223333* que estão anexados ao bucket *amzn-s3-demo-bucket*.

```
aws s3control list-access-points --account-id 111122223333 --bucket amzn-s3-demo-bucket
```

Para obter mais informações e exemplos, consulte list-access-points na Referência de comandos da AWS CLI.

Uso da API REST

É possível usar a API REST para listar os pontos de acesso. Para obter mais informações, consulte ListAccessPoints na Referência da API do Amazon Simple Storage Service.

Visualizar detalhes dos pontos de acesso para buckets de uso geral

Esta seção explica como visualizar detalhes de um ponto de acesso para um bucket de uso geral usando o AWS Management Console, a AWS Command Line Interface ou a API REST.

Usar o console do S3

Como visualizar os detalhes de um ponto de acesso na Conta da AWS

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Na barra de navegação na parte superior da página, escolha o nome da Região da AWS exibida no momento. Em seguida, escolha a região para a qual você deseja listar os pontos de acesso.
3. No painel de navegação, no lado esquerdo do console, escolha Pontos de acesso.
4. (Opcional) Pesquise pontos de acesso pelo nome. Somente os pontos de acesso na Região da AWS selecionada aparecerão aqui.
5. Escolha o nome do ponto de acesso que você deseja gerenciar ou usar.
6. Selecione a guia Propriedades para visualizar a fonte de dados do ponto de acesso, o ID da conta, a Região da AWS, a data de criação, a origem da rede, o URI do S3, o ARN e o alias para o ponto de acesso selecionado.
7. Selecione a guia Permissões para visualizar as configurações de bloqueio de acesso público e a política de ponto de acesso para o ponto de acesso selecionado.

> **Note**
>
> Não é possível alterar as configurações de bloqueio de acesso público para um ponto de acesso depois que ele é criado.

Como usar o AWS CLI

O exemplo de comando `get-access-point` a seguir mostra como você pode usar a AWS CLI para visualizar os detalhes de um ponto de acesso.

O comando a seguir lista os detalhes do ponto de acesso *`my-access-point`* para Conta da AWS *`111122223333`* anexado ao bucket do S3 *`amzn-s3-demo-bucket`*.

```
aws s3control get-access-point --name my-access-point --account-id 111122223333
```

Resultado do exemplo:

```
{
```

```
    "Name": "my-access-point",
    "Bucket": "amzn-s3-demo-bucket",
    "NetworkOrigin": "Internet",
    "PublicAccessBlockConfiguration": {
        "BlockPublicAcls": true,
        "IgnorePublicAcls": true,
        "BlockPublicPolicy": true,
        "RestrictPublicBuckets": true
    },
    "CreationDate": "2016-08-29T22:57:52Z",
    "Alias": "my-access-point-u1ny6bhm7moymqx8cuon8o1g4mwikuse2a-s3alias",
    "AccessPointArn": "arn:aws:s3:Região da AWS:111122223333:accesspoint/my-access-
point",
    "Endpoints": {
        "ipv4": "s3-accesspoint.Região da AWS.amazonaws.com",
        "fips": "s3-accesspoint-fips.Região da AWS.amazonaws.com",
        "fips_dualstack": "s3-accesspoint-fips.dualstack.Região da AWS.amazonaws.com",
        "dualstack": "s3-accesspoint.dualstack.Região da AWS.amazonaws.com"
    },
    "BucketAccountId": "111122223333"
}
```

O comando a seguir lista os detalhes do ponto de acesso *example-fsx-ap* para Conta da AWS *444455556666*. Esse ponto de acesso está anexado a um sistema de arquivos do Amazon FSx.

```
aws s3control get-access-point --name example-fsx-ap --account-id 444455556666
```

Resultado do exemplo:

```
{
    "Name": "example-fsx-ap",
    "Bucket": "",
    "NetworkOrigin": "Internet",
    "PublicAccessBlockConfiguration": {
        "BlockPublicAcls": true,
        "IgnorePublicAcls": true,
        "BlockPublicPolicy": true,
        "RestrictPublicBuckets": true
    },
    "CreationDate": "2025-01-19T14:16:12Z",
    "Alias": "example-fsx-ap-qrqbyebjtsxorhhaa5exx6r3q7-ext-s3alias",
    "AccessPointArn": "arn:aws:s3:Região da AWS:444455556666:accesspoint/example-fsx-
ap",
```

```
    "Endpoints": {
        "ipv4": "s3-accesspoint.Região da AWS.amazonaws.com",
        "fips": "s3-accesspoint-fips.Região da AWS.amazonaws.com",
        "fips_dualstack": "s3-accesspoint-fips.dualstack.Região da AWS.amazonaws.com",
        "dualstack": "s3-accesspoint.dualstack.Região da AWS.amazonaws.com"
    },
    "DataSourceId": "arn:aws::fsx:Região da AWS:444455556666:file-system/
fs-5432106789abcdef0/volume/vol-0123456789abcdef0",
    "DataSourceType": "FSX_OPENZFS"
}
```

Para obter mais informações e exemplos, consulte get-access-point na Referência de comandos da AWS CLI.

Uso da API REST

É possível usar a API REST para visualizar os detalhes de um ponto de acesso. Para obter mais informações, consulte GetAccessPoint na Referência da API do Amazon Simple Storage Service.

Excluir um ponto de acesso para um bucket de uso geral

Esta seção explica como excluir um ponto de acesso para um bucket de uso geral usando o AWS Management Console, a AWS Command Line Interface ou a API REST.

Usar o console do S3

Como excluir pontos de acesso na Conta da AWS

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Na barra de navegação na parte superior da página, escolha o nome da Região da AWS exibida no momento. Em seguida, escolha a região para a qual você deseja listar os pontos de acesso.
3. No painel de navegação, no lado esquerdo do console, escolha Pontos de acesso.
4. (Opcional) Pesquise pontos de acesso pelo nome. Somente os pontos de acesso na Região da AWS selecionada aparecerão aqui.
5. Escolha o nome do ponto de acesso que você deseja gerenciar ou usar.
6. Na página Ponto de acesso, selecione Excluir para excluir o ponto de acesso selecionado.
7. Para confirmar a exclusão, digite o nome do ponto de acesso e escolha Excluir.

Como usar o AWS CLI

O exemplo de comando `delete-access-point` a seguir mostra como você pode usar a AWS CLI para excluir um ponto de acesso.

O comando a seguir exclui o ponto de acesso *`my-access-point`* da Conta da AWS *`111122223333`*.

```
aws s3control delete-access-point --name my-access-point --account-id 111122223333
```

Para obter mais informações e exemplos, consulte delete-access-point na Referência de comandos da AWS CLI.

Uso da API REST

É possível usar a API REST para visualizar os detalhes de um ponto de acesso. Para obter mais informações, consulte DeleteAccessPoint na Referência da API do Amazon Simple Storage Service.

Usar o recurso Pontos de Acesso Amazon S3 para buckets de uso geral

Os exemplos a seguir demonstram como usar pontos de acesso para buckets de uso geral com operações compatíveis no Amazon S3.

> **Note**
>
> O S3 gera automaticamente aliases de ponto de acesso para todos os pontos de acesso e esses aliases podem ser usados em qualquer lugar em que um nome de bucket seja usado para realizar operações ao nível do objeto. Para obter mais informações, consulte Alias de ponto de acesso.

Você só pode usar pontos de acesso para buckets de uso geral para executar operações em objetos. Não é possível usar pontos de acesso para executar outras operações do Amazon S3, como modificar ou excluir buckets. Para obter uma lista completa das operações do S3 que oferecem suporte a pontos de acesso, consulte Compatibilidade dos pontos de acesso.

Tópicos

- Listar objetos por meio de um ponto de acesso para um bucket de uso geral
- Baixar um objeto por meio de um ponto de acesso para um bucket de uso geral

- Configurar listas de controle de acesso (ACLs) por meio de um ponto de acesso para um bucket de uso geral
- Fazer upload de um objeto por meio de um ponto de acesso para um bucket de uso geral
- Adicionar um conjunto de tags por meio de um ponto de acesso para um bucket de uso geral
- Excluir um objeto por meio de um ponto de acesso para um bucket de uso geral

Listar objetos por meio de um ponto de acesso para um bucket de uso geral

Esta seção explica como listar objetos por meio de um ponto de acesso para um bucket de uso geral usando o AWS Management Console, a AWS Command Line Interface ou a API REST.

Usar o console do S3

Como listar os objetos por meio de um ponto de acesso na Conta da AWS

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Na barra de navegação na parte superior da página, escolha o nome da Região da AWS exibida no momento. Em seguida, escolha a região para a qual você deseja listar os pontos de acesso.
3. No painel de navegação, no lado esquerdo do console, escolha Pontos de acesso.
4. (Opcional) Pesquise pontos de acesso pelo nome. Somente os pontos de acesso na Região da AWS selecionada aparecerão aqui.
5. Escolha o nome do ponto de acesso que você deseja gerenciar ou usar.
6. Na guia Objetos, é possível visualizar o nome dos objetos que deseja acessar por meio do ponto de acesso. Enquanto estiver usando o ponto de acesso, você só pode executar as operações de objeto permitidas pelas permissões do ponto de acesso.

> **Note**
>
> - A exibição do console sempre mostra todos os objetos no bucket. O uso de um ponto de acesso conforme descrito neste procedimento restringe as operações que você pode executar nesses objetos, mas não se você puder ver que eles existem no bucket.
> - O AWS Management Console não oferece suporte ao uso de pontos de acesso da nuvem privada virtual (VPC) para acessar recursos de bucket. Para acessar recursos

de bucket em um ponto de acesso da VPC, use a AWS CLI, os AWS SDKs ou as APIs REST do Amazon S3.

Como usar o AWS CLI

O exemplo de comando `list-objects-v2` a seguir mostra como você pode usar a AWS CLI para listar os objetos por meio de um ponto de acesso.

O comando a seguir lista os objetos da Conta da AWS *111122223333* usando o ponto de acesso *my-access-point*.

```
aws s3api list-objects-v2 --bucket arn:aws:s3:Região da
 AWS:111122223333:accesspoint/my-access-point
```

> **Note**
>
> O S3 gera automaticamente aliases de ponto de acesso para todos os pontos de acesso e esses aliases podem ser usados em qualquer lugar em que um nome de bucket seja usado para realizar operações ao nível do objeto. Para obter mais informações, consulte Alias de ponto de acesso.

Para obter mais informações e exemplos, consulte list-access-points na Referência de comandos da AWS CLI.

Uso da API REST

É possível usar a API REST para listar os pontos de acesso. Para obter mais informações, consulte ListObjectsV2 na Referência da API do Amazon Simple Storage Service.

Baixar um objeto por meio de um ponto de acesso para um bucket de uso geral

Esta seção explica como baixar um objeto por meio de um ponto de acesso para um bucket de uso geral usando o AWS Management Console, a AWS Command Line Interface ou a API REST.

Usar o console do S3

Como fazer download de um objeto por meio de um ponto de acesso na Conta da AWS

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Na barra de navegação na parte superior da página, escolha o nome da Região da AWS exibida no momento. Em seguida, escolha a região para a qual você deseja listar os pontos de acesso.
3. No painel de navegação, no lado esquerdo do console, escolha Pontos de acesso.
4. (Opcional) Pesquise pontos de acesso pelo nome. Somente os pontos de acesso na Região da AWS selecionada aparecerão aqui.
5. Escolha o nome do ponto de acesso que você deseja gerenciar ou usar.
6. Na guia Objetos, selecione o nome do objeto que você deseja baixar.
7. Escolha Baixar.

Como usar o AWS CLI

O exemplo de comando `get-object` a seguir mostra como você pode usar a AWS CLI para fazer download de um objeto por meio de um ponto de acesso.

O comando a seguir faz download do objeto `puppy.jpg` da Conta da AWS *`111122223333`* usando o ponto de acesso *`my-access-point`*. Você deve incluir um `outfile`, que é um nome de arquivo para o objeto baixado, como *`my_downloaded_image.jpg`*.

```
aws s3api get-object --bucket arn:aws:s3:Região da AWS:111122223333:accesspoint/my-access-point --key puppy.jpg my_downloaded_image.jpg
```

> **Note**
>
> O S3 gera automaticamente aliases de ponto de acesso para todos os pontos de acesso e esses aliases podem ser usados em qualquer lugar em que um nome de bucket seja usado para realizar operações ao nível do objeto. Para obter mais informações, consulte Alias de ponto de acesso.

Para obter mais informações e exemplos, consulte get-object na Referência de comandos da AWS CLI.

Uso da API REST

É possível usar a API REST para fazer download de um objeto por meio de um ponto de acesso. Para obter mais informações, consulte GetObject na Referência da API do Amazon Simple Storage Service.

Uso dos SDKs da AWS

É possível usar o AWS SDK para Python para baixar um objeto por meio de um ponto de acesso.

Python

No exemplo a seguir, o arquivo chamado *hello.txt* é baixado para a conta da AWS *111122223333* usando o ponto de acesso denominado *my-access-point*.

```
import boto3
s3 = boto3.client('s3')
s3.download_file('arn:aws:s3:us-east-1:111122223333:accesspoint/my-access-point',
 'hello.txt', '/tmp/hello.txt')
```

Configurar listas de controle de acesso (ACLs) por meio de um ponto de acesso para um bucket de uso geral

Esta seção explica como configurar ACLs por meio de um ponto de acesso para um bucket de uso geral usando o AWS Management Console, a AWS Command Line Interface ou a API REST. Para obter mais informações sobre ACLs, consulte Visão geral da lista de controle de acesso (ACL).

Usar o console do S3

Como configurar ACLs por meio de um ponto de acesso na Conta da AWS

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Na barra de navegação na parte superior da página, escolha o nome da Região da AWS exibida no momento. Em seguida, escolha a região para a qual você deseja listar os pontos de acesso.
3. No painel de navegação, no lado esquerdo do console, escolha Pontos de acesso.
4. (Opcional) Pesquise pontos de acesso pelo nome. Somente os pontos de acesso na Região da AWS selecionada aparecerão aqui.

5. Escolha o nome do ponto de acesso que você deseja gerenciar ou usar.
6. Na guia Objetos, selecione o nome do objeto para o qual você deseja configurar uma ACL.
7. Na guia Permissões, selecione Editar para configurar a ACL do objeto.

> **Note**
>
> Atualmente, o Amazon S3 não oferece suporte à alteração das configurações do bloqueio de acesso público após à criação de um ponto de acesso.

Como usar o AWS CLI

O exemplo de comando `put-object-acl` a seguir mostra como você pode usar a AWS CLI para configurar permissões de acesso por meio de um ponto de acesso usando uma ACL.

O comando a seguir aplica uma ACL a um objeto `puppy.jpg` existente por meio de um ponto de acesso pertencente à Conta da AWS *111122223333*.

```
aws s3api put-object-acl --bucket arn:aws:s3:Região da AWS:111122223333:accesspoint/my-access-point --key puppy.jpg --acl private
```

> **Note**
>
> O S3 gera automaticamente aliases de ponto de acesso para todos os pontos de acesso e esses aliases podem ser usados em qualquer lugar em que um nome de bucket seja usado para realizar operações ao nível do objeto. Para obter mais informações, consulte Alias de ponto de acesso.

Para obter mais informações e exemplos, consulte put-object-acl na Referência de comandos da AWS CLI.

Uso da API REST

É possível usar a API REST para configurar as permissões de acesso por meio de um ponto de acesso usando uma ACL. Para obter mais informações, consulte PutObjectAcl na Referência da API do Amazon Simple Storage Service.

Fazer upload de um objeto por meio de um ponto de acesso para um bucket de uso geral

Esta seção explica como fazer upload de um objeto por meio de um ponto de acesso para um bucket de uso geral usando o AWS Management Console, a AWS Command Line Interface ou a API REST.

Usar o console do S3

Como fazer upload de um objeto por meio de um ponto de acesso na Conta da AWS

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Na barra de navegação na parte superior da página, escolha o nome da Região da AWS exibida no momento. Em seguida, escolha a região para a qual você deseja listar os pontos de acesso.
3. No painel de navegação, no lado esquerdo do console, escolha Pontos de acesso.
4. (Opcional) Pesquise pontos de acesso pelo nome. Somente os pontos de acesso na Região da AWS selecionada aparecerão aqui.
5. Escolha o nome do ponto de acesso que você deseja gerenciar ou usar.
6. Na guia Objetos, selecione Fazer upload.
7. Arraste e solte os arquivos e as pastas que você deseja carregar aqui ou escolha Adicionar arquivos ou Adicionar pasta.

   > **Note**
   >
   > O tamanho máximo de arquivo que você pode carregar usando o console do Amazon S3 é de 160 GB. Para fazer upload de um arquivo com mais de 160 GB, use a AWS Command Line Interface (AWS CLI), AWS SDKs ou a API REST do Amazon S3.

8. Para alterar as permissões da lista de controle de acesso, escolha Permissions (Permissões).
9. Em Access control list (ACL) (Lista de controle de acesso (ACL)), edite as permissões.

   Para informações sobre permissões de acesso a objeto, consulte Usar o console do S3 para definir permissões de ACL para um objeto. Você pode conceder acesso de leitura aos seus objetos ao público (todos no mundo), para todos os arquivos que você está carregando. No entanto, recomendamos não alterar a configuração padrão para acesso de leitura público. Conceder acesso público de leitura é aplicável a um pequeno subconjunto de casos de uso,

como quando buckets são usados para sites. Você sempre pode alterar as permissões de objeto depois de carregar o objeto.

10. Para configurar outras propriedades, escolha Properties (Propriedades).
11. Na seção Classe de armazenamento escolha a classe de armazenamento para os arquivos que você está carregando.

    Para obter mais informações sobre classes de armazenamento, consulte Compreender e gerenciar classes de armazenamento do Amazon S3.
12. Para atualizar as configurações de criptografia para seus objetos, em Server-side encryption settings (Configurações de criptografia do lado do servidor), faça o seguinte.

    a. Escolha Specify an encryption key (Especificar uma chave de criptografia).

    b. Em Configurações de criptografia, escolha Usar configurações de bucket para criptografia padrão ou Substituir configurações de bucket para criptografia padrão.

    c. Se você escolher Substituir configurações do bucket para criptografia padrão, deverá definir as configurações de criptografia a seguir.

    - Para criptografar os arquivos carregados usando chaves gerenciadas pelo Amazon S3, escolha Chave gerenciada pelo Amazon S3 (SSE-S3).

      Para obter mais informações, consulte Usar a criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3).
    - Para criptografar os arquivos carregados usando chaves armazenadas no AWS Key Management Service (AWS KMS), selecione Chave do AWS Key Management Service (SSE-KMS). Depois, escolha uma das seguintes opções para a chave do AWS KMS:
      - Para escolher entre uma lista de chaves do KMS disponíveis, selecione Escolher de sua AWS KMS keys e escolha a chave do KMS na lista de chaves disponíveis.

        As chaves Chave gerenciada pela AWS (`aws/s3`) e as chaves gerenciadas pelo cliente são exibidas nessa lista. Para ter mais informações sobre chaves gerenciadas pelo cliente, consulte Chaves de clientes e chaves da AWS no Guia do desenvolvedor do AWS Key Management Service.
      - Para inserir o ARN da chave do KMS, selecione Inserir ARN da AWS KMS key e insira o ARN da chave do KMS no campo exibido.
      - Para criar uma chave gerenciada pelo cliente no console do AWS KMS, selecione Criar uma chave do KMS.

Para ter mais informações sobre como criar uma AWS KMS key, consulte Criação de chaves no Guia do desenvolvedor do AWS Key Management Service.

> **Important**
>
> Você só pode usar chaves do KMS disponíveis na mesma Região da AWS que o bucket. O console do Amazon S3 lista somente as primeiras 100 chaves do KMS na mesma região que o bucket. Para usar uma chave do KMS que não esteja listada, você deve inserir o ARN da chave do KMS. Se quiser usar uma chave do KMS que seja de propriedade de outra conta, primeiro você deverá ter permissão para usar a chave e, depois, inserir o ARN da chave do KMS.
> O Amazon S3 só é compatível com chaves do KMS de criptografia simétrica, e não com chaves assimétricas do KMS. Para ter mais informações, consulte Identificar chaves do KMS simétricas e assimétricas no Guia do desenvolvedor do AWS Key Management Service.

13. Para usar somas de verificação adicionais, escolha On (Ativar). Em seguida, em Checksum function (Função de soma de verificação), escolha a função que você gostaria de usar. O Amazon S3 calcula e armazena o valor da soma de verificação depois de receber o objeto inteiro. Você pode usar a caixa Precalculated value (Valor pré-calculado) para fornecer esse valor. Se fizer isso, o Amazon S3 vai comparar o valor que você forneceu com o valor calculado. Se os dois valores não corresponderem, o Amazon S3 gerará um erro.

    As somas de verificação adicionais permitem que você especifique o algoritmo de soma de verificação que gostaria de usar para verificar seus dados. Para obter mais informações sobre somas de verificação adicionais, consulte Verificar a integridade do objeto no Amazon S3.

14. Para adicionar tags a todos os objetos que você está carregando, escolha Add tag (Adicionar tag). Insira um nome de tag no campo Chave. Insira um valor para a tag.

    A marcação de objetos é uma forma de categorizar o armazenamento. Cada tag é um par de chave-valor. Os valores de chave e tag diferenciam maiúsculas de minúsculas. É possível ter até dez tags por objeto. Uma chave de tag pode ter até 128 caracteres Unicode e os valores de tag podem ter até 255 caracteres Unicode. Para obter mais informações sobre tags de objeto, consulte Categorizar seu armazenamento usando tags.

15. Para adicionar metadados, escolha Add metadata (Adicionar metadados).

a. Em Type (Tipo), escolha System defined (Definido pelo sistema) ou User defined (Definido pelo usuário).

   Para metadados definidos pelo sistema, você pode selecionar cabeçalhos HTTP comuns, como Content-Type e Content-Disposition. Para obter uma lista de metadados definidos pelo sistema e informações sobre a possibilidade de adicionar o valor, consulte Metadados do objeto definidos pelo sistema. Todos os metadados que começam com o prefixo `x-amz-meta-` são tratados como metadados definidos pelo usuário. Os metadados definidos pelo usuário são armazenados com o objeto e retornados quando você baixa o objeto. As chaves e seus valores devem estar em conformidade com os padrões US-ASCII. Metadados definidos pelo usuário podem ter até 2 KB. Para obter mais informações sobre metadados definidos pelo sistema e pelo usuário, consulte Trabalhar com metadados de objeto.

b. Para Key (Chave), escolha uma chave.

c. Digite um valor para a chave.

16. Para carregar seus objetos, escolha Upload (Fazer upload).

    O Amazon S3 faz o upload do objeto. Quando o upload for concluído, você pode ver uma mensagem de sucesso na página de Upload: status.

Como usar o AWS CLI

O exemplo de comando `put-object` a seguir mostra como você pode usar a AWS CLI para fazer upload de um objeto por meio de um ponto de acesso.

O comando a seguir faz upload do objeto `puppy.jpg` da Conta da AWS *111122223333* usando o ponto de acesso *my-access-point*.

```
aws s3api put-object --bucket arn:aws:s3:Região da AWS:111122223333:accesspoint/my-access-point --key puppy.jpg --body puppy.jpg
```

> **Note**
>
> O S3 gera automaticamente aliases de ponto de acesso para todos os pontos de acesso e esses aliases podem ser usados em qualquer lugar em que um nome de bucket seja usado

para realizar operações ao nível do objeto. Para obter mais informações, consulte Alias de ponto de acesso.

Para obter mais informações e exemplos, consulte put-object na Referência de comandos da AWS CLI.

Uso da API REST

É possível usar a API REST para fazer upload de um objeto por meio de um ponto de acesso. Para obter mais informações, consulte PutObject na Referência da API do Amazon Simple Storage Service.

Uso dos SDKs da AWS

É possível usar o AWS SDK para Python para fazer upload de um objeto por meio de um ponto de acesso.

Python

No exemplo a seguir, o arquivo chamado *hello.txt* é carregado na conta da AWS *111122223333* usando o ponto de acesso denominado *my-access-point*.

```
import boto3
s3 = boto3.client('s3')
s3.upload_file('/tmp/hello.txt', 'arn:aws:s3:us-east-1:111122223333:accesspoint/my-access-point', 'hello.txt')
```

Adicionar um conjunto de tags por meio de um ponto de acesso para um bucket de uso geral

Esta seção explica como adicionar um conjunto de tags por meio de um ponto de acesso para um bucket de uso geral usando o AWS Management Console, a AWS Command Line Interface ou a API REST. Para obter mais informações, consulte Categorizar seu armazenamento usando tags.

Usar o console do S3

Como adicionar um conjunto de tags por meio de um ponto de acesso na Conta da AWS

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Na barra de navegação na parte superior da página, escolha o nome da Região da AWS exibida no momento. Em seguida, escolha a região para a qual você deseja listar os pontos de acesso.
3. No painel de navegação, no lado esquerdo do console, escolha Pontos de acesso.
4. (Opcional) Pesquise pontos de acesso pelo nome. Somente os pontos de acesso na Região da AWS selecionada aparecerão aqui.
5. Escolha o nome do ponto de acesso que você deseja gerenciar ou usar.
6. Na guia Objetos, selecione o nome do objeto para o qual você deseja adicionar um conjunto de tags.
7. Na guia Propriedades, encontre o subcabeçalho Tags e escolha Editar.
8. Revise os objetos listados e escolha Adicionar tag.
9. Cada tag de objeto é um par de chave-valor. Insira uma Key (Chave) e um Value (Valor). Para adicionar outra tag, escolha Add Tag (Adicionar tag).

   Você pode digitar até 10 tags para um objeto.
10. Escolha Salvar alterações.

Como usar o AWS CLI

O exemplo de comando `put-object-tagging` a seguir mostra como você pode usar a AWS CLI para adicionar um conjunto de tags por meio de um ponto de acesso.

O comando a seguir adiciona um conjunto de tags ao objeto `puppy.jpg` existente usando o ponto de acesso *`my-access-point`*.

```
aws s3api put-object-tagging --bucket arn:aws:s3:Região da
 AWS:111122223333:accesspoint/my-access-point --key puppy.jpg --tagging
 TagSet=[{Key="animal",Value="true"}]
```

> **Note**
>
> O S3 gera automaticamente aliases de ponto de acesso para todos os pontos de acesso e esses aliases podem ser usados em qualquer lugar em que um nome de bucket seja usado para realizar operações ao nível do objeto. Para obter mais informações, consulte Alias de ponto de acesso.

Para obter mais informações e exemplos, consulte put-object-tagging na Referência de comandos da AWS CLI.

Uso da API REST

É possível usar a API REST para adicionar um conjunto de tags a um objeto por meio de um ponto de acesso. Para obter mais informações, consulte PutObjectTagging na Referência da API do Amazon Simple Storage Service.

Excluir um objeto por meio de um ponto de acesso para um bucket de uso geral

Esta seção explica como excluir um objeto por meio de um ponto de acesso para um bucket de uso geral usando o AWS Management Console, a AWS Command Line Interface ou a API REST.

Usar o console do S3

Como excluir um ou vários objetos por meio de um ponto de acesso na Conta da AWS

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Na barra de navegação na parte superior da página, escolha o nome da Região da AWS exibida no momento. Em seguida, escolha a região para a qual você deseja listar os pontos de acesso.
3. No painel de navegação, no lado esquerdo do console, escolha Pontos de acesso.
4. (Opcional) Pesquise pontos de acesso pelo nome. Somente os pontos de acesso na Região da AWS selecionada aparecerão aqui.
5. Escolha o nome do ponto de acesso que você deseja gerenciar ou usar.
6. Na guia Objetos, selecione os nomes dos objetos que você deseja excluir.
7. Revise os objetos listados para exclusão e digite delete na caixa de confirmação.
8. Escolha Delete objects (Excluir objetos).

Como usar o AWS CLI

O exemplo de comando `delete-object` a seguir mostra como você pode usar a AWS CLI para excluir um objeto por meio de um ponto de acesso.

O comando a seguir exclui o objeto `puppy.jpg` existente usando o ponto de acesso *`my-access-point`*.

```
aws s3api delete-object --bucket arn:aws:s3:Região da AWS:111122223333:accesspoint/my-access-point --key puppy.jpg
```

> **Note**
>
> O S3 gera automaticamente aliases de ponto de acesso para todos os pontos de acesso e esses aliases podem ser usados em qualquer lugar em que um nome de bucket seja usado para realizar operações ao nível do objeto. Para obter mais informações, consulte Alias de ponto de acesso.

Para obter mais informações e exemplos, consulte delete-object na Referência de comandos da AWS CLI.

Uso da API REST

É possível usar a API REST para excluir um objeto por meio de um ponto de acesso. Para obter mais informações, consulte DeleteObject na Referência da API do Amazon Simple Storage Service.

Gerenciar o acesso com a funcionalidade Concessões de Acesso do S3

Para aderir ao princípio do privilégio mínimo, defina o acesso granular aos dados do Amazon S3 com base em aplicações, personas, grupos ou unidades organizacionais. Você pode usar várias abordagens para obter acesso granular aos dados no Amazon S3, dependendo da escala e da complexidade dos padrões de acesso.

A abordagem mais simples para gerenciar o acesso a números pequenos a médios de conjuntos de dados no Amazon S3 por entidades principais do AWS Identity and Access Management (IAM) é definir políticas de permissões do IAM e políticas de buckets do S3. Essa estratégia funcionará se as políticas necessárias se encaixarem nos limites de tamanho das políticas de bucket do S3 (20 KB)

e das políticas do IAM (5 KB), bem como no número de entidades principais do IAM permitidas por conta.

À medida que o número de conjuntos de dados e casos de uso aumenta, talvez você precise de mais espaço para políticas. Uma abordagem que oferece muito mais espaço para declarações de política é usar os pontos de acesso do S3 como endpoints adicionais para buckets do S3, porque cada ponto de acesso pode ter sua própria política. Você pode definir padrões de controle de acesso bastante granulares, já que é possível ter milhares de pontos de acesso por Região da AWS por conta, com uma política de até 20 KB para cada ponto de acesso. Embora os pontos de acesso do S3 aumentem a quantidade de espaço disponível para políticas, é necessário um mecanismo para que os clientes descubram o ponto de acesso certo para o conjunto de dados certo.

Uma terceira abordagem é implementar um padrão de agente de sessão do IAM, no qual você implementa a lógica de decisão de acesso e gera dinamicamente credenciais de sessão do IAM de curto prazo para cada sessão de acesso. Embora a abordagem de agente de sessão do IAM ofereça suporte a padrões de permissões arbitrariamente dinâmicos e escale de forma eficaz, você deve criar a lógica do padrão de acesso.

Em vez de usar essas abordagens, você pode usar a funcionalidade Concessões de Acesso do S3 para gerenciar o acesso aos dados do Amazon S3. A funcionalidade Concessões de Acesso do S3 fornece um modelo simplificado para definir permissões de acesso aos dados no Amazon S3 por prefixo, bucket ou objeto. Além disso, você pode usar a funcionalidade Concessões de Acesso do S3 para conceder acesso às entidades principais do IAM e diretamente aos usuários ou grupos do diretório corporativo.

Em geral, você define permissões para os dados no Amazon S3 mapeando usuários e grupos para conjuntos de dados. Você pode usar a funcionalidade Concessões de Acesso do S3 para definir mapeamentos de acesso direto dos prefixos do S3 para usuários e perfis em buckets e objetos do Amazon S3. Com o esquema de acesso simplificado da funcionalidade Concessões de Acesso do S3, você pode conceder acesso somente leitura, somente gravação ou leitura e gravação com base em prefixo do S3 tanto para entidades principais do IAM quanto diretamente para usuários ou grupos de um diretório corporativo. Com esses recursos da funcionalidade Concessões de Acesso do S3, as aplicações podem solicitar dados do Amazon S3 em nome do usuário atualmente autenticado da aplicação.

Quando você integra a funcionalidade Concessões de Acesso do S3 ao recurso de propagação de identidades confiáveis do AWS IAM Identity Center, as aplicações podem fazer solicitações aos Serviços da AWS (incluindo a funcionalidade Concessões de Acesso do S3) diretamente em nome de um usuário autenticado do diretório corporativo. As aplicações não precisam mais primeiro

mapear o usuário para uma entidade principal do IAM. Além disso, como as identidades dos usuários finais são propagadas até o Amazon S3, a auditoria de qual usuário acessou qual objeto do S3 é simplificada. Você não precisa mais reconstruir o relacionamento entre diferentes usuários e sessões do IAM. Quando você usa a funcionalidade Concessões de Acesso do S3 com a propagação de identidades confiáveis do Centro de Identidade do IAM, cada evento de dados do AWS CloudTrail para o Amazon S3 contém uma referência direta ao usuário final em cujo nome os dados foram acessados.

A propagação de identidade confiável é um recurso do AWS IAM Identity Center que os administradores de Serviços da AWS conectados podem usar para conceder e auditar o acesso aos dados do serviço. O acesso a esses dados é baseado em atributos do usuário, como associações de grupo. A configuração da propagação de identidade confiável requer a colaboração entre os administradores de Serviços da AWS conectados e os administradores do Centro de Identidade do IAM. Para ter mais informações, consulte Prerequisites and considerations.

Para obter mais informações sobre a funcionalidade Concessões de Acesso do S3, consulte os tópicos a seguir.

Tópicos

- Conceitos da funcionalidade Concessões de Acesso do S3
- Concessões de Acesso do S3 e identidades de diretórios corporativos
- Conceitos básicos da funcionalidade Concessões de Acesso do S3
- Trabalhar com instâncias do recurso Concessão de Acesso do S3
- Trabalhar com locais do recurso Concessão de Acesso do S3
- Trabalhar com concessões no recurso Concessão de Acesso do S3
- Obter dados do S3 usando concessões de acesso
- Acesso entre contas da funcionalidade Concessões de Acesso do S3
- Usar etiquetas da AWS com a funcionalidade Concessões de Acesso do S3
- Limitações da funcionalidade Concessões de Acesso do S3
- Integrações da funcionalidade Concessões de Acesso do S3

Conceitos da funcionalidade Concessões de Acesso do S3

Fluxo de trabalho do recurso Concessão de Acesso do S3

O fluxo de trabalho do recurso Concessão de Acesso do S3 é:

1. Crie uma instância da funcionalidade Concessões de Acesso do S3. Consulte Trabalhar com instâncias do recurso Concessão de Acesso do S3.
2. Na instância do recurso Concessão de Acesso do S3, registre locais nos dados do Amazon S3 e associe esses locais a perfis do AWS Identity and Access Management (IAM). Consulte Registrar um local.
3. Crie concessões para os beneficiários, o que concede aos beneficiários acesso aos seus recursos do S3. Consulte Trabalhar com concessões no recurso Concessão de Acesso do S3.
4. O beneficiário solicita credenciais temporárias ao recurso Concessão de Acesso do S3. Consulte Solicitar acesso aos dados do Amazon S3 por meio da funcionalidade Concessões de Acesso do S3.
5. O beneficiário acessa os dados do S3 usando essas credenciais temporárias. Consulte Acessar os dados do S3 usando credenciais fornecidas pelo recurso Concessão de Acesso do S3.

Para obter mais informações, consulte Conceitos básicos da funcionalidade Concessões de Acesso do S3.

Instâncias da funcionalidade Concessões de Acesso do S3

Instância do recurso Concessão de Acesso do S3 é um contêiner lógico para concessões individuais. Ao criar uma instância do recurso Concessão de Acesso do S3, é necessário especificar um Região da AWS. Cada Região da AWS na sua Conta da AWS pode ter uma instância do recurso Concessão de Acesso do S3. Para obter mais informações, consulte Trabalhar com instâncias do recurso Concessão de Acesso do S3.

Se quiser usar o recurso Concessão de Acesso do S3 para conceder acesso às identidades de usuários e grupos no diretório corporativo, você também deverá associar a instância do recurso Concessão de Acesso do S3 a uma instância do AWS IAM Identity Center. Para obter mais informações, consulte Concessões de Acesso do S3 e identidades de diretórios corporativos.

Uma instância recém-criada do recurso Concessão de Acesso do S3 está vazia. É necessário registrar um local na instância, que pode ser o caminho padrão do S3 (`s3://`), um bucket ou um prefixo dentro de um bucket. Depois de registrar pelo menos uma localização, é possível criar concessões que dão acesso aos dados nessa localização registrada.

Locais

Uma localização do recurso Concessão de Acesso do S3 associa buckets ou prefixos a um perfil do AWS Identity and Access Management (IAM). O recurso Concessão de Acesso do S3 assume

esse perfil do IAM para fornecer credenciais temporárias ao beneficiário que está acessando aquela localização específica. Primeiro, é necessário registrar pelo menos uma localização na instância do recurso Concessão de Acesso do S3 para poder criar uma concessão de acesso.

Recomendamos registrar a localização padrão (`s3://`) e associá-la a um perfil do IAM. A localização no caminho padrão do S3 (`s3://`) abrange o acesso a todos os seus buckets do S3 na Região da AWS da sua conta. Ao criar uma concessão de acesso, é possível restringir o escopo da concessão a um bucket, um prefixo ou um objeto dentro da localização padrão.

Casos de uso de gerenciamento de acesso mais complexos podem exigir que você registre mais do que a localização padrão. Alguns exemplos desses casos de uso são:

- Suponha que *`amzn-s3-demo-bucket`* seja uma localização registrada em sua instância do recurso Concessão de Acesso do S3 com um perfil do IAM associado a ela, mas esse perfil do IAM tenha acesso negado a um prefixo específico no bucket. Nesse caso, é possível registrar o prefixo ao qual o perfil do IAM não tem acesso como uma localização separada e associar essa localização a um perfil do IAM diferente com o acesso necessário.
- Suponha que você queira criar concessões que restrinjam o acesso apenas aos usuários em um endpoint de nuvem privada virtual (VPC). Nesse caso, é possível registrar uma localização para um bucket no qual o perfil do IAM restringe o acesso ao endpoint da VPC. Posteriormente, quando um beneficiário solicita credenciais ao recurso Concessão de Acesso do S3, ele assume o perfil do IAM da localização para distribuir credenciais temporárias. Essa credencial negará acesso ao bucket específico, a menos que o chamador esteja dentro do endpoint da VPC. Essa permissão de negação é aplicada além da permissão READ, WRITE ou READWRITE normal especificada na concessão.

Se seu caso de uso exigir que você registre várias localizações em sua instância do recurso Concessão de Acesso do S3, você poderá registrar qualquer um dos seguintes:

- A localização padrão do S3 (`s3://`)
- Um bucket (por exemplo, *`amzn-s3-demo-bucket`*) ou vários buckets.
- Um bucket e um prefixo (por exemplo, *`amzn-s3-demo-bucket`*`/prefix*`) ou vários prefixos.

Para ter o número máximo de localizações que você pode registrar na instância do recurso Concessão de Acesso do S3, consulte Limitações da funcionalidade Concessões de Acesso do S3. Para ter mais informações sobre o registro de uma localização do recurso Concessão de Acesso do S3, consulte Registrar um local.

Depois de registrar a primeira localização na sua instância do recurso Concessão de Acesso do S3, ela ainda não terá nenhuma concessão de acesso individual. Portanto, nenhum acesso foi

concedido ainda a nenhum dos seus dados do S3. Agora é possível criar concessões de acesso para conceder acesso. Para ter mais informações sobre a criação de concessões, consulte Trabalhar com concessões no recurso Concessão de Acesso do S3.

Concessões

Uma concessão individual em uma instância do recurso Concessão de Acesso do S3 permite que uma identidade específica, ou seja, uma entidade principal do IAM ou um usuário ou grupo em um diretório corporativo, acesse uma localização registrada na instância do recurso Concessão de Acesso do S3.

Ao criar uma concessão, não é necessário conceder acesso a toda a localização registrada. É possível restringir o escopo de acesso da concessão em uma localização. Se a localização registrada for o caminho padrão do S3 (`s3://`), você deverá restringir o escopo da concessão a um bucket, um prefixo dentro de um bucket ou um objeto específico. Se a localização registrada da concessão for um bucket ou um prefixo, você poderá conceder acesso a todo o bucket ou ao prefixo ou, opcionalmente, restringir o escopo da concessão a um prefixo, um subprefixo ou um objeto.

Na concessão, também é possível definir o nível de acesso da concessão como READ, WRITE ou READWRITE. Suponha que você tenha uma concessão que dê ao grupo de diretórios corporativos acesso READ `01234567-89ab-cdef-0123-456789abcdef` ao bucket `s3://`*`amzn-s3-demo-bucket`*`/projects/items/*`. Os usuários desse grupo podem ter acesso READ a cada objeto que tenha um nome de chave de objeto que comece com o prefixo `projects/items/` no bucket denominado *`amzn-s3-demo-bucket`*.

Para ter o número máximo de concessões que você pode criar na instância do recurso Concessão de Acesso do S3, consulte Limitações da funcionalidade Concessões de Acesso do S3. Para ter mais informações sobre a criação de concessões, consulte Criar concessões.

Credenciais temporárias da funcionalidade Concessões de Acesso do S3

Depois de criar uma concessão, uma aplicação autorizada que utilize a identidade especificada na concessão pode solicitar credenciais de acesso just-in-time. Para fazer isso, a aplicação chama a operação da API GetDataAccess do S3. Os beneficiários podem usar essa operação da API para solicitar acesso aos dados do S3 que você compartilhou com eles.

A instância da funcionalidade Concessões de Acesso do S3 avalia a solicitação `GetDataAccess` em relação às concessões que ela tem. Se houver uma concessão correspondente, o recurso Concessão de Acesso do S3 assumirá o perfil do IAM associado à localização da concessão

correspondente. O recurso Concessão de Acesso do S3 define o escopo das credenciais temporárias para acessar apenas o bucket, o perfil ou o objeto do S3 especificado pelo escopo da concessão.

O tempo de expiração das credenciais temporárias de acesso é padronizado em 1 hora, mas você pode configurá-lo para qualquer valor entre 15 minutos a 12 horas. Veja a duração máxima da sessão na referência da API AssumeRole.

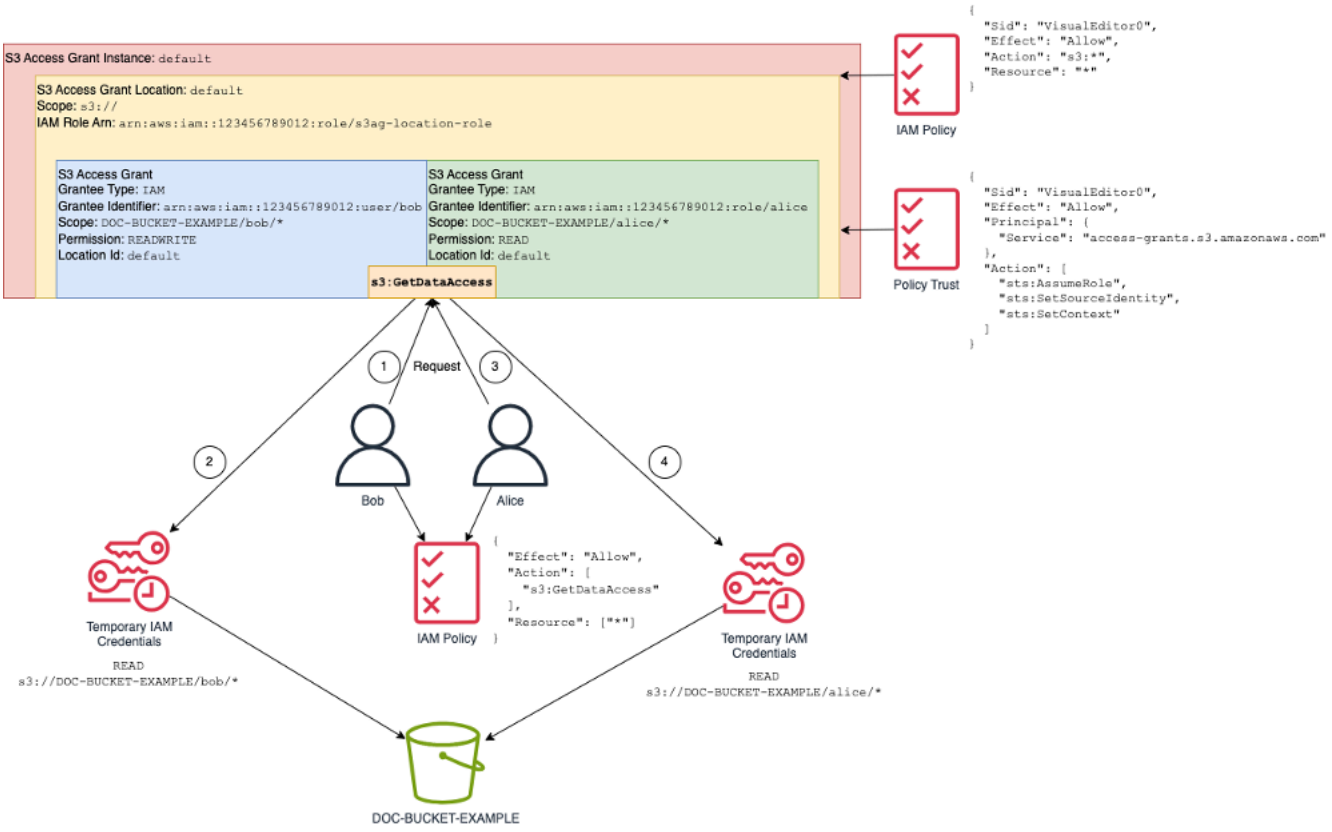
Como funciona

No diagrama a seguir, um local padrão do Amazon S3 com o escopo `s3://` é registrado com o perfil do IAM `s3ag-location-role`. Esse perfil do IAM tem permissões para realizar ações do Amazon S3 dentro da conta quando suas credenciais são obtidas por meio da funcionalidade Concessões de Acesso do S3.

Nesse local, duas concessões de acesso individuais são criadas para dois usuários do IAM. O usuário do IAM Bob recebe acesso `READ` e `WRITE` ao prefixo `bob/` no bucket `DOC-BUCKET-EXAMPLE`. Outro perfil do IAM, Alice, só recebe acesso `READ` ao prefixo `alice/` no bucket `DOC-BUCKET-EXAMPLE`. Uma concessão, mostrada em azul, é definida para que Bob acesse o prefixo `bob/` no bucket `DOC-BUCKET-EXAMPLE`. Uma concessão, mostrada em verde, é definida para que Alice acesse o prefixo `alice/` no bucket `DOC-BUCKET-EXAMPLE`.

Quando chega a hora de Bob coletar dados de `READ`, o perfil do IAM associado ao local em que sua concessão está chama a operação de API GetDataAccess da funcionalidade Concessões de Acesso do S3. Se Bob tentar usar `READ` em qualquer prefixo ou objeto do S3 que comece com `s3://DOC-BUCKET-EXAMPLE/bob/*`, a solicitação `GetDataAccess` retornará um conjunto de credenciais de sessão temporária do IAM com permissão para `s3://DOC-BUCKET-EXAMPLE/bob/*`. Da mesma forma, Bob pode usar `WRITE` em qualquer prefixo ou objeto do S3 que comece com `s3://DOC-BUCKET-EXAMPLE/bob/*`, porque a concessão também permite isso.

Da mesma forma, Alice pode usar `READ` em qualquer coisa que comece com `s3://DOC-BUCKET-EXAMPLE/alice/`. No entanto, se ela tentar usar `WRITE` em qualquer bucket, prefixo ou objeto em `s3://`, receberá um erro de Acesso negado (403 Forbidden), pois não há nenhuma concessão que lhe dê acesso `WRITE` a nenhum dado. Além disso, se Alice solicitar qualquer nível de acesso (`READ` ou `WRITE`) a dados fora de `s3://DOC-BUCKET-EXAMPLE/alice/`, ela receberá novamente um erro de Acesso negado.



Esse padrão se expande para um grande número de usuários e buckets e simplifica o gerenciamento dessas permissões. Em vez de editar políticas potencialmente grandes de bucket do S3 toda vez que quiser adicionar ou remover uma relação individual de acesso entre prefixo e usuário, você pode adicionar e remover concessões individuais e discretas.

Concessões de Acesso do S3 e identidades de diretórios corporativos

Você pode usar a funcionalidade Concessões de Acesso do Amazon S3 para conceder acesso às entidades principais do AWS Identity and Access Management (IAM) (usuários ou perfis), tanto na mesma Conta da AWS quanto em outras. No entanto, em muitos casos, a entidade que acessa os dados é um usuário final de um diretório corporativo. Em vez de conceder acesso às entidades principais do IAM, você pode usar a funcionalidade Concessões de Acesso do S3 para conceder acesso diretamente aos usuários e grupos corporativos. Com a funcionalidade Concessões de Acesso do S3, você não precisa mais mapear as identidades corporativas para entidades principais intermediárias do IAM a fim de acessar os dados do S3 por meio de aplicações corporativas.

Essa nova funcionalidade de suporte ao uso de identidades de usuário final para acessar dados é fornecida pela associação de uma instância da funcionalidade Concessões de Acesso do S3 a uma instância do AWS IAM Identity Center. O Centro de Identidade do IAM oferece suporte a

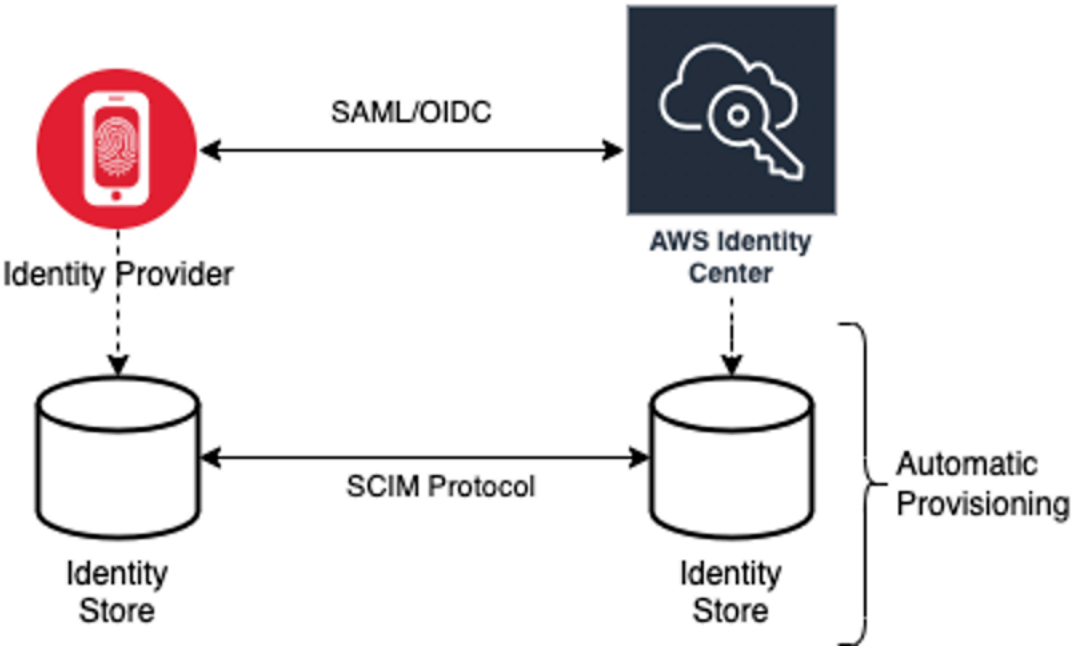
provedores de identidades baseados em padrões e é o centro de todos os serviços ou recursos na AWS, incluindo a funcionalidade Concessões de Acesso do S3, que oferecem suporte a identidades de usuário final. O Centro de Identidade do IAM oferece suporte de autenticação para identidades corporativas por meio de seu recurso de propagação de identidades confiáveis. Para obter mais informações, consulte Trusted identity propagation across applications.

Para começar a usar o suporte a identidades da força de trabalho na funcionalidade Concessões de Acesso do S3, como pré-requisito, comece no Centro de Identidade do IAM, configurando o provisionamento de identidades entre um provedor de identidades corporativas e o Centro de Identidade do IAM. O Centro de Identidade do IAM oferece suporte a provedores de identidades corporativas, como Okta, Microsoft Entra ID (antes chamado de Azure Active Directory) ou qualquer outro provedor de identidades (IdP) externo que ofereça suporte ao protocolo SCIM (Sistema de Gerenciamento de Usuários entre Domínios). Quando você conecta o Centro de Identidade do IAM ao IdP e habilita o provisionamento automático, os usuários e grupos do IdP são sincronizados no repositório de identidades do Centro de Identidade do IAM. Após essa etapa, o Centro de Identidade do IAM tem uma visão própria dos usuários e grupos, para que você possa consultá-los usando outros recurso e Serviços da AWS, como a funcionalidade Concessões de Acesso do S3. Para obter mais informações sobre como configurar o provisionamento automático do Centro de Identidade do IAM, consulte Automatic provisioning no Guia do usuário do AWS IAM Identity Center.

O Centro de Identidade do IAM é integrado com o AWS Organizations, o que permite que você gerencie centralmente as permissões em várias Contas da AWS sem configurar cada uma das contas manualmente. Em uma organização típica, o administrador de identidades configura uma instância do Centro de Identidade do IAM para toda a organização, como um único ponto de sincronização de identidades. Essa instância do Centro de Identidade do IAM normalmente é executada em uma Conta da AWS dedicada na organização. Nessa configuração comum, você pode se referir às identidades de usuários e grupos na funcionalidade Concessões de Acesso do S3 de qualquer Conta da AWS na organização.

No entanto, se o administrador do AWS Organizations ainda não configurou uma instância central do Centro de Identidade do IAM, você pode criar uma local na mesma conta da instância da funcionalidade Concessões de Acesso do S3. Essa configuração é mais comum para casos de uso de prova de conceito ou desenvolvimento local. Em todos os casos, a instância do Centro de Identidade do IAM deve estar na mesma Região da AWS que a instância da funcionalidade Concessões de Acesso do S3 à qual será associada.

No diagrama a seguir de uma configuração do Centro de Identidade do IAM com um IdP externo, o IdP é configurado com SCIM para sincronizar o repositório de identidades do IdP com o repositório de identidades no Centro de Identidade do IAM.



Para usar as identidades de diretório corporativo com a funcionalidade Concessões de Acesso do S3, faça o seguinte:

- Configure o provisionamento automático no Centro de Identidade do IAM para sincronizar as informações de usuários e grupos do seu IdP no Centro de Identidade do IAM.
- Configure a fonte de identidades externa no Centro de Identidade do IAM como um emissor de token confiável. Para obter mais informações, consulte Trusted identity propagation across applications no Guia do usuário do AWS IAM Identity Center.
- Associe a instância da funcionalidade Concessões de Acesso do S3 à instância do Centro de Identidade do IAM. Você pode fazer isso ao criar a instância da funcionalidade Concessões de Acesso do S3. Se você já criou a instância da funcionalidade Concessões de Acesso do S3, consulte Associar ou desassociar uma instância do Centro de Identidade do IAM.

Como as identidades do diretório podem acessar os dados do S3

Suponha que você tenha usuários do diretório corporativo que precisem acessar os dados do S3 por meio de uma aplicação corporativa, por exemplo, uma aplicação de visualização de documentos, integrada ao IdP externo (por exemplo, Okta) para autenticar usuários. A autenticação do usuário nessas aplicações geralmente é feita por meio de redirecionamentos no navegador da web do

usuário. Como os usuários no diretório não são entidades principais do IAM, a aplicação precisa de credenciais do IAM com as quais possa chamar a operação de API `GetDataAccess` da funcionalidade Concessões de Acesso do S3 para obter credenciais de acesso aos dados do S3 em nome dos usuários. Ao contrário dos usuários e perfis do IAM que recebem credenciais diretamente, a aplicação precisa de uma forma de representar um usuário do diretório, que não está mapeado para um perfil do IAM, para que o usuário possa obter acesso aos dados por meio da funcionalidade Concessões de Acesso do S3.

Essa transição, de usuário de diretório autenticado para um chamador do IAM que pode fazer solicitações à funcionalidade Concessões de Acesso do S3 em nome do usuário do diretório, é feita pela aplicação por meio do recurso de emissor de token confiável do Centro de Identidade do IAM. Depois de autenticar o usuário do diretório, a aplicação tem um token de identidade do IdP (por exemplo, Okta) que representa o usuário do diretório de acordo com Okta. A configuração do emissor de token confiável no Centro de Identidade do IAM permite que a aplicação troque esse token do Okta (o locatário do Okta é configurado como o “emissor confiável”) por outro token de identidade do Centro de Identidade do IAM que representará com segurança o usuário do diretório em Serviços da AWS. A aplicação de dados assumirá um perfil do IAM, fornecendo o token de usuário do diretório do Centro de Identidade do IAM como contexto adicional. A aplicação pode usar a sessão do IAM resultante para chamar a funcionalidade Concessões de Acesso do S3. O token representa tanto a identidade da aplicação (a própria entidade principal do IAM) quanto a identidade do usuário do diretório.

A principal etapa dessa transição é a troca de tokens. A aplicação realiza essa troca de tokens chamando a operação de API `CreateTokenWithIAM` no Centro de Identidade do IAM. É evidente que isso também é uma chamada de API da AWS e requer que uma entidade principal do IAM a assine. A entidade principal do IAM que faz essa solicitação geralmente é um perfil do IAM associado à aplicação. Por exemplo, se a aplicação é executada no Amazon EC2, a solicitação `CreateTokenWithIAM` normalmente é executada pelo perfil do IAM associado à instância do EC2 na qual a aplicação é executada. O resultado de uma chamada `CreateTokenWithIAM` bem-sucedida é um novo token de identidade, que será reconhecido em Serviços da AWS.

A próxima etapa, antes que a aplicação possa chamar `GetDataAccess` em nome do usuário do diretório, é que a aplicação obtenha uma sessão do IAM que inclua a identidade do usuário do diretório. A aplicação faz isso com uma solicitação `AssumeRole` do AWS Security Token Service (AWS STS) que também inclui o token do Centro de Identidade do IAM para o usuário do diretório como contexto de identidade adicional. Esse contexto adicional é o que permite que o Centro de Identidade do IAM propague a identidade do usuário do diretório para a próxima etapa. O perfil do

IAM que a aplicação assume é o perfil que precisará de permissões do IAM para chamar a operação `GetDataAccess`.

Tendo assumido o perfil do IAM do portador da identidade com o token do Centro de Identidade do IAM para o usuário do diretório como contexto adicional, a aplicação agora tem tudo o que precisa para fazer uma solicitação `GetDataAccess` assinada em nome do usuário do diretório autenticado.

A propagação do token se baseia nas seguintes etapas:

Criar uma aplicação do Centro de Identidade do IAM

Primeiro, crie uma aplicação no Centro de Identidade do IAM. Essa aplicação usará um modelo que permite que o Centro de Identidade do IAM identifique quais tipos de configurações de aplicação você pode usar. O comando para criar a aplicação exige que você forneça o nome do recurso da Amazon (ARN) da instância do Centro de Identidade do IAM, um nome de aplicação e o ARN do provedor de aplicações. O provedor de aplicações é o provedor SAML ou OAuth que a aplicação usará para fazer chamadas ao Centro de Identidade do IAM.

Para usar o comando a seguir, substitua os *`user input placeholders`* por suas próprias informações:

```
aws sso-admin create-application \
 --instance-arn "arn:aws:sso:::instance/ssoins-ssoins-1234567890abcdef" \
 --application-provider-arn "arn:aws:sso::aws:applicationProvider/custom" \
 --name MyDataApplication
```

Resposta:

```
{
   "ApplicationArn": "arn:aws:sso::123456789012:application/ssoins-
ssoins-1234567890abcdef/apl-abcd1234a1b2c3d"
}
```

Criar um emissor de token confiável

Agora que você tem uma aplicação do Centro de Identidade do IAM, a próxima etapa é configurar um emissor de token confiável que será usado para trocar os valores de `IdToken` do IdP por tokens do Centro de Identidade do IAM. Nesta etapa, você precisa fornecer os seguintes itens:

- O URL do emissor do provedor de identidades
- O nome do emissor de token confiável

- O caminho do atributo de reivindicação
- O caminho do atributo do repositório de identidades
- A opção de recuperação do JSON Web Key Set (JWKS)

O caminho do atributo de reivindicação é o atributo do provedor de identidades que será usado para mapear o atributo do repositório de identidades. Normalmente, o caminho do atributo de reivindicação é o endereço de e-mail do usuário, mas você pode usar outros atributos para realizar o mapeamento.

Crie um arquivo chamado `oidc-configuration.json` com o texto a seguir. Para usar esse arquivo, substitua os *`user input placeholders`* por suas próprias informações.

```
{
  "OidcJwtConfiguration":
     {
      "IssuerUrl": "https://login.microsoftonline.com/a1b2c3d4-abcd-1234-b7d5-
b154440ac123/v2.0",
      "ClaimAttributePath": "preferred_username",
      "IdentityStoreAttributePath": "userName",
      "JwksRetrievalOption": "OPEN_ID_DISCOVERY"
     }
}
```

Para criar o emissor de token confiável, execute o comando a seguir. Para usar esse exemplo de comando, substitua os *`user input placeholders`* por suas próprias informações.

```
aws sso-admin create-trusted-token-issuer \
  --instance-arn "arn:aws:sso:::instance/ssoins-1234567890abcdef" \
  --name MyEntraIDTrustedIssuer \
  --trusted-token-issuer-type OIDC_JWT \
  --trusted-token-issuer-configuration file://./oidc-configuration.json
```

Resposta

```
{
  "TrustedTokenIssuerArn": "arn:aws:sso::123456789012:trustedTokenIssuer/
ssoins-1234567890abcdef/tti-43b4a822-1234-1234-1234-a1b2c3d41234"
}
```

Conectar a aplicação do Centro de Identidade do IAM ao emissor de token confiável

O emissor de token confiável precisa de mais algumas configurações para funcionar. Defina o público em que o emissor de token confiável confiará. O público é o valor dentro do `IdToken` que é identificado pela chave e pode ser encontrado nas configurações do provedor de identidades. Por exemplo:

```
1234973b-abcd-1234-abcd-345c5a9c1234
```

Crie um arquivo chamado `grant.json` com o conteúdo a seguir. Para usar esse arquivo, altere o público para que corresponda às configurações do seu provedor de identidades e forneça o ARN do emissor de token confiável que foi retornado pelo comando anterior.

```
{
   "JwtBearer":
     {
       "AuthorizedTokenIssuers":
         [
           {
             "TrustedTokenIssuerArn": "arn:aws:sso::123456789012:trustedTokenIssuer/
ssoins-1234567890abcdef/tti-43b4a822-1234-1234-1234-a1b2c3d41234",
               "AuthorizedAudiences":
                 [
                   "1234973b-abcd-1234-abcd-345c5a9c1234"
                 ]
            }
         ]
     }
 }
```

Execute o exemplo de comando a seguir. Para usar esse comando, substitua *`user input placeholders`* por suas informações.

```
aws sso-admin put-application-grant \
  --application-arn "arn:aws:sso::123456789012:application/ssoins-
ssoins-1234567890abcdef/apl-abcd1234a1b2c3d" \
  --grant-type "urn:ietf:params:oauth:grant-type:jwt-bearer" \
  --grant file://./grant.json \
```

Esse comando define o emissor de token confiável com configurações para confiar no público do arquivo `grant.json` e vincular esse público à aplicação criada na primeira etapa para a troca de tokens do tipo `jwt-bearer`. A string `urn:ietf:params:oauth:grant-type:jwt-bearer` não

é uma string arbitrária. É um namespace registrado nos perfis de declaração de JSON Web Token (JWT) OAuth. Você pode encontrar mais informações sobre esse namespace em RFC 7523.

Depois, use o comando a seguir para configurar quais escopos o emissor de token confiável incluirá ao trocar valores de `IdToken` do seu provedor de identidades. Para a funcionalidade Concessões de Acesso do S3, o valor do parâmetro `--scope` é `s3:access_grants:read_write`.

```
aws sso-admin put-application-access-scope \
  --application-arn "arn:aws:sso::111122223333:application/ssoins-
ssoins-111122223333abcdef/apl-abcd1234a1b2c3d" \
  --scope "s3:access_grants:read_write"
```

A última etapa é anexar uma política de recursos à aplicação do Centro de Identidade do IAM. Essa política permitirá que o perfil do IAM da aplicação faça solicitações para a operação de API `sso-oauth:CreateTokenWithIAM` e receba os valores de `IdToken` do Centro de Identidade do IAM.

Crie um arquivo chamado `authentication-method.json` com o conteúdo a seguir. Substitua *123456789012* pelo ID da sua conta.

```
{
   "Iam":
       {
         "ActorPolicy":
             {
                "Version": "2012-10-17",
                    "Statement":
                    [
                        {
                           "Effect": "Allow",
                            "Principal":
                            {
                              "AWS": "arn:aws:iam::123456789012:role/webapp"
                            },
                           "Action": "sso-oauth:CreateTokenWithIAM",
                            "Resource": "*"
                        }
                    ]
                }
            }
        }
```

Para anexar a política à aplicação do Centro de Identidade do IAM, execute o seguinte comando:

```
aws sso-admin put-application-authentication-method \
   --application-arn "arn:aws:sso::123456789012:application/ssoins-
ssoins-1234567890abcdef/apl-abcd1234a1b2c3d" \
   --authentication-method-type IAM \
   --authentication-method file://./authentication-method.json
```

Isso conclui as configurações para usar a funcionalidade Concessões de Acesso do S3 com usuários de diretório por meio de uma aplicação web. Você pode testar essa configuração diretamente na aplicação ou chamar a operação de API `CreateTokenWithIAM` usando o seguinte comando de um perfil do IAM permitido na política da aplicação do Centro de Identidade do IAM:

```
aws sso-oidc create-token-with-iam \
   --client-id "arn:aws:sso::123456789012:application/ssoins-ssoins-1234567890abcdef/
apl-abcd1234a1b2c3d"  \
   --grant-type urn:ietf:params:oauth:grant-type:jwt-bearer \
   --assertion IdToken
```

A resposta será semelhante a esta:

```
{
    "accessToken": "<suppressed long string to reduce space>",
    "tokenType": "Bearer",
    "expiresIn": 3600,
    "refreshToken": "<suppressed long string to reduce space>",
    "idToken": "<suppressed long string to reduce space>",
    "issuedTokenType": "urn:ietf:params:oauth:token-type:refresh_token",
    "scope": [
      "sts:identity_context",
      "s3:access_grants:read_write",
      "openid",
      "aws"
    ]
}
```

Se você decodificar o valor de `IdToken` que está codificado com base64, poderá ver os pares de valor e chave no formato JSON. A chave `sts:identity_context` contém o valor que a aplicação precisa enviar na solicitação `sts:AssumeRole` para incluir as informações de identidade do usuário do diretório. Veja a seguir um exemplo do `IdToken` decodificado:

```
{
    "aws:identity_store_id": "d-996773e796",
```

```
    "sts:identity_context": "AQoJb3JpZ2luX2VjEOTtl;<SUPRESSED>",
    "sub": "83d43802-00b1-7054-db02-f1d683aacba5",
    "aws:instance_account": "123456789012",
    "iss": "https://identitycenter.amazonaws.com/ssoins-1234567890abcdef",
    "sts:audit_context": "AQoJb3JpZ2luX2VjEOT<SUPRESSED>==",
    "aws:identity_store_arn": "arn:aws:identitystore::232642235904:identitystore/
d-996773e796",
    "aud": "abcd12344U0gi7n4Yyp0-WV1LWNlbnRyYWwtMQ",
    "aws:instance_arn": "arn:aws:sso:::instance/ssoins-6987d7fb04cf7a51",
    "aws:credential_id": "EXAMPLEHI5glPh40y9TpApJn8...",
    "act": {
       "sub": "arn:aws:sso::232642235904:trustedTokenIssuer/
ssoins-6987d7fb04cf7a51/43b4a822-1020-7053-3631-cb2d3e28d10e"
    },
    "auth_time": "2023-11-01T20:24:28Z",
    "exp": 1698873868,
    "iat": 1698870268
}
```

Você pode obter o valor de `sts:identity_context` e enviar essas informações em uma chamada de `sts:AssumeRole`. Veja a seguir um exemplo da sintaxe na CLI. O perfil a ser assumido é um perfil temporário com permissões para invocar `s3:GetDataAccess`.

```
aws sts assume-role \
   --role-arn "arn:aws:iam::123456789012:role/temp-role" \
   --role-session-name "TempDirectoryUserRole" \
   --provided-contexts ProviderArn="arn:aws:iam::aws:contextProvider/
IdentityCenter",ContextAssertion="value from sts:identity_context"
```

Agora você pode usar as credenciais recebidas dessa chamada para invocar a operação de API `s3:GetDataAccess` e receber as credenciais finais com acesso aos recursos do S3.

Conceitos básicos da funcionalidade Concessões de Acesso do S3

A funcionalidade Concessões de Acesso do Amazon S3 é um recurso do Amazon S3 que fornece uma solução de controle de acesso escalável para os dados do S3. A funcionalidade Concessões de Acesso do S3 é um provedor de credenciais do S3, o que significa que você registra sua lista de concessões e respectivo nível na funcionalidade Concessões de Acesso do S3. Depois disso, quando os usuários ou clientes precisam acessar dados do S3, primeiro eles solicitam as credenciais à funcionalidade Concessões de Acesso do S3. Se houver uma concessão correspondente que autorize o acesso, a funcionalidade Concessões de Acesso do S3 proverá credenciais de acesso

temporário com privilégio mínimo. Os usuários ou clientes podem usar as credenciais providas pela funcionalidade Concessões de Acesso do S3 para acessar dados do S3. Com isso em mente, se seus requisitos de dados do S3 exigirem uma configuração de permissão complexa ou grande, você poderá usar a funcionalidade Concessões de Acesso do S3 para escalar as permissões de dados do S3 para usuários, grupos, perfis e aplicações.

Para a maioria dos casos de uso, você pode gerenciar o controle de acesso aos dados do S3 usando o AWS Identity and Access Management (IAM) com políticas de bucket ou políticas baseadas em identidade do IAM.

No entanto, se você tiver requisitos complexos de controle de acesso ao S3, como os seguintes, o uso da funcionalidade Concessões de Acesso do S3 poderá ser muito vantajoso:

- Você está atingindo o limite de tamanho da política de bucket de 20 KB.
- Você concede a identidades humanas, por exemplo, usuários e grupos do Microsoft Entra ID (antes chamado de Azure Active Directory), Okta ou Ping, acesso aos dados do S3 para análises e big data.
- Você precisa fornecer acesso entre contas sem fazer atualizações frequentes nas políticas do IAM.
- Seus dados são não estruturados e estão em nível de objeto, em vez de estruturados e em formato de linha e coluna.

O fluxo de trabalho da funcionalidade Concessões de Acesso do S3 é o seguinte:

Etapas	Descrição
1	Criar uma instância da funcionalidade Concessões de Acesso do S3 Para começar, inicie uma instância da funcionalidade Concessões de Acesso do S3 que conterá as concessões de acesso individuais.
2	Registrar um local Depois, registre um local de dados do S3 (como o padrão `s3://`) e especifique um perfil do IAM padrão que a funcional idade Concessões de Acesso do S3 assumirá ao fornecer acesso ao local de dados do S3. Você também pode adicionar

Etapas	Descrição
	locais personalizados a buckets ou prefixos específicos e mapeá-los para perfis do IAM personalizados.
3	Criar concessões Crie concessões de permissão individuais. Especifique nessas concessões de permissão o local registrado do S3, o escopo de acesso aos dados dentro do local, a identidade do beneficiário e o nível de acesso (`READ`, `WRITE` ou `READWRITE`).
4	Solicitar acesso aos dados do S3 Quando usuários, aplicações e Serviços da AWS desejam acessar dados do S3, primeiro eles fazem uma solicitação de acesso. A funcionalidade Concessões de Acesso do S3 determina se a solicitação deve ser autorizada. Se houver uma concessão correspondente que autorize o acesso, a funcional idade Concessões de Acesso do S3 usará o perfil do IAM do local registrado associado a essa concessão para prover credenciais temporárias ao solicitante.
5	Acessar dados do S3 As aplicações usam as credenciais temporárias fornecidas pela funcionalidade Concessões de Acesso do S3 para acessar os dados do S3.

Trabalhar com instâncias do recurso Concessão de Acesso do S3

Para começar a usar a funcionalidade Concessões de Acesso do Amazon S3, comece criando uma instância da funcionalidade Concessões de Acesso do S3. Você só pode criar uma instância da funcionalidade Concessões de Acesso do S3 por Região da AWS por conta. A instância da funcionalidade Concessões de Acesso do S3 serve como contêiner para as funcionalidades desse recurso, que incluem locais registrados e concessões.

Com a funcionalidade Concessões de Acesso do S3, você pode criar concessões de permissão para os dados do S3 para usuários e perfis do AWS Identity and Access Management (IAM). Se

você adicionou seu diretório de identidades corporativas ao AWS IAM Identity Center, poderá associar essa instância do Centro de Identidade do IAM do seu diretório corporativo à instância da funcionalidade Concessões de Acesso do S3. Depois de fazer isso, você poderá criar concessões de acesso para os usuários e grupos corporativos. Se você ainda não adicionou seu diretório de identidades corporativas ao Centro de Identidade do IAM, poderá associar a instância da funcionalidade Concessões de Acesso do S3 a uma instância do Centro de Identidade do IAM posteriormente.

Tópicos

- Criar uma instância da funcionalidade Concessões de Acesso do S3
- Obter os detalhes de uma instância do recurso Concessão de Acesso do S3
- Listar instâncias do recurso Concessão de Acesso do S3
- Associar ou desassociar uma instância do Centro de Identidade do IAM
- Excluir uma instância da funcionalidade Concessões de Acesso do S3

Criar uma instância da funcionalidade Concessões de Acesso do S3

Para começar a usar a funcionalidade Concessões de Acesso do Amazon S3, comece criando uma instância da funcionalidade Concessões de Acesso do S3. Você só pode criar uma instância da funcionalidade Concessões de Acesso do S3 por Região da AWS por conta. A instância da funcionalidade Concessões de Acesso do S3 serve como contêiner para as funcionalidades desse recurso, que incluem locais registrados e concessões.

Com a funcionalidade Concessões de Acesso do S3, você pode criar concessões de permissão para os dados do S3 para usuários e perfis do AWS Identity and Access Management (IAM). Se você adicionou seu diretório de identidades corporativas ao AWS IAM Identity Center, poderá associar essa instância do Centro de Identidade do IAM do seu diretório corporativo à instância da funcionalidade Concessões de Acesso do S3. Depois de fazer isso, você poderá criar concessões de acesso para os usuários e grupos corporativos. Se você ainda não adicionou seu diretório de identidades corporativas ao Centro de Identidade do IAM, poderá associar a instância da funcionalidade Concessões de Acesso do S3 a uma instância do Centro de Identidade do IAM posteriormente.

Você pode criar uma instância da funcionalidade Concessões de Acesso do S3 usando o console do Amazon S3, a AWS Command Line Interface (AWS CLI), AWS SDKs ou a API REST do Amazon S3.

Usar o console do S3

Antes de conceder acesso aos dados do S3 com a funcionalidade Concessões de Acesso do S3, primeiro é necessário criar uma instância da funcionalidade Concessões de Acesso do S3 na mesma Região da AWS dos dados do S3.

Pré-requisitos

Se você quiser conceder acesso aos dados do S3 usando identidades de um diretório corporativo, adicione o diretório de identidades corporativas ao AWS IAM Identity Center. Se você ainda não estiver com tudo pronto para fazer isso, poderá associar a instância da funcionalidade Concessões de Acesso do S3 a uma instância do Centro de Identidade do IAM posteriormente.

Como criar uma instância da funcionalidade Concessões de Acesso do S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Na barra de navegação, escolha o nome da Região da AWS exibida no momento. Em seguida, escolha a região para a qual você deseja mudar.
3. No painel de navegação, escolha Access Grants.
4. Na página Concessões de Acesso do S3, escolha Criar instância da funcionalidade Concessões de Acesso do S3.

    a. Na Etapa 1 do assistente Configurar instância do Access Grants, verifique se você deseja criar a instância na Região da AWS atual. Garanta que seja a mesma Região da AWS em que os dados do S3 estão localizados. Você pode criar uma instância da funcionalidade Concessões de Acesso do S3 por Região da AWS por conta.

    b. (Opcional) Se você adicionou seu diretório de identidades corporativas ao AWS IAM Identity Center, poderá associar essa instância do Centro de Identidade do IAM do seu diretório corporativo à instância da funcionalidade Concessões de Acesso do S3.

        Para fazer isso, selecione Adicionar instância do Centro de Identidade do IAM em ***região***. Depois, insira o nome do recurso da Amazon (ARN) da instância do Centro de Identidade do IAM.

        Se você ainda não adicionou seu diretório de identidades corporativas ao Centro de Identidade do IAM, poderá associar a instância da funcionalidade Concessões de Acesso do S3 a uma instância do Centro de Identidade do IAM posteriormente.

c. Para criar a instância da funcionalidade Concessões de Acesso do S3, escolha Próximo. Para registrar um local, consulte Etapa 2: Registrar um local.

5. Se as opções Próximo ou Criar instância da funcionalidade Concessões de Acesso do S3 estiverem desabilitadas:

   Não é possível criar a instância

   - Talvez você já tenha uma instância da funcionalidade Concessões de Acesso do S3 na mesma Região da AWS. No painel de navegação, escolha Access Grants. Na página Concessões de Acesso do S3, role para baixo até a seção Instância da funcionalidade Concessões de Acesso do S3 em sua conta para determinar se já existe uma instância.
   - Talvez você não tenha a permissão `s3:CreateAccessGrantsInstance` necessária para criar uma instância da funcionalidade Concessões de Acesso do S3. Entre em contato com o administrador da conta. Para conferir as permissões adicionais que são necessárias ao associar uma instância do Centro de Identidade do IAM a uma instância da funcionalidade Concessões de Acesso do S3, consulte CreateAccessGrantsInstance.

Como usar o AWS CLI

Para instalar a AWS CLI, consulte Instalar a AWS CLI no Guia do usuário da AWS Command Line Interface.

Para usar o comando a seguir, substitua os *`user input placeholders`* por suas próprias informações.

Example Criar uma instância da funcionalidade Concessões de Acesso do S3

```
aws s3control create-access-grants-instance \
--account-id 111122223333 \
--region us-east-2
```

Resposta:

```
{
    "CreatedAt": "2023-05-31T17:54:07.893000+00:00",
    "AccessGrantsInstanceId": "default",
    "AccessGrantsInstanceArn": "arn:aws:s3:us-east-2:111122223333:access-grants/
default"
```

```
}
```

Uso da API REST

Você pode usar a API REST do Amazon S3 para criar uma instância da funcionalidade Concessões de Acesso do S3. Para obter informações sobre o suporte à API REST para gerenciar instâncias da funcionalidade Concessões de Acesso do S3, consulte as seguintes seções na Referência da API do Amazon Simple Storage Service:

- AssociateAccessGrantsIdentityCenter
- CreateAccessGrantsInstance
- DeleteAccessGrantsInstance
- DissociateAccessGrantsIdentityCenter
- GetAccessGrantsInstance
- GetAccessGrantsInstanceForPrefix
- GetAccessGrantsInstanceResourcePolicy
- ListAccessGrantsInstances
- PutAccessGrantsInstanceResourcePolicy

Uso dos SDKs da AWS

Esta seção fornece um exemplo de como criar uma instância da funcionalidade Concessões de Acesso do S3 usando os AWS SDKs.

Java

Este exemplo cria a instância da funcionalidade Concessões de Acesso do S3, que serve como um contêiner para as concessões de acesso individuais. Você pode ter uma instância da funcionalidade Concessões de Acesso do S3 por Região da AWS em sua conta. A resposta inclui o ID de instância `default` e um nome do recurso da Amazon (ARN) que é gerado para a instância da funcionalidade Concessões de Acesso do S3.

Example Criar uma solicitação de instância da funcionalidade Concessões de Acesso do S3

```
public void createAccessGrantsInstance() {
CreateAccessGrantsInstanceRequest createRequest =
 CreateAccessGrantsInstanceRequest.builder().accountId("111122223333").build();
```

```
CreateAccessGrantsInstanceResponse createResponse =
 s3Control.createAccessGrantsInstance(createRequest);LOGGER.info("CreateAccessGrantsInstance
 " + createResponse);
}
```

Resposta:

```
CreateAccessGrantsInstanceResponse(
CreatedAt=2023-06-07T01:46:20.507Z,
AccessGrantsInstanceId=default,
AccessGrantsInstanceArn=arn:aws:s3:us-east-2:111122223333:access-grants/default)
```

Obter os detalhes de uma instância do recurso Concessão de Acesso do S3

É possível obter os detalhes de uma instância do recurso Concessão de Acesso do Amazon S3 em determinada Região da AWS. É possível obter os detalhes da instância do recurso Concessão de Acesso do S3 usando o console do Amazon S3, a AWS Command Line Interface (AWS CLI), a API REST do Amazon S3 e os SDKs da AWS.

Usar o console do S3

Como obter os detalhes de uma instância do recurso Concessão de Acesso do S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação, escolha Access Grants.
3. Na página Concessões de Acesso do S3, escolha a região que contém a instância da funcionalidade Concessões de Acesso do S3 com a qual você deseja trabalhar.
4. A página Concessões de Acesso do S3 lista as instâncias da funcionalidade Concessões de Acesso do S3 e todas as instâncias entre contas que foram compartilhadas com sua conta. Para ver os detalhes de uma instância, escolha Visualizar detalhes.

Como usar o AWS CLI

Para instalar a AWS CLI, consulte Instalar a AWS CLI no Guia do usuário da AWS Command Line Interface.

Para usar o comando a seguir, substitua os *user input placeholders* por suas próprias informações.

Example : obter os detalhes de uma instância da funcionalidade Concessões de Acesso do S3

```
aws s3control get-access-grants-instance \
 --account-id 111122223333 \
 --region us-east-2
```

Resposta:

```
{
    "AccessGrantsInstanceArn": "arn:aws:s3:us-east-2: 111122223333:access-grants/
default",
    "AccessGrantsInstanceId": "default",
    "CreatedAt": "2023-05-31T17:54:07.893000+00:00"
}
```

Uso da API REST

Para obter informações sobre o suporte à API REST do Amazon S3 para gerenciar instâncias da funcionalidade Concessões de Acesso do S3, consulte as seguintes seções na Referência da API do Amazon Simple Storage Service:

- GetAccessGrantsInstance
- GetAccessGrantsInstanceForPrefix

Uso dos SDKs da AWS

Esta seção fornece exemplos de como obter os detalhes de uma instância da funcionalidade Concessões de Acesso do S3 usando os AWS SDKs.

Para usar os exemplos a seguir, substitua *user input placeholders* por suas próprias informações.

Java

Example : obter uma instância da funcionalidade Concessões de Acesso do S3

```
public void getAccessGrantsInstance() {
GetAccessGrantsInstanceRequest getRequest = GetAccessGrantsInstanceRequest.builder()
.accountId("111122223333")
.build();
```

```
GetAccessGrantsInstanceResponse getResponse =
 s3Control.getAccessGrantsInstance(getRequest);
LOGGER.info("GetAccessGrantsInstanceResponse: " + getResponse);
}
```

Resposta:

```
GetAccessGrantsInstanceResponse(
AccessGrantsInstanceArn=arn:aws:s3:us-east-2: 111122223333:access-grants/default,
CreatedAt=2023-06-07T01:46:20.507Z)
```

Listar instâncias do recurso Concessão de Acesso do S3

Você também pode listar as instâncias do recurso Concessão de Acesso do S3, incluindo as instâncias compartilhadas com você por meio do AWS Resource Access Manager (AWS RAM).

É possível listar as instâncias do recurso Concessão de Acesso do S3 usando o console do Amazon S3, a AWS Command Line Interface (AWS CLI), a API REST do Amazon S3 ou os SDKs da AWS.

Usar o console do S3

Como listar instâncias do recurso Concessão de Acesso do S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação, escolha Access Grants.
3. Na página Concessões de Acesso do S3, escolha a região que contém a instância da funcionalidade Concessões de Acesso do S3 com a qual você deseja trabalhar.
4. A página Concessões de Acesso do S3 lista as instâncias da funcionalidade Concessões de Acesso do S3 e todas as instâncias entre contas que foram compartilhadas com sua conta. Para ver os detalhes de uma instância, escolha Visualizar detalhes.

Como usar o AWS CLI

Para instalar a AWS CLI, consulte Instalar a AWS CLI no Guia do usuário da AWS Command Line Interface.

Para usar o comando a seguir, substitua os *user input placeholders* por suas próprias informações.

Example : listar todas as instâncias da funcionalidade Concessões de Acesso do S3 para uma conta

Essa ação lista as instâncias da funcionalidade Concessões de Acesso do S3 para uma conta. Você só pode ter uma instância da funcionalidade Concessões de Acesso do S3 por Região da AWS. Essa ação também lista outras instâncias da funcionalidade Concessões de Acesso do S3 entre contas às quais sua conta tem acesso.

```
aws s3control list-access-grants-instances \
 --account-id 111122223333 \
 --region us-east-2
```

Resposta:

```
{
    "AccessGrantsInstanceArn": "arn:aws:s3:us-east-2: 111122223333:access-grants/
default",
    "AccessGrantsInstanceId": "default",
    "CreatedAt": "2023-05-31T17:54:07.893000+00:00"
}
```

Uso da API REST

Para obter informações sobre o suporte à API REST do Amazon S3 para gerenciar instâncias da funcionalidade Concessões de Acesso do S3, consulte as seguintes seções na Referência da API do Amazon Simple Storage Service:

- ListAccessGrantsInstances

Uso dos SDKs da AWS

Esta seção fornece exemplos de como obter os detalhes de uma instância da funcionalidade Concessões de Acesso do S3 usando os AWS SDKs.

Para usar os exemplos a seguir, substitua *user input placeholders* por suas próprias informações.

Java

Example : listar todas as instâncias da funcionalidade Concessões de Acesso do S3 para uma conta

Essa ação lista as instâncias da funcionalidade Concessões de Acesso do S3 para uma conta. Você só pode ter uma instância da funcionalidade Concessões de Acesso do S3 por região. Essa ação também pode listar outras instâncias da funcionalidade Concessões de Acesso do S3 entre contas às quais sua conta tem acesso.

```
public void listAccessGrantsInstances() {
ListAccessGrantsInstancesRequest listRequest =
 ListAccessGrantsInstancesRequest.builder()
.accountId("111122223333")
.build();
ListAccessGrantsInstancesResponse listResponse =
 s3Control.listAccessGrantsInstances(listRequest);
LOGGER.info("ListAccessGrantsInstancesResponse: " + listResponse);
}
```

Resposta:

```
ListAccessGrantsInstancesResponse(
AccessGrantsInstancesList=[
ListAccessGrantsInstanceEntry(
AccessGrantsInstanceId=default,
AccessGrantsInstanceArn=arn:aws:s3:us-east-2:111122223333:access-grants/default,
CreatedAt=2023-06-07T04:28:11.728Z
)
]
)
```

Associar ou desassociar uma instância do Centro de Identidade do IAM

Na funcionalidade Concessões de Acesso do Amazon S3, você pode associar a instância do AWS IAM Identity Center do diretório de identidades corporativas a uma instância da funcionalidade Concessões de Acesso do S3. Depois de fazer isso, você pode criar concessões de acesso para os usuários e grupos do diretório corporativo, além de usuários e perfis do AWS Identity and Access Management (IAM).

Se você não quiser mais criar concessões de acesso para os usuários e grupos do diretório corporativo, poderá desassociar a instância do Centro de Identidade do IAM da sua instância da funcionalidade Concessões de Acesso do S3.

Você pode associar ou desassociar uma instância do Centro de Identidade do IAM usando o console do Amazon S3, a AWS Command Line Interface (AWS CLI), a API REST do Amazon S3 e AWS SDKs.

Usar o console do S3

Antes de associar uma instância do Centro de Identidade do IAM a uma instância da funcionalidade Concessões de Acesso do S3, é necessário adicionar o diretório de identidades corporativas ao Centro de Identidade do IAM. Para obter mais informações, consulte the section called “Concessões de Acesso do S3 e identidades de diretórios corporativos”.

Como associar uma instância do Centro de Identidade do IAM a uma instância da funcionalidade Concessões de Acesso do S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação, escolha Access Grants.
3. Na página Concessões de Acesso do S3, escolha a região que contém a instância da funcionalidade Concessões de Acesso do S3 com a qual você deseja trabalhar.
4. Escolha Visualizar detalhes da instância.
5. Na página de detalhes, na seção Centro de Identidade do IAM, escolha Adicionar uma instância do Centro de Identidade do IAM ou Cancelar registro de uma instância do Centro de Identidade do IAM já associada.

Como usar o AWS CLI

Para instalar a AWS CLI, consulte Instalar a AWS CLI no Guia do usuário da AWS Command Line Interface.

Para usar o comando a seguir, substitua os *`user input placeholders`* por suas próprias informações.

Example : associar uma instância do Centro de Identidade do IAM a uma instância da funcionalidade Concessões de Acesso do S3

```
aws s3control associate-access-grants-identity-center \
 --account-id 111122223333 \
 --identity-center-arn arn:aws:sso:::instance/ssoins-1234a567bb89012c \
 --profile access-grants-profile \
 --region eu-central-1

// No response body
```

Example : desassociar uma instância do Centro de Identidade do IAM de uma instância da funcionalidade Concessões de Acesso do S3

```
aws s3control dissociate-access-grants-identity-center \
 --account-id 111122223333 \
 --profile access-grants-profile \
 --region eu-central-1

// No response body
```

Uso da API REST

Para obter informações sobre o suporte à API REST do Amazon S3 para gerenciar a associação entre uma instância do Centro de Identidade do IAM e uma instância da funcionalidade Concessões de Acesso do S3, consulte as seguintes seções na Referência da API do Amazon Simple Storage Service:

- AssociateAccessGrantsIdentityCenter
- DissociateAccessGrantsIdentityCenter

Excluir uma instância da funcionalidade Concessões de Acesso do S3

Você pode excluir uma instância da funcionalidade Concessões de Acesso do Amazon S3 de uma Região da AWS em sua conta. No entanto, antes de excluir uma instância da funcionalidade Concessões de Acesso do S3, é necessário fazer o seguinte:

- Exclua todos os recursos na instância da funcionalidade Concessões de Acesso do S3, incluindo todas as concessões e locais. Para obter mais informações, consulte Delete a grant e Delete a location.

- Se você associou uma instância do AWS IAM Identity Center à sua instância da funcionalidade Concessões de Acesso do S3, deverá desassociar a instância do Centro de Identidade do IAM. Para obter mais informações, consulte Associar ou desassociar uma instância do Centro de Identidade do IAM.

> **Important**
>
> Se você excluir uma instância da funcionalidade Concessões de Acesso do S3, a exclusão será permanente e não poderá ser desfeita. Todos os beneficiários que receberam acesso por meio das concessões nessa instância da funcionalidade Concessões de Acesso do S3 perderão o acesso aos dados do S3.

Você pode excluir uma instância da funcionalidade Concessões de Acesso do S3 usando o console do Amazon S3, a AWS Command Line Interface (AWS CLI), a API REST do Amazon S3 ou os AWS SDKs.

Usar o console do S3

Como excluir uma instância da funcionalidade Concessões de Acesso do S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação, escolha Access Grants.
3. Na página Concessões de Acesso do S3, escolha a região que contém a instância da funcionalidade Concessões de Acesso do S3 com a qual você deseja trabalhar.
4. Escolha Visualizar detalhes da instância.
5. Na página de detalhes da instância, escolha Excluir instância no canto superior direito.
6. Na caixa de diálogo exibida, escolha Excluir. Essa ação não pode ser desfeita.

Como usar o AWS CLI

Para instalar a AWS CLI, consulte Instalar a AWS CLI no Guia do usuário da AWS Command Line Interface.

Para usar o comando a seguir, substitua os *user input placeholders* por suas próprias informações.

> **Note**
>
> Antes de excluir uma instância da funcionalidade Concessões de Acesso do S3, primeiro é necessário excluir todas as concessões e locais criados na instância da funcionalidade Concessões de Acesso do S3. Se você associou uma instância do Centro de Identidade do IAM à sua instância da funcionalidade Concessões de Acesso do S3, deverá desassociá-la primeiro.

Example : excluir uma instância da funcionalidade Concessões de Acesso do S3

```
aws s3control delete-access-grants-instance \
--account-id 111122223333 \
--profile access-grants-profile \
--region us-east-2 \
--endpoint-url https://s3-control.us-east-2.amazonaws.com \

 // No response body
```

Uso da API REST

Para obter informações sobre o suporte à API REST do Amazon S3 para excluir uma instância da funcionalidade Concessões de Acesso do S3, consulte DeleteAccessGrantsInstance na Referência da API do Amazon Simple Storage Service.

Uso dos SDKs da AWS

Esta seção fornece exemplos de como excluir uma instância da funcionalidade Concessões de Acesso do S3 usando os AWS SDKs.

Para usar o exemplo a seguir, substitua os *user input placeholders* por suas próprias informações.

Java

> **Note**
>
> Antes de excluir uma instância da funcionalidade Concessões de Acesso do S3, primeiro é necessário excluir todas as concessões e locais criados na instância da funcionalidade Concessões de Acesso do S3. Se você associou uma instância do Centro de Identidade

do IAM à sua instância da funcionalidade Concessões de Acesso do S3, deverá desassociá-la primeiro.

Example : excluir uma instância da funcionalidade Concessões de Acesso do S3

```
public void deleteAccessGrantsInstance() {
DeleteAccessGrantsInstanceRequest deleteRequest =
 DeleteAccessGrantsInstanceRequest.builder()
.accountId("111122223333")
.build();
DeleteAccessGrantsInstanceResponse deleteResponse =
 s3Control.deleteAccessGrantsInstance(deleteRequest);
LOGGER.info("DeleteAccessGrantsInstanceResponse: " + deleteResponse);
}
```

Trabalhar com locais do recurso Concessão de Acesso do S3

Depois de criar uma instância do recurso Concessão de Acesso do Amazon S3 em uma Região da AWS na sua conta, registre uma localidade do S3 nessa instância. Uma localização do recurso Concessão de Acesso do S3 associa a localização padrão do S3 (`s3://`), um bucket ou um prefixo a um perfil do AWS Identity and Access Management (IAM). O recurso Concessão de Acesso do S3 assume esse perfil do IAM para distribuir credenciais temporárias ao beneficiário que está acessando aquela localização específica. Primeiro, é necessário registrar pelo menos uma localização na instância do recurso Concessão de Acesso do S3 para poder criar uma concessão de acesso.

É possível registrar um local, visualizar os respectivos detalhes, editar e excluir um local.

> **Note**
>
> Depois de registrar a primeira localização na sua instância do recurso Concessão de Acesso do S3, ela ainda não terá nenhuma concessão de acesso individual. Para criar uma concessão de acesso, consulte Criar concessões.

Tópicos

- Registrar um local
- Visualizar os detalhes de um local registrado

- Atualizar um local registrado
- Excluir um local registrado

Registrar um local

Depois de criar uma instância do recurso Concessão de Acesso do Amazon S3 em uma Região da AWS na sua conta, registre uma localidade do S3 nessa instância. Uma localização do recurso Concessão de Acesso do S3 associa a localização padrão do S3 (`s3://`), um bucket ou um prefixo a um perfil do AWS Identity and Access Management (IAM). O recurso Concessão de Acesso do S3 assume esse perfil do IAM para distribuir credenciais temporárias ao beneficiário que está acessando aquela localização específica. Primeiro, é necessário registrar pelo menos uma localização na instância do recurso Concessão de Acesso do S3 para poder criar uma concessão de acesso.

Caso de uso recomendado

Recomendamos registrar a localização padrão (`s3://`) e associá-la a um perfil do IAM. A localização no caminho padrão do S3 (`s3://`) abrange o acesso a todos os seus buckets do S3 nessa Região da AWS da sua conta. Ao criar uma concessão de acesso, é possível restringir o escopo da concessão a um bucket, um prefixo ou um objeto dentro da localização padrão.

Casos de uso de gerenciamento de acesso complexo

Casos de uso de gerenciamento de acesso mais complexos podem exigir que você registre mais do que a localização padrão. Alguns exemplos desses casos de uso são:

- Suponha que *`amzn-s3-demo-bucket`* seja uma localização registrada em sua instância do recurso Concessão de Acesso do S3 com um perfil do IAM associado a ela, mas esse perfil do IAM tenha acesso negado a um prefixo específico no bucket. Nesse caso, é possível registrar o prefixo ao qual o perfil do IAM não tem acesso como uma localização separada e associar essa localização a um perfil do IAM diferente com o acesso necessário.
- Suponha que você queira criar concessões que restrinjam o acesso apenas aos usuários em um endpoint de nuvem privada virtual (VPC). Nesse caso, é possível registrar uma localização para um bucket no qual o perfil do IAM restringe o acesso ao endpoint da VPC. Posteriormente, quando um beneficiário solicita credenciais ao recurso Concessão de Acesso do S3, ele assume o perfil do IAM da localização para distribuir credenciais temporárias. Essa credencial negará acesso ao bucket específico, a menos que o chamador esteja dentro do endpoint da VPC. Essa permissão de negação é aplicada além da permissão READ, WRITE ou READWRITE normal especificada na concessão.

Ao registrar uma localização, também é necessário especificar o perfil do IAM que o recurso Concessão de Acesso do S3 assume para distribuir credenciais temporárias e definir o escopo das permissões de uma concessão específica.

Se seu caso de uso exigir que você registre várias localizações em sua instância do recurso Concessão de Acesso do S3, você poderá registrar qualquer um dos seguintes:

URI do S3	Perfil do IAM	Descrição
`s3://`	*`Default-IAM-role`*	O local padrão `s3://` inclui todos os buckets na Região da AWS.
`s3://`*`amzn-s3-demo-bucket1`*`/`	*`IAM-role-For-bucket`*	Esse local inclui todos os objetos no bucket especificado.
`s3://`*`amzn-s3-demo-bucket1`*`/`*`prefix-name`	*`IAM-role-For-prefix`*	Essa localização inclui todos os objetos no bucket com um nome de chave de objeto que começa com esse prefixo.

Para registrar um bucket ou um prefixo específico, faça o seguinte:

- Crie um ou mais buckets que contenham os dados aos quais você deseja conceder acesso. Esses buckets devem estar localizados na mesma Região da AWS da instância da funcionalidade Concessões de Acesso do S3. Para mais informações, consulte Criar um bucket.

  Adicionar um prefixo é uma etapa opcional. Os prefixos são strings no início do nome da chave de um objeto. É possível usá-los para organizar objetos no bucket, bem como para gerenciar o acesso. Para adicionar um prefixo a um bucket, consulte Criar nomes de chave de objeto.
- Crie um perfil do IAM com as permissões para acessar os dados do S3 na Região da AWS. Para ter mais informações, consulte Criação de funções do IAM no Guia do usuário do AWS IAM Identity Center.
- Na política de confiança do perfil do IAM, dê à entidade principal do serviço Concessão de Acesso do S3 (`access-grants.s3.amazonaws.com`) acesso ao perfil do IAM que você criou. Para fazer isso, você pode criar um arquivo JSON que contém as instruções a seguir. Para adicionar a política de confiança à sua conta, consulte Criar uma função usando políticas de confiança personalizadas.

  TestRolePolicy.json

```
{
  "Version": "2012-10-17",
    "Statement": [
    {
      "Sid": "TestRolePolicy",
      "Effect": "Allow",
      "Principal": {
        "Service":"access-grants.s3.amazonaws.com"
      },
      "Action": [
        "sts:AssumeRole",
        "sts:SetSourceIdentity"
      ],
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount":"accountId",
          "aws:SourceArn":"arn:aws:s3:region:accountId:access-grants/default"
        }
      }
    }
  ]
}
```

Como alternativa, para um caso de uso do Centro de Identidade do IAM, use a seguinte política, que inclui uma segunda declaração:

```
{
  "Version": "2012-10-17",
    "Statement": [
    {
      "Sid": "TestRolePolicyIdentityCenter",
      "Effect": "Allow",
      "Principal": {
        "Service":"access-grants.s3.amazonaws.com"
      },
      "Action": [
        "sts:AssumeRole",
        "sts:SetSourceIdentity"
      ],
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount":"accountId",
```

```
          "aws:SourceArn":"arn:aws:s3:region:accountId:access-grants/default"
        }
      }
    },
    {
      "Sid": "Stmt1234567891012",
        "Effect": "Allow",
        "Principal": {
          "Service": "access-grants.s3.amazonaws.com"
        },
        "Action": "sts:SetContext",
        "Condition":{
          "StringEquals":{
            "aws:SourceAccount":"accountId",
            "aws:SourceArn":"arn:aws:s3:region:accountId:access-grants/default"
          },
          "ForAllValues:ArnEquals": {
            "sts:RequestContextProviders":"arn:aws:iam::aws:contextProvider/
IdentityCenter"
          }
        }
      }
  ]
}
```

- Crie uma política do IAM para anexar permissões do Amazon S3 ao perfil do IAM que você criou. Confira o exemplo de arquivo `iam-policy.json` a seguir e substitua os *`user input placeholders`* por suas próprias informações.

> **Note**
>
> - Se você usa criptografia do lado do servidor com chaves do AWS Key Management Service (AWS KMS) para criptografar os dados, o exemplo a seguir inclui as permissões do AWS KMS necessárias para o perfil do IAM na política. Se você não usa esse recurso, remova essas permissões da política do IAM.
> - Você pode restringir um perfil do IAM para acessar dados do S3 somente se as credenciais forem fornecidas pela funcionalidade Concessões de Acesso do S3. Este exemplo mostra como adicionar uma instrução `Condition` para uma instância específica da funcionalidade Concessões de Acesso do S3. Para usar essa `Condition`, substitua o ARN da instância do recurso Concessão de Acesso do S3 na declaração

Condition pelo ARN da instância do recurso Concessão de Acesso do S3, que tem o formato: `arn:aws:s3:region:accountId:access-grants/default`.

iam-policy.json

```
{
   "Version":"2012-10-17",
   "Statement": [
       {
         "Sid": "ObjectLevelReadPermissions",
         "Effect":"Allow",
         "Action":[
            "s3:GetObject",
            "s3:GetObjectVersion",
            "s3:GetObjectAcl",
            "s3:GetObjectVersionAcl",
            "s3:ListMultipartUploadParts"
         ],
         "Resource":[
            "arn:aws:s3:::*"
         ],
         "Condition":{
            "StringEquals": { "aws:ResourceAccount": "accountId" },
            "ArnEquals": {
                "s3:AccessGrantsInstanceArn": ["arn:aws:s3:region:accountId:access-
grants/default"]
            }
        }
      },
      {
         "Sid": "ObjectLevelWritePermissions",
         "Effect":"Allow",
         "Action":[
            "s3:PutObject",
            "s3:PutObjectAcl",
            "s3:PutObjectVersionAcl",
            "s3:DeleteObject",
            "s3:DeleteObjectVersion",
            "s3:AbortMultipartUpload"
         ],
         "Resource":[
```

```
            "arn:aws:s3:::*"
         ],
         "Condition":{
            "StringEquals": { "aws:ResourceAccount": "accountId" },
            "ArnEquals": {
                "s3:AccessGrantsInstanceArn": ["arn:aws:s3:Região da
 AWS:accountId:access-grants/default"]
            }
         }
      },
      {
         "Sid": "BucketLevelReadPermissions",
         "Effect":"Allow",
         "Action":[
            "s3:ListBucket"
         ],
         "Resource":[
            "arn:aws:s3:::*"
         ],
         "Condition":{
            "StringEquals": { "aws:ResourceAccount": "accountId" },
            "ArnEquals": {
                "s3:AccessGrantsInstanceArn": ["arn:aws:s3:Região da
 AWS:accountId:access-grants/default"]
            }
         }
      },
   //Optionally add the following section if you use SSE-KMS encryption
      {
         "Sid": "KMSPermissions",
         "Effect":"Allow",
         "Action":[
            "kms:Decrypt",
            "kms:GenerateDataKey"
         ],
         "Resource":[
            "*"
         ]
      }
   ]
}
```

Você pode registrar um local na instância da funcionalidade Concessões de Acesso do S3 usando o console do Amazon S3, a AWS Command Line Interface (AWS CLI), a API REST do Amazon S3 ou os AWS SDKs.

> **Note**
>
> Depois de registrar a primeira localização na sua instância do recurso Concessão de Acesso do S3, ela ainda não terá nenhuma concessão de acesso individual. Para criar uma concessão de acesso, consulte Criar concessões.

Usar o console do S3

Antes de poder conceder acesso aos dados do S3 com a funcionalidade Concessões de Acesso do S3, é necessário ter pelo menos um local registrado.

Como registrar um local em uma instância da funcionalidade Concessões de Acesso do S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação, escolha Access Grants.
3. Na página Concessões de Acesso do S3, escolha a região que contém a instância da funcionalidade Concessões de Acesso do S3 com a qual você deseja trabalhar.

   Se você estiver usando a instância da funcionalidade Concessões de Acesso do S3 pela primeira vez, conclua a Etapa 1: Criar uma instância da funcionalidade Concessões de Acesso do S3 e navegue até a Etapa 2 do assistente Configurar instância do Access Grants. Se você já tiver uma instância da funcionalidade Concessões de Acesso do S3, escolha Visualizar detalhes, depois selecione Registrar local na guia Locais.

   a. Em Escopo do local, escolha Procurar no S3 ou insira o caminho do URI do S3 para o local que você deseja registrar. Para conferir os formatos de URI do S3, consulte a tabela de formatos de local. Depois de inserir um URI, você pode escolher Visualizar para procurar o local.

   b. Em Perfil do IAM, escolha uma das seguintes opções:

      - Escolher entre perfis do IAM existentes

Escolha um perfil do IAM na lista suspensa. Depois de escolher um perfil, selecione Visualizar para garantir que esse perfil tenha as permissões necessárias para gerenciar o local que você está registrando. Especificamente, garanta que esse perfil conceda à funcionalidade Concessões de Acesso do S3 as permissões `sts:AssumeRole` e `sts:SetSourceIdentity`.

- Inserir ARN do perfil do IAM

  Navegue até o console do IAM. Copie o nome do recurso da Amazon (ARN) do perfil do IAM e cole-o nesta caixa.

c. Para finalizar, escolha Próximo ou Registrar local.

4. Solucionar problemas:

   Não é possível registrar o local

   - O local pode já estar registrado.

     Talvez você não tenha a permissão `s3:CreateAccessGrantsLocation` para registrar locais. Entre em contato com o administrador da conta.

Como usar o AWS CLI

Para instalar a AWS CLI, consulte Instalar a AWS CLI no Guia do usuário da AWS Command Line Interface.

Você pode registrar o local padrão `s3://` ou um local personalizado na instância da funcionalidade Concessões de Acesso do S3. Primeiro, crie um perfil do IAM com acesso de entidade principal ao local, depois conceda permissão à funcionalidade Concessões de Acesso do S3 para assumir esse perfil.

Para usar os comandos a seguir, substitua os *`user input placeholders`* por suas próprias informações.

Example Criar uma política de recursos

Crie uma política que permita que a funcionalidade Concessões de Acesso do S3 assuma o perfil do IAM. Para fazer isso, você pode criar um arquivo JSON que contém as instruções a seguir. Para adicionar a política de recursos à sua conta, consulte Criar e anexar sua primeira política gerenciada pelo cliente.

TestRolePolicy.json

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1234567891011",
      "Action": ["sts:AssumeRole", "sts:SetSourceIdentity"],
      "Effect": "Allow",
      "Principal": {"Service":"access-grants.s3.amazonaws.com"}
    }
  ]
}
```

Example Criar o perfil

Execute o comando do IAM a seguir para criar o perfil.

```
aws iam create-role --role-name accessGrantsTestRole \
 --region us-east-2 \
 --assume-role-policy-document file://TestRolePolicy.json
```

A execução do comando `create-role` retorna a política:

```
{
    "Role": {
        "Path": "/",
        "RoleName": "accessGrantsTestRole",
        "RoleId": "AROASRDGX4WM4GH55GIDA",
        "Arn": "arn:aws:iam::111122223333:role/accessGrantsTestRole",
        "CreateDate": "2023-05-31T18:11:06+00:00",
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Sid": "Stmt1685556427189",
                    "Action": [
                        "sts:AssumeRole",
                        "sts:SetSourceIdentity"
                    ],
                    "Effect": "Allow",
                    "Principal": {
```

```
                        "Service":"access-grants.s3.amazonaws.com"
                    }
                }
            ]
        }
    }
}
```

Example

Crie uma política do IAM para anexar permissões do Amazon S3 ao perfil do IAM. Confira o exemplo de arquivo `iam-policy.json` a seguir e substitua os *`user input placeholders`* por suas próprias informações.

> **Note**
>
> Se você usa criptografia do lado do servidor com chaves do AWS Key Management Service (AWS KMS) para criptografar os dados, o exemplo a seguir adiciona as permissões do AWS KMS necessárias para o perfil do IAM na política. Se você não usa esse recurso, remova essas permissões da política do IAM.
>
> Para garantir que o perfil do IAM só possa ser usado para acessar dados no S3 se as credenciais forem fornecidas pela funcionalidade Concessões de Acesso do S3, esse exemplo mostra como adicionar uma instrução `Condition` que especifica a instância da funcionalidade Concessões de Acesso do S3 (`s3:AccessGrantsInstance:`*`InstanceArn`*) na política do IAM. Ao usar o exemplo de política a seguir, substitua os *`user input placeholders`* por suas próprias informações.

iam-policy.json

```
{
   "Version":"2012-10-17",
   "Statement": [
       {
         "Sid": "ObjectLevelReadPermissions",
         "Effect":"Allow",
         "Action":[
            "s3:GetObject",
            "s3:GetObjectVersion",
            "s3:GetObjectAcl",
```

```
            "s3:GetObjectVersionAcl",
            "s3:ListMultipartUploadParts"
         ],
         "Resource":[
            "arn:aws:s3:::*"
         ],
         "Condition":{
            "StringEquals": { "aws:ResourceAccount": "accountId" },
            "ArnEquals": {
                "s3:AccessGrantsInstanceArn": ["arn:aws:s3:region:accountId:access-
grants/default"]
            }
        }
      },
      {
         "Sid": "ObjectLevelWritePermissions",
         "Effect":"Allow",
         "Action":[
            "s3:PutObject",
            "s3:PutObjectAcl",
            "s3:PutObjectVersionAcl",
            "s3:DeleteObject",
            "s3:DeleteObjectVersion",
            "s3:AbortMultipartUpload"
         ],
         "Resource":[
            "arn:aws:s3:::*"
         ],
         "Condition":{
            "StringEquals": { "aws:ResourceAccount": "accountId" },
            "ArnEquals": {
                "s3:AccessGrantsInstanceArn": ["arn:aws:s3:Região da
 AWS:accountId:access-grants/default"]
            }
         }
      },
      {
         "Sid": "BucketLevelReadPermissions",
         "Effect":"Allow",
         "Action":[
            "s3:ListBucket"
         ],
         "Resource":[
            "arn:aws:s3:::*"
```

```
         ],
         "Condition":{
            "StringEquals": { "aws:ResourceAccount": "accountId" },
            "ArnEquals": {
                "s3:AccessGrantsInstanceArn": ["arn:aws:s3:Região da
 AWS:accountId:access-grants/default"]
            }
         }
      },
      {
         "Sid": "KMSPermissions",
         "Effect":"Allow",
         "Action":[
            "kms:Decrypt",
            "kms:GenerateDataKey"
         ],
         "Resource":[
            "*"
         ]
      }
   ]
}
```

Example

Execute o seguinte comando:

```
aws iam put-role-policy \
--role-name accessGrantsTestRole \
--policy-name accessGrantsTestRole \
--policy-document file://iam-policy.json
```

Example Registrar o local padrão

```
aws s3control create-access-grants-location \
 --account-id 111122223333 \
 --location-scope s3:// \
 --iam-role-arn arn:aws:iam::111122223333:role/accessGrantsTestRole
```

Resposta:

```
{"CreatedAt": "2023-05-31T18:23:48.107000+00:00",
```

```
    "AccessGrantsLocationId": "default",
    "AccessGrantsLocationArn": "arn:aws:s3:us-east-2:111122223333:access-grants/
default/location/default",
    "LocationScope": "s3://"
    "IAMRoleArn": "arn:aws:iam::111122223333:role/accessGrantsTestRole"
}
```

Example Registrar um local personalizado

```
aws s3control create-access-grants-location \
 --account-id 111122223333 \
 --location-scope s3://DOC-BUCKET-EXAMPLE/ \
 --iam-role-arn arn:aws:iam::123456789012:role/accessGrantsTestRole
```

Resposta:

```
{"CreatedAt": "2023-05-31T18:23:48.107000+00:00",
    "AccessGrantsLocationId": "635f1139-1af2-4e43-8131-a4de006eb456",
    "AccessGrantsLocationArn": "arn:aws:s3:us-east-2: 111122223333:access-grants/
default/location/635f1139-1af2-4e43-8131-a4de006eb888",
    "LocationScope": "s3://DOC-BUCKET-EXAMPLE/",
    "IAMRoleArn": "arn:aws:iam::111122223333:role/accessGrantsTestRole"
}
```

Uso da API REST

Para obter informações sobre o suporte à API REST do Amazon S3 para gerenciar instâncias da funcionalidade Concessões de Acesso do S3, consulte as seguintes seções na Referência da API do Amazon Simple Storage Service:

- CreateAccessGrantsLocation
- DeleteAccessGrantsLocation
- GetAccessGrantsLocation
- ListAccessGrantsLocations
- UpdateAccessGrantsLocation

Uso dos SDKs da AWS

Esta seção fornece exemplos de como registrar locais usando os AWS SDKs.

Para usar os exemplos a seguir, substitua *user input placeholders* por suas próprias informações.

Java

Você pode registrar o local padrão `s3://` ou um local personalizado na instância da funcionalidade Concessões de Acesso do S3. Primeiro, crie um perfil do IAM com acesso de entidade principal ao local, depois conceda permissão à funcionalidade Concessões de Acesso do S3 para assumir esse perfil.

Para usar os comandos a seguir, substitua os *user input placeholders* por suas próprias informações.

Example Registrar um local padrão

Solicitação:

```
public void createAccessGrantsLocation() {
CreateAccessGrantsLocationRequest createRequest =
 CreateAccessGrantsLocationRequest.builder()
.accountId("111122223333")
.locationScope("s3://")
.iamRoleArn("arn:aws:iam::123456789012:role/accessGrantsTestRole")
.build();
CreateAccessGrantsLocationResponse createResponse =
 s3Control.createAccessGrantsLocation(createRequest);
LOGGER.info("CreateAccessGrantsLocationResponse: " + createResponse);
}
```

Resposta:

```
CreateAccessGrantsLocationResponse(
CreatedAt=2023-06-07T04:35:11.027Z,
AccessGrantsLocationId=default,
AccessGrantsLocationArn=arn:aws:s3:us-east-2:111122223333:access-grants/default/
location/default,
LocationScope=s3://,
IAMRoleArn=arn:aws:iam::111122223333:role/accessGrantsTestRole
)
```

Example Registrar um local personalizado

Solicitação:

```
public void createAccessGrantsLocation() {
CreateAccessGrantsLocationRequest createRequest =
 CreateAccessGrantsLocationRequest.builder()
.accountId("111122223333")
.locationScope("s3://DOC-BUCKET-EXAMPLE/")
.iamRoleArn("arn:aws:iam::111122223333:role/accessGrantsTestRole")
.build();
CreateAccessGrantsLocationResponse createResponse =
 s3Control.createAccessGrantsLocation(createRequest);
LOGGER.info("CreateAccessGrantsLocationResponse: " + createResponse);
}
```

Resposta:

```
CreateAccessGrantsLocationResponse(
CreatedAt=2023-06-07T04:35:10.027Z,
AccessGrantsLocationId=18cfe6fb-eb5a-4ac5-aba9-8d79f04c2012,
AccessGrantsLocationArn=arn:aws:s3:us-east-2:111122223333:access-grants/default/
location/18cfe6fb-eb5a-4ac5-aba9-8d79f04c2666,
LocationScope= s3://test-bucket-access-grants-user123/,
IAMRoleArn=arn:aws:iam::111122223333:role/accessGrantsTestRole
)
```

Visualizar os detalhes de um local registrado

Você pode obter os detalhes de um local registrado na instância da funcionalidade Concessões de Acesso do S3 usando o console do Amazon S3, a AWS Command Line Interface (AWS CLI), a API REST do Amazon S3 e os AWS SDKs.

Usar o console do S3

Como visualizar os locais registrados na instância da funcionalidade Concessões de Acesso do S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação, escolha Access Grants.

3. Na página Concessões de Acesso do S3, escolha a região que contém a instância da funcionalidade Concessões de Acesso do S3 com a qual você deseja trabalhar.
4. Escolha Visualizar detalhes da instância.
5. Na página de detalhes da instância, escolha a guia Locais.
6. Encontre o local registrado que você deseja visualizar. Para filtrar a lista de locais registrados, use a caixa de pesquisa.

Como usar o AWS CLI

Para instalar a AWS CLI, consulte Instalar a AWS CLI no Guia do usuário da AWS Command Line Interface.

Para usar o comando a seguir, substitua os *user input placeholders* por suas próprias informações.

Example : obter os detalhes de um local registrado

```
aws s3control get-access-grants-location \
--account-id 111122223333 \
--access-grants-location-id default
```

Resposta:

```
{
    "CreatedAt": "2023-05-31T18:23:48.107000+00:00",
    "AccessGrantsLocationId": "default",
    "AccessGrantsLocationArn": "arn:aws:s3:us-east-2:111122223333:access-grants/
default/location/default",
    "IAMRoleArn": "arn:aws:iam::111122223333:role/accessGrantsTestRole"
}
```

Example : listar todos os locais registrados em uma instância da funcionalidade Concessões de Acesso do S3

Para restringir os resultados a um prefixo ou bucket do S3, há a opção de usar o parâmetro `--location-scope s3://bucket-and-or-prefix`.

```
aws s3control list-access-grants-locations \
```

```
--account-id 111122223333 \
--region us-east-2
```

Resposta:

```
{"AccessGrantsLocationsList": [
  {
    "CreatedAt": "2023-05-31T18:23:48.107000+00:00",
    "AccessGrantsLocationId": "default",
    "AccessGrantsLocationArn": "arn:aws:s3:us-east-2:111122223333:access-grants/
default/location/default",
    "LocationScope": "s3://"
    "IAMRoleArn": "arn:aws:iam::111122223333:role/accessGrantsTestRole"
     },
  {
    "CreatedAt": "2023-05-31T18:23:48.107000+00:00",
    "AccessGrantsLocationId": "635f1139-1af2-4e43-8131-a4de006eb456",
    "AccessGrantsLocationArn": "arn:aws:s3:us-east-2:111122223333:access-grants/
default/location/635f1139-1af2-4e43-8131-a4de006eb888",
    "LocationScope": "s3://amzn-s3-demo-bucket/prefixA*",
    "IAMRoleArn": "arn:aws:iam::111122223333:role/accessGrantsTestRole"
     }
   ]
  }
```

Uso da API REST

Para obter informações sobre o suporte à API REST do Amazon S3 para obter os detalhes de um local registrado ou listar todos os locais registrados em uma instância da funcionalidade Concessões de Acesso do S3, consulte as seguintes seções na Referência da API do Amazon Simple Storage Service:

- GetAccessGrantsLocation
- ListAccessGrantsLocations

Uso dos SDKs da AWS

Esta seção fornece exemplos de como obter os detalhes de um local registrado ou listar todos os locais registrados em uma instância da funcionalidade Concessões de Acesso do S3 usando os AWS SDKs.

Para usar os exemplos a seguir, substitua *user input placeholders* por suas próprias informações.

Java

Example : obter os detalhes de um local registrado

```
public void getAccessGrantsLocation() {
GetAccessGrantsLocationRequest getAccessGrantsLocationRequest =
 GetAccessGrantsLocationRequest.builder()
.accountId("111122223333")
.accessGrantsLocationId("default")
.build();
GetAccessGrantsLocationResponse getAccessGrantsLocationResponse =
 s3Control.getAccessGrantsLocation(getAccessGrantsLocationRequest);
LOGGER.info("GetAccessGrantsLocationResponse: " + getAccessGrantsLocationResponse);
}
```

Resposta:

```
GetAccessGrantsLocationResponse(
CreatedAt=2023-06-07T04:35:10.027Z,
AccessGrantsLocationId=default,
AccessGrantsLocationArn=arn:aws:s3:us-east-2:111122223333:access-grants/default/
location/default,
LocationScope= s3://,
IAMRoleArn=arn:aws:iam::111122223333:role/accessGrantsTestRole
)
```

Example : listar todos os locais registrados em uma instância da funcionalidade Concessões de Acesso do S3

Para restringir os resultados a um prefixo ou bucket do S3, há a opção de enviar um URI do S3, como `s3://bucket-and-or-prefix`, no parâmetro `LocationScope`.

```
public void listAccessGrantsLocations() {

ListAccessGrantsLocationsRequest listRequest =
 ListAccessGrantsLocationsRequest.builder()
.accountId("111122223333")
.build();
```

```
ListAccessGrantsLocationsResponse listResponse =
 s3Control.listAccessGrantsLocations(listRequest);
LOGGER.info("ListAccessGrantsLocationsResponse: " + listResponse);
}
```

Resposta:

```
ListAccessGrantsLocationsResponse(
AccessGrantsLocationsList=[
ListAccessGrantsLocationsEntry(
CreatedAt=2023-06-07T04:35:11.027Z,
AccessGrantsLocationId=default,
AccessGrantsLocationArn=arn:aws:s3:us-east-2:111122223333:access-grants/default/
location/default,
LocationScope=s3://,
IAMRoleArn=arn:aws:iam::111122223333:role/accessGrantsTestRole
),
ListAccessGrantsLocationsEntry(
CreatedAt=2023-06-07T04:35:10.027Z,
AccessGrantsLocationId=635f1139-1af2-4e43-8131-a4de006eb456,
AccessGrantsLocationArn=arn:aws:s3:us-east-2:111122223333:access-grants/default/
location/635f1139-1af2-4e43-8131-a4de006eb888,
LocationScope=s3://amzn-s3-demo-bucket/prefixA*,
IAMRoleArn=arn:aws:iam::111122223333:role/accessGrantsTestRole
)
]
)
```

Atualizar um local registrado

Você pode atualizar o perfil do AWS Identity and Access Management (IAM) de um local registrado na instância da funcionalidade Concessões de Acesso do Amazon S3. Para cada novo perfil do IAM que você usa para registrar um local na funcionalidade Concessões de Acesso do S3, conceda à entidade principal de serviço da funcionalidade Concessões de Acesso do S3 (`access-grants.s3.amazonaws.com`) acesso a esse perfil. Para isso, adicione uma entrada para o novo perfil do IAM no mesmo arquivo JSON de política de confiança que você usou quando registrou o local pela primeira vez.

Você pode atualizar um local na instância da funcionalidade Concessões de Acesso do S3 usando o console do Amazon S3, a AWS Command Line Interface (AWS CLI), a API REST do Amazon S3 e os AWS SDKs.

Usar o console do S3

Como atualizar o perfil do IAM de um local registrado na instância da funcionalidade Concessões de Acesso do S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação, escolha Access Grants.
3. Na página Concessões de Acesso do S3, escolha a região que contém a instância da funcionalidade Concessões de Acesso do S3 com a qual você deseja trabalhar.
4. Escolha Visualizar detalhes da instância.
5. Na página de detalhes da instância, escolha a guia Locais.
6. Encontre o local que deseja atualizar. Para filtrar a lista de locais, use a caixa de pesquisa.
7. Selecione o botão de opções ao lado do local registrado que deseja atualizar.
8. Atualize o perfil do IAM e escolha Salvar alterações.

Como usar o AWS CLI

Para instalar a AWS CLI, consulte Instalar a AWS CLI no Guia do usuário da AWS Command Line Interface.

Para usar o comando a seguir, substitua os *user input placeholders* por suas próprias informações.

Example : atualizar o perfil do IAM de um local registrado

```
aws s3control update-access-grants-location \
--account-id 111122223333 \
--access-grants-location-id 635f1139-1af2-4e43-8131-a4de006eb999 \
--iam-role-arn arn:aws:iam::777788889999:role/accessGrantsTestRole
```

Resposta:

```
{
    "CreatedAt": "2023-05-31T18:23:48.107000+00:00",
    "AccessGrantsLocationId": "635f1139-1af2-4e43-8131-a4de006eb999",
    "AccessGrantsLocationArn": "arn:aws:s3:us-east-2:777788889999:access-grants/
default/location/635f1139-1af2-4e43-8131-a4de006eb888",
```

```
    "LocationScope": "s3://amzn-s3-demo-bucket/prefixB*",
    "IAMRoleArn": "arn:aws:iam::777788889999:role/accessGrantsTestRole"
}
```

Uso da API REST

Para obter informações sobre o suporte à API REST do Amazon S3 para atualizar um local na instância da funcionalidade Concessões de Acesso do S3, consulte UpdateAccessGrantsLocation na Referência da API do Amazon Simple Storage Service.

Uso dos SDKs da AWS

Esta seção fornece exemplos de como atualizar o perfil do IAM de um local registrado usando os AWS SDKs.

Para usar o exemplo a seguir, substitua os *user input placeholders* por suas próprias informações.

Java

Example : atualizar o perfil do IAM de um local registrado

```
public void updateAccessGrantsLocation() {
UpdateAccessGrantsLocationRequest updateRequest =
 UpdateAccessGrantsLocationRequest.builder()
.accountId("111122223333")
.accessGrantsLocationId("635f1139-1af2-4e43-8131-a4de006eb999")
.iamRoleArn("arn:aws:iam::777788889999:role/accessGrantsTestRole")
.build();
UpdateAccessGrantsLocationResponse updateResponse =
 s3Control.updateAccessGrantsLocation(updateRequest);
LOGGER.info("UpdateAccessGrantsLocationResponse: " + updateResponse);
}
```

Resposta:

```
UpdateAccessGrantsLocationResponse(
CreatedAt=2023-06-07T04:35:10.027Z,
AccessGrantsLocationId=635f1139-1af2-4e43-8131-a4de006eb999,
AccessGrantsLocationArn=arn:aws:s3:us-east-2:777788889999:access-grants/default/
location/635f1139-1af2-4e43-8131-a4de006eb888,
LocationScope=s3://amzn-s3-demo-bucket/prefixB*,
IAMRoleArn=arn:aws:iam::777788889999:role/accessGrantsTestRole
```

```
)
```

Excluir um local registrado

Você pode excluir um registro de local de uma instância da funcionalidade Concessões de Acesso do Amazon S3. A exclusão do local cancela o registro na instância da funcionalidade Concessões de Acesso do S3.

Antes de remover um registro de local de uma instância da funcionalidade Concessões de Acesso do S3, é necessário excluir todas as concessões associadas a esse local. Para obter informações sobre como excluir concessões, consulte Delete a grant.

Você pode excluir um local na instância da funcionalidade Concessões de Acesso do S3 usando o console do Amazon S3, a AWS Command Line Interface (AWS CLI), a API REST do Amazon S3 e os AWS SDKs.

Usar o console do S3

Como excluir um registro de local de uma instância da funcionalidade Concessões de Acesso do S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação, escolha Access Grants.
3. Na página Concessões de Acesso do S3, escolha a região que contém a instância da funcionalidade Concessões de Acesso do S3 com a qual você deseja trabalhar.
4. Escolha Visualizar detalhes da instância.
5. Na página de detalhes da instância, escolha a guia Locais.
6. Encontre o local que deseja atualizar. Para filtrar a lista de locais, use a caixa de pesquisa.
7. Selecione o botão de opções ao lado do local registrado que deseja excluir.
8. Escolha Cancelar registro.
9. É exibida uma caixa de diálogo avisando que essa ação não poderá ser desfeita. Para excluir o local, escolha Cancelar registro.

Como usar o AWS CLI

Para instalar a AWS CLI, consulte Instalar a AWS CLI no Guia do usuário da AWS Command Line Interface.

Para usar o comando a seguir, substitua os *user input placeholders* por suas próprias informações.

Example : excluir um registro de local

```
aws s3control delete-access-grants-location \
--account-id 111122223333 \
--access-grants-location-id  a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
 // No response body
```

Uso da API REST

Para obter informações sobre o suporte à API REST do Amazon S3 para excluir um local de uma instância da funcionalidade Concessões de Acesso do S3, consulte DeleteAccessGrantsLocation na Referência da API do Amazon Simple Storage Service.

Uso dos SDKs da AWS

Esta seção fornece um exemplo de como excluir um local usando os AWS SDKs.

Para usar o exemplo a seguir, substitua os *user input placeholders* por suas próprias informações.

Java

Example : excluir um registro de local

```
public void deleteAccessGrantsLocation() {
DeleteAccessGrantsLocationRequest deleteRequest =
 DeleteAccessGrantsLocationRequest.builder()
.accountId("111122223333")
.accessGrantsLocationId("a1b2c3d4-5678-90ab-cdef-EXAMPLE11111")
.build();
DeleteAccessGrantsLocationResponse deleteResponse =
 s3Control.deleteAccessGrantsLocation(deleteRequest);
LOGGER.info("DeleteAccessGrantsLocationResponse: " + deleteResponse);
}
```

Resposta:

```
DeleteAccessGrantsLocationResponse()
```

Trabalhar com concessões no recurso Concessão de Acesso do S3

Uma concessão de acesso individual em uma instância do recurso Concessão de Acesso do S3 permite que uma identidade específica, ou seja, uma entidade principal do AWS Identity and Access Management (IAM), um usuário ou um grupo em um diretório corporativo, acesse uma localização registrada na instância do recurso Concessão de Acesso do S3. Uma localização associa buckets ou prefixos a um perfil do IAM. O recurso Concessão de Acesso do S3 assume esse perfil do IAM para distribuir credenciais temporárias aos beneficiários.

Depois de registrar pelo menos uma localização na instância do recurso Concessão de Acesso do S3, você poderá criar uma concessão de acesso.

O beneficiário pode ser um usuário ou um perfil do IAM ou um usuário ou um grupo de diretório. Um usuário de diretório é um usuário do seu diretório corporativo ou fonte de identidades externa que você associou à instância do recurso Concessão de Acesso do S3. Para obter mais informações, consulte Concessões de Acesso do S3 e identidades de diretórios corporativos. Para criar uma concessão para um usuário ou um grupo de diretório específico do Centro de Identidade do IAM, encontre o GUID usado para identificar esse usuário no Centro de Identidade do IAM, por exemplo, `a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`. Para ter mais informações sobre como usar o Centro de Identidade do IAM para visualizar as informações do usuário, consulte View user and group assignments no Manual do usuário do AWS IAM Identity Center.

É possível conceder acesso a um bucket, um prefixo ou um objeto. Um prefixo no Amazon S3 é uma string de caracteres no início de um nome de chave de objeto que é usado para organizar os objetos dentro de um bucket. Pode ser qualquer string de caracteres permitidos, por exemplo, nomes de chave de objeto em um bucket que comece com o prefixo `engineering/`.

Tópicos

- Criar concessões
- Visualizar uma concessão
- Excluir uma concessão

Criar concessões

Uma concessão de acesso individual em uma instância do recurso Concessão de Acesso do S3 permite que uma identidade específica, ou seja, uma entidade principal do AWS Identity and Access Management (IAM), um usuário ou um grupo em um diretório corporativo, acesse uma localização registrada na instância do recurso Concessão de Acesso do S3. Uma localização associa buckets ou

prefixos a um perfil do IAM. O recurso Concessão de Acesso do S3 assume esse perfil do IAM para distribuir credenciais temporárias aos beneficiários.

Depois de registrar pelo menos uma localização na instância do recurso Concessão de Acesso do S3, você poderá criar uma concessão de acesso.

O beneficiário pode ser um usuário ou um perfil do IAM ou um usuário ou um grupo de diretório. Um usuário de diretório é um usuário do seu diretório corporativo ou fonte de identidades externa que você associou à instância do recurso Concessão de Acesso do S3. Para obter mais informações, consulte Concessões de Acesso do S3 e identidades de diretórios corporativos. Para criar uma concessão para um usuário ou um grupo de diretório específico do Centro de Identidade do IAM, encontre o GUID usado para identificar esse usuário no Centro de Identidade do IAM, por exemplo, `a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`. Para ter mais informações sobre como usar o Centro de Identidade do IAM para visualizar as informações do usuário, consulte View user and group assignments no Manual do usuário do AWS IAM Identity Center.

É possível conceder acesso a um bucket, um prefixo ou um objeto. Um prefixo no Amazon S3 é uma string de caracteres no início de um nome de chave de objeto que é usado para organizar os objetos dentro de um bucket. Pode ser qualquer string de caracteres permitidos, por exemplo, nomes de chave de objeto em um bucket que comece com o prefixo `engineering/`.

Subprefixo

Ao conceder acesso a uma localização registrada, é possível usar o campo `Subprefix` para restringir o escopo de acesso a um subconjunto do escopo da localização. Se a localização registrada que você escolher para a concessão for o caminho padrão do S3 (`s3://`), você deverá restringir o escopo da concessão. Não é possível criar uma concessão de acesso para a localização padrão (`s3://`), o que concederia ao beneficiário acesso a todos os buckets em uma Região da AWS. Em vez disso, é necessário restringir o escopo da concessão a um dos seguintes:

- Um bucket: `s3://`*`bucket`*`/*`
- Um prefixo em um bucket: `s3://`*`bucket`*`/`*`prefix`*`*`
- Um prefixo em um prefixo: `s3://`*`bucket`*`/`*`prefixA`*`/`*`prefixB`*`*`
- Um objeto: `s3://`*`bucket`*`/`*`object-key-name`*

Se você estiver criando uma concessão de acesso em que a localização registrada seja um bucket, poderá enviar uma das seguintes opções no campo `Subprefix` para restringir o escopo da concessão:

- Um prefixo no bucket: *prefix**
- Um prefixo em um prefixo: *prefixA/prefixB**
- Um objeto: */object-key-name*

Depois de criar a concessão, o escopo da concessão exibido no console do Amazon S3 ou o `GrantScope` exibido na resposta da API ou da AWS Command Line Interface (AWS CLI) é o resultado da concatenação do caminho da localização com o `Subprefix`. Garanta que esse caminho concatenado seja mapeado corretamente para o bucket, prefixo ou objeto do S3 ao qual você deseja conceder acesso.

> **Note**
>
> - Se você precisar criar uma concessão de acesso que dê acesso a apenas um objeto, deverá especificar que o tipo de concessão é para um objeto. Para fazer isso em uma chamada de API ou em um comando da CLI, transmita o parâmetro `s3PrefixType` com o valor `Object`. No console do Amazon S3, ao criar a concessão, depois de selecionar uma localização, em Escopo da concessão, marque a caixa de seleção O escopo da concessão é um objeto.
> - Não é possível criar uma concessão para um bucket que ainda não existe. No entanto, é possível criar uma concessão para um prefixo que ainda não existe.
> - Para ter o número máximo de concessões que você pode criar na instância do recurso Concessão de Acesso do S3, consulte Limitações da funcionalidade Concessões de Acesso do S3.

Você pode criar uma concessão de acesso usando o console do Amazon S3, a AWS CLI, a API REST do Amazon S3 ou os AWS SDKs.

Usar o console do S3

Como criar uma concessão de acesso

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação, escolha Access Grants.

3. Na página Concessões de Acesso do S3, escolha a região que contém a instância da funcionalidade Concessões de Acesso do S3 com a qual você deseja trabalhar.

   Se você estiver usando a instância da funcionalidade Concessões de Acesso do S3 pela primeira vez, conclua a Etapa 2: Registrar um local e navegue até a Etapa 3 do assistente Configurar instância do Access Grants. Se você já tiver uma instância da funcionalidade Concessões de Acesso do S3, escolha Visualizar detalhes, depois selecione Criar concessão na guia Concessões.

   a. Na seção Escopo da concessão, selecione ou insira um local registrado.

      Se você selecionou o local `s3://` padrão, use a caixa Subprefixo para restringir o escopo da concessão de acesso. Para obter mais informações, consulte Subprefix. Se você estiver concedendo acesso somente a um objeto, selecione O escopo da concessão é um objeto.

   b. Em Permissões e acesso, selecione o nível de Permissão: Leitura, Gravação ou ambos.

      Depois, escolha o Tipo de beneficiário. Se você adicionou seu diretório corporativo ao Centro de Identidade do IAM e associou essa instância do Centro de Identidade do IAM à instância da funcionalidade Concessões de Acesso do S3, poderá escolher a opção Identidade de diretório do Centro de Identidade do IAM. Se você escolher essa opção, obtenha o ID do usuário ou grupo no Centro de Identidade do IAM e insira-o nesta seção.

      Se o Tipo de beneficiário for um usuário ou perfil do IAM, escolha Entidade principal do IAM. Em Tipo de entidade principal do IAM, escolha Usuário ou Perfil. Depois, em Usuário da entidade principal do IAM, escolha na lista ou insira o ID da identidade.

   c. Para criar a concessão da funcionalidade Concessões de Acesso do S3, escolha Próximo ou Criar concessão.

4. Se as opções Próximo ou Criar concessão estiverem desabilitadas:

   Não é possível criar concessão

   - Poderá ser necessário registrar um local na instância da funcionalidade Concessões de Acesso do S3 primeiro.
   - Talvez você não tenha a permissão `s3:CreateAccessGrant` para criar uma concessão de acesso. Entre em contato com o administrador da conta.

Como usar o AWS CLI

Para instalar a AWS CLI, consulte Instalar a AWS CLI no Guia do usuário da AWS Command Line Interface.

Os exemplos a seguir mostram como criar uma solicitação de concessão de acesso para uma entidade principal do IAM e como criar uma solicitação de concessão de acesso para um usuário ou grupo de diretório corporativo.

Para usar os comandos a seguir, substitua os *user input placeholders* por suas próprias informações.

> **Note**
>
> Se você estiver criando uma concessão de acesso que dá acesso a apenas um objeto, inclua o parâmetro `--s3-prefix-type Object` necessário.

Example Criar uma solicitação de concessão de acesso para uma entidade principal do IAM

```
aws s3control create-access-grant \
--account-id 111122223333 \
--access-grants-location-id a1b2c3d4-5678-90ab-cdef-EXAMPLE22222 \
--access-grants-location-configuration S3SubPrefix=prefixB* \
--permission READ \
--grantee GranteeType=IAM,GranteeIdentifier=arn:aws:iam::123456789012:user/data-consumer-3
```

Example Criar uma resposta de concessão de acesso

```
{"CreatedAt": "2023-05-31T18:41:34.663000+00:00",
    "AccessGrantId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "AccessGrantArn": "arn:aws:s3:us-east-2:111122223333:access-grants/default/grant/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Grantee": {
        "GranteeType": "IAM",
        "GranteeIdentifier": "arn:aws:iam::111122223333:user/data-consumer-3"
    },
    "AccessGrantsLocationId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "AccessGrantsLocationConfiguration": {
        "S3SubPrefix": "prefixB*"
    },
```

```
    "GrantScope": "s3://DOC-BUCKET-EXAMPLE/prefix*",
    "Permission": "READ"
}
```

Criar uma solicitação de concessão de acesso para um usuário ou grupo de diretório

Para criar uma solicitação de concessão de acesso para um usuário ou grupo de diretório, primeiro é necessário obter o GUID do usuário ou grupo de diretório por meio da execução de um dos comandos a seguir.

Example Obter o GUID de um usuário ou grupo de diretório

Você pode encontrar o GUID de um usuário do Centro de Identidade do IAM por meio do console do Centro de Identidade do IAM ou usando a AWS CLI ou os AWS SDKs. O comando a seguir lista os usuários na instância especificada do Centro de Identidade do IAM, com os respectivos nomes e identificadores.

```
aws identitystore list-users --identity-store-id d-1a2b3c4d1234
```

Esse comando lista os grupos na instância especificada do Centro de Identidade do IAM.

```
aws identitystore list-groups --identity-store-id d-1a2b3c4d1234
```

Example Criar uma concessão de acesso para um usuário ou grupo de diretório

Esse comando é semelhante à criação de uma concessão para usuários ou perfis do IAM, exceto que o tipo de beneficiário é `DIRECTORY_USER` ou `DIRECTORY_GROUP` e o identificador do beneficiário é o GUID do usuário ou grupo de diretório.

```
aws s3control create-access-grant \
--account-id 123456789012 \
--access-grants-location-id default \
--access-grants-location-configuration S3SubPrefix="amzn-s3-demo-bucket/rafael/*" \
--permission READWRITE \
--grantee GranteeType=DIRECTORY_USER,GranteeIdentifier=83d43802-00b1-7054-db02-
f1d683aacba5 \
```

Uso da API REST

Para obter informações sobre o suporte à API REST do Amazon S3 para gerenciar concessões de acesso, consulte as seguintes seções na Referência da API do Amazon Simple Storage Service:

- CreateAccessGrant
- DeleteAccessGrant
- GetAccessGrant
- ListAccessGrants

Uso dos SDKs da AWS

Esta seção fornece exemplos de como criar uma concessão de acesso usando os AWS SDKs.

Java

Para usar o exemplo a seguir, substitua *user input placeholders* por suas próprias informações.

> **Note**
>
> Se você estiver criando uma concessão de acesso que dá acesso a apenas um objeto, inclua o parâmetro `.s3PrefixType(S3PrefixType.Object)` necessário.

Example Criar uma solicitação de concessão de acesso

```
public void createAccessGrant() {
CreateAccessGrantRequest createRequest = CreateAccessGrantRequest.builder()
.accountId("111122223333")
.accessGrantsLocationId("a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa")
.permission("READ")
.accessGrantsLocationConfiguration(AccessGrantsLocationConfiguration.builder().s3SubPrefix("
.grantee(Grantee.builder().granteeType("IAM").granteeIdentifier("arn:aws:iam::111122223333:u
data-consumer-3").build())
.build();
CreateAccessGrantResponse createResponse =
 s3Control.createAccessGrant(createRequest);
LOGGER.info("CreateAccessGrantResponse: " + createResponse);
}
```

Example Criar uma resposta de concessão de acesso

```
CreateAccessGrantResponse(
CreatedAt=2023-06-07T05:20:26.330Z,
```

```
AccessGrantId=a1b2c3d4-5678-90ab-cdef-EXAMPLE33333,
AccessGrantArn=arn:aws:s3:us-east-2:444455556666:access-grants/default/grant/
a1b2c3d4-5678-90ab-cdef-EXAMPLE33333,
Grantee=Grantee(
GranteeType=IAM,
GranteeIdentifier=arn:aws:iam::111122223333:user/data-consumer-3
),
AccessGrantsLocationId=a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa,
AccessGrantsLocationConfiguration=AccessGrantsLocationConfiguration(
S3SubPrefix=prefixB*
),
GrantScope=s3://DOC-BUCKET-EXAMPLE/prefixB,
Permission=READ
)
```

Visualizar uma concessão

Você pode ver os detalhes de uma concessão de acesso na instância da funcionalidade Concessões de Acesso do S3 usando o console do Amazon S3, a AWS Command Line Interface (AWS CLI), a API REST do Amazon S3 e os AWS SDKs.

Usar o console do S3

Como visualizar os detalhes de uma concessão de acesso

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação, escolha Access Grants.
3. Na página Concessões de Acesso do S3, escolha a região que contém a instância da funcionalidade Concessões de Acesso do S3 com a qual você deseja trabalhar.
4. Escolha Visualizar detalhes da instância.
5. Na página de detalhes, escolha a guia Concessões.
6. Na seção Concessões, encontre a concessão de acesso que deseja visualizar. Use a caixa de pesquisa para filtrar a lista de concessões.

Como usar o AWS CLI

Para instalar a AWS CLI, consulte Instalar a AWS CLI no Guia do usuário da AWS Command Line Interface.

Para usar os comandos a seguir, substitua os *user input placeholders* por suas próprias informações.

Example : visualizar os detalhes de uma concessão de acesso

```
aws s3control get-access-grant \
--account-id 111122223333 \
--access-grant-id a1b2c3d4-5678-90ab-cdef-EXAMPLE22222
```

Resposta:

```
{
    "CreatedAt": "2023-05-31T18:41:34.663000+00:00",
    "AccessGrantId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "AccessGrantArn": "arn:aws:s3:us-east-2:111122223333:access-grants/default/
grant-a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "Grantee": {
        "GranteeType": "IAM",
        "GranteeIdentifier": "arn:aws:iam::111122223333:user/data-consumer-3"
    },
    "Permission": "READ",
    "AccessGrantsLocationId": "12a6710f-5af8-41f5-b035-0bc795bf1a2b",
    "AccessGrantsLocationConfiguration": {
        "S3SubPrefix": "prefixB*"
    },
    "GrantScope": "s3://amzn-s3-demo-bucket/"
}
```

Example : listar todas as concessões de acesso em uma instância da funcionalidade Concessões de Acesso do S3

Opcionalmente, você pode usar os seguintes parâmetros para restringir os resultados a um prefixo do S3 ou a uma identidade do AWS Identity and Access Management (IAM):

- Subprefixo: `--grant-scope s3://bucket-name/prefix*`
- Identidade do IAM: `--grantee-type IAM` e `--grantee-identifier arn:aws:iam::123456789000:role/accessGrantsConsumerRole`

```
aws s3control list-access-grants \
--account-id 111122223333
```

Resposta:

```
{
    "AccessGrantsList": [{"CreatedAt": "2023-06-14T17:54:46.542000+00:00",
            "AccessGrantId": "dd8dd089-b224-4d82-95f6-975b4185bbaa",
            "AccessGrantArn": "arn:aws:s3:us-east-2:111122223333:access-grants/default/
grant/dd8dd089-b224-4d82-95f6-975b4185bbaa",
            "Grantee": {
                "GranteeType": "IAM",
                "GranteeIdentifier": "arn:aws:iam::111122223333:user/data-consumer-3"
            },
            "Permission": "READ",
            "AccessGrantsLocationId": "23514a34-ea2e-4ddf-b425-d0d4bfcarda1",
            "GrantScope": "s3://amzn-s3-demo-bucket/prefixA*"
        },
        {"CreatedAt": "2023-06-24T17:54:46.542000+00:00",
            "AccessGrantId": "ee8ee089-b224-4d72-85f6-975b4185a1b2",
            "AccessGrantArn": "arn:aws:s3:us-east-2:111122223333:access-grants/default/
grant/ee8ee089-b224-4d72-85f6-975b4185a1b2",
            "Grantee": {
                "GranteeType": "IAM",
                "GranteeIdentifier": "arn:aws:iam::111122223333:user/data-consumer-9"
            },
            "Permission": "READ",
            "AccessGrantsLocationId": "12414a34-ea2e-4ddf-b425-d0d4bfcacao0",
            "GrantScope": "s3://amzn-s3-demo-bucket/prefixB*"
        },

    ]
}
```

Uso da API REST

Você pode usar as operações de API do Amazon S3 para visualizar os detalhes de uma concessão de acesso e listar todas as concessões de acesso em uma instância da funcionalidade Concessões de Acesso do S3. Para obter informações sobre o suporte à API REST para gerenciar concessões de acesso, consulte as seguintes seções na Referência da API do Amazon Simple Storage Service:

- GetAccessGrant
- ListAccessGrants

Uso dos SDKs da AWS

Esta seção fornece exemplos de como obter os detalhes de uma concessão de acesso usando os AWS SDKs.

Para usar os exemplos a seguir, substitua *user input placeholders* por suas próprias informações.

Java

Example : visualizar os detalhes de uma concessão de acesso

```
public void getAccessGrant() {
GetAccessGrantRequest getRequest = GetAccessGrantRequest.builder()
.accountId("111122223333")
.accessGrantId("a1b2c3d4-5678-90ab-cdef-EXAMPLE22222")
.build();
GetAccessGrantResponse getResponse = s3Control.getAccessGrant(getRequest);
LOGGER.info("GetAccessGrantResponse: " + getResponse);
}
```

Resposta:

```
GetAccessGrantResponse(
CreatedAt=2023-06-07T05:20:26.330Z,
AccessGrantId=a1b2c3d4-5678-90ab-cdef-EXAMPLE22222,
AccessGrantArn=arn:aws:s3:us-east-2:111122223333:access-grants/default/
grant-fd3a5086-42f7-4b34-9fad-472e2942c70e,
Grantee=Grantee(
GranteeType=IAM,
GranteeIdentifier=arn:aws:iam::111122223333:user/data-consumer-3
),
Permission=READ,
AccessGrantsLocationId=12a6710f-5af8-41f5-b035-0bc795bf1a2b,
AccessGrantsLocationConfiguration=AccessGrantsLocationConfiguration(
S3SubPrefix=prefixB*
),
GrantScope=s3://amzn-s3-demo-bucket/
)
```

Example : listar todas as concessões de acesso em uma instância da funcionalidade Concessões de Acesso do S3

Opcionalmente, você pode usar os seguintes parâmetros para restringir os resultados a um prefixo do S3 ou a uma identidade do IAM:

- Escopo: `GrantScope=s3://bucket-name/prefix*`
- Beneficiário: `GranteeType=IAM` e `GranteeIdentifier= arn:aws:iam::111122223333:role/accessGrantsConsumerRole`

```
public void listAccessGrants() {
ListAccessGrantsRequest listRequest = ListAccessGrantsRequest.builder()
.accountId("111122223333")
.build();
ListAccessGrantsResponse listResponse = s3Control.listAccessGrants(listRequest);
LOGGER.info("ListAccessGrantsResponse: " + listResponse);
}
```

Resposta:

```
ListAccessGrantsResponse(
AccessGrantsList=[
ListAccessGrantEntry(
CreatedAt=2023-06-14T17:54:46.540z,
AccessGrantId=dd8dd089-b224-4d82-95f6-975b4185bbaa,
AccessGrantArn=arn:aws:s3:us-east-2:111122223333:access-grants/default/
grant/dd8dd089-b224-4d82-95f6-975b4185bbaa,
Grantee=Grantee(
GranteeType=IAM, GranteeIdentifier= arn:aws:iam::111122223333:user/data-consumer-3
),
Permission=READ,
AccessGrantsLocationId=23514a34-ea2e-4ddf-b425-d0d4bfcarda1,
GrantScope=s3://amzn-s3-demo-bucket/prefixA
),
ListAccessGrantEntry(
CreatedAt=2023-06-24T17:54:46.540Z,
AccessGrantId=ee8ee089-b224-4d72-85f6-975b4185a1b2,
AccessGrantArn=arn:aws:s3:us-east-2:111122223333:access-grants/default/
grant/ee8ee089-b224-4d72-85f6-975b4185a1b2,
Grantee=Grantee(
```

```
GranteeType=IAM, GranteeIdentifier= arn:aws:iam::111122223333:user/data-consumer-9
),
Permission=READ,
AccessGrantsLocationId=12414a34-ea2e-4ddf-b425-d0d4bfcacao0,
GrantScope=s3://amzn-s3-demo-bucket/prefixB*
)
]
)
```

Excluir uma concessão

Você pode excluir concessões de acesso de uma instância da funcionalidade Concessões de Acesso do Amazon S3. Não é possível desfazer a exclusão de uma concessão de acesso. Depois de excluir uma concessão de acesso, o beneficiário perderá o acesso aos dados do Amazon S3.

Você pode excluir uma concessão de acesso usando o console do Amazon S3, a AWS Command Line Interface (AWS CLI), a API REST do Amazon S3 ou os AWS SDKs.

Usar o console do S3

Como excluir uma concessão de acesso

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação, escolha Access Grants.
3. Na página Concessões de Acesso do S3, escolha a região que contém a instância da funcionalidade Concessões de Acesso do S3 com a qual você deseja trabalhar.
4. Escolha Visualizar detalhes da instância.
5. Na página de detalhes, escolha a guia Concessões.
6. Procure a concessão que deseja excluir. Ao encontrar a concessão, escolha o botão de opções ao lado dela.
7. Escolha Excluir. É exibida uma caixa de diálogo avisando que a ação não poderá ser desfeita. Escolha Excluir novamente para excluir a concessão.

Como usar o AWS CLI

Para instalar a AWS CLI, consulte Instalar a AWS CLI no Guia do usuário da AWS Command Line Interface.

Para usar o comando a seguir, substitua os *user input placeholders* por suas próprias informações.

Example : excluir uma concessão de acesso

```
aws s3control delete-access-grant \
--account-id 111122223333 \
--access-grant-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111

// No response body
```

Uso da API REST

Para obter informações sobre o suporte à API REST do Amazon S3 para gerenciar concessões de acesso, consulte DeleteAccessGrant na Referência da API do Amazon Simple Storage Service.

Uso dos SDKs da AWS

Esta seção fornece exemplos de como excluir uma concessão de acesso usando os AWS SDKs. Para usar o exemplo a seguir, substitua os *user input placeholders* por suas próprias informações.

Java

Example : excluir uma concessão de acesso

```
public void deleteAccessGrant() {
DeleteAccessGrantRequest deleteRequest = DeleteAccessGrantRequest.builder()
.accountId("111122223333")
.accessGrantId("a1b2c3d4-5678-90ab-cdef-EXAMPLE11111")
.build();
DeleteAccessGrantResponse deleteResponse =
 s3Control.deleteAccessGrant(deleteRequest);
LOGGER.info("DeleteAccessGrantResponse: " + deleteResponse);
}
```

Resposta:

```
DeleteAccessGrantResponse()
```

Obter dados do S3 usando concessões de acesso

Os beneficiários que receberam acesso aos dados do S3 por meio do recurso Concessão de Acesso do S3 devem solicitar credenciais temporárias desse recurso, as quais eles usam para acessar os dados do S3. Para obter mais informações, consulte Solicitar acesso aos dados do Amazon S3 por meio da funcionalidade Concessões de Acesso do S3. Posteriormente, os beneficiários vão usar as credenciais temporárias para realizar ações permitidas do S3 nos dados do S3. Para obter mais informações, consulte Acessar os dados do S3 usando credenciais fornecidas pelo recurso Concessão de Acesso do S3. Os beneficiários também podem solicitar uma lista de concessões de acesso referente a uma Conta da AWS antes de solicitar essas credenciais. Para obter mais informações, consulte Listar as concessões de acesso do chamador.

Tópicos

- Solicitar acesso aos dados do Amazon S3 por meio da funcionalidade Concessões de Acesso do S3
- Acessar os dados do S3 usando credenciais fornecidas pelo recurso Concessão de Acesso do S3
- Listar as concessões de acesso do chamador

Solicitar acesso aos dados do Amazon S3 por meio da funcionalidade Concessões de Acesso do S3

Depois de criar uma concessão de acesso usando a funcionalidade Concessão de Acesso do S3, os beneficiários podem solicitar credenciais para acessar os dados do S3 aos quais receberam acesso. Os beneficiários podem ser entidades principais do AWS Identity and Access Management (IAM), suas identidades de diretório corporativo ou aplicações autorizadas.

Uma aplicação ou um AWS service (Serviço da AWS) pode usar a operação de API `GetDataAccess` da Concessão de Acesso do S3 para pedir a esse recurso acesso aos dados do S3 em nome de um beneficiário. Primeiro, `GetDataAccess` verifica se você concedeu acesso aos dados a essa entidade. Em seguida, a funcionalidade Concessões de Acesso do S3 usa a operação de API AssumeRole para obter um token de credencial temporário e o envia ao solicitante. Esse token temporário de credencial é um token do AWS Security Token Service (AWS STS).

A solicitação `GetDataAccess` deve incluir o parâmetro `target`, que especifica o escopo dos dados do S3 aos quais as credenciais temporárias se aplicam. Esse escopo `target` pode ser igual ao escopo da concessão ou um subconjunto desse escopo, mas o escopo `target` deve estar dentro do escopo da concessão dada à entidade autorizada. A solicitação também deve especificar o parâmetro `permission` para indicar o nível de permissão das credenciais temporárias, seja `READ`, `WRITE` ou `READWRITE`.

Privilege

O solicitante pode especificar o nível de privilégio do token temporário na solicitação de credencial. Usando o parâmetro `privilege`, o solicitante pode reduzir ou aumentar o escopo de acesso das credenciais temporárias, dentro dos limites do escopo da concessão. O valor padrão do parâmetro `privilege` é `Default`, o que significa que o escopo target da credencial retornada é o escopo original da concessão. O outro valor possível para `privilege` é `Minimal`. Se o escopo `target` for reduzido do escopo original da concessão, a credencial temporária será reduzida para corresponder ao escopo `target`, desde que o escopo `target` esteja dentro do escopo da concessão.

A tabela a seguir detalha o efeito do parâmetro `privilege` em duas concessões. Uma concessão tem o escopo `S3://amzn-s3-demo-bucket1/bob/*`, que inclui todo o prefixo `bob/` no bucket *amzn-s3-demo-bucket1*. A outra concessão tem o escopo `S3://amzn-s3-demo-bucket1/bob/reports/*`, que inclui apenas o prefixo `bob/reports/` no bucket *amzn-s3-demo-bucket1*.

Escopo da concessão	Escopo solicitado	Privilege	Escopo retornado	Efeito
`S3://amzn-s3-demo-bucket1 /bob/*`	*amzn-s3-demo-bucket1* `/bob/*`	`Default`	*amzn-s3-demo-bucket1* `/bob/*`	O solicitante tem acesso a todos os objetos que têm nomes de chave que começam com o prefixo *bob/* no bucket *amzn-s3-demo-bucket1* .
`S3://amzn-s3-demo-bucket1 /bob/*`	*amzn-s3-demo-bucket1* `/bob/`	`Minimal`	*amzn-s3-demo-bucket1* `/bob/`	Sem um caractere curinga * depois do nome do prefixo bob/, o solicitante tem acesso somente ao objeto chamado bob/ no bucket

Escopo da concessão	Escopo solicitado	Privilege	Escopo retornado	Efeito
				amzn-s3-demo-bucket1 . Não é comum ter esse objeto. O solicitante não tem acesso a nenhum outro objeto, incluindo aqueles que têm nomes de chave que começam com o prefixo bob/.
S3://*amzn-s3-demo-bucket1* /bob/*	*amzn-s3-demo-bucket1* /bob/images/*	Minimal	*amzn-s3-demo-bucket1* /bob/images/*	O solicitante tem acesso a todos os objetos que têm nomes de chave que começam com o prefixo *bob/images/* * no bucket *amzn-s3-demo-bucket1* .
S3://*amzn-s3-demo-bucket1* /bob/reports/*	*amzn-s3-demo-bucket1* /bob/reports/file.txt	Default	*amzn-s3-demo-bucket1* /bob/reports/*	O solicitante tem acesso a todos os objetos que têm nomes de chave que começam com o prefixo bob/reports no bucket *amzn-s3-demo-bucket1* , que é o escopo da concessão correspondente.

Escopo da concessão	Escopo solicitado	Privilege	Escopo retornado	Efeito
S3://*amzn-s3-demo-bucket1* /bob/reports/*	*amzn-s3-demo-bucket1* /bob/reports/file.txt	Minimal	*amzn-s3-demo-bucket1* /bob/reports/file.txt	O solicitante tem acesso somente ao objeto com o nome de chave bob/reports/file.txt no bucket *amzn-s3-demo-bucket1* . O solicitante não tem acesso a nenhum outro objeto.

Identidades de diretório

`GetDataAccess` considera todas as identidades envolvidas em uma solicitação ao correlacionar concessões adequadas. Para identidades de diretórios corporativos, `GetDataAccess` também retorna as concessões da identidade do IAM que é usada para a sessão com reconhecimento de identidade. Consulte mais informações sobre sessões com reconhecimento de identidade em Como conceder permissões para usar sessões de console com reconhecimento de identidade no Guia do usuário do AWS Identity and Access Management. `GetDataAccess` gera credenciais que restringem o escopo à concessão mais restritiva, conforme mostrado na seguinte tabela:

Escopo de concessão para identidade do IAM	Escopo de concessão para identidade de diretório	Escopo solicitado	Escopo retornado	Privilege	Efeito
S3://*amzn-s3-demo-bucke*	*amzn-s3-demo-bucket1* /	S3://*amzn-s3-demo-bucket1* /	S3://*amzn-s3-demo-bucket1* /bob/images/*	Default	O solicitante tem acesso a todos os objetos que têm nomes de chave que começam com

Escopo de concessão para identidade do IAM	Escopo de concessão para identidade de diretório	Escopo solicitado	Escopo retornado	Privilege	Efeito
t1 / bob/*	bob/images/*	bob/images/image1.jpeg			o prefixo bob/ como parte da concessão para o perfil do IAM, mas está restrito aos prefixos bob/images/ como parte da concessão para a identidade do diretório. Tanto o perfil do IAM quanto a identidade do diretório fornecem acesso ao escopo solicitado, que é `bob/images/image1.jpeg`, mas a identidade do diretório tem uma concessão mais restritiva. Portanto, o escopo retornado é restrito à concessão mais restritiva da identidade do diretório.

Escopo de concessão para identidade do IAM	Escopo de concessão para identidade de diretório	Escopo solicitado	Escopo retornado	Privilege	Efeito
S3://*amzn-s3-demo-bucket1* / bob/*	*amzn-s3-demo-bucket1* / bob/images/*	S3://*amzn-s3-demo-bucket1* / bob/images/image1.jpeg	S3://*amzn-s3-demo-bucket1* / bob/images/image1.jpeg	Minimal	Como o privilégio está definido como Minimal, mesmo que a identidade tenha acesso a um escopo maior, somente o escopo bob/images/image1.jpeg solicitado é retornado.

Escopo de concessão para identidade do IAM	Escopo de concessão para identidade de diretório	Escopo solicitado	Escopo retornado	Privilege	Efeito
S3://*amzn-s3-demo-bucket1* / bob/images/*	*amzn-s3-demo-bucket1* / bob/*	S3://*amzn-s3-demo-bucket1* / bob/images/image1.jpeg	S3://*amzn-s3-demo-bucket1* / bob/images/*	Default	O solicitante tem acesso a todos os objetos que têm nomes de chave que começam com o prefixo bob/ como parte da concessão da identidade do diretório, mas está restrito aos prefixos bob/images/ como parte da concessão para o perfil do IAM. Tanto o perfil do IAM quanto a identidade do diretório fornecem acesso ao escopo solicitado, que é `bob/images/image1.jpeg` , mas o perfil do IAM tem uma concessão mais restritiva. Portanto, o escopo retornado é restrito à concessão mais restritiva do perfil do IAM.

Escopo de concessão para identidade do IAM	Escopo de concessão para identidade de diretório	Escopo solicitado	Escopo retornado	Privilege	Efeito
S3://*amzn-s3-demo-bucket1* / bob/images/*	*amzn-s3-demo-bucket1* / bob/*	S3://*amzn-s3-demo-bucket1* / bob/images/image1.jpeg	S3://*amzn-s3-demo-bucket1* / bob/images/image1.jpeg	Minimal	Como o privilégio está definido como Minimal, mesmo que a identidade tenha acesso a um escopo maior, somente o escopo bob/images/image1.jpeg solicitado é retornado.

Duração

O parâmetro durationSeconds define a duração da credencial temporária, em segundos. O valor padrão é 3600 segundos (1 hora), mas o solicitante (o beneficiário) pode especificar um intervalo que varia de 900 segundos (15 minutos) até 43200 segundos (12 horas). Se o beneficiário solicitar um valor maior do que esse máximo, a solicitação falhará.

> **Note**
>
> Na solicitação de token temporário, se o local for um objeto, defina o valor do parâmetro targetType na solicitação como Object. Esse parâmetro só será necessário se o local for um objeto e o nível de privilégio for Minimal. Se o local for um bucket ou um prefixo, você não precisará especificar esse parâmetro.

Exemplos

É possível solicitar credenciais temporárias usando a AWS Command Line Interface (AWS CLI), a API REST do Amazon S3 e os SDKs da AWS. Consulte estes exemplos.

Consulte mais informações em GetDataAccess na Referência de API do Amazon Simple Storage Service.

Como usar o AWS CLI

Para instalar a AWS CLI, consulte Instalar a AWS CLI no Guia do usuário da AWS Command Line Interface.

Para usar o comando a seguir, substitua os *user input placeholders* por suas próprias informações.

Example Solicitar credenciais temporárias

Solicitação:

```
aws s3control get-data-access \
--account-id 111122223333 \
--target s3://amzn-s3-demo-bucket/prefixA* \
--permission READ \
--privilege Default \
--region us-east-2
```

Resposta:

```
{
"Credentials": {
"AccessKeyId": "Example-key-id",
"SecretAccessKey": "Example-access-key",
"SessionToken": "Example-session-token",
"Expiration": "2023-06-14T18:56:45+00:00"},
"MatchedGrantTarget": "s3://amzn-s3-demo-bucket/prefixA**",
"Grantee": {
    "GranteeType": "IAM",
    "GranteeIdentifier": "arn:aws:iam::111122223333:role/role-name"
 }
}
```

Uso da API REST

Para obter informações sobre o suporte à API REST do Amazon S3 para solicitar credenciais temporárias da funcionalidade Concessões de Acesso do S3, consulte GetDataAccess na Referência da API do Amazon Simple Storage Service.

Uso dos SDKs da AWS

Esta seção fornece um exemplo de como os beneficiários solicitam credenciais temporárias da funcionalidade Concessões de Acesso do S3 usando os AWS SDKs.

Java

O exemplo de código a seguir retorna as credenciais temporárias que o beneficiário usa para acessar os dados do S3. Para usar esse exemplo de código, substitua os *`user input placeholders`* por suas próprias informações.

Example Obter credenciais temporárias

Solicitação:

```
public void getDataAccess() {
GetDataAccessRequest getDataAccessRequest = GetDataAccessRequest.builder()
.accountId("111122223333")
.permission(Permission.READ)
.privilege(Privilege.MINIMAL)
.target("s3://amzn-s3-demo-bucket/prefixA*")
.build();
GetDataAccessResponse getDataAccessResponse =
 s3Control.getDataAccess(getDataAccessRequest);
LOGGER.info("GetDataAccessResponse: " + getDataAccessResponse);
}
```

Resposta:

```
GetDataAccessResponse(
Credentials=Credentials(
AccessKeyId="Example-access-key-id",
SecretAccessKey="Example-secret-access-key",
SessionToken="Example-session-token",
Expiration=2023-06-07T06:55:24Z
))
```

Acessar os dados do S3 usando credenciais fornecidas pelo recurso Concessão de Acesso do S3

Depois que um beneficiário obtém credenciais temporárias por meio de uma concessão de acesso, ele pode usar essas credenciais temporárias para chamar as operações de API do Amazon S3 para acessar os dados.

Os beneficiários podem acessar dados do S3 usando a AWS Command Line Interface (AWS CLI), os AWS SDKs e a API REST do Amazon S3. Além disso, é possível usar os plug-ins Python e Java da AWS para chamar o recurso Concessão de Acesso do S3.

Como usar o AWS CLI

Depois que o beneficiário obtém as credenciais temporárias da funcionalidade Concessões de Acesso do S3, ele pode configurar um perfil com essas credenciais para recuperar os dados.

Para instalar a AWS CLI, consulte Instalar a AWS CLI no Guia do usuário da AWS Command Line Interface.

Para usar os comandos a seguir, substitua os *user input placeholders* por suas próprias informações.

Example : configurar um perfil

```
aws configure set aws_access_key_id "$accessKey" --profile access-grants-consumer-access-profile
aws configure set aws_secret_access_key "$secretKey" --profile access-grants-consumer-access-profile
aws configure set aws_session_token "$sessionToken" --profile access-grants-consumer-access-profile
```

Para usar o comando a seguir, substitua os *user input placeholders* por suas próprias informações.

Example : obter os dados do S3

O beneficiário pode usar o comando get-object da AWS CLI para acessar os dados. O beneficiário também pode usar put-object, ls e outros comandos da AWS CLI do S3.

```
aws s3api get-object \
```

```
--bucket amzn-s3-demo-bucket1 \
--key myprefix \
--region us-east-2 \
--profile access-grants-consumer-access-profile
```

Uso dos SDKs da AWS

Esta seção fornece exemplos de como os beneficiários podem acessar os dados do S3 usando os AWS SDKs.

Java

Para obter exemplos de como obter dados do S3 usando credenciais temporárias, consulte como obter um objeto usando os AWS SDKs e exemplos de código do Amazon S3 para o AWS SDK for Java 2.x.

Ações do S3 aceitas no recurso Concessão de Acesso do S3

Um beneficiário pode usar a credencial temporária fornecida pelo recurso Concessão de Acesso do S3 para realizar ações do S3 nos dados do S3 aos quais ele tem acesso. Veja a seguir uma lista de ações permitidas do S3 que um beneficiário pode realizar. As ações permitidas dependem do nível de permissão indicado na concessão de acesso, como `READ`, `WRITE` ou `READWRITE`.

> **Note**
>
> Além das permissões do Amazon S3 listadas abaixo, o Amazon S3 pode chamar a permissão Decrypt do AWS Key Management Service (AWS KMS) (`kms:decrypt`) `READ` ou a GenerateDataKey do (AWS KMS) (`kms:generateDataKey`) `WRITE`. Essas permissões não autorizam acesso direto à chave do AWS KMS.

Ação do IAM no S3	Ação e documentação da API	Permissão do recurso Concessão de Acesso do S3	Recurso do S3			
`s3:GetObject`	GetObject	`READ`	Objeto			

Ação do IAM no S3	Ação e documentação da API	Permissão do recurso Concessão de Acesso do S3	Recurso do S3			
`s3:GetObjectVersion`	GetObject	`READ`	Objeto			
`s3:GetObjectAcl`	GetObjectAcl	`READ`	Objeto			
`s3:GetObjectVersionAcl`	GetObjectAcl	`READ`	Objeto			
`s3:ListMultipartUploads`	ListParts	`READ`	Objeto			
`s3:PutObject`	PutObject, CreateMultipartUpload, UploadPart, UploadPartCopy, CompleteMultipartUpload	`WRITE`	Objeto			
`s3:PutObjectAcl`	PutObjectAcl	`WRITE`	Objeto			
`s3:PutObjectVersionAcl`	PutObjectAcl	`WRITE`	Objeto			
`s3:DeleteObject`	DeleteObject	`WRITE`	Objeto			

Ação do IAM no S3	Ação e documentação da API	Permissão do recurso Concessão de Acesso do S3	Recurso do S3
`s3:DeleteObjectVersion`	DeleteObject	`WRITE`	Objeto
`s3:AbortMultipartUpload`	AbortMultipartUpload	`WRITE`	Objeto
`s3:ListBucket`	HeadBucket, ListObjectsV2, ListObjects	`READ`	Bucket
`s3:ListBucketVersions`	ListObjectVersions	`READ`	Bucket
`s3:ListBucketMultipartUploads`	ListMultipartUploads	`READ`	Bucket

Listar as concessões de acesso do chamador

Os proprietários de dados do S3 podem usar o recurso Concessão de Acesso do S3 para criar concessões de acesso para identidades do AWS Identity and Access Management (IAM) ou identidades de diretórios corporativos do AWS IAM Identity Center. As identidades do IAM e de diretório do Centro de Identidade do IAM podem, por sua vez, usar a API `ListCallerAccessGrants` para listar todos os buckets, prefixos e objetos do Amazon S3 que elas podem acessar, conforme definido pelo recurso Concessão de Acesso do S3. Use essa API para descobrir todos os dados do S3 que uma identidade do IAM ou de diretório pode acessar por meio do recurso Concessão de Acesso do S3.

É possível usar esse recurso para criar aplicações que mostrem os dados acessíveis a usuários finais específicos. Por exemplo, o AWS Storage Browser para S3, um componente de interface de usuário de código aberto que os clientes usam para acessar buckets do S3, usa esse recurso para apresentar aos usuários finais os dados aos quais eles têm acesso no Amazon S3, com base no recurso Concessão de Acesso do S3. Outro exemplo é que, ao criar uma aplicação para navegar, fazer upload ou baixar dados no Amazon S3, é possível usar esse recurso para criar uma estrutura em árvore na aplicação pela qual um usuário final possa navegar.

> **Note**
>
> Para identidades de diretórios corporativos, ao listar as concessões de acesso do chamador, a Concessão de Acesso do S3 retorna as concessões da identidade do IAM que é usada para a sessão com reconhecimento de identidade. Consulte mais informações sobre sessões com reconhecimento de identidade em Como conceder permissões para usar sessões de console com reconhecimento de identidade no Guia do usuário do AWS Identity and Access Management.

O beneficiário, seja uma identidade do IAM ou uma identidade de diretório corporativo, pode obter uma lista de concessões de acesso usando a AWS Command Line Interface (AWS CLI), a API REST do Amazon S3 e os SDKs da AWS.

Como usar o AWS CLI

Para instalar a AWS CLI, consulte Instalar a AWS CLI no Guia do usuário da AWS Command Line Interface.

Para usar o comando a seguir, substitua os *`user input placeholders`* por suas próprias informações.

Example Listar as concessões de acesso de um chamador

Solicitação:

```
aws s3control list-caller-access-grants \
--account-id 111122223333 \
--region us-east-2
--max-results 5
```

Resposta:

```
{
 "NextToken": "6J9S...",
 "CallerAccessGrantsList": [
  {
   "Permission": "READWRITE",
   "GrantScope": "s3://amzn-s3-demo-bucket/prefix1/sub-prefix1/*",
   "ApplicationArn": "NA"
  },
  {
   "Permission": "READWRITE",
   "GrantScope": "s3://amzn-s3-demo-bucket/prefix1/sub-prefix2/*",
   "ApplicationArn": "ALL"
  },
  {
   "Permission": "READWRITE",
   "GrantScope": "s3://amzn-s3-demo-bucket/prefix1/sub-prefix3/*",
   "ApplicationArn": "arn:aws:sso::111122223333:application/ssoins-
ssoins-1234567890abcdef/apl-abcd1234a1b2c3d"
  }
 ]
}
```

Example Listar as concessões de acesso de um chamador para um bucket

É possível limitar o escopo dos resultados usando o parâmetro `grantscope`.

Solicitação:

```
aws s3control list-caller-access-grants \
--account-id 111122223333 \
--region us-east-2
--grant-scope "s3://amzn-s3-demo-bucket""
--max-results 1000
```

Resposta:

```
{
 "NextToken": "6J9S...",
 "CallerAccessGrantsList": [
```

```
  {
   "Permission": "READ",
   "GrantScope": "s3://amzn-s3-demo-bucket*",
   "ApplicationArn": "ALL"
  },
  {
   "Permission": "READ",
   "GrantScope": "s3://amzn-s3-demo-bucket/prefix1/*",
   "ApplicationArn": "arn:aws:sso::111122223333:application/ssoins-
ssoins-1234567890abcdef/apl-abcd1234a1b2c3d"
  }
 ]
}
```

Uso da API REST

Para ter informações sobre o suporte à API REST do Amazon S3 e obter uma lista de concessões de acesso do chamador da API, consulte ListCallerAccessGrants na Referência da API do Amazon Simple Storage Service.

Uso dos SDKs da AWS

Esta seção fornece um exemplo de como os beneficiários solicitam credenciais temporárias da funcionalidade Concessões de Acesso do S3 usando os AWS SDKs.

Java

O exemplo de código a seguir exibe as concessões de acesso do chamador da API aos dados do S3 de uma Conta da AWS específica. Para usar esse exemplo de código, substitua os *user input placeholders* por suas próprias informações.

Example Listar as concessões de acesso de um chamador

Solicitação:

```
Public void ListCallerAccessGrants() {
 ListCallerAccessGrantsRequest listRequest = ListCallerAccessGrantsRequest.builder()
    .withMaxResults(1000)
    .withGrantScope("s3://")
    .accountId("111122223333");
 ListCallerAccessGrantsResponse listResponse =
 s3control.listCallerAccessGrants(listRequest);
```

```
 LOGGER.info("ListCallerAccessGrantsResponse: " + listResponse);
 }
```

Resposta:

```
ListCallerAccessGrantsResponse(
CallerAccessGrantsList=[
 ListCallerAccessGrantsEntry(
  S3Prefix=s3://amzn-s3-demo-bucket/prefix1/,
  Permission=READ,
  ApplicationArn=ALL
 )
])
```

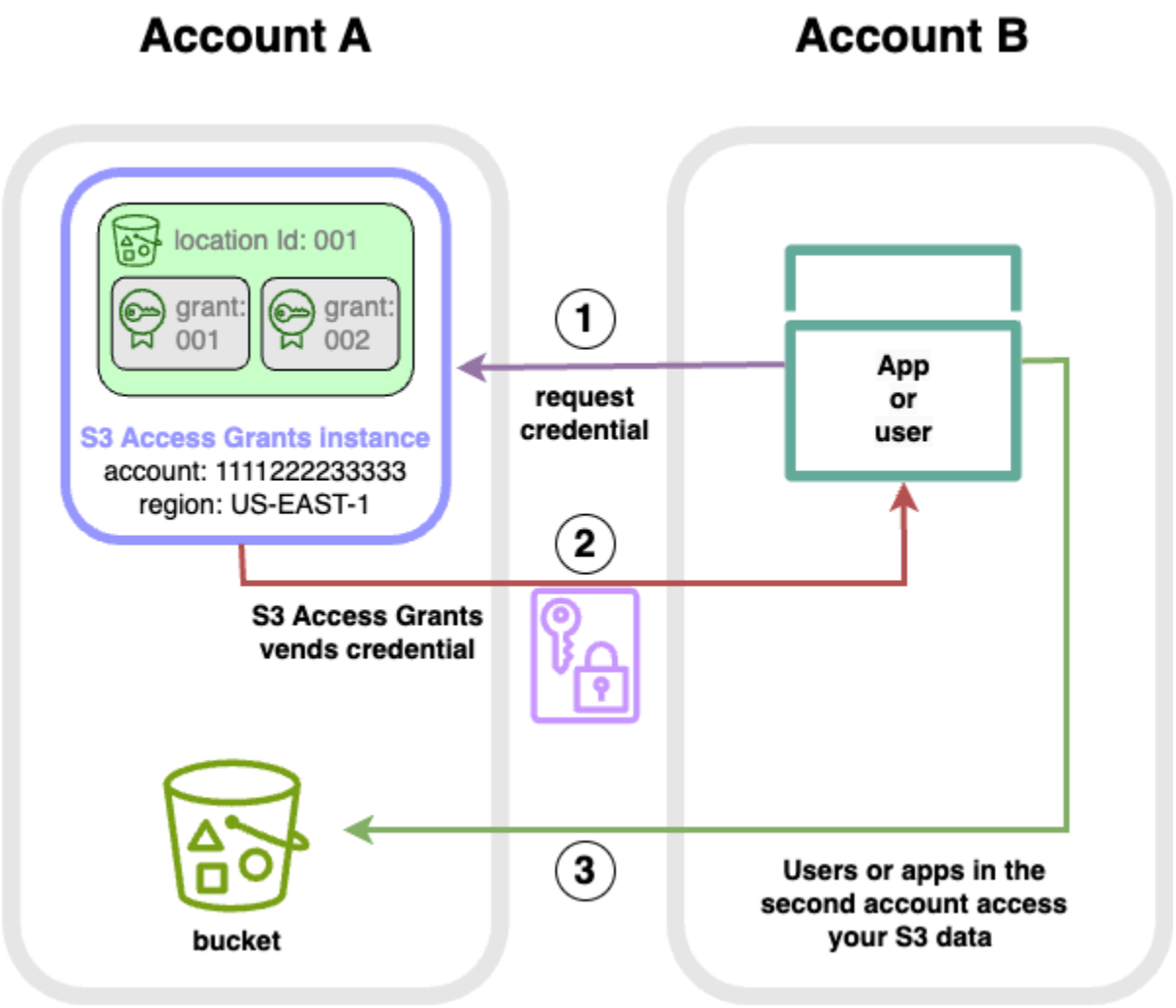
Acesso entre contas da funcionalidade Concessões de Acesso do S3

Com a funcionalidade Concessões de Acesso do S3, você pode conceder acesso aos dados do Amazon S3 ao seguinte:

- Identidades do AWS Identity and Access Management (IAM) em sua conta
- Identidades do IAM em outras contas da AWS
- Diretório de usuários ou grupos na instância do AWS IAM Identity Center

Primeiro, configure o acesso entre contas para a outra conta. Essa ação requer a concessão de acesso à instância da funcionalidade Concessões de Acesso do S3 por meio de uma política de recursos. Em seguida, conceda acesso aos seus dados do S3 (buckets, prefixos ou objetos) usando concessões.

Após a configuração do acesso entre contas, a outra conta pode solicitar credenciais de acesso temporário aos seus dados do Amazon S3 por meio da funcionalidade Concessões de Acesso do S3. A imagem a seguir mostra o fluxo de usuários para acesso entre contas ao S3 por meio da funcionalidade Concessões de Acesso do S3:



1. Os usuários ou as aplicações em uma segunda conta (B) solicitam credenciais da instância da funcionalidade Concessões de Acesso do S3 em sua conta (A), na qual os dados do Amazon S3 são armazenados. Para obter mais informações, consulte Solicitar acesso aos dados do Amazon S3 por meio da funcionalidade Concessões de Acesso do S3.
2. A instância da funcionalidade Concessões de Acesso do S3 em sua conta (A) retornará credenciais temporárias se houver uma concessão que dê à segunda conta acesso aos seus dados do Amazon S3. Para ter mais informações sobre concessões de acesso, consulte Trabalhar com concessões no recurso Concessão de Acesso do S3.
3. Os usuários ou as aplicações na segunda conta (B) usam as credenciais fornecidas pela funcionalidade Concessões de Acesso do S3 para acessar os dados do S3 em sua conta (A).

Acesso entre contas da funcionalidade Concessões de Acesso do S3

Para conceder acesso entre contas ao S3 por meio da funcionalidade Concessões de Acesso do S3, siga estas etapas:

- Etapa 1: configure uma instância da funcionalidade Concessões de Acesso do S3 em sua conta (por exemplo, ID de conta 111122223333), na qual os dados do S3 são armazenados.
- Etapa 2: configure a política de recursos para a instância da funcionalidade Concessões de Acesso do S3 em sua conta 111122223333 para dar acesso à segunda conta (por exemplo, ID de conta 444455556666).
- Etapa 3: configure as permissões do IAM para a entidade principal do IAM na segunda conta (444455556666) para solicitar credenciais da instância da funcionalidade Concessões de Acesso do S3 em sua conta 111122223333.
- Etapa 4: crie uma concessão em sua conta 111122223333 que dê à entidade principal do IAM na segunda conta (444455556666) acesso a alguns dos dados do S3 em sua conta 111122223333.

Etapa 1: configurar uma instância da funcionalidade Concessões de Acesso do S3 em sua conta

Primeiro, você deve ter uma instância da funcionalidade Concessões de Acesso do S3 em sua conta 111122223333 para gerenciar o acesso aos dados do Amazon S3. É necessário criar uma instância da funcionalidade Concessões de Acesso do S3 em cada Região da AWS na qual os dados do S3 que você deseja compartilhar são armazenados. Se você compartilhar dados em mais de uma Região da AWS, repita cada uma dessas etapas de configuração para cada Região da AWS. Se você já tiver uma instância da funcionalidade Concessões de Acesso do S3 na Região da AWS local em que os dados do S3 são armazenados, passe para a próxima etapa. Se você não configurou uma instância da funcionalidade Concessões de Acesso do S3, consulte Trabalhar com instâncias do recurso Concessão de Acesso do S3 para concluir esta etapa.

Etapa 2: configurar a política de recursos da instância da funcionalidade Concessões de Acesso do S3 para conceder acesso entre contas

Depois de criar uma instância da funcionalidade Concessões de Acesso do S3 em sua conta 111122223333 para acesso entre contas, configure a política baseada em recursos para a instância da funcionalidade Concessões de Acesso do S3 em sua conta 111122223333 a fim de conceder acesso entre contas. A instância da funcionalidade Concessões de Acesso do S3 é compatível com políticas baseadas em recurso. Com a política baseada em recursos correta em vigor, você pode conceder a usuários ou perfis do AWS Identity and Access Management (IAM) de outras Contas da

AWS acesso à sua instância da funcionalidade Concessões de Acesso do S3. O acesso entre contas concede somente estas permissões (ações):

- `s3:GetAccessGrantsInstanceForPrefix`: o usuário, o perfil ou a aplicação pode recuperar a instância da funcionalidade Concessões de Acesso do S3 que contém um prefixo específico.
- `s3:ListAccessGrants`
- `s3:ListAccessLocations`
- `s3:ListCallerAccessGrants`
- `s3:GetDataAccess`: o usuário, o perfil ou a aplicação pode solicitar credenciais temporárias com base no acesso concedido por meio da funcionalidade Concessões de Acesso do S3. Use essas credenciais para acessar os dados do S3 aos quais você recebeu acesso.

Você pode escolher quais dessas permissões deseja incluir na política de recursos. Essa política de recursos na instância da funcionalidade Concessões de Acesso do S3 é uma política normal baseada em recursos e é compatível com tudo o que a linguagem de política do IAM permite. Na mesma política, você pode conceder acesso a identidades do IAM específicas na conta `111122223333` (por exemplo, usando a condição `aws:PrincipalArn`), mas não precisa fazer isso com a funcionalidade Concessões de Acesso do S3. Em vez disso, na instância da funcionalidade Concessões de Acesso do S3, é possível criar concessões para identidades do IAM individuais de sua conta, bem como para a outra conta. Ao gerenciar cada concessão de acesso por meio da funcionalidade Concessões de Acesso do S3, você pode escalar suas permissões.

Se você já usa o AWS Resource Access Manager (AWS RAM), é possível utilizá-lo para compartilhar recursos do `s3:AccessGrants` com outras contas ou dentro da sua organização. Para obter mais informações, consulte Working with shared AWS resources. Se você não usa o AWS RAM, também pode adicionar a política de recursos usando as operações de API da funcionalidade Concessões de Acesso do S3 ou a AWS Command Line Interface (AWS CLI).

Usar o console do S3

Recomendamos que você use o console do AWS Resource Access Manager (AWS RAM) para compartilhar recursos do `s3:AccessGrants` com outras contas ou dentro da sua organização. Para compartilhar a funcionalidade Concessões de Acesso do S3 entre contas, faça o seguinte:

Para configurar a política de recursos da instância da funcionalidade Concessões de Acesso do S3:

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.

2. Selecione a Região da AWS no seletor de Região da AWS.
3. No painel de navegação esquerdo, escolha Concessões de acesso.
4. Na página da instância da funcionalidade Concessões de Acesso, na seção Instância nesta conta, selecione Compartilhar instância. Isso redirecionará você para o console do AWS RAM.
5. Selecione Criar compartilhamento de recursos.
6. Siga as etapas do AWS RAM para criar um compartilhamento de recursos. Para obter mais informações, consulte Creating a resource share in AWS RAM.

Como usar o AWS CLI

Para instalar a AWS CLI, consulte Instalar a AWS CLI no Guia do usuário da AWS Command Line Interface.

Você pode adicionar a política de recursos usando o comando `put-access-grants-instance-resource-policy` da CLI.

Quanto ao acesso entre contas para a instância da funcionalidade Concessões de Acesso do S3 que está em sua conta `111122223333`, se você quiser concedê-lo à segunda conta (`444455556666`), a política de recursos da instância da funcionalidade Concessões de Acesso do S3 em sua conta `111122223333` deve dar à segunda conta (`444455556666`) permissão para realizar as seguintes ações:

- `s3:ListAccessGrants`
- `s3:ListAccessGrantsLocations`
- `s3:GetDataAccess`
- `s3:GetAccessGrantsInstanceForPrefix`

Na política de recursos da instância da funcionalidade Concessões de Acesso do S3, especifique o ARN da sua instância da funcionalidade Concessões de Acesso do S3 como o `Resource` e a segunda conta (`444455556666`) como a `Principal`. Para usar o exemplo a seguir, substitua os *`espaços reservados para entrada do usuário`* por suas próprias informações.

```
{
"Version": "2012-10-17",
"Statement": [
{
 "Effect": "Allow",
```

```
 "Principal": {
 "AWS": "444455556666"
},
 "Action": [
  "s3:ListAccessGrants",
  "s3:ListAccessGrantsLocations",
  "s3:GetDataAccess",
  "s3:GetAccessGrantsInstanceForPrefix"
 ],
 "Resource": "arn:aws:s3:us-east-2:111122223333:access-grants/default"
} ]
}
```

Para adicionar ou atualizar a política de recursos da instância da funcionalidade Concessões de Acesso do S3, use o comando a seguir. Ao usar o comando de exemplo a seguir, substitua os *user input placeholders* por suas próprias informações.

Example Adicionar ou atualizar uma política de recursos da instância da funcionalidade Concessões de Acesso do S3

```
aws s3control put-access-grants-instance-resource-policy \
--account-id 111122223333 \
--policy file://resourcePolicy.json \
--region us-east-2
{
 "Policy": "{\n
   \"Version\": \"2012-10-17\",\n
   \"Statement\": [{\n
  \"Effect\": \"Allow\",\n
  \"Principal\": {\n
    \"AWS\": \"444455556666\"\n
  },\n
  \"Action\": [\n
    \"s3:ListAccessGrants\",\n
    \"s3:ListAccessGrantsLocations\",\n
    \"s3:GetDataAccess\",\n
    \"s3:GetAccessGrantsInstanceForPrefix\",\n
    \"s3:ListCallerAccessGrants\"\n
  ],\n
  \"Resource\": \"arn:aws:s3:us-east-2:111122223333:access-grants/default\"\n
    }\n
   ]\n
```

```
    }\n",
  "CreatedAt": "2023-06-16T00:07:47.473000+00:00"
 }
```

Example Obter uma política de recursos da funcionalidade Concessões de Acesso do S3

Você também pode usar a CLI para obter ou excluir uma política de recursos para uma instância da funcionalidade Concessões de Acesso do S3.

Para obter uma política de recursos da funcionalidade Concessões de Acesso do S3, use o comando de exemplo a seguir. Para usar esse exemplo de comando, substitua os *user input placeholders* por suas próprias informações.

```
aws s3control get-access-grants-instance-resource-policy \
--account-id 111122223333 \
--region us-east-2

{
"Policy": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect\":\"Allow
\",\"Principal\":{\"AWS\":\"arn:aws:iam::111122223333:root\"},\"Action\":
[\"s3:ListAccessGrants\",\"s3:ListAccessGrantsLocations\",\"s3:GetDataAccess\",
\"s3:GetAccessGrantsInstanceForPrefix\",\"s3:ListCallerAccessGrants\"],\"Resource\":
\"arn:aws:
s3:us-east-2:111122223333:access-grants/default\"}]}",
"CreatedAt": "2023-06-16T00:07:47.473000+00:00"
}
```

Example Excluir uma política de recursos da funcionalidade Concessões de Acesso do S3

Para excluir uma política de recursos da funcionalidade Concessões de Acesso do S3, use o comando de exemplo a seguir. Para usar esse exemplo de comando, substitua os *user input placeholders* por suas próprias informações.

```
aws s3control delete-access-grants-instance-resource-policy \
--account-id 111122223333 \
--region us-east-2

// No response body
```

Uso da API REST

Você pode adicionar a política de recursos usando a API PutAccessGrantsInstanceResourcePolicy.

Quanto ao acesso entre contas para a instância da funcionalidade Concessões de Acesso do S3 que está em sua conta 111122223333, se você quiser concedê-lo à segunda conta (444455556666), a política de recursos da instância da funcionalidade Concessões de Acesso do S3 em sua conta 111122223333 deve dar à segunda conta (444455556666) permissão para realizar as seguintes ações:

- `s3:ListAccessGrants`
- `s3:ListAccessGrantsLocations`
- `s3:GetDataAccess`
- `s3:GetAccessGrantsInstanceForPrefix`

Na política de recursos da instância da funcionalidade Concessões de Acesso do S3, especifique o ARN da sua instância da funcionalidade Concessões de Acesso do S3 como o `Resource` e a segunda conta (444455556666) como a `Principal`. Para usar o exemplo a seguir, substitua os *espaços reservados para entrada do usuário* por suas próprias informações.

```
{
"Version": "2012-10-17",
"Statement": [
{
 "Effect": "Allow",
 "Principal": {
 "AWS": "444455556666"
},
 "Action": [
  "s3:ListAccessGrants",
  "s3:ListAccessGrantsLocations",
  "s3:GetDataAccess",
  "s3:GetAccessGrantsInstanceForPrefix"
 ],
 "Resource": "arn:aws:s3:us-east-2:111122223333:access-grants/default"
} ]
}
```

Em seguida, você pode usar a API PutAccessGrantsInstanceResourcePolicy para configurar a política.

Para obter informações sobre o suporte à API REST para atualizar, obter ou excluir uma política de recursos para a instância da funcionalidade Concessões de Acesso do S3, consulte as seguintes seções na Referência da API do Amazon Simple Storage Service:

- PutAccessGrantsInstanceResourcePolicy
- GetAccessGrantsInstanceResourcePolicy
- DeleteAccessGrantsInstanceResourcePolicy

Uso dos SDKs da AWS

Esta seção fornece exemplos de SDK da AWS sobre como configurar sua política de recursos da funcionalidade Concessões de Acesso do S3 para conceder a uma segunda conta da AWS acesso a alguns dos seus dados do S3.

Java

Adicione, atualize, obtenha ou exclua uma política de recursos para gerenciar o acesso entre contas a uma instância da funcionalidade Concessões de Acesso do S3.

Example Adicionar ou atualizar uma política de recursos da instância da funcionalidade Concessões de Acesso do S3

Quanto ao acesso entre contas para a instância da funcionalidade Concessões de Acesso do S3 que está em sua conta `111122223333`, se você quiser concedê-lo à segunda conta (`444455556666`), a política de recursos da instância da funcionalidade Concessões de Acesso do S3 em sua conta `111122223333` deve dar à segunda conta (`444455556666`) permissão para realizar as seguintes ações:

- `s3:ListAccessGrants`
- `s3:ListAccessGrantsLocations`
- `s3:GetDataAccess`
- `s3:GetAccessGrantsInstanceForPrefix`

Na política de recursos da instância da funcionalidade Concessões de Acesso do S3, especifique o ARN da sua instância da funcionalidade Concessões de Acesso do S3 como o `Resource` e a segunda conta (`444455556666`) como a `Principal`. Para usar o exemplo a seguir, substitua os *`espaços reservados para entrada do usuário`* por suas próprias informações.

```
{
"Version": "2012-10-17",
"Statement": [
{
 "Effect": "Allow",
 "Principal": {
 "AWS": "444455556666"
},
 "Action": [
  "s3:ListAccessGrants",
  "s3:ListAccessGrantsLocations",
  "s3:GetDataAccess",
  "s3:GetAccessGrantsInstanceForPrefix"
 ],
 "Resource": "arn:aws:s3:us-east-2:111122223333:access-grants/default"
} ]
}
```

Para adicionar ou atualizar uma política de recursos da instância da funcionalidade Concessões de Acesso do S3, você pode usar o seguinte código de exemplo:

```
public void putAccessGrantsInstanceResourcePolicy() {
 PutAccessGrantsInstanceResourcePolicyRequest putRequest =
 PutAccessGrantsInstanceResourcePolicyRequest.builder()
 .accountId(111122223333)
 .policy(RESOURCE_POLICY)
 .build();
 PutAccessGrantsInstanceResourcePolicyResponse putResponse =
 s3Control.putAccessGrantsInstanceResourcePolicy(putRequest);
 LOGGER.info("PutAccessGrantsInstanceResourcePolicyResponse: " + putResponse);
 }
```

Resposta:

```
PutAccessGrantsInstanceResourcePolicyResponse(
 Policy={
 "Version": "2012-10-17",
 "Statement": [{
 "Effect": "Allow",
 "Principal": {
 "AWS": "444455556666"
 },
```

```
 "Action": [
 "s3:ListAccessGrants",
 "s3:ListAccessGrantsLocations",
 "s3:GetDataAccess",
 "s3:GetAccessGrantsInstanceForPrefix",
 "s3:ListCallerAccessGrants"
 ],
 "Resource": "arn:aws:s3:us-east-2:111122223333:access-grants/default"
 }]
 }
 )
```

Example Obter uma política de recursos da funcionalidade Concessões de Acesso do S3

Para obter uma política de recursos da funcionalidade Concessões de Acesso do S3, você pode usar o código de exemplo a seguir. Para usar o comando a seguir, substitua os *user input placeholders* por suas próprias informações.

```
public void getAccessGrantsInstanceResourcePolicy() {
 GetAccessGrantsInstanceResourcePolicyRequest getRequest =
 GetAccessGrantsInstanceResourcePolicyRequest.builder()
 .accountId(111122223333)
 .build();
 GetAccessGrantsInstanceResourcePolicyResponse getResponse =
 s3Control.getAccessGrantsInstanceResourcePolicy(getRequest);
 LOGGER.info("GetAccessGrantsInstanceResourcePolicyResponse: " + getResponse);
 }
```

Resposta:

```
GetAccessGrantsInstanceResourcePolicyResponse(
 Policy={"Version":"2012-10-17","Statement":[{"Effect":"Allow","Principal":
{"AWS":"arn:aws:iam::444455556666:root"},"Action":
["s3:ListAccessGrants","s3:ListAccessGrantsLocations","s3:GetDataAccess","s3:GetAccessGrants
east-2:111122223333:access-grants/default"}]},
 CreatedAt=2023-06-15T22:54:44.319Z
 )
```

Example Excluir uma política de recursos da funcionalidade Concessões de Acesso do S3

Para excluir uma política de recursos da funcionalidade Concessões de Acesso do S3, você pode usar o código de exemplo a seguir. Para usar o comando a seguir, substitua os *user input placeholders* por suas próprias informações.

```
public void deleteAccessGrantsInstanceResourcePolicy() {
 DeleteAccessGrantsInstanceResourcePolicyRequest deleteRequest =
 DeleteAccessGrantsInstanceResourcePolicyRequest.builder()
 .accountId(111122223333)
 .build();
 DeleteAccessGrantsInstanceResourcePolicyResponse deleteResponse =
 s3Control.putAccessGrantsInstanceResourcePolicy(deleteRequest);
 LOGGER.info("DeleteAccessGrantsInstanceResourcePolicyResponse: " + deleteResponse);
 }
```

Resposta:

```
DeleteAccessGrantsInstanceResourcePolicyResponse()
```

Etapa 3: conceder às identidades do IAM em uma segunda conta permissão para chamar a instância da funcionalidade Concessões de Acesso do S3 em sua conta

Depois que o proprietário dos dados do Amazon S3 configurar a política entre contas para a instância da funcionalidade Concessões de Acesso do S3 na conta 111122223333, o proprietário da segunda conta (444455556666) deverá criar uma política baseada em identidade para seus usuários ou perfis do IAM e o proprietário deverá conceder a eles acesso à instância da funcionalidade Concessões de Acesso do S3. Na política baseada em identidade, inclua uma ou mais das seguintes ações, dependendo do que é concedido na política de recursos da instância da funcionalidade Concessões de Acesso do S3 e das permissões que você deseja conceder:

- `s3:ListAccessGrants`
- `s3:ListAccessGrantsLocations`
- `s3:GetDataAccess`
- `s3:GetAccessGrantsInstanceForPrefix`
- `s3:ListCallerAccessGrants`

De acordo com o padrão de acesso entre contas da AWS, os usuários ou perfis do IAM na segunda conta (444455556666) devem ter explicitamente uma ou mais dessas permissões. Por exemplo, conceda a permissão `s3:GetDataAccess` para que o usuário ou perfil do IAM possa chamar a instância da funcionalidade Concessões de Acesso do S3 na conta 111122223333 para solicitar credenciais.

Para usar esse exemplo de comando, substitua os *`user input placeholders`* por suas próprias informações.

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
  "Effect": "Allow",
  "Action": [
   "s3:GetDataAccess",
  ],
   "Resource": "arn:aws:s3:us-east-2:111122223333:access-grants/default"
  }
 ]
}
```

Para obter mais informações sobre como editar uma política do IAM baseada em identidade, consulte Edição de políticas do IAM no AWS Identity and Access ManagementGuia do usuário do IAM.

Etapa 4: criar uma concessão na instância da funcionalidade Concessões de Acesso do S3 de sua conta que dê à entidade principal do IAM na segunda conta acesso a alguns de seus dados do S3.

Na etapa final de configuração, você pode criar uma concessão na instância da funcionalidade Concessões de Acesso do S3 em sua conta 111122223333 que dê acesso à identidade do IAM na segunda conta (444455556666) a alguns dos dados do S3 em sua conta. Isso pode ser feito usando o console do Amazon S3, a CLI, a API e os SDKs. Para obter mais informações, consulte Criar concessões.

Na concessão, especifique o ARN da AWS da identidade do IAM da segunda conta e especifique a qual local nos seus dados do S3 (um bucket, prefixo ou objeto) você está concedendo acesso. Esse local já deve estar registrado na instância da funcionalidade Concessões de Acesso do S3.

Para obter mais informações, consulte Registrar um local. Você tem a opção de especificar um subprefixo. Por exemplo, se o local ao qual você está concedendo acesso for um bucket e quiser limitar ainda mais o acesso a um objeto específico nesse bucket, passe o nome da chave do objeto no campo `S3SubPrefix`. Ou, se você quiser limitar o acesso aos objetos no bucket com nomes de chave que começam com um prefixo específico, como `2024-03-research-results/`, passe `S3SubPrefix=2024-03-research-results/`.

Veja a seguir um exemplo de comando da CLI para criar uma concessão de acesso para uma identidade na segunda conta. Consulte Criar concessões para obter mais informações. Para usar esse exemplo de comando, substitua os *`user input placeholders`* por suas próprias informações.

```
aws s3control create-access-grant \
--account-id 111122223333 \
--access-grants-location-id default \
--access-grants-location-configuration S3SubPrefix=prefixA* \
--permission READ \
--grantee GranteeType=IAM,GranteeIdentifier=arn:aws:iam::444455556666:role/data-consumer-1
```

Depois de configurar o acesso entre contas, o usuário ou perfil na segunda conta pode fazer o seguinte:

- Chamar `ListAccessGrantsInstances` para listar as instâncias da funcionalidade Concessões de Acesso do S3 compartilhadas com ele por meio do AWS RAM. Para obter mais informações, consulte Obter os detalhes de uma instância do recurso Concessão de Acesso do S3.
- Solicitar credenciais temporárias da funcionalidade Concessões de Acesso do S3. Para obter informações sobre como fazer essas solicitações, consulte Solicitar acesso aos dados do Amazon S3 por meio da funcionalidade Concessões de Acesso do S3.

Usar etiquetas da AWS com a funcionalidade Concessões de Acesso do S3

As etiquetas na funcionalidade Concessões de Acesso do Amazon S3 têm características semelhantes às etiquetas de objeto no Amazon S3. Cada tag é um par de chave/valor. Os recursos na funcionalidade Concessões de Acesso do S3 que você pode marcar são instâncias, locais e concessões da funcionalidade Concessões de Acesso do S3.

> **Note**
>
> A marcação na funcionalidade Concessões de Acesso do S3 usa operações de API diferentes da marcação de objetos. A funcionalidade Concessões de Acesso do S3 usa as operações de API TagResource, UntagResource e ListTagsForResource, em que um recurso pode ser uma instância, um local registrado ou uma concessão de acesso da funcionalidade Concessões de Acesso do S3.

Semelhante às etiquetas de objeto, as seguintes limitações se aplicam:

- Você pode adicionar etiquetas a novos recursos da funcionalidade Concessões de Acesso do S3 ao criá-los, ou pode adicionar etiquetas a recursos existentes.
- Você pode associar até 10 etiquetas a um recurso. Se várias etiquetas estiverem associadas ao mesmo recurso, elas deverão ter chaves de etiqueta exclusivas.
- Um chave de tag pode ter até 128 caracteres Unicode e os valores de tag podem ter até 256 caracteres Unicode. As etiquetas são representadas internamente em UTF-16. Em UTF-16, os caracteres utilizam posições de um ou de dois caracteres.
- As chaves e os valores diferenciam letras maiúsculas de minúsculas.

Para obter mais informações sobre restrições de etiquetas, consulte Restrições de tags definidas pelo usuário no Guia do usuário do AWS Billing.

Você pode marcar recursos na funcionalidade Concessões de Acesso do S3 usando a AWS Command Line Interface (AWS CLI), a API REST do Amazon S3 ou os AWS SDKs.

Como usar o AWS CLI

Para instalar a AWS CLI, consulte Instalar a AWS CLI no Guia do usuário da AWS Command Line Interface.

Você pode marcar um recurso da funcionalidade Concessões de Acesso do S3 durante a criação ou depois de criá-lo. Os exemplos a seguir mostram como marcar ou desmarcar uma instância da funcionalidade Concessões de Acesso do S3. Você pode realizar operações semelhantes para locais registrados e concessões de acesso.

Para usar os comandos a seguir, substitua os *`user input placeholders`* por suas próprias informações.

Example : criar uma instância da funcionalidade Concessões de Acesso do S3

```
aws s3control create-access-grants-instance \
 --account-id 111122223333 \
 --profile access-grants-profile \
 --region us-east-2 \
 --tags Key=tagKey1,Value=tagValue1
```

Resposta:

```
 {
    "CreatedAt": "2023-10-25T01:09:46.719000+00:00",
    "AccessGrantsInstanceId": "default",
    "AccessGrantsInstanceArn": "arn:aws:s3:us-east-2:111122223333:access-grants/
default"
}
```

Example : marcar uma instância já criada da funcionalidade Concessões de Acesso do S3

```
aws s3control tag-resource \
--account-id 111122223333 \
--resource-arn "arn:aws:s3:us-east-2:111122223333:access-grants/default" \
--profile access-grants-profile \
--region us-east-2 \
--tags Key=tagKey2,Value=tagValue2
```

Example : listar as etiquetas da instância da funcionalidade Concessões de Acesso do S3

```
aws s3control list-tags-for-resource \
--account-id 111122223333 \
--resource-arn "arn:aws:s3:us-east-2:111122223333:access-grants/default" \
--profile access-grants-profile \
--region us-east-2
```

Resposta:

```
{
    "Tags": [
        {
            "Key": "tagKey1",
```

```
            "Value": "tagValue1"
        },
        {
            "Key": "tagKey2",
            "Value": "tagValue2"
        }
    ]
}
```

Example : desmarcar a instância da funcionalidade Concessões de Acesso do S3

```
aws s3control untag-resource \
 --account-id 111122223333 \
 --resource-arn "arn:aws:s3:us-east-2:111122223333:access-grants/default" \
 --profile access-grants-profile \
 --region us-east-2 \
 --tag-keys "tagKey2"
```

Uso da API REST

Você pode usar a API do Amazon S3 para marcar, desmarcar ou listar as etiquetas de uma instância, um local registrado ou uma concessão de acesso da funcionalidade Concessões de Acesso do S3. Para obter informações sobre o suporte à API REST para gerenciar a funcionalidade Concessões de Acesso do S3, consulte as seguintes seções na Referência da API do Amazon Simple Storage Service:

- TagResource
- UntagResource
- ListTagsForResource

Limitações da funcionalidade Concessões de Acesso do S3

A funcionalidade Concessões de Acesso do S3 tem as seguintes limitações:

> **Note**
>
> Se o seu caso de uso exceder essas limitações, entre em contato com o AWS Support para solicitar limites maiores.

Instância da funcionalidade Concessões de Acesso do S3

Você pode criar uma instância da funcionalidade Concessões de Acesso do S3 por Região da AWS por conta. Consulte Criar uma instância da funcionalidade Concessões de Acesso do S3.

Local da funcionalidade Concessões de Acesso do S3

Você pode registrar 1.000 locais da funcionalidade Concessões de Acesso do S3 por instância da funcionalidade Concessões de Acesso do S3. Consulte Register an S3 Access Grants location.

Concessão

Você pode criar 100.000 concessões por instância da funcionalidade Concessões de Acesso do S3. Consulte Create a grant.

Regiões da AWS de Concessões de Acesso do S3

No momento, a Concessão de Acesso do S3 está disponível nas seguintes Regiões da AWS:

Código Região da AWS	Nome da Região da AWS
`us-east-1`	Leste dos EUA (Norte da Virgínia)
`us-east-2`	Leste dos EUA (Ohio)
`us-west-1`	Oeste dos EUA (Norte da Califórnia)
`us-west-2`	Oeste dos EUA (Oregon)
`af-south-1`	África (Cidade do Cabo)
`ap-east-1`	Ásia Pacífico (Hong Kong)
`ap-northeast-1`	Ásia-Pacífico (Tóquio)
`ap-northeast-2`	Ásia-Pacífico (Seul)
`ap-northeast-3`	Asia Pacific (Osaka)
`ap-south-1`	Ásia-Pacífico (Mumbai)
`ap-south-2`	Ásia-Pacífico (Hyderabad)

Código Região da AWS	Nome da Região da AWS
ap-southeast-1	Ásia-Pacífico (Singapura)
ap-southeast-2	Ásia-Pacífico (Sydney)
ap-southeast-3	Ásia-Pacífico (Jacarta)
ap-southeast-4	Ásia-Pacífico (Melbourne)
ca-central-1	Canadá (Central)
ca-west-1	Oeste do Canadá (Calgary)
eu-central-1	Europa (Frankfurt)
eu-central-2	Europa (Zurique)
eu-north-1	Europa (Estocolmo)
eu-south-1	Europa (Milão)
eu-south-2	Europa (Espanha)
eu-west-1	Europa (Irlanda)
eu-west-2	Europa (Londres)
eu-west-3	Europa (Paris)
il-central-1	Israel (Tel Aviv)
me-central-1	Oriente Médio (Emirados Árabes Unidos)
me-south-1	Middle East (Bahrain)
sa-east-1	South America (São Paulo)
us-gov-east-1	AWS GovCloud (Leste dos EUA)
us-gov-west-1	AWS GovCloud (Oeste dos EUA)

Integrações da funcionalidade Concessões de Acesso do S3

A funcionalidade Concessões de Acesso do S3 pode ser usada com os seguintes serviços e recursos da AWS. Esta página será atualizada à medida que novas integrações forem disponibilizadas.

> **Tip**
>
> Este workshop da AWS sobre o Concessão de Acesso do S3 explica como usar esse recurso com usuários do AWS Identity and Access Management (IAM), usuários do Centro de Identidade do IAM, o Amazon EMR e o AWS Transfer Family.

Amazon Athena

- Usar grupos de trabalho do Athena habilitados para o Centro de Identidade do IAM

Amazon EMR

- Launch an Amazon EMR cluster with S3 Access Grants

Amazon EMR no EKS

- Launch an Amazon EMR on EKS cluster with S3 Access Grants

Aplicação do Amazon EMR Sem Servidor

- Launch an Amazon EMR Serverless application with S3 Access Grants

Amazon Redshift

- Amazon Redshift integration with Amazon S3 Access Grants

Amazon SageMaker AI Studio

- Usar a funcionalidade Concessão de Acesso do Amazon S3 com o Amazon SageMaker AI Studio e o plug-in SDK para Python (Boto3)

  Usar a funcionalidade Concessão de Acesso do S3 em cadernos do Amazon SageMaker AI Studio agora ficou mais fácil utilizando o plug-in SDK para Python (Boto3). Configure concessões de acesso para entidades principais do IAM e usuários do diretório do AWS IAM Identity Center com antecedência. Embora o Amazon SageMaker AI Studio não comporte de modo nativo usuários do diretório de provedores de identidades, é possível escrever código Python

personalizado usando o plug-in que permite que essas identidades acessem dados do S3 por meio da funcionalidade Concessão de Acesso do S3. O acesso aos dados ocorre com a ajuda do plug-in e não por meio do Amazon SageMaker AI.

AWS Glue

- Concessão de Acesso do Amazon S3 com o AWS Glue

AWS IAM Identity Center

- Trusted identity propagation across applications

AWS Transfer Family

- Configurar a funcionalidade Concessão de Acesso do Amazon S3 para o AWS Transfer Family

Navegador de Armazenamento para S3

- Gerenciar o acesso aos dados em grande escala usando o Navegador de Armazenamento para S3

Frameworks Python de código aberto

- O recurso Concessão de Acesso do Amazon S3 agora se integra a frameworks Python de código aberto.

Gerenciar o acesso com ACLs

As listas de controle de acesso (ACLs) são uma das opções baseadas em recursos que podem ser usadas para gerenciar o acesso a buckets e objetos. Use as ACLs para conceder permissões básicas de leitura/gravação a outras Contas da AWS. Existem limites para gerenciar permissões usando ACLs.

Por exemplo, é possível conceder permissões apenas a outras Contas da AWS. Não é possível conceder permissões a usuários da sua conta. Não é possível conceder permissões condicionais, nem negar permissões explicitamente. As ACLs são adequadas para cenários específicos. Por exemplo, se um proprietário do bucket permite que outras Contas da AWS carreguem objetos, as permissões para esses objetos só podem ser gerenciadas com a ACL do objeto pela Conta da AWS que é proprietária do objeto.

A Propriedade de objetos do S3 é uma configuração no nível do bucket do Amazon S3 que você pode usar para controlar a propriedade de objetos carregados no bucket e para desabilitar

ou habilitar as ACLs. Por padrão, a Propriedade de Objetos está definida com a configuração Imposto pelo proprietário do bucket e todas as ACLs estão desabilitadas. Quando as ACLs são desabilitadas, o proprietário do bucket possui todos os objetos do bucket e gerencia o acesso a eles exclusivamente usando políticas de gerenciamento de acesso.

A maioria dos casos de uso modernos no Amazon S3 não exige mais o uso de ACLs. Recomendamos manter as ACLs desabilitadas, exceto em circunstâncias incomuns em que seja necessário controlar o acesso para cada objeto individualmente. Com as ACLs desabilitadas, é possível usar políticas para controlar o acesso a todos os objetos no bucket, independentemente de quem carregou os objetos para o bucket. Para obter mais informações, consulte Controlar a propriedade de objetos e desabilitar ACLs para seu bucket.

> **Important**
>
> Se o bucket de uso geral utilizar a configuração “Imposto pelo proprietário do bucket” para a Propriedade de objetos do S3, será necessário usar políticas para conceder acesso ao bucket de uso geral e aos objetos contidos nele. Quando a configuração Imposto pelo proprietário do bucket estiver habilitada, as solicitações para definir listas de controle de acesso (ACLs) ou atualizar ACLs falharão e retornarão o código de erro `AccessControlListNotSupported`. Ainda há suporte para solicitações de leitura de ACLs.

Para obter mais informações sobre ACLs, consulte os tópicos a seguir.

Tópicos

- Visão geral da lista de controle de acesso (ACL)
- Configurar ACLs
- Exemplos de política para ACLs

Visão geral da lista de controle de acesso (ACL)

As listas de controle de acesso (ACLs) do Amazon S3 permitem o gerenciamento do acesso aos buckets e objetos. Cada bucket e objeto tem uma ACL anexada como um sub-recurso. Ela define a quais grupos ou Contas da AWS o acesso é concedido, bem como o tipo de acesso. Quando um recurso é solicitado, o Amazon S3 consulta a ACL correspondente para verificar se o solicitante tem as permissões de acesso necessárias.

A Propriedade de objetos do S3 é uma configuração no nível do bucket do Amazon S3 que você pode usar para controlar a propriedade de objetos carregados no bucket e para desabilitar ou habilitar as ACLs. Por padrão, a Propriedade de Objetos está definida com a configuração Imposto pelo proprietário do bucket e todas as ACLs estão desabilitadas. Quando as ACLs são desabilitadas, o proprietário do bucket possui todos os objetos do bucket e gerencia o acesso a eles exclusivamente usando políticas de gerenciamento de acesso.

A maioria dos casos de uso modernos no Amazon S3 não exige mais o uso de ACLs. Recomendamos manter as ACLs desabilitadas, exceto em circunstâncias incomuns em que seja necessário controlar o acesso para cada objeto individualmente. Com as ACLs desabilitadas, é possível usar políticas para controlar o acesso a todos os objetos no bucket, independentemente de quem carregou os objetos para o bucket. Para obter mais informações, consulte Controlar a propriedade de objetos e desabilitar ACLs para seu bucket.

> **Important**
>
> Se o bucket de uso geral utilizar a configuração “Imposto pelo proprietário do bucket” para a Propriedade de objetos do S3, será necessário usar políticas para conceder acesso ao bucket de uso geral e aos objetos contidos nele. Quando a configuração Imposto pelo proprietário do bucket estiver habilitada, as solicitações para definir listas de controle de acesso (ACLs) ou atualizar ACLs falharão e retornarão o código de erro `AccessControlListNotSupported`. Ainda há suporte para solicitações de leitura de ACLs.

Quando você cria um bucket ou um objeto, o Amazon S3 cria uma ACL padrão que concede ao proprietário do recurso controle total sobre o recurso. Isso é exibido no seguinte exemplo de ACL de bucket (a ACL de objeto padrão tem a mesma estrutura):

Example

```
<?xml version="1.0" encoding="UTF-8"?>
<AccessControlPolicy xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Owner>
    <ID>*** Owner-Canonical-User-ID ***</ID>
    <DisplayName>owner-display-name</DisplayName>
  </Owner>
  <AccessControlList>
    <Grant>
```

```
      <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
               xsi:type="Canonical User">
        <ID>*** Owner-Canonical-User-ID ***</ID>
        <DisplayName>display-name</DisplayName>
      </Grantee>
      <Permission>FULL_CONTROL</Permission>
    </Grant>
  </AccessControlList>
</AccessControlPolicy>
```

A ACL de exemplo inclui um elemento `Owner` que identifica o proprietário pelo ID de usuário canônico da Conta da AWS. Para obter instruções sobre como encontrar seu ID de usuário canônico, consulte Encontrar um ID de usuário canônico da Conta da AWS. O elemento `Grant` identifica o favorecido (uma Conta da AWS ou um grupo predefinido) e a permissão concedida. Esta ACL padrão tem um elemento `Grant` para o proprietário. Conceda permissões adicionando elementos `Grant`, com cada concessão identificando o favorecido e a permissão.

> **Note**
>
> Uma ACL pode ter até 100 concessões.

Tópicos

- Quem é o favorecido?
- Quais permissões posso conceder?
- Valores aclRequired para solicitações comuns do Amazon S3
- Amostra de ACL
- ACL pré-configurada

Quem é o favorecido?

> **Important**
>
> Aviso de fim de suporte: a partir de 1.º de outubro de 2025, o Amazon S3 interromperá o suporte à criação de listas de controle de acesso (ACL) de beneficiários por e-mail. As ACLs de beneficiários por e-mail criadas antes dessa data continuarão funcionando e permanecerão acessíveis por meio do Console de Gerenciamento da AWS, da interface de

linha de comandos (CLI), dos SDKs e da API REST. No entanto, você não poderá mais criar outras ACLs de beneficiários por e-mail.
Entre 15 de julho de 2025 e 1.º de outubro de 2025, você começará a ver uma taxa crescente de erros `HTTP 405` nas solicitações ao Amazon S3 ao tentar criar ACLs de beneficiários por e-mail.
Essa mudança afeta as seguintes regiões:Regiões da AWS: Leste dos EUA (Norte da Virgínia), Oeste dos EUA (N. da Califórnia), Oeste dos EUA (Oregon), Ásia-Pacífico (Singapura), Ásia-Pacífico (Sydney), Ásia-Pacífico (Tóquio), Europa (Irlanda) e América do Sul (São Paulo).

O favorecido pode ser uma Conta da AWS ou um dos grupos predefinidos do Amazon S3. Você concede permissão a uma Conta da AWS usando o endereço de e-mail ou o ID de usuário canônico. No entanto, se você fornecer um endereço de e-mail na solicitação de concessão, o Amazon S3 encontrará o ID de usuário canônico para essa conta e o adicionará à ACL. As ACLs resultantes sempre conterão o ID de usuário canônico para a Conta da AWS, e não o endereço de e-mail da Conta da AWS.

Ao conceder direitos de acesso, você especifica cada favorecido como um par de *`type`*`"`*`value`*`"`, em que *`type`* é um dos seguintes:

- `id`: se o valor especificado é o ID de usuário canônico de uma Conta da AWS
- `uri`: se as permissões estiverem sendo concedidas a um grupo predefinido
- `emailAddress`: se o valor especificado é o endereço de e-mail de uma Conta da AWS

Important

O uso de endereços de e-mail para especificar um favorecido tem suporte somente nas seguintes regiões da AWS:

- Leste dos EUA (Norte da Virgínia)
- Oeste dos EUA (Norte da Califórnia)
- Oeste dos EUA (Oregon)
- Ásia-Pacífico (Singapura)
- Ásia-Pacífico (Sydney)
- Ásia-Pacífico (Tóquio)

- Europa (Irlanda)
- América do Sul (São Paulo)

Para obter uma lista de todas as regiões e endpoints compatíveis com o Amazon S3, consulte Regiões e endpoints na Referência geral da Amazon Web Services.

Example Exemplo: endereço de e-mail

Por exemplo, o cabeçalho `x-amz-grant-read` a seguir concede às Contas da AWS identificadas por endereços de e-mail permissões para ler dados de objetos e os respectivos metadados:

```
x-amz-grant-read: emailAddress="xyz@example.com", emailAddress="abc@example.com"
```

Warning

Ao conceder aos recursos acesso a outras Contas da AWS, esteja ciente de que as Contas da AWS podem delegar as permissões delas a usuários de suas próprias contas. Isso é conhecido como acesso entre contas. Para obter informações sobre como usar o acesso entre contas, consulte Criar uma função para delegar permissões a um usuário do IAM no Guia do usuário do IAM.

Encontrar um ID de usuário canônico da Conta da AWS

O ID de usuário canônico está associado à Conta da AWS. Esse ID é uma longa string de caracteres, como:

`79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be`

Para obter informações sobre como encontrar o ID de usuário canônico de sua conta, consulte Find the canonical user ID for your Conta da AWS no Guia de referência de gerenciamento de contas da AWS.

Você também pode pesquisar o ID de usuário canônico de uma Conta da AWS lendo a ACL de um bucket ou objeto para o qual a Conta da AWS tem permissões de acesso. Quando uma Conta da AWS individual recebe permissões por meio de uma solicitação de concessão, um registro de concessão é adicionado à ACL com o ID de usuário canônico da conta.

> **Note**
>
> Se você tornar seu bucket público (não recomendado) qualquer usuário não autenticado poderá carregar objetos para o bucket. Esses usuários anônimos não têm uma Conta da AWS. Quando um usuário anônimo carrega um objeto no bucket, o Amazon S3 adiciona um ID de usuário canônico especial (`65a011a29cdf8ec533ec3d1ccaae921c`) como o proprietário do objeto na ACL. Para obter mais informações, consulte Propriedade de bucket e objeto do Amazon S3.

Grupos predefinidos do Amazon S3

O Amazon S3 tem um conjunto de grupos predefinidos. Ao conceder acesso de conta a um grupo, especifique um dos URIs do Amazon S3 em vez do ID de usuário canônico. O Amazon S3 fornece os seguintes grupos predefinidos:

- Grupo Usuários autenticados: representado por `http://acs.amazonaws.com/groups/global/AuthenticatedUsers`.

  Este grupo representa todas as Contas da AWS. A permissão de acesso a esse grupo permite que qualquer Conta da AWS acesse o recurso. No entanto, todas as solicitações devem estar assinadas (autenticadas).

  > **Warning**
  >
  > Quando você concede acesso ao grupo Usuários autenticados, qualquer usuário autenticado da AWS em todo o mundo pode acessar seu recurso.

- Grupo Todos os usuários: representado por `http://acs.amazonaws.com/groups/global/AllUsers`.

  A permissão de acesso a esse grupo permite que qualquer um acesse o recurso. As solicitações podem estar assinadas (autenticadas) ou não (anônimas). As solicitações não assinadas omitem o cabeçalho Autenticação na solicitação.

  > **Warning**
  >
  > Recomendamos fortemente que você nunca conceda ao grupo All Users permissões `WRITE`, `WRITE_ACP` ou `FULL_CONTROL`. Por exemplo, embora as permissões `WRITE`

impeçam que não proprietários substituam ou excluam objetos existentes, as permissões `WRITE` ainda permitem que qualquer pessoa armazene objetos no bucket, e isso é cobrado de você. Para obter mais informações sobre essas permissões, consulte a seguinte seção Quais permissões posso conceder?.

- Grupo Entrega de logs: representado por `http://acs.amazonaws.com/groups/s3/LogDelivery`.

  A permissão `WRITE` em um bucket permite que esse grupo grave logs de acesso ao servidor (consulte Registrar em log as solicitações com registro em log de acesso ao servidor) no bucket.

> **Note**
>
> Ao usar ACLs, um favorecido pode ser uma Conta da AWS ou um dos grupos predefinidos do Amazon S3. No entanto, o favorecido não pode ser um usuário do IAM. Para obter mais informações sobre usuários da AWS e permissões no IAM, consulte Usar o AWS Identity and Access Management.

Quais permissões posso conceder?

A tabela a seguir lista o conjunto de permissões para as quais o Amazon S3 oferece suporte em uma ACL. O conjunto de permissões da ACL é o mesmo para a ACL de objetos e para a ACL de bucket. No entanto, dependendo do contexto (ACL de buckets ou ACL de objetos), essas permissões da ACL concedem permissão para operações de bucket ou objeto específicas. A tabela lista as permissões e descreve seus significados no contexto de objetos e buckets.

Para obter mais informações sobre permissões de ACL no console do Amazon S3, consulte Configurar ACLs.

Permissão	Quando concedida em um bucket	Quando concedida em um objeto
`READ`	Permite ao favorecido listar os objetos no bucket	Permite ao favorecido ler os dados do objeto e seus metadados
`WRITE`	Permite que o favorecido crie novos objetos no bucket. Para os proprietários de bucket e objeto de objetos existente	Não aplicável

Permissão	Quando concedida em um bucket	Quando concedida em um objeto
	s, também permite exclusões e substituições desses objetos.	
`READ_ACP`	Permite ao favorecido ler a ACL do bucket	Permite ao favorecido ler a ACL do objeto
`WRITE_ACP`	Permite ao favorecido gravar a ACL para o bucket aplicável	Permite ao favorecido gravar a ACL para o objeto aplicável
`FULL_CONTROL`	Permite ao beneficiário as permissões `READ`, `WRITE`, `READ_ACP` e `WRITE_ACP` no bucket	Permite ao beneficiário as permissões `READ`, `READ_ACP` e `WRITE_ACP` no objeto

> **Warning**
>
> Tenha cuidado ao conceder permissões de acesso a buckets e objetos do S3. Por exemplo, conceder acesso de `WRITE` a um bucket permite que o favorecido crie objetos no bucket. É altamente recomendável que você leia toda a seção Visão geral da lista de controle de acesso (ACL) antes de conceder permissões.

Mapeamento das permissões da ACL e das permissões da política de acesso

Conforme mostrado na tabela anterior, uma ACL concede apenas um conjunto finito de permissões, em comparação com o número de permissões que pode ser definido em uma política de acesso (consulte Ações de políticas para o Amazon S3). Cada uma dessas permissões permite uma ou mais operações do Amazon S3.

A tabela a seguir mostra como cada uma das permissões da ACL se correlaciona com as permissões de política de acesso correspondentes. Como você pode ver, a política de acesso permite mais permissões que uma ACL. Use ACLs principalmente para conceder permissões básicas de leitura/gravação, similares às permissões de sistema de arquivos. Para obter mais informações sobre quando usar uma ACL, consulte Gerenciamento de identidade e acesso para o Amazon S3.

Para obter mais informações sobre permissões de ACL no console do Amazon S3, consulte Configurar ACLs.

Permissão da ACL	Permissões correspondentes da política de acesso quando permissões da ACL são concedidas em um bucket	Permissões correspondentes da política de acesso quando permissões da ACL são concedidas em um objeto
READ	s3:ListBucket , s3:ListBucketVersions , e s3:ListBucketMultipartUploads	s3:GetObject e s3:GetObjectVersion
WRITE	s3:PutObject O proprietário do bucket pode criar, substituir e excluir qualquer objeto no bucket, e o proprietário do objeto tem FULL_CONTROL sobre seu objeto. Além disso, quando o favorecido é o proprietário do bucket, conceder a permissão WRITE em uma ACL do bucket permite que a ação s3:DeleteObjectVersion seja executada em qualquer versão naquele bucket.	Não aplicável
READ_ACP	s3:GetBucketAcl	s3:GetObjectAcl e s3:GetObjectVersionAcl
WRITE_ACP	s3:PutBucketAcl	s3:PutObjectAcl e s3:PutObjectVersionAcl
FULL_CONTROL	Equivalente a conceder as permissões READ, WRITE, READ_ACP e WRITE_ACP da ACL. Assim, essa permissão da ACL equivale à combinação das permissões correspondentes da política de acesso.	Equivalente a conceder as permissões READ, READ_ACP e WRITE_ACP da ACL. Assim, essa permissão da ACL equivale à combinação das permissões correspondentes da política de acesso.

Chaves de condição

Ao conceder permissões de política de acesso, você pode usar chaves de condição para restringir o valor da ACL em um objeto usando uma política de bucket. As chaves de contexto a seguir correspondem a ACLs. Você pode usar essas chaves de contexto para obrigar a usar uma ACL específica em uma solicitação:

- `s3:x-amz-grant-read`: exigir acesso de leitura.
- `s3:x-amz-grant-write`: exigir acesso de gravação.
- `s3:x-amz-grant-read-acp`: exigir acesso de leitura à ACL do bucket.
- `s3:x-amz-grant-write-acp`: exigir acesso de gravação à ACL do bucket.
- `s3:x-amz-grant-full-control`: exigir controle total.
- `s3:x-amz-acl`: exigir um ACL pré-configurada.

Para obter exemplos de políticas que envolvem cabeçalhos específicos de ACL, consulte Conceder a permissão s3:PutObject com uma condição que exige que o proprietário do bucket obtenha controle total. Consulte uma lista completa de chaves de condição específicas do Amazon S3 em Actions, resources, and condition keys for Amazon S3 na Referência de autorização do serviço.

Para ter mais informações sobre as permissões referentes a operações de API do S3 de acordo com os tipos de recurso do S3, consulte Permissões obrigatórias para operações de API do Amazon S3.

Valores **`aclRequired`** para solicitações comuns do Amazon S3

Para identificar solicitações do Amazon S3 que exigiam ACLs para autorização, você pode usar o valor `aclRequired` nos logs de acesso do servidor do Amazon S3 ou do AWS CloudTrail. O valor `aclRequired` que aparece nos logs de acesso ao servidor do CloudTrail ou do Amazon S3 depende de quais operações foram chamadas e de determinadas informações sobre o solicitante, o proprietário do objeto e o proprietário do bucket. Se nenhuma ACLs for necessária, ou se você estiver configurando a ACL `bucket-owner-full-control` predefinida, ou se as solicitações forem permitidas pela política de bucket, a string de valor `aclRequired` será "`-`" nos logs de acesso ao servidor do Amazon S3 e estará ausente no CloudTrail.

As tabelas a seguir listam os valores esperados de `aclRequired` nos logs de acesso ao servidor do CloudTrail ou do Amazon S3 para as várias operações de API do Amazon S3. É possível usar essas informações para entender quais operações do Amazon S3 dependem de ACLs para autorização. Nas tabelas a seguir, A, B e C representam as diferentes contas associadas ao solicitante, ao

proprietário do objeto e ao proprietário do bucket. As entradas com um asterisco (*) indicam qualquer uma das contas A, B ou C.

> **Note**
>
> As operações `PutObject` na tabela a seguir, a menos que especificado de outra forma, indicam solicitações que não definem uma ACL, a não ser que a ACL seja `bucket-owner-full-control`. Um valor nulo para `aclRequired` indica que `aclRequired` está ausente nos logs do AWS CloudTrail.

A tabela a seguir mostra os valores de `aclRequired` para o CloudTrail.

Nome da operação	Solicitante	Proprietário do objeto	Bucket owner	A política de bucket concede acesso	Valor do **`aclRequired`**	Motivo
`GetObject`	A	A	A	Yes ou No	nulo	Acesso na mesma conta
`GetObject`	A	B	A	Yes ou No	nulo	Acesso à mesma conta com o proprietário do bucket aplicado
`GetObject`	A	A	B	Sim	nulo	Acesso entre contas concedido pela política de bucket

Nome da operação	Solicitante	Proprietário do objeto	Bucket owner	A política de bucket concede acesso	Valor do **`aclRequired`**	Motivo
`GetObject`	A	A	B	Não	Sim	O acesso entre contas depende da ACL
`GetObject`	A	A	B	Sim	nulo	Acesso entre contas concedido pela política de bucket
`GetObject`	A	B	B	Não	Sim	O acesso entre contas depende da ACL
`GetObject`	A	B	C	Sim	nulo	Acesso entre contas concedido pela política de bucket

Nome da operação	Solicitante	Proprietário do objeto	Bucket owner	A política de bucket concede acesso	Valor do **`aclRequired`**	Motivo
`GetObject`	A	B	C	Não	Sim	O acesso entre contas depende da ACL
`PutObject`	A	Não aplicável	A	Yes ou No	nulo	Acesso na mesma conta
`PutObject`	A	Não aplicável	B	Sim	nulo	Acesso entre contas concedido pela política de bucket
`PutObject`	A	Não aplicável	B	Não	Sim	O acesso entre contas depende da ACL
`PutObject` com uma ACL (exceto por `bucket-owner-full-control`)	*	Não aplicável	*	Yes ou No	Sim	ACL de concessões de solicitação

Nome da operação	Solicitante	Proprietário do objeto	Bucket owner	A política de bucket concede acesso	Valor do **aclRequired**	Motivo
`ListObjects`	A	Não aplicável	A	Yes ou No	nulo	Acesso na mesma conta
`ListObjects`	A	Não aplicável	B	Sim	nulo	Acesso entre contas concedido pela política de bucket
`ListObjects`	A	Não aplicável	B	Não	Sim	O acesso entre contas depende da ACL
`DeleteObject`	A	Não aplicável	A	Yes ou No	nulo	Acesso na mesma conta
`DeleteObject`	A	Não aplicável	B	Sim	nulo	Acesso entre contas concedido pela política de bucket

Nome da operação	Solicitante	Proprietário do objeto	Bucket owner	A política de bucket concede acesso	Valor do **aclRequired**	Motivo
`DeleteObject`	A	Não aplicável	B	Não	Sim	O acesso entre contas depende da ACL
`PutObjectAcl`	*	*	*	Yes ou No	Sim	ACL de concessões de solicitação
`PutBucketAcl`	*	Não aplicável	*	Yes ou No	Sim	ACL de concessões de solicitação

> **Note**
>
> As operações `REST.PUT.OBJECT` na tabela a seguir, a menos que especificado de outra forma, indicam solicitações que não definem uma ACL, a não ser que a ACL seja `bucket-owner-full-control`. Uma string de valor `aclRequired` de "`-`" indica um valor nulo nos logs de acesso ao servidor do Amazon S3.

A tabela a seguir mostra os valores de `aclRequired` para logs de acesso ao servidor do Amazon S3.

Nome da operação	Solicitante	Proprietário do objeto	Bucket owner	A política de bucket concede acesso	Valor do **aclRequired**	Motivo
REST.GET.OBJECT	A	A	A	Yes ou No	-	Acesso na mesma conta
REST.GET.OBJECT	A	B	A	Yes ou No	-	Acesso à mesma conta com o proprietário do bucket aplicado
REST.GET.OBJECT	A	A	B	Sim	-	Acesso entre contas concedido pela política de bucket
REST.GET.OBJECT	A	A	B	Não	Sim	O acesso entre contas depende da ACL
REST.GET.OBJECT	A	B	B	Sim	-	Acesso entre contas concedido pela

Nome da operação	Solicitante	Proprietário do objeto	Bucket owner	A política de bucket concede acesso	Valor do **aclRequired**	Motivo
						política de bucket
REST.GET.OBJECT	A	B	B	Não	Sim	O acesso entre contas depende da ACL
REST.GET.OBJECT	A	B	C	Sim	-	Acesso entre contas concedido pela política de bucket
REST.GET.OBJECT	A	B	C	Não	Sim	O acesso entre contas depende da ACL
REST.PUT.OBJECT	A	Não aplicável	A	Yes ou No	-	Acesso na mesma conta

Nome da operação	Solicitante	Proprietário do objeto	Bucket owner	A política de bucket concede acesso	Valor do **aclRequired**	Motivo
REST.PUT.OBJECT	A	Não aplicável	B	Sim	-	Acesso entre contas concedido pela política de bucket
REST.PUT.OBJECT	A	Não aplicável	B	Não	Sim	O acesso entre contas depende da ACL
REST.PUT.OBJECT com uma ACL (exceto por bucket-owner-full-control)	*	Não aplicável	*	Yes ou No	Sim	ACL de concessões de solicitação
REST.GET.BUCKET	A	Não aplicável	A	Yes ou No	-	Acesso na mesma conta

Nome da operação	Solicitante	Proprietário do objeto	Bucket owner	A política de bucket concede acesso	Valor do **aclRequired**	Motivo
REST.GET.BUCKET	A	Não aplicável	B	Sim	-	Acesso entre contas concedido pela política de bucket
REST.GET.BUCKET	A	Não aplicável	B	Não	Sim	O acesso entre contas depende da ACL
REST.DELETE.OBJECT	A	Não aplicável	A	Yes ou No	-	Acesso na mesma conta
REST.DELETE.OBJECT	A	Não aplicável	B	Sim	-	Acesso entre contas concedido pela política de bucket
REST.DELETE.OBJECT	A	Não aplicável	B	Não	Sim	O acesso entre contas depende da ACL

Nome da operação	Solicitante	Proprietário do objeto	Bucket owner	A política de bucket concede acesso	Valor do **aclRequired**	Motivo
REST.PUT.ACL	*	*	*	Yes ou No	Sim	ACL de concessões de solicitação

Amostra de ACL

A seguir, a amostra de ACL em um bucket identifica o proprietário do recurso e um conjunto de concessões. O formato é a representação XML de uma ACL na API REST do Amazon S3. O proprietário do bucket tem FULL_CONTROL sobre o recurso. Além disso, a ACL mostra como as permissões são concedidas em um recurso para duas Contas da AWS, identificadas pelo ID de usuário canônico, e para dois grupos predefinidos do Amazon S3 discutidos na seção anterior.

Example

```
<?xml version="1.0" encoding="UTF-8"?>
<AccessControlPolicy xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Owner>
    <ID>Owner-canonical-user-ID</ID>
    <DisplayName>display-name</DisplayName>
  </Owner>
  <AccessControlList>
    <Grant>
      <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:type="CanonicalUser">
        <ID>Owner-canonical-user-ID</ID>
        <DisplayName>display-name</DisplayName>
      </Grantee>
      <Permission>FULL_CONTROL</Permission>
    </Grant>

    <Grant>
      <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:type="CanonicalUser">
        <ID>user1-canonical-user-ID</ID>
```

```
        <DisplayName>display-name</DisplayName>
      </Grantee>
      <Permission>WRITE</Permission>
    </Grant>

    <Grant>
      <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:type="CanonicalUser">
        <ID>user2-canonical-user-ID</ID>
        <DisplayName>display-name</DisplayName>
      </Grantee>
      <Permission>READ</Permission>
    </Grant>

    <Grant>
      <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="Group">
        <URI>http://acs.amazonaws.com/groups/global/AllUsers</URI>
      </Grantee>
      <Permission>READ</Permission>
    </Grant>
    <Grant>
      <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="Group">
        <URI>http://acs.amazonaws.com/groups/s3/LogDelivery</URI>
      </Grantee>
      <Permission>WRITE</Permission>
    </Grant>

  </AccessControlList>
</AccessControlPolicy>
```

ACL pré-configurada

O Amazon S3 oferece suporte a um conjunto de concessões predefinidas, conhecidas como ACLs pré-configuradas. Cada ACL pré-configurada tem um conjunto predefinido de concessões e permissões. A tabela a seguir lista o conjunto de ACLs pré-configuradas e as concessões predefinidas associadas.

ACL pré-configurada	Aplica-se a	Permissões adicionadas à ACL
`private`	Bucket e objeto	O proprietário obtém `FULL_CONTROL` . Ninguém mais tem direitos de acesso (padrão).
`public-read`	Bucket e objeto	O proprietário obtém `FULL_CONTROL` . O grupo `AllUsers` (consulte Quem é o favorecido?) obtém acesso `READ`.
`public-read-write`	Bucket e objeto	O proprietário obtém `FULL_CONTROL` . O grupo `AllUsers` obtém os acessos `READ` e `WRITE`. Essa concessão não costuma ser recomendada em um bucket.
`aws-exec-read`	Bucket e objeto	O proprietário obtém `FULL_CONTROL` . O Amazon EC2 obtém acesso `READ` a `GET` um pacote de imagem de máquina da Amazon (AMI) do Amazon S3.
`authenticated-read`	Bucket e objeto	O proprietário obtém `FULL_CONTROL` . O grupo `AuthenticatedUsers` obtém acesso `READ`.
`bucket-owner-read`	Objeto	O proprietário do objeto obtém `FULL_CONTROL` . O proprietário do bucket obtém acesso `READ`. Se você especificar essa ACL pré-configurada ao criar um bucket, o Amazon S3 a ignorará.
`bucket-owner-full-control`	Objeto	Os proprietários do objeto e do bucket obtêm `FULL_CONTROL` sobre o objeto. Se você especific ar essa ACL pré-configurada ao criar um bucket, o Amazon S3 a ignorará.
`log-delivery-write`	Bucket	O grupo `LogDelivery` obtém as permissões `WRITE` e `READ_ACP` no bucket. Para obter mais informações sobre logs, consulte (Registrar em log as solicitações com registro em log de acesso ao servidor).

> **Note**
>
> Você pode especificar apenas uma dessas ACLs pré-configuradas na solicitação.

Especifique uma ACL pré-configurada na solicitação usando o cabeçalho de solicitação `x-amz-acl`. Quando o Amazon S3 recebe uma solicitação com uma ACL pré-configurada, ele adiciona as concessões predefinidas à ACL do recurso.

Configurar ACLs

Esta seção explica como gerenciar permissões de acesso para buckets do S3 e objetos usando listas de controle de acesso (ACLs). Você pode adicionar concessões à ACL do recurso usando o AWS Management Console, a AWS Command Line Interface (CLI), a API REST ou os AWS SDKs.

As permissões do bucket e de objeto são independentes uma da outra. Um objeto não herda as permissões de seu bucket. Por exemplo, se criar um bucket e conceder acesso de gravação a outro usuário, você não poderá acessar os objetos desse usuário, a menos que ele conceda o acesso explicitamente.

Você pode conceder permissões a outros usuários da Conta da AWS ou a grupos predefinidos. O usuário ou o grupo para o qual você concede permissões é chamado de usuário favorecido. Por padrão, o proprietário, que é a Conta da AWS que criou o bucket, tem permissões totais.

Cada permissão concedida a um usuário ou a um grupo adiciona uma entrada na ACL associada ao bucket. A ACL lista concessões, o que identifica o usuário favorecido e a permissão concedida.

A Propriedade de objetos do S3 é uma configuração no nível do bucket do Amazon S3 que você pode usar para controlar a propriedade de objetos carregados no bucket e para desabilitar ou habilitar as ACLs. Por padrão, a Propriedade de Objetos está definida com a configuração Imposto pelo proprietário do bucket e todas as ACLs estão desabilitadas. Quando as ACLs são desabilitadas, o proprietário do bucket possui todos os objetos do bucket e gerencia o acesso a eles exclusivamente usando políticas de gerenciamento de acesso.

A maioria dos casos de uso modernos no Amazon S3 não exige mais o uso de ACLs. Recomendamos manter as ACLs desabilitadas, exceto em circunstâncias incomuns em que seja necessário controlar o acesso para cada objeto individualmente. Com as ACLs desabilitadas, é possível usar políticas para controlar o acesso a todos os objetos no bucket, independentemente de quem carregou os objetos para o bucket. Para obter mais informações, consulte Controlar a propriedade de objetos e desabilitar ACLs para seu bucket.

Important

Se o bucket de uso geral utilizar a configuração “Imposto pelo proprietário do bucket” para a Propriedade de objetos do S3, será necessário usar políticas para conceder acesso ao bucket de uso geral e aos objetos contidos nele. Quando a configuração Imposto pelo proprietário do bucket estiver habilitada, as solicitações para definir listas de controle de acesso (ACLs) ou atualizar ACLs falharão e retornarão o código de erro `AccessControlListNotSupported`. Ainda há suporte para solicitações de leitura de ACLs.

Warning

Recomendamos que você evite conceder acesso de gravação aos grupos Todos (acesso público) ou Usuários autenticados (todos os usuários autenticados da AWS). Para obter mais informações sobre os efeitos da concessão de acesso de gravação a esses grupos, consulte Grupos predefinidos do Amazon S3.

Usar o console do S3 para definir permissões de ACL para um bucket

O console exibe concessões de acesso combinadas para favorecidos duplicados. Para ver a lista completa de ACLs, use a API REST do Amazon S3, a AWS CLI ou os AWS SDKs.

A tabela a seguir mostra as permissões de ACL que você pode configurar para buckets no console do Amazon S3.

Permissões de ACL do console do Amazon S3 para buckets

Permissão do console	Permissão da ACL	Acesso
Objetos - listar	`READ`	Permite ao favorecido listar os objetos no bucket
Objetos - gravar	`WRITE`	Permite que o favorecido crie novos objetos no bucket. Para os proprietários de bucket e objeto de objetos existentes, também permite exclusões e substituições desses objetos.

Permissão do console	Permissão da ACL	Acesso
ACL de bucket: ler	`READ_ACP`	Permite ao favorecido ler a ACL do bucket
ACL do bucket - gravar	`WRITE_ACP`	Permite ao favorecido gravar a ACL para o bucket aplicável
Todos (acesso público): Objetos - listar	`READ`	Concede acesso público de leitura para os objetos no bucket. Quando você concede acesso à lista a Todos (acesso público), qualquer pessoa no mundo pode acessar os objetos no bucket.
Todos (acesso público): ACL do bucket - Ler	`READ_ACP`	Concede acesso de leitura pública para a ACL de bucket. Quando você concede acesso de leitura a Todos (acesso público), qualquer pessoa no mundo pode acessar a ACL de bucket.

Para obter mais informações sobre permissões de ACL, consulte Visão geral da lista de controle de acesso (ACL).

> **Important**
>
> Se o bucket de uso geral utilizar a configuração “Imposto pelo proprietário do bucket” para a Propriedade de objetos do S3, será necessário usar políticas para conceder acesso ao bucket de uso geral e aos objetos contidos nele. Quando a configuração Imposto pelo proprietário do bucket estiver habilitada, as solicitações para definir listas de controle de acesso (ACLs) ou atualizar ACLs falharão e retornarão o código de erro `AccessControlListNotSupported`. Ainda há suporte para solicitações de leitura de ACLs.

Para definir permissões de ACL para um bucket

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets de uso geral.
3. Na lista Buckets, escolha o nome do bucket para o qual você deseja definir permissões.
4. Escolha Permissions (Permissões).
5. Em Access control list (Lista de controle de acesso), escolha Edit (Editar).

   Você pode editar as seguintes permissões de ACL para o bucket:

   Objetos

   - List (Listar): permite ao favorecido listar os objetos no bucket.
   - Gravação: permite que o favorecido crie novos objetos no bucket. Para os proprietários de bucket e objeto de objetos existentes, também permite exclusões e substituições desses objetos.

     No console do S3, você só pode conceder acesso de gravação ao grupo de entrega de log do S3 e ao proprietário do bucket (sua Conta da AWS). É recomendável não conceder acesso de gravação a outros favorecidos. No entanto, se você precisar conceder acesso de gravação, poderá usar a AWS CLI, os AWS SDKs ou a API REST.

   Bucket ACL

   - Read (Ler): permite ao beneficiário ler a ACL do bucket.
   - Write (Gravar): permite ao beneficiário gravar a ACL para o bucket aplicável.
6. Para alterar as permissões do proprietário do bucket, ao lado de Proprietário do bucket (sua conta da Conta da AWS), desmarque ou selecione uma das seguintes permissões de ACL:

   - Objetos: listar ou gravar
   - ACL de bucket: ler ou gravar

   O proprietário refere-se ao Usuário raiz da conta da AWS, e não a um usuário do AWS Identity and Access Management (IAM). Para obter mais informações sobre o usuário raiz, consulte O Usuário raiz da conta da AWS no Guia do usuário do IAM.

7. Para conceder ou desfazer permissões para o público em geral (todos na Internet), ao lado de Everyone (public access) (Todos (acesso público)), limpe ou selecione uma das seguintes permissões da ACL:

   - Objetos: listar
   - ACL de bucket: ler

   > **Warning**
   >
   > Tenha cuidado ao conceder ao grupo Everyone (Todos) acesso público ao seu bucket do S3. Quando você concede acesso a esse grupo, qualquer pessoa no mundo pode acessar seu bucket. É altamente recomendável que você nunca conceda nenhum tipo de acesso público de gravação ao seu bucket do S3.

8. Para conceder ou cancelar as permissões de qualquer pessoa com uma Conta da AWS, ao lado de Grupo de usuários autenticados (qualquer pessoa com uma Conta da AWS), selecione ou desmarque uma das seguintes permissões de ACL:

   - Objetos: listar
   - ACL de bucket: ler

9. Para conceder ou desfazer permissões para o Amazon S3 gravar logs de acesso ao servidor no bucket, em S3 log delivery group (Grupo de entrega de log do S3), limpe ou selecione uma das seguintes permissões ACL:

   - Objetos: listar ou gravar
   - ACL de bucket: ler ou gravar

   Se um bucket for configurado como o bucket de destino para receber logs de acesso, as permissões do bucket devem permitir ao grupo Log Delivery (Entrega de logs) acesso de gravação ao bucket. Quando você ativa o registro em log do acesso ao servidor em um bucket, o console do Amazon S3 concede acesso de gravação ao grupo Log Delivery (Entrega de logs) para o bucket de destino do qual você opta por receber os logs. Para obter mais informações sobre o registro em log de acesso ao servidor, consulte Habilitar o log de acesso ao servidor do Amazon S3.

10. Para conceder acesso a outra Conta da AWS, faça o seguinte:

    a. Escolha Add grantee (Adicionar beneficiário).

b. Na caixa Grantee (Beneficiário), insira o ID canônico da outra Conta da AWS.

c. Selecione uma das seguintes permissões de ACL:

- Objetos: listar ou gravar
- ACL de bucket: ler ou gravar

> **Warning**
>
> Ao conceder aos recursos acesso a outras Contas da AWS, esteja ciente de que as Contas da AWS podem delegar as permissões delas a usuários de suas próprias contas. Isso é conhecido como acesso entre contas. Para obter informações sobre como usar o acesso entre contas, consulte Criar uma função para delegar permissões a um usuário do IAM no Guia do usuário do IAM.

11. Para remover o acesso a outra Conta da AWS, em Acesso a outras Contas da AWS, selecione Remover.
12. Para salvar suas alterações, escolha Save changes (Salvar alterações).

Usar o console do S3 para definir permissões de ACL para um objeto

O console exibe concessões de acesso combinadas para favorecidos duplicados. Para ver a lista completa de ACLs, use a API REST do Amazon S3, a AWS CLI ou os AWS SDKs. A tabela a seguir mostra as permissões de ACL que você pode configurar para objetos no console do Amazon S3.

Permissões de ACL do console do Amazon S3 para objetos

Permissão do console	Permissão da ACL	Acesso
Objeto - Ler	`READ`	Permite ao favorecido ler os dados do objeto e seus metadados.
ACL do objeto - ler	`READ_ACP`	Permite ao favorecido ler a ACL do objeto
ACL Objeto - gravar	`WRITE_ACP`	Permite ao favorecido gravar a ACL para o objeto aplicável

Para obter mais informações sobre permissões de ACL, consulte Visão geral da lista de controle de acesso (ACL).

> **Important**
>
> Se o bucket de uso geral utilizar a configuração “Imposto pelo proprietário do bucket” para a Propriedade de objetos do S3, será necessário usar políticas para conceder acesso ao bucket de uso geral e aos objetos contidos nele. Quando a configuração Imposto pelo proprietário do bucket estiver habilitada, as solicitações para definir listas de controle de acesso (ACLs) ou atualizar ACLs falharão e retornarão o código de erro `AccessControlListNotSupported`. Ainda há suporte para solicitações de leitura de ACLs.

Para definir permissões de ACL para um objeto

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Na lista Buckets, escolha o nome do bucket que contém o objeto.
3. Na lista Name (Nome), escolha o nome do objeto para o qual você deseja definir permissões.
4. Escolha Permissions (Permissões).
5. Na lista do controle de acesso (ACL), escolha Edit (Editar).

   Você pode editar as seguintes permissões de ACL para o objeto:

   Objeto

   - Read (Ler): permite ao favorecido ler os dados do objeto e seus metadados.

   ACL do objeto

   - Read (Ler): permite ao favorecido ler a ACL do objeto.
   - Write (Gravar): permite ao favorecido gravar a ACL para o objeto aplicável. No console do S3, você só pode conceder acesso de gravação ao proprietário do bucket (sua Conta da AWS). É recomendável não conceder acesso de gravação a outros favorecidos. No entanto, se você precisar conceder acesso de gravação, poderá usar a AWS CLI, os AWS SDKs ou a API REST.

6. É possível gerenciar as permissões de acesso do objeto ao seguinte:

   a. Acesso para o proprietário do objeto

      O proprietário refere-se ao Usuário raiz da conta da AWS, e não a um usuário do AWS Identity and Access Management (IAM). Para obter mais informações sobre o usuário raiz, consulte O Usuário raiz da conta da AWS no Guia do usuário do IAM.

      Para alterar as permissões de acesso ao objeto do proprietário, em Acesso para o proprietário do objeto, selecione Sua AWS (proprietário).

      Marque as caixas de seleção das permissões que você deseja alterar e escolha Save (Salvar).

   b. Acesso para outras Contas da AWS

      Para conceder permissões a um usuário da AWS de uma Conta da AWS diferente, em Acesso a outras Contas da AWS, selecione Adicionar conta. No campo Enter an ID (Inserir um ID), digite o ID canônico do usuário da AWS ao qual você deseja conceder permissões para o objeto. Para obter informações sobre como encontrar um ID canônico, consulte Identificadores de Conta da AWS no Referência geral da Amazon Web Services. Você pode adicionar até 99 usuários.

      Marque as caixas de seleção das permissões que você deseja conceder ao usuário e escolha Save (Salvar). Para exibir informações sobre as permissões, escolha os ícones da Ajuda.

   c. Acesso público

      Para conceder acesso ao seu objeto para o público geral (todos no mundo), em Public access (Acesso público), escolha Everyone (Todos). Conceder permissões de acesso público significa que todos no mundo podem acessar o objeto.

      Marque as caixas de seleção das permissões que você deseja conceder e escolha Save (Salvar).

      > ⚠ Warning
      >
      > - Tenha cuidado ao conceder ao grupo Everyone (Todos) acesso anônimo aos seus objetos do Amazon S3. Quando você concede acesso a esse grupo, qualquer pessoa no mundo pode acessar seu objeto. Se você precisar conceder

acesso a todos, é altamente recomendável que só conceda permissões para Read objects (Ler objetos).

- Recomendamos fortemente que você não conceda ao grupo Everyone (Todos) permissões de gravação no objeto. Isso permite que qualquer pessoa substitua as permissões da ACL para o objeto.

Uso dos SDKs da AWS

Esta seção fornece exemplos de como configurar concessões na lista de controle de acesso (ACL) em buckets e objetos.

Important

Se o bucket de uso geral utilizar a configuração “Imposto pelo proprietário do bucket” para a Propriedade de objetos do S3, será necessário usar políticas para conceder acesso ao bucket de uso geral e aos objetos contidos nele. Quando a configuração Imposto pelo proprietário do bucket estiver habilitada, as solicitações para definir listas de controle de acesso (ACLs) ou atualizar ACLs falharão e retornarão o código de erro `AccessControlListNotSupported`. Ainda há suporte para solicitações de leitura de ACLs.

Java

Esta seção fornece exemplos de como configurar concessões na lista de controle de acesso (ACL) em buckets e objetos. O primeiro exemplo cria um bucket com uma ACL padrão (consulte ACL pré-configurada), cria uma lista de concessões de permissão personalizadas e, em seguida, substitui a ACL padrão por uma ACL que contém concessões personalizadas. O segundo exemplo mostra como modificar uma ACL usando o método `AccessControlList.grantPermission()`.

Example Crie um bucket e especifique uma ACL pré-configurada que conceda permissão ao grupo de entrega de logs do S3

Este exemplo cria um bucket. Na solicitação, o exemplo especifica uma ACL padrão que concede permissão ao grupo de Entrega de logs para gravar logs no bucket.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.*;

import java.io.IOException;
import java.util.ArrayList;

public class CreateBucketWithACL {

    public static void main(String[] args) throws IOException {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "*** Bucket name ***";
        String userEmailForReadPermission = "*** user@example.com ***";

        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withRegion(clientRegion)
                    .build();

            // Create a bucket with a canned ACL. This ACL will be replaced by the
            // setBucketAcl()
            // calls below. It is included here for demonstration purposes.
            CreateBucketRequest createBucketRequest = new
 CreateBucketRequest(bucketName, clientRegion.getName())
                    .withCannedAcl(CannedAccessControlList.LogDeliveryWrite);
            s3Client.createBucket(createBucketRequest);

            // Create a collection of grants to add to the bucket.
            ArrayList<Grant> grantCollection = new ArrayList<Grant>();

            // Grant the account owner full control.
            Grant grant1 = new Grant(new
 CanonicalGrantee(s3Client.getS3AccountOwner().getId()),
                    Permission.FullControl);
            grantCollection.add(grant1);

            // Grant the LogDelivery group permission to write to the bucket.
            Grant grant2 = new Grant(GroupGrantee.LogDelivery, Permission.Write);
            grantCollection.add(grant2);
```

```
            // Save grants by replacing all current ACL grants with the two we just
 created.
            AccessControlList bucketAcl = new AccessControlList();
            bucketAcl.grantAllPermissions(grantCollection.toArray(new Grant[0]));
            s3Client.setBucketAcl(bucketName, bucketAcl);

            // Retrieve the bucket's ACL, add another grant, and then save the new
 ACL.
            AccessControlList newBucketAcl = s3Client.getBucketAcl(bucketName);
            Grant grant3 = new Grant(new
 EmailAddressGrantee(userEmailForReadPermission), Permission.Read);
            newBucketAcl.grantAllPermissions(grant3);
            s3Client.setBucketAcl(bucketName, newBucketAcl);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Example Atualizar ACL em um objeto existente

Este exemplo atualiza a ACL em um objeto. O exemplo realiza as seguintes tarefas:

- Recupera a ACL de um objeto
- Limpa a ACL removendo todas as permissões existentes
- Adiciona duas permissões: acesso total do proprietário, e WRITE_ACP (consulte Quais permissões posso conceder?) para o usuário identificado por endereço de e-mail
- Salva a ACL no objeto

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
```

```
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.AccessControlList;
import com.amazonaws.services.s3.model.CanonicalGrantee;
import com.amazonaws.services.s3.model.EmailAddressGrantee;
import com.amazonaws.services.s3.model.Permission;

import java.io.IOException;

public class ModifyACLExistingObject {

    public static void main(String[] args) throws IOException {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "*** Bucket name ***";
        String keyName = "*** Key name ***";
        String emailGrantee = "*** user@example.com ***";

        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(clientRegion)
                    .build();

            // Get the existing object ACL that we want to modify.
            AccessControlList acl = s3Client.getObjectAcl(bucketName, keyName);

            // Clear the existing list of grants.
            acl.getGrantsAsList().clear();

            // Grant a sample set of permissions, using the existing ACL owner for
 Full
            // Control permissions.
            acl.grantPermission(new CanonicalGrantee(acl.getOwner().getId()),
 Permission.FullControl);
            acl.grantPermission(new EmailAddressGrantee(emailGrantee),
 Permission.WriteAcp);

            // Save the modified ACL back to the object.
            s3Client.setObjectAcl(bucketName, keyName, acl);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
```

```
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

.NET

Example Crie um bucket e especifique uma ACL pré-configurada que conceda permissão ao grupo de entrega de logs do S3

Este exemplo do C# cria um bucket. Na solicitação, o código também especifica uma ACL padrão que concede permissões ao grupo de Entrega de logs para gravar os logs no bucket.

Para obter informações sobre como configurar e executar exemplos de código, consulte Conceitos básicos do AWS SDK for .NET no Guia do desenvolvedor do AWS SDK for .NET.

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class ManagingBucketACLTest
    {
        private const string newBucketName = "*** bucket name ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 client;

        public static void Main()
        {
            client = new AmazonS3Client(bucketRegion);
            CreateBucketUseCannedACLAsync().Wait();
        }

        private static async Task CreateBucketUseCannedACLAsync()
        {
            try
```

```
            {
                // Add bucket (specify canned ACL).
                PutBucketRequest putBucketRequest = new PutBucketRequest()
                {
                    BucketName = newBucketName,
                    BucketRegion = S3Region.EUW1, // S3Region.US,
                                                  // Add canned ACL.
                    CannedACL = S3CannedACL.LogDeliveryWrite
                };
                PutBucketResponse putBucketResponse = await
 client.PutBucketAsync(putBucketRequest);

                // Retrieve bucket ACL.
                GetACLResponse getACLResponse = await client.GetACLAsync(new
 GetACLRequest
                {
                    BucketName = newBucketName
                });
            }
            catch (AmazonS3Exception amazonS3Exception)
            {
                Console.WriteLine("S3 error occurred. Exception: " +
 amazonS3Exception.ToString());
            }
            catch (Exception e)
            {
                Console.WriteLine("Exception: " + e.ToString());
            }
        }
    }
}
```

Example Atualizar ACL em um objeto existente

Este exemplo do C# atualiza a ACL em um objeto existente. O exemplo realiza as seguintes tarefas:

- Recupera a ACL de um objeto.
- Limpa a ACL removendo todas as permissões existentes.
- Adiciona duas permissões: acesso total do proprietário, e WRITE_ACP para o usuário identificado por endereço de e-mail.
- Salva a ACL enviando uma solicitação `PutAcl`.

Para obter informações sobre como configurar e executar exemplos de código, consulte Conceitos básicos do AWS SDK for .NET no Guia do desenvolvedor do AWS SDK for .NET.

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Collections.Generic;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class ManagingObjectACLTest
    {
        private const string bucketName = "*** bucket name ***";
        private const string keyName = "*** object key name ***";
        private const string emailAddress = "*** email address ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 client;
        public static void Main()
        {
            client = new AmazonS3Client(bucketRegion);
            TestObjectACLTestAsync().Wait();
        }
        private static async Task TestObjectACLTestAsync()
        {
            try
            {
                    // Retrieve the ACL for the object.
                    GetACLResponse aclResponse = await client.GetACLAsync(new
 GetACLRequest
                    {
                        BucketName = bucketName,
                        Key = keyName
                    });

                    S3AccessControlList acl = aclResponse.AccessControlList;

                    // Retrieve the owner (we use this to re-add permissions after
 we clear the ACL).
                    Owner owner = acl.Owner;
```

```
                    // Clear existing grants.
                    acl.Grants.Clear();

                    // Add a grant to reset the owner's full permission (the
 previous clear statement removed all permissions).
                    S3Grant fullControlGrant = new S3Grant
                    {
                        Grantee = new S3Grantee { CanonicalUser = owner.Id },
                        Permission = S3Permission.FULL_CONTROL

                    };

                    // Describe the grant for the permission using an email address.
                    S3Grant grantUsingEmail = new S3Grant
                    {
                        Grantee = new S3Grantee { EmailAddress = emailAddress },
                        Permission = S3Permission.WRITE_ACP
                    };
                    acl.Grants.AddRange(new List<S3Grant> { fullControlGrant,
 grantUsingEmail });

                    // Set a new ACL.
                    PutACLResponse response = await client.PutACLAsync(new
 PutACLRequest
                    {
                        BucketName = bucketName,
                        Key = keyName,
                        AccessControlList = acl
                    });
            }
            catch (AmazonS3Exception amazonS3Exception)
            {
                Console.WriteLine("An AmazonS3Exception was thrown. Exception: " +
 amazonS3Exception.ToString());
            }
            catch (Exception e)
            {
                Console.WriteLine("Exception: " + e.ToString());
            }
        }
    }
}
```

Uso da API REST

As APIs do Amazon S3 permitem a definição de uma ACL quando você cria um bucket ou um objeto. O Amazon S3 também fornece API para definir uma ACL em um bucket ou objeto existente. Estas APIs oferecem os seguintes métodos para definir uma ACL:

- Definir ACL usando cabeçalhos de solicitação: ao enviar uma solicitação para criar um recurso (bucket ou objeto), defina uma ACL usando os cabeçalhos de solicitação. Com esses cabeçalhos, você pode especificar uma ACL pré-configurada ou especificar concessões explicitamente (identificando o favorecido e as permissões de maneira explícita).
- Definir ACL usando o corpo da solicitação: ao enviar uma solicitação para definir uma ACL em um recurso existente, defina a ACL no cabeçalho da solicitação ou no corpo.

Para obter informações sobre o suporte à API REST para gerenciar ACLs, consulte as seções a seguir na Referência da API do Amazon Simple Storage Service:

- GetBucketAcl
- PutBucketAcl
- GetObjectAcl
- PutObjectAcl
- PutObject
- CreateBucket
- CopyObject
- CreateMultipartUpload

> **Important**
>
> Se o bucket de uso geral utilizar a configuração “Imposto pelo proprietário do bucket” para a Propriedade de objetos do S3, será necessário usar políticas para conceder acesso ao bucket de uso geral e aos objetos contidos nele. Quando a configuração Imposto pelo proprietário do bucket estiver habilitada, as solicitações para definir listas de controle de acesso (ACLs) ou atualizar ACLs falharão e retornarão o código de erro `AccessControlListNotSupported`. Ainda há suporte para solicitações de leitura de ACLs.

Lista de controle de acesso (ACL - Access Control List) - Cabeçalhos específicos de solicitação

Você pode usar cabeçalhos para conceder permissões baseadas em lista de controle de acesso (ACL). Por padrão, todos os objetos são privados. Somente o proprietário tem controle total de acesso. Ao adicionar um novo objeto, você pode conceder permissões a Contas da AWS individuais ou a grupos predefinidos pelo Amazon S3. Depois essas permissões são adicionadas à lista de controle de acesso (ACL) no objeto. Para obter mais informações, consulte Visão geral da lista de controle de acesso (ACL).

Com esta operação, você pode conceder permissões de acesso usando um destes dois métodos:

- Canned ACL (**`x-amz-acl`**) (ACL pré-configurada) — O Amazon S3 oferece suporte a um conjunto de ACLs predefinidas, conhecidas como ACLs pré-configuradas. Cada ACL pré-configurada tem um conjunto predefinido de concessões e permissões. Para obter mais informações, consulte ACL pré-configurada.
- Access Permissions (Permissões de acesso): para conceder explicitamente permissões de acesso a grupos ou Contas da AWS específicos, use os seguintes cabeçalhos. Cada cabeçalho mapeia para permissões específicas compatíveis com o Amazon S3 em uma ACL. Para obter mais informações, consulte Visão geral da lista de controle de acesso (ACL). No cabeçalho, você especifica uma lista de favorecidos que obtêm a permissão específica.
  - x-amz-grant-read
  - x-amz-grant-write
  - x-amz-grant-read-acp
  - x-amz-grant-write-acp
  - x-amz-grant-full-control

Como usar o AWS CLI

Para obter mais informações sobre como gerenciar ACLs usando a AWS CLI, consulte put-bucket-acl na Referência de comandos da AWS CLI.

> **Important**
>
> Se o bucket de uso geral utilizar a configuração “Imposto pelo proprietário do bucket” para a Propriedade de objetos do S3, será necessário usar políticas para conceder acesso ao bucket de uso geral e aos objetos contidos nele. Quando a configuração Imposto pelo proprietário do bucket estiver habilitada, as solicitações para definir listas

de controle de acesso (ACLs) ou atualizar ACLs falharão e retornarão o código de erro `AccessControlListNotSupported`. Ainda há suporte para solicitações de leitura de ACLs.

Exemplos de política para ACLs

É possível usar chaves de condição em políticas de bucket para controlar o acesso ao Amazon S3.

Tópicos

- Conceder a permissão s3:PutObject com uma condição que exige que o proprietário do bucket obtenha controle total
- Conceder a permissão s3:PutObject com uma condição no cabeçalho x-amz-acl

Conceder a permissão s3:PutObject com uma condição que exige que o proprietário do bucket obtenha controle total

A operação PUT Object permite cabeçalhos específicos da lista de controle de acesso (ACL) que você usa para conceder permissões baseadas em ACL. Usando essas chaves, o proprietário do bucket pode definir uma condição para exigir permissões de acesso específicas quando o usuário faz upload de um objeto.

Suponha que a conta A seja proprietária de um bucket e que o administrador da conta queira conceder a Dave, um usuário na conta B, permissões para fazer upload de objetos. Por padrão, os objetos que Dave carrega são de propriedade da conta B, e a conta A não tem permissões nesses objetos. Como o proprietário do bucket é quem paga a fatura, ele quer permissões completas nos objetos que Dave carrega. O administrador da conta A pode fazer isso concedendo a Dave a permissão `s3:PutObject`, com a condição de que a solicitação inclua cabeçalhos específicos da ACL, que concede permissão total explícita ou usa uma ACL pré-configurada. Para obter mais informações, consulte Objeto PUT.

Exigir o cabeçalho x-amz-full-control

Você pode exigir o cabeçalho `x-amz-full-control` na solicitação com permissão de controle total do proprietário do bucket. A política de bucket a seguir concede ao usuário Dave a permissão `s3:PutObject` com uma condição de uso da chave de condição `s3:x-amz-grant-full-control`, que exige que a solicitação inclua o cabeçalho `x-amz-full-control`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "statement1",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::AccountB-ID:user/Dave"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::awsexamplebucket1/*",
      "Condition": {
        "StringEquals": {
          "s3:x-amz-grant-full-control": "id=AccountA-CanonicalUserID"
        }
      }
    }
  ]
}
```

> **Note**
>
> Este exemplo trata da permissão entre contas. Contudo, se Dave (a quem é concedida a permissão) pertencer à Conta da AWS que é proprietária do bucket, essa permissão condicional não será necessária. Isso acontece porque a conta pai à qual o Dave pertence é proprietária dos objetos que o usuário carrega.

Adicionar negação explícita

A política de bucket anterior concede permissão condicional ao usuário Dave na conta B. Enquanto essa política estiver em vigor, Dave poderá obter a mesma permissão sem nenhuma condição por meio de alguma outra política. Por exemplo, Dave pode pertencer a um grupo e você concede ao grupo a permissão `s3:PutObject` sem nenhuma condição. Para evitar essas brechas de permissão, você pode elaborar uma política de acesso mais estrita adicionando uma negação explícita. Neste exemplo, você nega explicitamente a permissão de upload ao usuário Dave se ele não incluir os cabeçalhos necessários na solicitação, concedendo permissões totais ao proprietário do bucket. A negação explícita sempre se sobrepõe a qualquer outra permissão concedida. Veja a seguir um exemplo de política de acesso revisada com a negação explícita adicionada.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "statement1",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::AccountB-ID:user/AccountBadmin"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::awsexamplebucket1/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-grant-full-control": "id=AccountA-CanonicalUserID"
                }
            }
        },
        {
            "Sid": "statement2",
            "Effect": "Deny",
            "Principal": {
                "AWS": "arn:aws:iam::AccountB-ID:user/AccountBadmin"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::awsexamplebucket1/*",
            "Condition": {
                "StringNotEquals": {
                    "s3:x-amz-grant-full-control": "id=AccountA-CanonicalUserID"
                }
            }
        }
    ]
}
```

Testar a política com a AWS CLI

Se você tiver duas Contas da AWS, teste a política usando a AWS Command Line Interface (AWS CLI). Anexe a política e use as credenciais de Dave para testar a permissão usando o seguinte comando `put-object` da AWS CLI. Você fornece as credenciais de Dave adicionando o parâmetro `--profile`. Você concede permissão de controle total ao proprietário do bucket adicionando o parâmetro `--grant-full-control`. Consulte mais informações sobre como configurar e usar a AWS CLI em Developing with Amazon S3 using the AWS CLI na Referência de API do Amazon S3.

```
aws s3api put-object --bucket examplebucket --key HappyFace.jpg --body c:\HappyFace.jpg
 --grant-full-control id="AccountA-CanonicalUserID" --profile AccountBUserProfile
```

Exigir o cabeçalho x-amz-acl

Você pode exigir o cabeçalho `x-amz-acl` com uma ACL padrão que concede permissão de controle total ao proprietário do bucket. Para exigir o cabeçalho `x-amz-acl` na solicitação, você pode substituir o par de chave-valor no bloco `Condition` e especificar a chave de condição `s3:x-amz-acl`, conforme o exemplo abaixo.

```
"Condition": {
    "StringEquals": {
        "s3:x-amz-acl": "bucket-owner-full-control"
    }
}
```

Para testar a permissão usando a AWS CLI, especifique o parâmetro `--acl`. Em seguida, a AWS CLI adiciona o cabeçalho `x-amz-acl` ao enviar a solicitação.

```
aws s3api put-object --bucket examplebucket --key HappyFace.jpg --body c:\HappyFace.jpg
 --acl "bucket-owner-full-control" --profile AccountBadmin
```

Conceder a permissão s3:PutObject com uma condição no cabeçalho x-amz-acl

A política de bucket a seguir concederá a permissão `s3:PutObject` a duas Contas da AWS se a solicitação incluir o cabeçalho `x-amz-acl`, tornando o objeto publicamente legível. O bloco `Condition` usa a condição `StringEquals` e recebe um par de chave/valor, `"s3:x-amz-acl": ["public-read"]`, para avaliação. No par de chave-valor, `s3:x-amz-acl` é uma chave específica do Amazon S3, conforme indicado pelo prefixo `s3:`.

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
         "Sid":"AddCannedAcl",
            "Effect":"Allow",
         "Principal": {
                "AWS": [
                "arn:aws:iam::Account1-ID:root",
```

```
    "arn:aws:iam::Account2-ID:root"
    ]
            },
         "Action":"s3:PutObject",
            "Resource": ["arn:aws:s3:::awsexamplebucket1/*"],
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl":["public-read"]
                }
            }
        }
    ]
}
```

> **Important**
>
> Nem todas as condições fazem sentido para todas as ações. Por exemplo, faz sentido incluir uma condição `s3:LocationConstraint` em uma política que concede a permissão `s3:CreateBucket` do Amazon S3. No entanto, não faz sentido incluir essa condição em uma política que conceda a permissão `s3:GetObject`. O Amazon S3 pode testar erros de semântica para esse tipo que envolve condições específicas do Amazon S3. Contudo, se você estiver criando uma política para um perfil ou usuário do IAM e incluir uma condição do Amazon S3 semanticamente inválida, nenhum erro será relatado porque o IAM não pode validar condições do Amazon S3.

Bloquear o acesso público ao armazenamento do Amazon S3

O recurso Bloqueio de acesso público do Amazon S3 fornece configurações para pontos de acesso, buckets e contas para ajudar você a gerenciar o acesso público aos recursos do Amazon S3. Por padrão, novos buckets, pontos de acesso e objetos não permitem acesso público. No entanto, os usuários podem modificar políticas de bucket, políticas de ponto de acesso ou permissões de objeto para permitir acesso público. As configurações do Bloqueio de acesso público do S3 substituem essas políticas e permissões, de maneira que seja possível limitar o acesso público a esses recursos.

Com o Bloqueio de acesso público do S3, os administradores de conta e os proprietários de bucket podem configurar facilmente os controles centralizados impostos para limitar o acesso público aos recursos do Amazon S3, independentemente de como os recursos são criados.

Para obter instruções sobre como configurar o acesso público a blocos, consulte Configurar o bloqueio de acesso público.

Ao receber uma solicitação para acessar um bucket ou um objeto, o Amazon S3 determina se o bucket ou a conta do proprietário do bucket tem uma configuração do Bloqueio de acesso público aplicada. Se a solicitação foi feita por meio de um ponto de acesso, o Amazon S3 também verificará se há configurações do Bloqueio de acesso público para o ponto de acesso. Caso haja uma configuração do Bloqueio de acesso público que proíba o acesso solicitado, o Amazon S3 rejeitará a solicitação.

O Bloqueio de acesso público do Amazon S3 fornece quatro configurações. Essas configurações são independentes e podem ser usadas em qualquer combinação. Cada configuração pode ser aplicada a um ponto de acesso, a um bucket ou a uma Conta da AWS inteira. Se as configurações do Bloqueio de acesso público para o ponto de acesso, o bucket ou a conta forem diferentes, o Amazon S3 aplicará a combinação mais restritiva das configurações de ponto de acesso, bucket e conta.

Quando o Amazon S3 avalia se uma operação é proibida por uma configuração do Bloqueio de acesso público, ela rejeita qualquer solicitação que viole uma configuração de ponto de acesso, bucket ou conta.

Important

O acesso público aos buckets e objetos é concedido através de listas de controle de acesso (ACLs), políticas de ponto de acesso, políticas de bucket ou todos. Para garantir que todos os seus pontos de acesso, buckets e objetos do Amazon S3 tenham o acesso público bloqueado, recomendamos ativar as quatro configurações de bloqueio de acesso público na sua conta. Estas configurações bloqueiam o acesso público a todos os buckets e pontos de acesso atuais e futuros.

Antes de aplicar estas configurações, verifique se seus aplicativos funcionarão corretamente sem acesso público. Se você precisa de um nível determinado de acesso público aos buckets ou objetos, por exemplo, para hospedar um site estático como descrito em Hospedagem de um site estático usando o Amazon S3, é possível personalizar as configurações individualmente para atender aos seus casos de uso de armazenamento. Habilitar o Bloqueio de Acesso Público ajuda a proteger seus recursos, impedindo que o acesso público seja concedido por meio de políticas de recursos ou listas de controle de acesso (ACLs) diretamente vinculadas aos recursos do S3. Além de habilitar o Bloqueio de

Acesso Público, inspecione cuidadosamente as seguintes políticas para garantir que elas não concedam acesso público:

- Políticas baseadas em identidade vinculadas a entidades principais da AWS associadas (por exemplo, perfis do IAM).
- Políticas baseadas em recursos anexadas a recursos da AWS associados [por exemplo, chaves do AWS Key Management Service (KMS)]

Note

- Você pode habilitar as configurações de bloqueio de acesso público somente para pontos de acesso, buckets e Contas da AWS. O Amazon S3 não oferece suporte a configurações de bloqueio de acesso público por objeto.
- Quando você aplica configurações de bloqueio de acesso público a uma conta, as configurações se aplicam a todas as Regiões da AWS globalmente. As configurações talvez não entrem em vigor em todas as regiões imediata ou simultaneamente, mas acabam se propagando para todas as regiões.

Tópicos

- Configurações do bloqueio de acesso público
- Executar operações de bloqueio de acesso público em um ponto de acesso
- O significado de "público"
- Usar o IAM Access Analyzer para S3 para revisar buckets públicos
- Permissões
- Configurar o bloqueio de acesso público
- Configurar o bloqueio de acesso público para sua conta
- Configurar o bloqueio de acesso público para seus buckets do S3

Configurações do bloqueio de acesso público

O Bloqueio de acesso público do S3 fornece quatro configurações. É possível aplicar essas configurações em qualquer combinação a pontos de acesso individuais, buckets ou Contas da AWS

inteiras. Caso você aplique uma configuração a uma conta, ela se aplica a todos os buckets e pontos de acesso de propriedade dessa conta. Da mesma forma, se você aplicar uma configuração a um bucket, ela se aplicará a todos os pontos de acesso associados a esse bucket.

A tabela a seguir contém as configurações disponíveis.

Nome	Descrição
`BlockPublicAcls`	A definição dessa opção como `TRUE` causa o seguinte comportamento: • As chamadas `PutBucketAcl` e `PutObjectAcl` falharão se a lista de controle de acesso (ACL) especificada for pública. • As chamadas `PutObject` falharão se a solicitação incluir uma ACL pública. • Se essa configuração for aplicada a uma conta, as chamadas a `PUT Bucket` falharão se a solicitação incluir uma ACL pública. Quando essa configuração for definida como `TRUE`, as operações especificadas falharão (quer por meio da API REST, da AWS CLI ou dos AWS SDKs). Porém, as políticas e as ACLs existentes para buckets e objetos não são modificadas. Essa configuração permite se proteger contra acesso público ao mesmo tempo em que permite auditar, refinar ou alterar as políticas e as ACLs existentes para os buckets e os objetos. **Note** Os pontos de acesso não têm ACLs associadas a eles. Se você aplicar essa configuração a um ponto de acesso, ela atuará como uma passagem para o bucket subjacente. Se um ponto de acesso tiver essa configuração ativada, as solicitações feitas por meio do ponto de acesso se comportam como se o bucket subjacente tivesse essa configuração ativada, independentemente de o bucket realmente ter essa configuração ativada.

Nome	Descrição
`IgnorePublicAcls`	A definição dessa opção como `TRUE` faz o Amazon S3 ignorar todas as ACLs públicas em um bucket e todos os objetos contidos. Essa configuração permite bloquear com segurança o acesso público concedido por ACLs ao mesmo tempo que permite chamadas a `PutObject` que incluam uma ACL pública (ao contrário de `BlockPublicAcls`, que rejeita chamadas a `PutObject` que incluam uma ACL pública). A habilitação dessa configuração não afeta a persistência de ACLs existentes nem evita a definição de novas ACLs públicas. **Note** Os pontos de acesso não têm ACLs associadas a eles. Se você aplicar essa configuração a um ponto de acesso, ela atuará como uma passagem para o bucket subjacente. Se um ponto de acesso tiver essa configuração ativada, as solicitações feitas por meio do ponto de acesso se comportam como se o bucket subjacente tivesse essa configuração ativada, independentemente de o bucket realmente ter essa configuração ativada.

Nome	Descrição
`BlockPublicPolicy`	A configuração dessa opção como `TRUE` para um bucket faz com que o Amazon S3 rejeite chamadas a `PutBucketPolicy` caso a política de bucket especificada permita acesso público. A definição dessa opção como `TRUE` para um bucket também faz com que o Amazon S3 rejeite chamadas a `PutAccessPointPolicy` dos pontos de acesso na mesma conta do bucket caso a política especificada permita acesso público. A configuração dessa opção como `TRUE` para um ponto de acesso faz com que o Amazon S3 rejeite chamadas a `PutAccessPointPolicy` e `PutBucketPolicy` feitas por meio do ponto de acesso caso a política especificada (para o ponto de acesso ou o bucket subjacente) permita acesso público. Use essa configuração para permitir que os usuários gerenciem políticas de ponto de acesso e bucket sem permitir que compartilhem publicamente o bucket ou os objetos contidos. Habilitar essa configuração não afeta as políticas de ponto de acesso ou de bucket existentes. **Important** Para usar essa configuração de maneira efetiva, recomendamos que aplique-a na conta. Uma política de bucket pode permitir que os usuários alterem as configurações do Bloqueio de acesso público de um bucket. Portanto, os usuários com permissão para alterar a política de bucket podem inserir uma política que os permita desabilitar as configurações do Bloqueio de acesso público do bucket. Caso essa configuração esteja habilitada para toda a conta, em vez de um bucket específico, o Amazon S3 bloqueia as políticas públicas, mesmo que um usuário altere a política de bucket para desabilitar essa configuração.

Nome	Descrição
`RestrictPublicBuckets`	A definição dessa opção como `TRUE` restringe o acesso a um ponto de acesso ou a um bucket com uma política pública apenas a entidades principais de serviço da AWS e a usuários autorizados dentro da conta do proprietário do bucket e da conta do proprietário do ponto de acesso. Essa definição bloqueia todo o acesso entre contas ao ponto de acesso ou ao bucket (exceto por principais de serviços da AWS), ao mesmo tempo que continua permitindo que usuários dentro da conta gerenciem o ponto de acesso ou o bucket. A ativação dessa configuração não afeta políticas de ponto de acesso ou bucket existentes, exceto se o Amazon S3 bloquear os acessos público e entre contas derivados de qualquer política pública de ponto de acesso ou bucket, inclusive delegação não pública a contas específicas.

Important

- As chamadas a `GetBucketAcl` e `GetObjectAcl` sempre retornam as permissões efetivas implantadas para o bucket ou o objeto especificado. Por exemplo, suponhamos que um bucket tenha uma ACL que conceda acesso público, mas o bucket também tenha a configuração `IgnorePublicAcls` habilitada. Nesse caso, `GetBucketAcl` retorna uma ACL que reflete as permissões de acesso que o Amazon S3 está aplicando, em vez da ACL real associada ao bucket.
- As configurações do Bloqueio de acesso público não alteram as políticas ou ACLs existentes. Portanto, a remoção de uma configuração do Bloqueio de acesso público disponibiliza novamente um bucket ou um objeto com uma política pública ou uma ACL.

Executar operações de bloqueio de acesso público em um ponto de acesso

Para realizar operações do Block Public Access em um ponto de acesso, use o serviço `s3control` da AWS CLI.

> **Important**
>
> Não é possível alterar uma configuração de bloqueio de acesso público de um ponto de acesso após a criação do ponto de acesso. É possível especificar configurações de bloqueio de acesso público para um ponto de acesso somente ao criar o ponto de acesso.

O significado de "público"

ACLs

O Amazon S3 considerará uma ACL de bucket de objeto pública se ela conceder alguma permissão a membros dos grupos `AllUsers` ou `AuthenticatedUsers` predefinidos. Para obter mais informações sobre grupos predefinidos, consulte Grupos predefinidos do Amazon S3.

Políticas de buckets

Ao avaliar uma política de bucket, o Amazon S3 começa presumindo que a política é pública. Em seguida, ele avalia a política para determinar se ela se qualifica como não pública. Para ser considerada não pública, uma política de bucket deve conceder acesso apenas a valores fixos (valores que não contenham um curinga nem uma variável de política do AWS Identity and Access Management) para um ou mais dos seguintes itens:

- Um principal, um usuário, uma função ou um principal do produto da AWS (por exemplo, `aws:PrincipalOrgID`)
- Um conjunto de blocos de Encaminhamento Entre Domínios Sem Classificação (CIDR), usando `aws:SourceIp`. Para obter mais informações sobre o CIDR, consulte RFC 4632 no site RFC Editor.

> **Note**
>
> As políticas de bucket que concedem acesso condicionado à chave de condição `aws:SourceIp` com intervalos de IPs muito amplos (por exemplo, 0.0.0.0/1) são avaliadas como “públicas”. Isso inclui valores maiores que `/8` para IPv4 e `/32` para IPv6 (exceto intervalos privados RFC1918). O bloqueio de acesso público rejeitará essas políticas “públicas” e impedirá o acesso entre contas a buckets que já usem essas políticas “públicas”.

- `aws:SourceArn`
- `aws:SourceVpc`
- `aws:SourceVpce`
- `aws:SourceOwner`
- `aws:SourceAccount`
- `aws:userid`, fora do padrão "`AROLEID:*`"
- `s3:DataAccessPointArn`

> **Note**
>
> Quando usado em uma política de bucket, esse valor pode conter um curinga para o nome do ponto de acesso sem tornar a política pública, desde que o ID da conta seja corrigido. Por exemplo, permitir acesso a `arn:aws:s3:us-west-2:123456789012:accesspoint/*` permitiria o acesso a qualquer ponto de acesso associado à conta `123456789012` na região `us-west-2`, sem tornar pública a política de bucket. Esse comportamento é diferente para políticas de ponto de acesso. Para obter mais informações, consulte Pontos de acesso.

- `s3:DataAccessPointAccount`

Para obter mais informações sobre políticas de bucket, consulte Políticas de bucket para o Amazon S3.

> **Note**
>
> Ao utilizar chaves de contexto multivaloradas, você deve usar os operadores de conjunto `ForAllValues` ou `ForAnyValue`.

Example : Políticas públicas de buckets

Nessas regras, as políticas de exemplo a seguir são consideradas públicas.

```
{
  "Principal": "*",
  "Resource": "*",
  "Action": "s3:PutObject",
```

```
  "Effect": "Allow"
 }
```

```
{
  "Principal": "*",
  "Resource": "*",
  "Action": "s3:PutObject",
  "Effect": "Allow",
  "Condition": { "StringLike": {"aws:SourceVpc": "vpc-*"}}
 }
```

É possível tornar essas políticas não públicas com a inclusão de alguma das chaves de condição listadas anteriormente usando-se um valor fixo. Por exemplo, a última política acima pode se tornar não pública com a definição de `aws:SourceVpc` como um valor fixo como o seguinte.

```
{
  "Principal": "*",
  "Resource": "*",
  "Action": "s3:PutObject",
  "Effect": "Allow",
  "Condition": {"StringEquals": {"aws:SourceVpc": "vpc-91237329"}}
 }
```

Como o Amazon S3 avalia uma política de bucket que contém concessões de acesso público e não público

Este exemplo mostra como o Amazon S3 avalia uma política de bucket que contém concessões de acesso público e não público.

Suponhamos que um bucket tenha uma política que conceda acesso a um conjunto de entidades principais fixas. Segundo as regras descritas anteriormente, essa política não é pública. Por isso, se você habilitar a configuração `RestrictPublicBuckets`, a política permanecerá em vigor como escrita, porque `RestrictPublicBuckets` só se aplica a buckets que tenham políticas públicas. No entanto, se você adicionar uma instrução pública à política, o `RestrictPublicBuckets` será ativado no bucket. Isso permite que somente principais de serviço da AWS e usuários autorizados da conta do proprietário do bucket acessem o bucket.

Como exemplo, suponhamos que um bucket de propriedade de "Account-1" tenha uma política que contenha o seguinte:

1. Uma instrução que conceda acesso ao AWS CloudTrail (uma entidade principal de serviço da AWS)
2. Uma instrução que conceda acesso à conta "Account-2"
3. Uma instrução que conceda acesso ao público, por exemplo, especificando `"Principal": "*"` sem limitação de `Condition`

Essa política é qualificada como pública por causa da terceira instrução. Com essa política implementada e `RestrictPublicBuckets` ativado, o Amazon S3 permite o acesso somente pelo CloudTrail. Embora a instrução 2 não seja pública, o Amazon S3 desabilita o acesso de "Account-2". Isso porque a instrução 3 renderiza toda a política pública. Assim, `RestrictPublicBuckets` se aplica. Dessa forma, o Amazon S3 desabilita o acesso entre contas, mesmo que a política delegue acesso a uma conta específica, "Account-2". Porém, se você remover a instrução 3 da política, esta não se qualificará como pública e `RestrictPublicBuckets` deixará de se aplicar. Por isso, "Account-2" retoma o acesso ao bucket, mesmo caso você deixe `RestrictPublicBuckets` habilitado.

Pontos de acesso

O Amazon S3 avalia as configurações do Bloqueio de acesso público de maneira um pouco diferente para os pontos de acesso em comparação com os buckets. As regras que o Amazon S3 aplica para determinar quando uma política de ponto de acesso é pública são geralmente as mesmas para pontos de acesso e para buckets, exceto nas seguintes situações:

- Um ponto de acesso que tenha uma origem de rede da VPC é sempre considerado não público, independentemente do conteúdo da política de ponto de acesso.
- Uma política de ponto de acesso que concede acesso a um conjunto de pontos de acesso usando `s3:DataAccessPointArn` é considerada pública. Observe que esse comportamento é diferente para políticas de bucket. Por exemplo, uma política de bucket que concede acesso a valores de `s3:DataAccessPointArn` que correspondem a `arn:aws:s3:us-west-2:123456789012:accesspoint/*` não é considerada pública. No entanto, a mesma instrução em uma política de ponto de acesso tornaria o ponto de acesso público.

Usar o IAM Access Analyzer para S3 para revisar buckets públicos

É possível usar o IAM Access Analyzer para S3 para revisar buckets com ACLs de bucket, políticas de bucket ou políticas de ponto de acesso que concedem acesso público. O IAM Access Analyzer

para S3 alerta você sobre buckets que são configurados para permitir o acesso a qualquer pessoa na internet ou a outras Contas da AWS, incluindo Contas da AWS fora da organização. Para cada bucket público ou compartilhado, você recebe descobertas que relatam a origem e o nível de acesso público ou compartilhado.

No IAM Access Analyzer para S3, é possível bloquear todo o acesso público a um bucket com um único clique. Você também pode detalhar as configurações de permissão no nível do bucket para definir níveis granulares de acesso. Para casos de uso específicos e verificados que exigem acesso público ou compartilhado, você pode confirmar e registrar sua intenção de que o bucket permaneça público ou compartilhado arquivando as descobertas do bucket.

Em casos raros, o analisador de acesso do IAM para S3 e a avaliação da funcionalidade Bloqueio de Acesso Público do Amazon S3 podem divergir sobre um bucket ser público ou não. Esse comportamento ocorre porque a funcionalidade Bloqueio de Acesso Público do Amazon S3 realiza a validação da existência de ações, além de avaliar o acesso público. Suponha que a política do bucket contenha uma instrução `Action` que permita o acesso público a uma ação que não é compatível com o Amazon S3 (por exemplo, `s3:NotASupportedAction`). Nesse caso, a funcionalidade Bloqueio de Acesso Público do Amazon S3 avalia o bucket como público porque tal instrução tem o potencial de tornar o bucket público se a ação se tornar compatível posteriormente. Nos casos em que a funcionalidade Bloqueio de Acesso Público do Amazon S3 e o analisador de acesso do IAM para S3 diferem em suas avaliações, recomendamos revisar a política do bucket e remover quaisquer ações incompatíveis.

Para obter mais informações sobre o IAM Access Analyzer para S3, consulte Revisar o acesso de bucket usando o IAM Access Analyzer para S3.

Permissões

Para usar os recursos do Bloqueio de acesso público do Amazon S3, você deve ter as permissões a seguir.

Operação	Permissões obrigatórias
Status da política de bucket `GET`	`s3:GetBucketPolicyStatus`
Configurações do Bloqueio de Acesso Público do bucket `GET`	`s3:GetBucketPublicAccessBlock`

Operação	Permissões obrigatórias
Configurações do Bloqueio de Acesso Público do bucket PUT	`s3:PutBucketPublicAccessBlock`
Configurações do Bloqueio de Acesso Público do bucket DELETE	`s3:PutBucketPublicAccessBlock`
Configurações do Bloqueio de Acesso Público da conta GET	`s3:GetAccountPublicAccessBlock`
Configurações do Bloqueio de Acesso Público da conta PUT	`s3:PutAccountPublicAccessBlock`
Configurações do Bloqueio de Acesso Público da conta DELETE	`s3:PutAccountPublicAccessBlock`
Configurações do Bloqueio de acesso público do ponto de acesso PUT	`s3:CreateAccessPoint`

> **Note**
>
> As operações DELETE exigem as mesmas permissões das operações PUT. Não há permissões separadas para as operações DELETE.

Configurar o bloqueio de acesso público

Para ter mais informações sobre como configurar o Bloqueio de Acesso Público para a Conta da AWS, os buckets do Amazon S3 e os pontos de acesso, consulte os seguintes tópicos:

- Configurar o bloqueio de acesso público para sua conta
- Configurar o bloqueio de acesso público para seus buckets do S3
- Executar operações de bloqueio de acesso público em um ponto de acesso

Configurar o bloqueio de acesso público para sua conta

O Bloqueio de acesso público do Amazon S3 fornece configurações para pontos de acesso, buckets e contas para ajudar você a gerenciar o acesso público aos recursos do Amazon S3. Por padrão, novos buckets, pontos de acesso e objetos não permitem acesso público.

Para obter mais informações, consulte Bloquear o acesso público ao armazenamento do Amazon S3.

> **Note**
>
> As configurações no nível da conta substituem as configurações de objetos individuais. Configurar a conta para bloquear o acesso público substituirá todas as configurações de acesso público feitas a objetos individuais na conta.

Você pode usar o console do S3, a AWS CLI, os AWS SDKs e a API REST para definir as configurações de bloqueio de acesso público para todos os buckets da sua conta. Para obter mais informações, consulte as seções abaixo.

Para definir as configurações do bloqueio de acesso público para os buckets, consulte Configurar o bloqueio de acesso público para seus buckets do S3. Para obter mais informações sobre pontos de acesso, consulte Executar operações de bloqueio de acesso público em um ponto de acesso.

Uso do console do S3

O bloqueio de acesso público do Amazon S3 evita a aplicação de todas as configurações que permitem acesso público a dados dentro de buckets do S3. Esta seção descreve como editar as configurações de bloqueio de acesso público para todos os buckets do S3 na sua Conta da AWS. Para obter mais informações sobre como bloquear o acesso público, consulte Bloquear o acesso público ao armazenamento do Amazon S3.

Para editar configurações de bloqueio de acesso público para todos os buckets do S3 em uma Conta da AWS

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Escolha Block Public Access settings for this account (Configurações Bloquear acesso público para esta conta).

3. Escolha Edit (Editar) para alterar as configurações de acesso público de bloqueio para todos os buckets na Conta da AWS.
4. Escolha as configurações que deseja alterar e selecione Save (Salvar).
5. Quando a confirmação é solicitada, digite **`confirm`**. Em seguida, escolha Confirm (Confirmar) para salvar as alterações.

Como usar o AWS CLI

Você pode usar o bloqueio de acesso público do Amazon S3 por meio da AWS CLI. Para obter mais informações sobre como configurar e usar a AWS CLI, consulte O que é a AWS Command Line Interface?

Conta

Para realizar operações do Block Public Access em uma conta, use o serviço da AWS CLI `s3control`. As operações no nível da conta que usam esse serviço são:

- `PutPublicAccessBlock` (para uma conta)
- `GetPublicAccessBlock` (para uma conta)
- `DeletePublicAccessBlock` (para uma conta)

Consulte mais informações e exemplos em put-public-access-block na Referência da AWS CLI.

Uso dos SDKs da AWS

Java

Os exemplos a seguir mostram como usar o bloqueio de acesso público do Amazon S3 com o AWS SDK para Java para colocar uma configuração de bloqueio de acesso público em uma conta do Amazon S3.

```
AWSS3ControlClientBuilder controlClientBuilder =
 AWSS3ControlClientBuilder.standard();
controlClientBuilder.setRegion(<region>);
controlClientBuilder.setCredentials(<credentials>);

AWSS3Control client = controlClientBuilder.build();
client.putPublicAccessBlock(new PutPublicAccessBlockRequest()
```

```
  .withAccountId(<account-id>)
  .withPublicAccessBlockConfiguration(new PublicAccessBlockConfiguration()
    .withIgnorePublicAcls(<value>)
    .withBlockPublicAcls(<value>)
    .withBlockPublicPolicy(<value>)
    .withRestrictPublicBuckets(<value>)));
```

> **Important**
>
> Este exemplo pertence apenas a operações no nível da conta, que usam a classe cliente `AWSS3Control`. Para operações no nível do bucket, consulte o exemplo anterior.

Other SDKs

Consulte informações sobre como usar outros SDKs da AWS em Developing with Amazon S3 using the AWS SDKs na Referência de API do Amazon S3.

Uso da API REST

Para obter informações sobre o uso do Bloqueio de acesso público do Amazon S3 por meio das APIs REST, consulte os tópicos a seguir na Referência da API do Amazon Simple Storage Service.

- Operações no nível da conta
  - PutPublicAccessBlock
  - GetPublicAccessBlock
  - DeletePublicAccessBlock

Configurar o bloqueio de acesso público para seus buckets do S3

O Bloqueio de acesso público do Amazon S3 fornece configurações para pontos de acesso, buckets e contas para ajudar você a gerenciar o acesso público aos recursos do Amazon S3. Por padrão, novos buckets, pontos de acesso e objetos não permitem acesso público.

Para obter mais informações, consulte Bloquear o acesso público ao armazenamento do Amazon S3.

É possível usar o console do S3, a AWS CLI, os AWS SDKs e a API REST para conceder acesso público a um ou mais buckets. Também é possível bloquear o acesso público a buckets que já são públicos. Para obter mais informações, consulte as seções abaixo.

Para definir as configurações do Bloqueio de Acesso Público para todos os buckets em sua conta, consulte Configurar o bloqueio de acesso público para sua conta. Para obter informações sobre como configurar o bloqueio de acesso público para pontos de acesso, consulte Executar operações de bloqueio de acesso público em um ponto de acesso.

Uso do console do S3

O bloqueio de acesso público do Amazon S3 evita a aplicação de todas as configurações que permitem acesso público a dados dentro de buckets do S3. Esta seção descreve como editar configurações de acesso público de bloqueio para um ou mais buckets do S3. Para obter informações sobre como bloquear o acesso público usando a AWS CLI, os AWS SDKs e as APIs REST do Amazon S3, consulte Bloquear o acesso público ao armazenamento do Amazon S3.

Você pode ver se o bucket está acessível ao público na lista Buckets, na coluna Analisador de acesso do IAM. Para obter mais informações, consulte Revisar o acesso de bucket usando o IAM Access Analyzer para S3.

Se você vir um `Error` ao listar seus buckets e as respectivas configurações de acesso público, talvez você não tenha as permissões necessárias. Confira se você tem as seguintes permissões adicionadas à política de usuário ou perfil:

```
s3:GetAccountPublicAccessBlock
s3:GetBucketPublicAccessBlock
s3:GetBucketPolicyStatus
s3:GetBucketLocation
s3:GetBucketAcl
s3:ListAccessPoints
s3:ListAllMyBuckets
```

Em alguns casos raros, as solicitações também podem falhar devido a uma interrupção da Região da AWS.

Para editar as configurações de bloqueio de acesso público do Amazon S3 para um bucket do S3

Siga essas etapas caso você precise alterar as configurações de acesso público para um único bucket do S3.

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Na lista Bucket name (Nome do bucket), escolha o nome do bucket que você deseja.
3. Escolha Permissions (Permissões).
4. Escolha Editar ao lado de Bloquear acesso público (configurações de bucket) para alterar as configurações de acesso público referentes ao bucket. Para obter mais informações sobre as quatro configurações do Bloqueio de acesso público do Amazon S3, consulte Configurações do bloqueio de acesso público.
5. Selecione uma das configurações e escolha Salvar alterações.
6. Quando a confirmação é solicitada, digite **`confirm`**. Em seguida, escolha Confirm (Confirmar) para salvar as alterações.

Também é possível alterar as configurações de Bloqueio de Acesso Público do Amazon S3 ao criar um bucket. Para obter mais informações, consulte Criar um bucket de uso geral.

Usar a AWS CLI

Para bloquear o acesso público em um bucket ou excluir o Bloqueio de Acesso Público, use o `s3api` do serviço da AWS CLI. As operações no nível do bucket que usam esse serviço são:

- `PutPublicAccessBlock` (para um bucket)
- `GetPublicAccessBlock` (para um bucket)
- `DeletePublicAccessBlock` (para um bucket)
- `GetBucketPolicyStatus`

Para obter mais informações e exemplos, consulte put-public-access-block na Referência da AWS CLI.

Uso dos SDKs da AWS

Java

```
AmazonS3 client = AmazonS3ClientBuilder.standard()
   .withCredentials(<credentials>)
   .build();
```

```
client.setPublicAccessBlock(new SetPublicAccessBlockRequest()
  .withBucketName(<bucket-name>)
  .withPublicAccessBlockConfiguration(new PublicAccessBlockConfiguration()
    .withBlockPublicAcls(<value>)
    .withIgnorePublicAcls(<value>)
    .withBlockPublicPolicy(<value>)
    .withRestrictPublicBuckets(<value>)));
```

> **Important**
>
> Este exemplo pertence apenas a operações no nível do bucket, que usam a classe cliente `AmazonS3`. Para operações no nível da conta, consulte o exemplo a seguir.

Other SDKs

Consulte informações sobre como usar outros SDKs da AWS em Developing with Amazon S3 using the AWS SDKs na Referência de API do Amazon S3.

Uso da API REST

Para obter informações sobre o uso do Bloqueio de acesso público do Amazon S3 por meio das APIs REST, consulte os tópicos a seguir na Referência da API do Amazon Simple Storage Service.

- Operações no nível do bucket
  - PutPublicAccessBlock
  - GetPublicAccessBlock
  - DeletePublicAccessBlock
  - GetBucketPolicyStatus

Revisar o acesso de bucket usando o IAM Access Analyzer para S3

O IAM Access Analyzer para S3 alerta você sobre buckets do S3 que são configurados para permitir o acesso a qualquer pessoa na internet ou a outras Contas da AWS, incluindo Contas da AWS fora da organização. Para cada bucket público ou compartilhado, você recebe descobertas sobre

a origem e o nível de acesso público ou compartilhado. Por exemplo, o IAM Access Analyzer para S3 pode mostrar que um bucket tem acesso de leitura ou gravação fornecido por meio de uma lista de controle de acesso (ACL) de bucket, uma política de bucket, uma política de ponto de acesso multirregional ou uma política de ponto de acesso. Com essas descobertas, você pode tomar medidas corretivas imediatas e precisas para restaurar o acesso ao bucket da forma desejada.

Ao revisar um bucket em risco no IAM Access Analyzer para S3, é possível bloquear todo o acesso público ao bucket com um único clique. Recomendamos que você bloqueie todo o acesso aos buckets, a menos que exija acesso público para dar suporte a um caso de uso específico. Antes de bloquear todo o acesso público, certifique-se de que os aplicativos continuarão funcionando corretamente sem acesso público. Para obter mais informações, consulte Bloquear o acesso público ao armazenamento do Amazon S3.

Você também pode detalhar as configurações de permissão no nível do bucket para definir níveis granulares de acesso. Para casos de uso específicos e verificados que exigem acesso público, como hospedagem estática de sites, downloads públicos ou compartilhamento entre contas, você pode reconhecer e registrar sua intenção de que o bucket permaneça público ou compartilhado arquivando as descobertas do bucket. Você pode acessar novamente e modificar essas configurações de bucket a qualquer momento. Você também pode fazer download das descobertas como um relatório CSV para fins de auditoria.

O IAM Access Analyzer para S3 está disponível sem custo adicional no console do Amazon S3. O IAM Access Analyzer para S3 usa tecnologia do AWS Identity and Access Management (IAM) Access Analyzer. Para usar o IAM Access Analyzer para S3 no console do Amazon S3, é necessário acessar o console do IAM e habilitar o IAM Access Analyzer por região.

Para obter mais informações sobre o IAM Access Analyzer, consulte O que é o IAM Access Analyzer? no Guia do usuário do IAM. Para obter mais informações sobre o IAM Access Analyzer para S3, consulte as seções a seguir.

Important

- O IAM Access Analyzer para S3 requer um analisador de nível de conta. Para usar o IAM Access Analyzer para S3, é necessário acessar o IAM Access Analyzer e criar um analisador que tenha uma conta como a zona de confiança. Para obter mais informações, consulte Habilitar o IAM Access Analyzer no Guia do usuário do IAM.
- O IAM Access Analyzer para S3 não analisa a política de ponto de acesso vinculada a pontos de acesso entre contas. Esse comportamento ocorre porque o ponto de acesso

e sua política estão fora da zona de confiança, ou seja, fora da conta. Os buckets que delegam acesso a um ponto de acesso entre contas estão listados em Buckets with public access (Buckets com acesso público) caso você não tenha aplicado a configuração de bloqueio de acesso público `RestrictPublicBuckets` ao bucket ou à conta. Quando você aplica a configuração de bloqueio de acesso público `RestrictPublicBuckets`, o bucket é relatado em Buckets com acesso de outras Contas da AWS, inclusive Contas da AWS de terceiros.

- Quando uma política de bucket ou a ACL do bucket é adicionada ou modificada, o IAM Access Analyzer gera e atualiza descobertas com base na alteração em até 30 minutos. As descobertas relacionadas às configurações de bloqueio de acesso público na conta podem não ser geradas nem atualizadas por até 6 horas após a alteração das configurações. As descobertas relacionadas a pontos de acesso multirregionais podem não ser geradas nem atualizadas até seis horas após o ponto de acesso multirregional ser criado, excluído ou você alterar sua política.

Tópicos

- Quais informações o IAM Access Analyzer para S3 fornece?
- Habilitar o IAM Access Analyzer para S3
- Bloquear todo o acesso público
- Revisar e alterar o acesso ao bucket
- Arquivar descobertas de bucket
- Ativar uma descoberta de bucket arquivada
- Visualizar detalhes de descobertas
- Baixar um relatório do IAM Access Analyzer para S3

Quais informações o IAM Access Analyzer para S3 fornece?

O IAM Access Analyzer para S3 fornece descobertas para buckets que podem ser acessados fora da sua Conta da AWS. Os buckets listados em Buckets with public access (Buckets com acesso público) podem ser acessados por qualquer pessoa na internet. Se o IAM Access Analyzer para S3 identificar buckets públicos, você também verá um aviso na parte superior da página que mostra o número de buckets públicos na região. Os buckets listados em Buckets com acesso de outrasContas da AWS, inclusive Contas da AWS de terceiros são compartilhados condicionalmente com outras Contas da AWS, inclusive com contas fora de sua organização.

Para cada bucket, o IAM Access Analyzer para S3 fornece as seguintes informações:

- Nome do bucket
- Descoberto pelo Access Analyzer: quando o IAM Access Analyzer para S3 descobriu o acesso a bucket público ou compartilhado.
- Compartilhado por: como o bucket é compartilhado, por meio de uma política de bucket, uma ACL de bucket ou uma política de ponto de acesso multirregional ou uma política de ponto de acesso. Pontos de acesso multirregionais e pontos de acesso entre contas são refletidos em pontos de acesso. Um bucket pode ser compartilhado por meio de políticas e ACLs. Se você quiser descobrir e analisar a origem do acesso ao bucket, poderá usar as informações nesta coluna como um ponto de partida para tomar medidas corretivas imediatas e precisas.
- Status – O status da descoberta do bucket. O IAM Access Analyzer para S3 exibe descobertas para todos os buckets públicos e compartilhados.
  - Ativa – a descoberta não foi analisada.
  - Arquivada – a descoberta foi analisada e confirmada conforme pretendido.
  - All (Todas): todas as descobertas de buckets que são públicos ou compartilhados com outras Contas da AWS, incluindo Contas da AWS fora da sua organização.
- Nível de acesso — permissões de acesso concedidas para o bucket:
  - Lista – lista de recursos.
  - Leitura – ler, mas não editar o conteúdo e os atributos do recurso.
  - Gravação – criar, excluir ou modificar recursos.
  - Permissões – conceder ou modificar permissões de recursos.
  - Atribuição de tags – atualizar as tags associadas ao recurso.

Habilitar o IAM Access Analyzer para S3

Para usar o IAM Access Analyzer para S3, é necessário concluir as etapas de pré-requisito a seguir.

1. Conceda as permissões necessárias aos usuários.

   Para obter mais informações, consulte Permissões necessárias para usar o IAM Access Analyzer no Guia do usuário do IAM.
2. Acesse o IAM para criar um analisador de nível de conta para cada região onde você deseja usar o IAM Access Analyzer.

O IAM Access Analyzer para S3 requer um analisador de nível de conta. Para usar o IAM Access Analyzer para S3, é necessário criar um analisador que tenha uma conta como a zona de confiança. Para obter mais informações, consulte Habilitar o IAM Access Analyzer no Guia do usuário do IAM.

Bloquear todo o acesso público

Se você quiser bloquear todo o acesso a um bucket com um único clique, use o botão Bloquear todo o acesso público no IAM Access Analyzer para S3. Quando você bloquear todo o acesso público a um bucket, nenhum acesso público será concedido. Recomendamos que você bloqueie todo o acesso público aos buckets, a menos que exija acesso público para dar suporte a um caso de uso específico e verificado. Antes de bloquear todo o acesso público, certifique-se de que os aplicativos continuarão funcionando corretamente sem acesso público.

Se não quiser bloquear todo o acesso público ao bucket, você pode editar as configurações de bloqueio de acesso público no console do Amazon S3 para configurar níveis granulares de acesso aos buckets. Para obter mais informações, consulte Bloquear o acesso público ao armazenamento do Amazon S3.

Em casos raros, o analisador de acesso do IAM para S3 e a avaliação da funcionalidade Bloqueio de Acesso Público do Amazon S3 podem divergir sobre um bucket ser público ou não. Esse comportamento ocorre porque a funcionalidade Bloqueio de Acesso Público do Amazon S3 realiza a validação da existência de ações, além de avaliar o acesso público. Suponha que a política do bucket contenha uma instrução `Action` que permita o acesso público a uma ação que não é compatível com o Amazon S3 (por exemplo, `s3:NotASupportedAction`). Nesse caso, a funcionalidade Bloqueio de Acesso Público do Amazon S3 avalia o bucket como público porque tal instrução tem o potencial de tornar o bucket público se a ação se tornar compatível posteriormente. Nos casos em que a funcionalidade Bloqueio de Acesso Público do Amazon S3 e o analisador de acesso do IAM para S3 diferem em suas avaliações, recomendamos revisar a política do bucket e remover quaisquer ações incompatíveis.

Para bloquear todo o acesso público a um bucket usando o IAM Access Analyzer para S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, em Dashboards (Painéis), escolha Access Analyzer for S3.
3. No IAM Access Analyzer para S3, escolha um bucket.

4. Selecione Block all public access (Bloquear todo o acesso público).
5. Para confirmar sua intenção de bloquear todo o acesso público ao bucket, em Block all public access (bucket settings) (Bloquear todo o acesso público [configurações de bucket]), digite **`confirm`**.

   O Amazon S3 bloqueia todo o acesso público ao bucket. O status da descoberta do bucket é atualizado para resolvido e o bucket desaparece da listagem do IAM Access Analyzer para S3. Se você quiser revisar os buckets resolvidos, abra o IAM Access Analyzer no console do IAM.

Revisar e alterar o acesso ao bucket

Se você não pretendia conceder acesso às contas públicas ou outras Contas da AWS, incluindo contas fora da organização, você pode modificar a ACL de bucket, a política de bucket ou a política de ponto de acesso multirregional para remover o acesso ao bucket. A coluna Shared through (Compartilhado por) mostra todas as origens de acesso ao bucket: política de bucket, ACL de bucket e/ou política de ponto de acesso. Pontos de acesso multirregionais e pontos de acesso entre contas são refletidos em pontos de acesso.

Para revisar e alterar uma política de bucket, uma ACL de bucket, um ponto de acesso multirregional ou uma política de ponto de acesso

1. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação, escolha Access Analyzer for S3 (Analisador de acesso para S3).
3. Para ver se o acesso público ou o acesso compartilhado é concedido por meio de uma política de bucket, uma ACL de bucket ou uma política de ponto de acesso multirregional, verifique a coluna Shared through (Compartilhado por).
4. Em Buckets, escolha o nome do bucket com a política de bucket, a ACL de bucket ou a política de ponto de acesso multirregional que deseja alterar ou revisar.
5. Se você quiser alterar ou exibir uma ACL de bucket:

   a. Escolha Permissions (Permissões).

   b. Escolha Access Control List.

   c. Revise a ACL de bucket e faça as alterações conforme necessário.

      Para obter mais informações, consulte Configurar ACLs.
6. Se você quiser alterar ou revisar uma política de bucket:

a. Escolha Permissions (Permissões).

b. Escolha Bucket Policy.

c. Revise ou altere a política de bucket conforme necessário.

Para obter mais informações, consulte Adicionar uma política de bucket usando o console do Amazon S3.

7. Se você quiser alterar ou exibir uma política de ponto de acesso multirregional:

a. Escolha Multi-Region Access Point (Ponto de acesso multirregional).

b. Escolha o nome do ponto de acesso multirregional.

c. Revise ou altere a política de pontos de acesso multirregionais, conforme necessário.

Para obter mais informações, consulte Permissões.

8. Se você quiser revisar ou alterar uma política de ponto de acesso:

a. Escolha access points (pontos de acesso).

b. Escolha o nome do ponto de acesso.

c. Revise ou altere o acesso conforme necessário.

Para obter mais informações, consulte Gerenciar o recurso Pontos de Acesso Amazon S3 para buckets de uso geral.

Se você editar ou remover uma ACL de bucket, uma política de bucket ou uma política de ponto de acesso para remover o acesso público ou compartilhado, o status das descobertas do bucket será atualizado para resolved (resolvido). As descobertas de bucket resolvidas desaparecem da lista do IAM Access Analyzer para S3, mas é possível visualizá-las no IAM Access Analyzer.

Arquivar descobertas de bucket

Se um bucket conceder acesso a contas públicas ou outras Contas da AWS, inclusive contas fora da organização, para comportar um caso de uso específico (por exemplo, um site estático, downloads públicos ou compartilhamento entre contas), você poderá arquivar a descoberta do bucket. Ao arquivar descobertas de bucket, você reconhece e registra sua intenção de que o bucket permaneça público ou compartilhado. As descobertas de bucket arquivadas permanecem na listagem do IAM Access Analyzer para S3 para que você sempre saiba quais buckets são públicos ou compartilhados.

Como arquivar descobertas de bucket no IAM Access Analyzer para S3

1. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação, escolha Access Analyzer for S3 (Analisador de acesso para S3).
3. No IAM Access Analyzer para S3, escolha um bucket ativo.
4. Para confirmar sua intenção de que esse bucket seja acessado pelas contas públicas ou outras Contas da AWS, inclusive contas fora da organização, escolha Archive (Arquivar).
5. Digite **`confirm`** e escolha Archive (Arquivar).

Ativar uma descoberta de bucket arquivada

Depois de arquivar descobertas, você sempre poderá revisitá-las e alterar o status novamente para ativo, indicando que o bucket requer outra análise.

Como ativar uma descoberta de bucket arquivado no IAM Access Analyzer para S3

1. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação, escolha Access Analyzer for S3 (Analisador de acesso para S3).
3. Escolha as descobertas do bucket arquivadas.
4. Escolha Mark as active (Marcar como ativo).

Visualizar detalhes de descobertas

Se você precisar ver mais informações sobre um bucket, poderá abrir os detalhes de descobertas de bucket no IAM Access Analyzer no console do IAM.

Para visualizar detalhes de descoberta no IAM Access Analyzer para S3

1. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação, escolha Access Analyzer for S3 (Analisador de acesso para S3).
3. No IAM Access Analyzer para S3, escolha um bucket.
4. Escolha View details (Exibir detalhes).

   Os detalhes de descobertas são abertos no IAM Access Analyzer no console do IAM.

Baixar um relatório do IAM Access Analyzer para S3

Você pode fazer download das descobertas de bucket como um relatório CSV que pode ser usado para fins de auditoria. O relatório inclui as mesmas informações que você vê no IAM Access Analyzer para S3 no console do Amazon S3.

Como fazer download de um relatório

1. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Access Analyzer for S3 (Analisador de acesso para S3).
3. No filtro Região, escolha a região.

   O IAM Access Analyzer para S3 é atualizado para mostrar buckets para a região escolhida.
4. Escolha Download report (Fazer download do relatório).

   Um relatório CSV é gerado e salvo no computador.

Verificar a propriedade do bucket com a condição de proprietário do bucket

A condição de proprietário do bucket do Amazon S3 garante que os buckets que você usa em suas operações do S3 pertençam às Contas da AWS que você espera.

A maioria das operações do S3 lê ou grava em buckets específicos do S3. Essas operações incluem fazer upload, cópia e download de objetos, recuperar ou modificar as configurações de bucket e recuperar ou modificar as configurações de objeto. Ao executar essas operações, você especifica o bucket que deseja usar, incluindo seu nome com a solicitação. Por exemplo, para recuperar um objeto do S3, você faz uma solicitação que especifica o nome de um bucket e a chave de objeto a ser recuperada desse bucket.

Como o Amazon S3 identifica buckets com base em seus nomes, uma aplicação que usa um nome de bucket incorreto em uma solicitação pode executar operações inadvertidamente em um bucket diferente do esperado. Para ajudar a evitar interações não intencionais de bucket em situações como essa, você pode usar a condição do proprietário do bucket. A condição de proprietário do bucket permite que você verifique se o bucket de destino pertence à Conta da AWS esperada, fornecendo

uma camada adicional de garantia de que suas operações do S3 estão tendo os efeitos que você pretende.

Tópicos

- Quando usar a condição do proprietário do bucket
- Verificar um proprietário do bucket
- Exemplos
- Restrições e limitações

Quando usar a condição do proprietário do bucket

Recomendamos usar a condição de proprietário do bucket sempre que você executar uma operação compatível do S3 e conhecer o ID da conta do proprietário do bucket esperado. A condição do proprietário do bucket está disponível para todas as operações de objeto do S3 e para a maioria das operações de bucket do S3. Para obter uma lista de operações do S3 que não oferecem suporte à condição de proprietário do bucket, consulte Restrições e limitações.

Para ver o benefício de usar a condição de proprietário do bucket, considere o seguinte cenário envolvendo a cliente da AWS, Bea:

1. Bea desenvolve uma aplicação que usa o Amazon S3. Durante o desenvolvimento, Bea usa sua Conta da AWS somente para testes para criar um bucket chamado `bea-data-test` e configura sua aplicação para fazer solicitações a `bea-data-test`.
2. Bea implanta sua aplicação, mas esquece de reconfigurá-la para usar um bucket em sua Conta da AWS de produção.
3. Na produção, a aplicação de Bea faz solicitações para `bea-data-test`, que são bem-sucedidas. Isso resulta na gravação de dados de produção no bucket na conta de teste da Bea.

Bea pode ajudar a evitar situações como esta usando a condição de proprietário do bucket. Com a condição de proprietário do bucket, Bea pode incluir o ID da Conta da AWS do proprietário do bucket esperado em suas solicitações. O Amazon S3, então, verifica o ID da conta do proprietário do bucket antes de processar cada solicitação. Se o proprietário real do bucket não corresponder ao proprietário do bucket esperado, a solicitação falhará.

Se Bea usar a condição de proprietário do bucket, o cenário descrito anteriormente não resultará na gravação inadvertida da aplicação de Bea em um bucket de teste. Em vez disso, as solicitações

que a aplicação dela fizer na etapa 3 falharão e apresentarão uma mensagem de erro de `Access Denied`. Ao usar a condição de proprietária do bucket, Bea ajuda a eliminar o risco de interagir acidentalmente com buckets na Conta da AWS errada.

Verificar um proprietário do bucket

Para usar a condição de proprietário do bucket, você inclui um parâmetro com sua solicitação que especifica o proprietário do bucket esperado. A maioria das operações do S3 envolve apenas um único bucket e requer apenas esse parâmetro único para usar a condição de proprietário do bucket. Para operações `CopyObject`, esse primeiro parâmetro especifica o proprietário esperado do bucket de destino e você inclui um segundo parâmetro para especificar o proprietário esperado do bucket de origem.

Quando você faz uma solicitação que inclui um parâmetro de condição do proprietário do bucket, o S3 verifica o ID da conta do proprietário do bucket em relação ao parâmetro especificado antes de processar a solicitação. Se o parâmetro corresponder ao ID da conta do proprietário do bucket, o S3 processará a solicitação. Se o parâmetro não corresponder ao ID da conta do proprietário do bucket, a solicitação falhará e apresentará uma mensagem de erro de `Access Denied`.

Você pode usar a condição de proprietário do bucket com a AWS Command Line Interface (AWS CLI), AWS SDKs e APIs REST do Amazon S3. Ao usar a condição de proprietário do bucket com a AWS CLI e as APIs REST do Amazon S3, utilize os seguintes nomes de parâmetros.

Método de acesso	Parâmetro para operações sem cópia	Copiar parâmetro de origem da operação	Copiar parâmetro de destino da operação
AWS CLI	`--expected-bucket-owner`	`--expected-source-bucket-owner`	`--expected-bucket-owner`
APIs REST do Amazon S3	`x-amz-expected-bucket-owner` Cabeçalho	`x-amz-source-expected-bucket-owner` Cabeçalho	`x-amz-expected-bucket-owner` Cabeçalho

Os nomes de parâmetros necessários para usar a condição de proprietário do bucket com os AWS SDKs variam dependendo da linguagem. Para determinar os parâmetros necessários, consulte a documentação do SDK para o idioma desejado. Você pode encontrar a documentação do SDK em Ferramentas para criar na AWS.

Exemplos

Os exemplos a seguir mostram como você pode implementar a condição de proprietário do bucket no Amazon S3 usando a AWS CLI ou o AWS SDK for Java 2.x.

Example

Exemplo: fazer upload de um objeto

O exemplo a seguir carrega um objeto para o bucket do S3 *amzn-s3-demo-bucket1* usando a condição de proprietário do bucket para garantir que *amzn-s3-demo-bucket1* seja de propriedade da Conta da AWS 111122223333.

AWS CLI

```
aws s3api put-object \
                 --bucket amzn-s3-demo-bucket1 --key exampleobject --
body example_file.txt \
                 --expected-bucket-owner 111122223333
```

AWS SDK for Java 2.x

```
public void putObjectExample() {
    S3Client s3Client = S3Client.create();;
    PutObjectRequest request = PutObjectRequest.builder()
            .bucket("amzn-s3-demo-bucket1")
            .key("exampleobject")
            .expectedBucketOwner("111122223333")
            .build();
    Path path = Paths.get("example_file.txt");
    s3Client.putObject(request, path);
}
```

Example

Exemplo: copiar um objeto

O exemplo a seguir copia o objeto `object1` do bucket do S3 *amzn-s3-demo-bucket1* para o bucket do S3 *amzn-s3-demo-bucket2*. Ele usa a condição de proprietário do bucket para garantir que os buckets sejam de propriedade das contas esperadas de acordo com a tabela a seguir.

Bucket	Proprietário esperado
amzn-s3-demo-bucket1	111122223333
amzn-s3-demo-bucket2	444455556666

AWS CLI

```
aws s3api copy-object --copy-source amzn-s3-demo-bucket1/object1 \
                            --bucket amzn-s3-demo-bucket2 --key object1copy \
                            --expected-source-bucket-owner 111122223333 --expected-
bucket-owner 444455556666
```

AWS SDK for Java 2.x

```
public void copyObjectExample() {
        S3Client s3Client = S3Client.create();
        CopyObjectRequest request = CopyObjectRequest.builder()
                .copySource("amzn-s3-demo-bucket1/object1")
                .destinationBucket("amzn-s3-demo-bucket2")
                .destinationKey("object1copy")
                .expectedSourceBucketOwner("111122223333")
                .expectedBucketOwner("444455556666")
                .build();
        s3Client.copyObject(request);
    }
```

Example

Exemplo: recuperar uma política de bucket

O exemplo a seguir recupera a política de acesso para o bucket do S3 *amzn-s3-demo-bucket1* usando a condição de proprietário do bucket para garantir que *amzn-s3-demo-bucket1* seja de propriedade da Conta da AWS 111122223333.

AWS CLI

```
aws s3api get-bucket-policy --bucket amzn-s3-demo-bucket1 --expected-bucket-
owner 111122223333
```

AWS SDK for Java 2.x

```
public void getBucketPolicyExample() {
    S3Client s3Client = S3Client.create();
    GetBucketPolicyRequest request = GetBucketPolicyRequest.builder()
            .bucket("amzn-s3-demo-bucket1")
            .expectedBucketOwner("111122223333")
            .build();
    try {
        GetBucketPolicyResponse response = s3Client.getBucketPolicy(request);
    }
    catch (S3Exception e) {
        // The call was transmitted successfully, but Amazon S3 couldn't process
        // it, so it returned an error response.
        e.printStackTrace();
    }
}
```

Restrições e limitações

A condição de proprietário do bucket do Amazon S3 tem as seguintes restrições e limitações:

- O valor do parâmetro de condição do proprietário do bucket deve ser um ID de Conta da AWS (valor numérico de 12 dígitos). Não há compatibilidade com os principais de serviço.
- A condição do proprietário do bucket não está disponível para CreateBucket, ListBuckets ou qualquer uma das operações incluídas no AWS S3 Control. O Amazon S3 ignora todos os parâmetros de condição do proprietário do bucket incluídos nas solicitações para essas operações.
- A condição do proprietário do bucket verifica apenas se a conta especificada no parâmetro de verificação é proprietária do bucket. A condição do proprietário do bucket não verifica a configuração do bucket. Também não garante que a configuração do bucket atenda a quaisquer condições específicas ou corresponda a qualquer estado passado.

Controlar a propriedade de objetos e desabilitar ACLs para seu bucket

A Propriedade de objeto do S3 é uma configuração no nível do bucket do Amazon S3 que você pode usar para controlar a propriedade de objetos carregados no bucket e desabilitar ou habilitar as listas de controle de acesso (ACLs). Por padrão, a Propriedade de objeto está definida com a configuração Imposto pelo proprietário do bucket e todas as ACLs estão desabilitadas. Quando as ACLs são desabilitadas, o proprietário do bucket possui todos os objetos do bucket e gerencia o acesso aos dados usando políticas de gerenciamento de acesso.

A maioria dos casos de uso modernos no Amazon S3 não requer mais o uso de ACLs e, portanto, recomendamos manter as ACLs desabilitadas exceto em circunstâncias incomuns em que seja necessário controlar o acesso para cada objeto individualmente. Com as ACLs desativadas, é possível usar políticas para controlar mais facilmente o acesso a cada objeto no bucket, independentemente de quem carregou os objetos no bucket.

Há três configurações em Object Ownership que podem ser usadas para controlar a propriedade de objetos carregados no bucket e para desabilitar ou habilitar ACLs:

ACLs desabilitadas

- Imposto pelo proprietário do bucket (padrão): as ACLs são desabilitadas e o proprietário do bucket automaticamente tem a propriedade e o controle total sobre todos os objetos do bucket. As ACLs não afetam mais as permissões nos dados no bucket do S3. O bucket usa políticas para definir o controle de acesso.

ACLs habilitadas

- Bucket owner preferred (Preferencial do proprietário do bucket): o proprietário do bucket tem a propriedade e o controle total sobre novos objetos que outras contas gravam no bucket com a ACL `bucket-owner-full-control` pré-configurada.
- Object writer (Gravador de objetos): a Conta da AWS que carrega um objeto é a proprietária do objeto, tem controle total sobre ele e pode conceder acesso a outros usuários por meio de ACLs.

Na maioria dos casos de uso modernos do S3, recomendamos manter as ACLs desabilitadas escolhendo a configuração imposta pelo proprietário do bucket e usar sua política de bucket para compartilhar dados com usuários fora da conta, conforme necessário. Essa abordagem simplifica

o gerenciamento de permissões. É possível desabilitar as ACLs em buckets recém-criados e já existentes. Para buckets recém-criados, as ACLs são desabilitadas por padrão. No caso de um bucket existente que já contenha objetos, depois que você desabilitar ACLs, as ACLs de objeto e bucket não farão mais parte de uma avaliação de acesso, e o acesso será concedido ou negado com base em políticas. Para buckets existentes, você pode habilitar novamente as ACLs a qualquer momento após desabilitá-las, e suas ACLs de objeto e bucket preexistentes serão restauradas.

Antes de desabilitar as ACLs, recomendamos revisar sua política de bucket para garantir que ela abranja todas as maneiras pelas quais você pretende conceder acesso ao bucket fora da conta. Depois que você desabilitar as ACLs, o bucket aceitará somente solicitações PUT que não especificam uma ACL ou solicitações PUT com ACLs de controle total do proprietário do bucket, como a ACL predefinida `bucket-owner-full-control` ou formas equivalentes dessa ACL expressas em XML. Aplicações existentes compatíveis com ACLs de controle total do proprietário do bucket não são afetadas. Solicitações PUT que contêm outras ACLs (por exemplo, concessões personalizadas para determinadas Contas da AWS) falham e retornam um erro `400` com o código de erro `AccessControlListNotSupported`.

Em contrapartida, um bucket com a configuração preferencial do proprietário do bucket continua aceitando e respeitando as ACLs de bucket e objeto. Com essa configuração, novos objetos que são escritos com a ACL `bucket-owner-full-control` pré-configurada são automaticamente de propriedade do proprietário do bucket, e não do gravador de objeto. Todos os outros comportamentos da ACL permanecem em vigor. Para exigir que todas as operações PUT do Amazon S3 incluam a ACL `bucket-owner-full-control` pré-configurada, adicione uma política de bucket que permita somente o carregamento de objetos que usam essa ACL.

Para ver quais configurações da Propriedade de Objeto são aplicadas aos seus buckets, você pode usar as métricas da Lente de Armazenamento do Amazon S3. A Lente de Armazenamento do S3 é um recurso de análise de armazenamento em nuvem que você pode usar para obter visibilidade em toda a organização sobre o uso e a atividade do armazenamento de objetos. Para obter mais informações, consulte Como usar a Lente de Armazenamento do S3 para encontrar configurações da Propriedade de Objeto.

> **Note**
>
> Para obter mais informações sobre o uso da classe de armazenamento Amazon S3 Express One Zone com buckets de diretório, consulte S3 Express One Zone e Trabalhar com buckets de diretório.

Configurações do Object Ownership

Esta tabela mostra como cada configuração do Object Ownership afeta ACLs, objetos, propriedade de objetos e carregamentos de objetos.

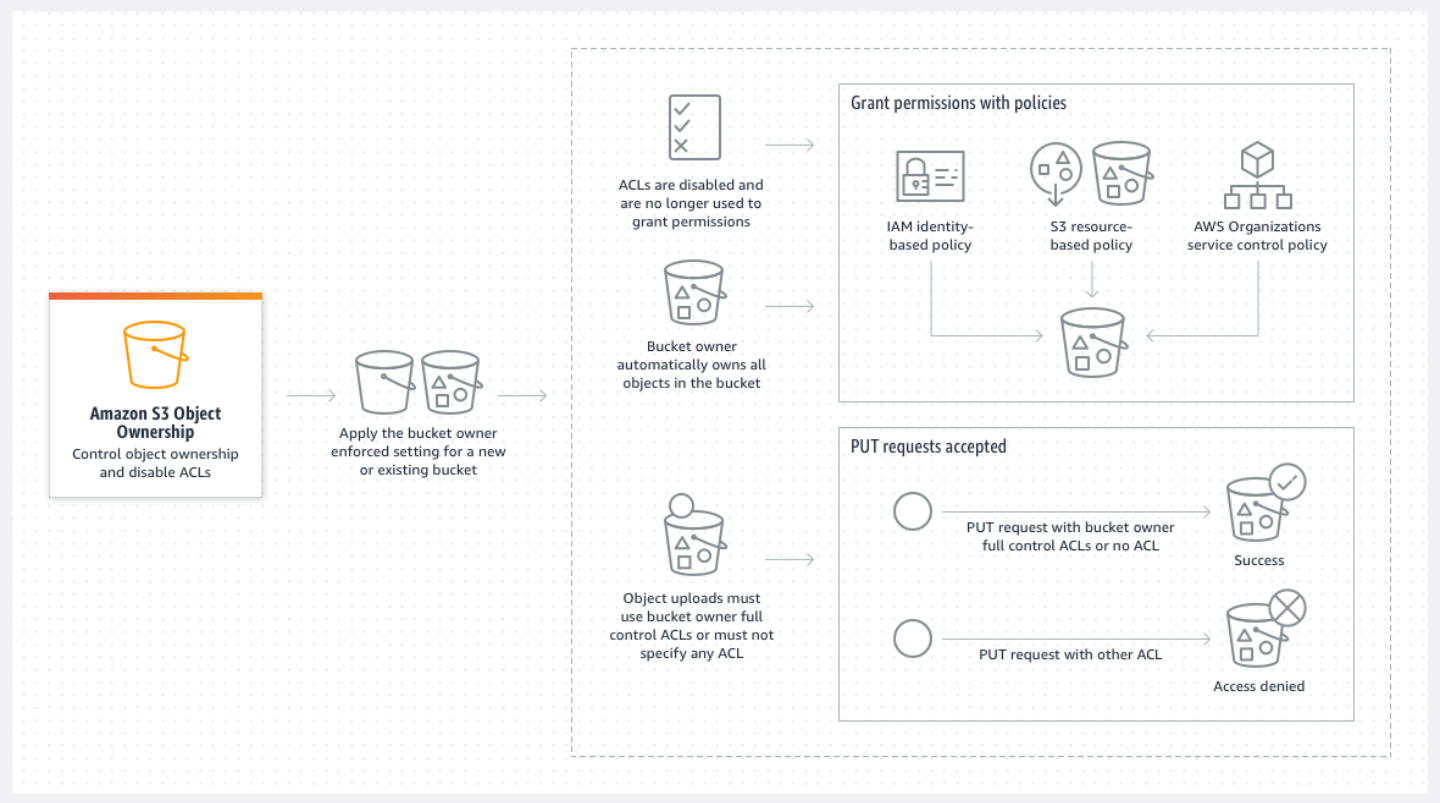
Configuração	Aplica-se a	Efeito na propriedade de objetos	Efeito nas ACLs	Carregamentos aceitos
Imposto pelo proprietário do bucket (padrão)	Objetos novos e existentes	O proprietário do bucket possui todos os objetos.	As ACLs estão desabilitadas e não afetam mais as permissões de acesso ao bucket. As solicitações para definir ou atualizar ACLs falham. Porém, há suporte para solicitações de leitura de ACLs. O proprietário do bucket tem total propriedade e controle. O gravador de objetos não tem mais total propriedade e controle.	Carregamentos com ACLs de controle total do proprietário do bucket ou carregamentos que não especificam uma ACL
Preferencial do proprietário do bucket	Novos objetos	Se um carregamento de objeto incluir a	As ACLs podem ser atualizadas e podem conceder permissões.	Todos os carregamentos

Configuração	Aplica-se a	Efeito na propriedade de objetos	Efeito nas ACLs	Carregamentos aceitos
		ACL `bucket-owner-full-control` pré-configurada, o proprietário do bucket terá o objeto. Os objetos carregados com outras ACLs são de propriedade da conta de gravação.	Se um carregamento de objeto incluir a ACL `bucket-owner-full-control` pré-configurada, o proprietário do bucket terá acesso de controle total, e o gravador de objetos não terá mais acesso de controle total.	
Autor do objeto	Novos objetos	O gravador de objetos é o proprietário do objeto.	As ACLs podem ser atualizadas e podem conceder permissões. O gravador de objetos tem total acesso de controle.	Todos os carregamentos

Alterações introduzidas ao desabilitar ACLs

Quando a configuração Imposto pelo proprietário do bucket para a Propriedade de objeto é utilizada, as ACLs são desabilitadas e você automaticamente se torna o proprietário e assume controle total sobre todos os objetos do bucket sem realizar nenhuma outra ação. A configuração Imposto pelo proprietário do bucket é a configuração padrão para todos os buckets recém-criados. Ao adotar a configuração Imposto pelo proprietário do bucket, você verá três alterações:

- Todas as ACLs de bucket e as ACLs de objeto estão desabilitadas, dando a você acesso total, como o proprietário do bucket. Ao executar uma solicitação de ACL de leitura em seu bucket ou objeto, você verá que o acesso total é dado somente ao proprietário do bucket.
- Você, como proprietário do bucket, automaticamente tem a propriedade e o controle total sobre todos os objetos de seu bucket.
- As ACLs não afetam mais as permissões de acesso ao bucket. Como resultado, o controle de acesso aos seus dados é baseado em políticas, como políticas baseadas em identidade do AWS Identity and Access Management (IAM), políticas de bucket do Amazon S3, políticas de endpoint da VPC e políticas de controle de serviços (SCPs) ou políticas de controle de recursos (RCPs) do Organizations.



Se você usar o versionamento do S3, o proprietário do bucket terá propriedade e controle total sobre todas as versões de objeto do bucket. Adotar a configuração Imposto pelo proprietário do bucket não adiciona uma nova versão de um objeto.

Será possível carregar novos objetos no bucket somente se eles usarem ACLs de controle total do proprietário do bucket ou não especificarem uma ACL. Os carregamentos de objetos falharão se especificarem qualquer outra ACL. Para obter mais informações, consulte Solução de problemas.

Como a operação `PutObject` do exemplo a seguir usando a AWS Command Line Interface (AWS CLI) contém a ACL `bucket-owner-full-control` pré-configurada, o objeto pode ser carregado em um bucket com ACLs desabilitadas.

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key key-name --body path-to-file --
acl bucket-owner-full-control
```

Como a operação `PutObject` não especifica uma ACL, ela também funciona em um bucket com ACLs desabilitadas.

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key key-name --body path-to-file
```

> **Note**
>
> Se outras Contas da AWS precisarem de acesso a objetos após o carregamento, será necessário conceder outras permissões a essas contas por meio de políticas de bucket. Para obter mais informações, consulte Demonstrações que usam políticas para gerenciar o acesso a recursos do Amazon S3.

Habilitar ACLs novamente

É possível habilitar novamente as ACLs alterando a configuração Imposto pelo proprietário do bucket para outra configuração de Propriedade de objeto a qualquer momento. Se você usou ACLs de objeto para gerenciamento de permissões antes de adotar a configuração Imposto pelo proprietário do bucket e não migrou essas permissões de ACL de objeto para a política de bucket, essas permissões serão restauradas quando as ACLs forem habilitadas novamente. Além disso, os objetos gravados no bucket enquanto a configuração Imposto pelo proprietário do bucket foi usada ainda pertencem ao proprietário do bucket.

Por exemplo, ao mudar da configuração Imposto pelo proprietário do bucket para a configuração Autor do objeto, você, como proprietário do bucket, não terá mais propriedade e controle total sobre objetos que anteriormente pertenciam a outras Contas da AWS. Em vez disso, as contas de carregamento voltam a ser proprietárias desses objetos. Objetos pertencentes a outras contas usam ACLs para permissões. Portanto, você não pode usar políticas para conceder permissões a esses objetos. No entanto, como proprietário do bucket, você ainda possui os objetos que foram gravados no bucket enquanto a configuração Imposto pelo proprietário do bucket foi usada. Esses objetos não pertencem ao gravador de objetos, mesmo que você habilite as ACLs novamente.

Para obter instruções sobre como habilitar e gerenciar ACLs usando o AWS Management Console, a AWS Command Line Interface (CLI), a API REST ou AWS SDKs, consulte Configurar ACLs.

Pré-requisitos para desabilitar ACLs

Antes de desabilitar as ACLs de um bucket existente, cumpra os pré-requisitos a seguir.

- Revise as ACLs de bucket e de objeto e migre permissões de ACLs
- Identificar as solicitações que exigiram uma ACL para autorização
- Revisar e atualizar políticas de bucket que usam chaves de condição relacionadas à ACL

Permissões do Object Ownership

Para aplicar, atualizar ou excluir uma configuração do Object Ownership de um bucket, é necessária a permissão `s3:PutBucketOwnershipControls`. Para retornar a configuração do Object Ownership para um bucket, é necessário ter a permissão `s3:GetBucketOwnershipControls`. Para obter mais informações, consulte Configurar Object Ownership ao criar um bucket e Visualizar a configuração do Object Ownership de um bucket do Amazon S3.

Desabilitar ACLs para todos os novos buckets

Por padrão, todos os novos buckets são criados usando a configuração Imposto pelo proprietário do bucket e as ACLs são desabilitadas. Recomendamos manter as ACLs desabilitadas. Como regra geral, recomendamos o uso de políticas baseadas em recursos do S3 (políticas de bucket e políticas de ponto de acesso) ou políticas do IAM para controle de acesso, em vez de ACLs. As políticas são uma opção de controle de acesso simplificada e mais flexível. Com políticas de bucket e políticas de ponto de acesso, é possível definir regras que se aplicam amplamente a todas as solicitações para seus recursos do Amazon S3.

Replicação e Object Ownership

Quando você usa a replicação do S3 e os buckets de origem e destino pertencem a diferentes Contas da AWS, é possível desabilitar ACLs (com a configuração Imposto pelo proprietário do bucket em Propriedade de objeto) para alterar a propriedade da réplica para a Conta da AWS que possui o bucket de destino. Essa configuração imita o comportamento de substituição do proprietário existente sem a necessidade da permissão `s3:ObjectOwnerOverrideToBucketOwner`. Todos os objetos

que são replicados para o bucket de destino com a configuração Imposto pelo proprietário do bucket pertencem ao proprietário do bucket de destino. Para obter mais informações sobre a opção de substituição do proprietário para configurações de replicação, consulte Alterar o proprietário da réplica.

Configurar propriedade de objeto

É possível aplicar uma configuração de Propriedade de objeto usando o console do Amazon S3, a AWS CLI, AWS SDKs, a API REST do Amazon S3 ou o AWS CloudFormation. A seguinte API REST e comandos da AWS CLI são compatíveis com o Object Ownership:

API REST	AWS CLI	Descrição
PutBucketOwnershipControls	put-bucket-ownership-controls	Cria ou modifica a configuração do Object Ownership para um bucket do S3 existente.
CreateBucket	create-bucket	Cria um bucket usando o cabeçalho de solicitação `x-amz-object-ownership` para especificar a configuração do Object Ownership.
GetBucketOwnershipControls	get-bucket-ownership-controls	Recupera a configuração do Object Ownership de um bucket do Amazon S3.
DeleteBucketOwnershipControls	delete-bucket-ownership-controls	Exclui a configuração do Object Ownership de um bucket do Amazon S3.

Para obter mais informações sobre como aplicar e trabalhar com configurações de Object Ownership, consulte os tópicos a seguir.

Tópicos

- Pré-requisitos para desabilitar ACLs
- Configurar Object Ownership ao criar um bucket

- Configurar propriedade de objeto em um bucket existente
- Visualizar a configuração do Object Ownership de um bucket do Amazon S3
- Desabilitar ACLs de todos os novos buckets e aplicar Object Ownership
- Solução de problemas

Pré-requisitos para desabilitar ACLs

Uma lista de controle de acesso (ACL) do bucket no Amazon S3 é um mecanismo que permite definir permissões detalhadas para objetos individuais dentro de um bucket do S3, especificando quais grupos ou contas da AWS podem acessar e modificar esses objetos. A maioria dos casos de uso modernos no Amazon S3 não exige mais o uso de ACLs. Recomendamos que você use políticas de bucket e do AWS Identity and Access Management (IAM) para gerenciar o acesso e manter as ACLs desabilitadas, exceto em circunstâncias incomuns em que seja necessário controlar o acesso para cada objeto individualmente.

Se você tiver ACLs habilitadas no bucket, antes de desabilitá-las, atenda aos seguintes pré-requisitos:

Tópicos

- Revise as ACLs de bucket e de objeto e migre permissões de ACLs
- Identificar as solicitações que exigiram uma ACL para autorização
- Revisar e atualizar políticas de bucket que usam chaves de condição relacionadas à ACL
- Exemplo de casos de uso

Revise as ACLs de bucket e de objeto e migre permissões de ACLs

Quando você desabilita ACLs, as permissões concedidas por ACLs de bucket e de objeto não afetam mais o acesso. Antes de desabilitar as ACLs, revise suas ACLs de objeto e de bucket.

Cada uma das ACLs de objeto e de bucket existentes tem um equivalente em uma política do IAM. Os exemplos de política de bucket a seguir mostram como as permissões `READ` e `WRITE` para ACLs de objeto e de bucket são mapeadas para permissões do IAM. Para obter mais informações sobre como cada ACL é convertida em permissões do IAM, consulte Mapeamento das permissões da ACL e das permissões da política de acesso.

Antes de desabilitar as ACLs:

- Se a ACL do bucket conceder acesso fora da conta da AWS, será necessário migrar as permissões de ACL do bucket para a política do bucket.
- A seguir, redefina a ACL de bucket para a ACL privada padrão.
- Também recomendamos revisar as permissões de ACL no nível de objeto e migrá-las para a política de bucket.

Se as ACLs de bucket concederem permissões de leitura ou gravação a outras pessoas fora da conta, antes de desabilitar as ACLs, será necessário migrar essas permissões para a política de bucket. Depois de migrar essas permissões, você pode definir a Propriedade do objeto com a configuração Imposto pelo proprietário do bucket. Se você não migrar ACLs de bucket que concedem acesso de leitura ou gravação fora de sua conta, a solicitação para aplicar a configuração Imposto pelo proprietário do bucket falhará e retornará o código de erro InvalidBucketAclWithObjectOwnership.

Se a ACL de bucket conceder acesso fora de sua Conta da AWS, antes de desabilitar as ACLs, é ncessário migrar suas permissões de ACL de bucket para a política de bucket e redefinir a ACL de bucket para a ACL privada padrão. Se você não migrar e redefinir, a solicitação para adotar a configuração de imposto pelo proprietário do bucket para desabilitar ACLs falhará e retornará o código de erro InvalidBucketAclWithObjectOwnership. Também recomendamos revisar suas permissões de ACL de objeto e migrá-las para a política de bucket.

Para revisar e migrar permissões de ACL para políticas de bucket, consulte os tópicos a seguir.

Tópicos

- Exemplos de políticas de bucket
- Usar o console do S3 para revisar e migrar permissões de ACL
- Usar a AWS CLI para revisar e migrar permissões de ACL

Exemplos de políticas de bucket

Esses exemplos de políticas de bucket mostram como migrar permissões de ACL de bucket e de objeto `READ` e `WRITE` para uma Conta da AWS de terceiros para uma política de bucket. As ACLs `READ_ACP` e `WRITE_ACP` são menos relevantes para políticas porque concedem permissões relacionadas a ACLs (`s3:GetBucketAcl`, `s3:GetObjectAcl`, `s3:PutBucketAcl` e `s3:PutObjectAcl`).

Example – ACL **READ** para um bucket

Se o bucket tiver uma ACL READ que conceda permissão à Conta da AWS *111122223333* para listar o conteúdo do bucket, você poderá escrever uma política de bucket que conceda as permissões `s3:ListBucket`, `s3:ListBucketVersions` e `s3:ListBucketMultipartUploads` para o bucket.

```
{
  "Version": "2012-10-17",
  "Statement": [
   {
    "Sid": "Permission to list the objects in a bucket",
    "Effect": "Allow",
    "Principal": {
     "AWS": [

      "arn:aws:iam::111122223333:root"
     ]
    },
    "Action": [
     "s3:ListBucket",
     "s3:ListBucketVersions",
     "s3:ListBucketMultipartUploads"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket"
   }
  ]
 }
```

Example – ACLs **READ** para cada objeto de um bucket

Se cada objeto no bucket tiver uma ACL READ que conceda acesso à Conta da AWS *111122223333*, você poderá escrever uma política de bucket que conceda as permissões `s3:GetObject` e `s3:GetObjectVersion` a essa conta para cada objeto do bucket.

```
{
  "Version": "2012-10-17",
  "Statement": [
   {
    "Sid": "Read permission for every object in a bucket",
    "Effect": "Allow",
    "Principal": {
```

```
     "AWS": [
      "arn:aws:iam::111122223333:root"
     ]
    },
    "Action": [
     "s3:GetObject",
     "s3:GetObjectVersion"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
   }
  ]
 }
```

Esse elemento de recurso de exemplo concede acesso a um objeto específico.

```
"Resource": "arn:aws:s3:::amzn-s3-demo-bucket/OBJECT-KEY"
```

Example – ACL **`WRITE`** que concede permissões para gravar objetos em um bucket

Se o bucket tiver uma ACL `WRITE` que conceda permissão à Conta da AWS *111122223333* para gravar objetos no bucket, você poderá escrever uma política de bucket que conceda a permissão `s3:PutObject` para o bucket.

```
{
  "Version": "2012-10-17",
  "Statement": [
   {
    "Sid": "Permission to write objects to a bucket",
    "Effect": "Allow",
    "Principal": {
     "AWS": [
      "arn:aws:iam::111122223333:root"
     ]
    },
    "Action": [
     "s3:PutObject"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
   }
  ]
 }
```

Usar o console do S3 para revisar e migrar permissões de ACL

Como revisar as permissões de ACL de um bucket

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Na lista Buckets (Buckets), escolha o nome do bucket.
3. Escolha a aba Permissões.
4. Em Access control list (ACL) (Lista de controle de acesso [ACL]), revise suas permissões de ACL de bucket.

Como revisar as permissões de ACL de um objeto

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Na lista Buckets, escolha o nome do bucket que contém o objeto.
3. Na lista Objects (Objetos), escolha o nome do objeto.
4. Escolha a aba Permissões.
5. Em Access control list (ACL) (Lista de controle de acesso [ACL]), revise suas permissões de ACL de objeto.

Para migrar permissões de ACL e atualizar a ACL de bucket

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Na lista Buckets (Buckets), escolha o nome do bucket.
3. Na guia Permissions (Permissões), escolha Bucket policy (Política de bucket), Edit (Editar).
4. Na caixa Policy (Política), adicione ou atualize a política de bucket.

   Para obter exemplos de políticas de bucket, consulte Exemplos de políticas de bucket e Exemplo de casos de uso.
5. Escolha Salvar alterações.
6. Atualize sua ACL de bucket para remover concessões de ACL para outros grupos ou Contas da AWS.
7. Adote a configuração Imposto pelo proprietário do bucket em Propriedade de objeto.

Usar a AWS CLI para revisar e migrar permissões de ACL

1. Para retornar a ACL para o bucket, use o comando get-bucket-acl da AWS CLI:

```
aws s3api get-bucket-acl --bucket amzn-s3-demo-bucket
```

Por exemplo, essa ACL de bucket concede acesso `WRITE` e `READ` a uma conta de terceiros. Nessa ACL, a conta de terceiros é identificada pelo ID de usuário canônico. Para adotar a configuração Imposto pelo proprietário do bucket e desabilitar ACLs, é necessário migrar essas permissões à conta de terceiros para uma política de bucket.

```
{
  "Owner": {
   "DisplayName": "DOC-EXAMPLE-ACCOUNT-OWNER",
   "ID": "852b113e7a2f25102679df27bb0ae12b3f85be6BucketOwnerCanonicalUserID"
  },
  "Grants": [
   {
    "Grantee": {
     "DisplayName": "DOC-EXAMPLE-ACCOUNT-OWNER",
     "ID": "852b113e7a2f25102679df27bb0ae12b3f85be6BucketOwnerCanonicalUserID",
     "Type": "CanonicalUser"
    },
    "Permission": "FULL_CONTROL"
   },
   {
    "Grantee": {
     "DisplayName": "THIRD-PARTY-EXAMPLE-ACCOUNT",
     "ID":
"72806de9d1ae8b171cca9e2494a8d1335dfced4ThirdPartyAccountCanonicalUserID",
     "Type": "CanonicalUser"
    },
    "Permission": "READ"
   },
   {
    "Grantee": {
     "DisplayName": "THIRD-PARTY-EXAMPLE-ACCOUNT",
     "ID":
"72806de9d1ae8b171cca9e2494a8d1335dfced4ThirdPartyAccountCanonicalUserID",
     "Type": "CanonicalUser"
    },
    "Permission": "WRITE"
```

```
   }
  ]
 }
```

Para ver outros exemplos de ACL, consulte Exemplo de casos de uso.

2. Migre suas permissões de ACL de bucket para uma política de bucket:

   Este exemplo de política de bucket concede as permissões `s3:PutObject` e `s3:ListBucket` para uma conta de terceiros. Na política de bucket, a conta de terceiros é identificada pelo ID da Conta da AWS (*111122223333*).

```
aws s3api put-bucket-policy --bucket amzn-s3-demo-bucket --policy file://
policy.json

 policy.json:
 {
  "Version": "2012-10-17",
  "Statement": [
   {
    "Sid": "PolicyForCrossAccountAllowUpload",
    "Effect": "Allow",
    "Principal": {
     "AWS": [
      "arn:aws:iam::111122223333:root"
     ]
    },
    "Action": [
     "s3:PutObject",
     "s3:ListBucket"
    ],
    "Resource": [
     "arn:aws:s3:::amzn-s3-demo-bucket",
     "arn:aws:s3:::amzn-s3-demo-bucket/*"
   }
  ]
 }
```

   Para obter mais exemplos de políticas de bucket, consulte Exemplos de políticas de bucket e Exemplo de casos de uso.

3. Para retornar a ACL para um objeto específico, use o comando get-object-acl da AWS CLI.

```
aws s3api get-object-acl --bucket amzn-s3-demo-bucket --key EXAMPLE-OBJECT-KEY
```

4. Se necessário, migre as permissões de ACL de objeto para a política de bucket.

   Esse elemento de recurso de exemplo concede acesso a um objeto específico em uma política de bucket.

   ```
   "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/EXAMPLE-OBJECT-KEY"
   ```

5. Redefina a ACL de bucket para a ACL padrão.

   ```
   aws s3api put-bucket-acl --bucket amzn-s3-demo-bucket --acl private
   ```

6. Adote a configuração Imposto pelo proprietário do bucket em Propriedade de objeto.

Identificar as solicitações que exigiram uma ACL para autorização

Para identificar solicitações do Amazon S3 que exigiam ACLs para autorização, você pode usar o valor `aclRequired` nos logs de acesso do servidor do Amazon S3 ou do AWS CloudTrail. Se a solicitação exigiu uma ACL para autorização ou se você tem solicitações PUT que especificam uma ACL, a string é `Yes`. Se nenhuma ACL for necessária, ou se você estiver configurando uma ACL `bucket-owner-full-control` predefinida, ou se as solicitações forem permitidas pela política de bucket, a string de valor `aclRequired` será "`-`" nos logs de acesso ao servidor do Amazon S3 e estará ausente no CloudTrail. Para obter mais informações sobre valores `aclRequired` esperados, consulte Valores `aclRequired` para solicitações comuns do Amazon S3.

Se você tiver solicitações `PutBucketAcl` ou `PutObjectAcl` com cabeçalhos que concedam permissões baseadas em ACL, com exceção da ACL `bucket-owner-full-control` predefinida, será necessário remover esses cabeçalhos antes de poder desabilitar as ACLs. Caso contrário, as solicitações falharão.

Para todas as outras solicitações que exigiram uma ACL para autorização, migre essas permissões de ACL para políticas de bucket. Depois, remova todas as ACLs do bucket antes de habilitar a configuração imposta pelo proprietário do bucket.

> **Note**
>
> Não remova ACLs de objetos. Caso contrário, as aplicações que dependem de ACLs de objetos para obter permissões perderão o acesso.

Se você perceber que nenhuma solicitação exigiu uma ACL para autorização, será possível continuar desabilitando as ACLs. Para obter mais informações sobre como identificar solicitações, consulte Usar logs de acesso ao servidor do Amazon S3 para identificar solicitações e Identificar solicitações do Amazon S3 usando o CloudTrail.

Revisar e atualizar políticas de bucket que usam chaves de condição relacionadas à ACL

Depois de adotar a configuração Imposto pelo proprietário do bucket para desabilitar ACLs, será possível carregar novos objetos no bucket somente se a solicitação usar ACLs de controle total do proprietário do bucket ou não especificar uma ACL. Antes de desabilitar as ACLs, revise a política de bucket para chaves de condição relacionadas à ACL.

Se a política de bucket usar uma chave de condição relacionada à ACL para exigir a ACL `bucket-owner-full-control` pré-configurada (por exemplo, `s3:x-amz-acl`), não será necessário atualizar sua política de bucket. A política de bucket a seguir usa `s3:x-amz-acl` para exigir a ACL `bucket-owner-full-control` pré-configurada para solicitações `PutObject` do S3. Essa política ainda requer que o gravador de objetos especifique a ACL `bucket-owner-full-control` pré-configurada. No entanto, buckets com ACLs desabilitadas ainda aceitam essa ACL, então as solicitações continuam sendo bem-sucedidas sem necessidade de alterações no lado do cliente.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Only allow writes to my bucket with bucket owner full control",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::111122223333:user/ExampleUser"
                ]
            },
            "Action": [
```

```
                "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control"
                }
            }
        }
    ]
}
```

Porém, se a política de bucket usar uma chave de condição relacionada à ACL que requer uma ACL diferente, será necessário remover essa chave de condição. Este exemplo de política de bucket requer a ACL `public-read` pré-configurada para solicitações `PutObject` do S3 e devem ser atualizadas antes de desabilitar as ACLs.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Only allow writes to my bucket with public read access",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::111122223333:user/ExampleUser"                ]
            },
            "Action": [
                "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "public-read"
                }
            }
        }
    ]
}
```

Exemplo de casos de uso

Os exemplos a seguir mostram como migrar permissões de ACL para políticas de bucket para casos de uso específicos.

Tópicos

- Conceder acesso ao grupo de entrega de logs do S3 para registro em log de acesso ao servidor
- Conceder acesso público de leitura aos objetos do bucket
- Conceder ao Amazon ElastiCache (Redis OSS) acesso ao bucket do S3

Conceder acesso ao grupo de entrega de logs do S3 para registro em log de acesso ao servidor

Para adotar a configuração Imposto pelo proprietário do bucket a fim de desabilitar ACLs para um bucket de destino de logs de acesso ao servidor (também conhecido como bucket-alvo), é necessário migrar permissões de ACL de bucket para o grupo de entrega de logs do S3 para a entidade principal de serviço do registro em log (`logging.s3.amazonaws.com`) em uma política de bucket. Para obter mais informações sobre permissões de entrega de logs, consulte Permissões para entrega de logs.

Essa ACL de bucket concede acesso `WRITE` e `READ_ACP` ao grupo de entrega de logs do S3:

```
{
    "Owner": {
        "DisplayName": "DOC-EXAMPLE-ACCOUNT-OWNER",
        "ID": "852b113e7a2f25102679df27bb0ae12b3f85be6BucketOwnerCanonicalUserID"
    },
    "Grants": [
        {
            "Grantee": {
                "Type": "CanonicalUser",
                "DisplayName": "DOC-EXAMPLE-ACCOUNT-OWNER",
                "ID":
 "852b113e7a2f25102679df27bb0ae12b3f85be6BucketOwnerCanonicalUserID"
            },
            "Permission": "FULL_CONTROL"
        },
        {
            "Grantee": {
                "Type": "Group",
                "URI": "http://acs.amazonaws.com/groups/s3/LogDelivery"
            },
```

```
            "Permission": "WRITE"
        },
        {
            "Grantee": {
                "Type": "Group",
                "URI": "http://acs.amazonaws.com/groups/s3/LogDelivery"
            },
            "Permission": "READ_ACP"
        }
    ]
}
```

Para migrar permissões de ACL de bucket para o grupo de entrega de log do S3 para a entidade principal do serviço de log em uma política de bucket

1. Adicione a política de bucket a seguir ao bucket de destino, substituindo os valores de exemplo.

```
aws s3api put-bucket-policy --bucket amzn-s3-demo-bucket --policy file://
policy.json

policy.json:      {
    {
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "S3ServerAccessLogsPolicy",
            "Effect": "Allow",
            "Principal": {
                "Service": "logging.s3.amazonaws.com"
            },
            "Action": [
                "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/EXAMPLE-LOGGING-PREFIX*",
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:s3:::SOURCE-BUCKET-NAME"
                },
                "StringEquals": {
                    "aws:SourceAccount": "SOURCE-AWS-ACCOUNT-ID"
                }
            }
        }
```

```
    ]
}
```

2. Redefina a ACL do bucket de destino para a ACL padrão.

```
aws s3api put-bucket-acl --bucket amzn-s3-demo-bucket --acl private
```

3. Aplique a configuração Imposto pelo proprietário do bucket para a Propriedade de Objetos no bucket de destino.

Conceder acesso público de leitura aos objetos do bucket

Se as ACLs de objeto concederem acesso público de leitura a todos os objetos no bucket, será possível migrar essas permissões de ACL para uma política de bucket.

Essa ACL de objeto concede acesso público de leitura a um objeto de um bucket:

```
{
    "Owner": {
        "DisplayName": "DOC-EXAMPLE-ACCOUNT-OWNER",
        "ID": "852b113e7a2f25102679df27bb0ae12b3f85be6BucketOwnerCanonicalUserID"
    },
    "Grants": [
        {
            "Grantee": {
                "DisplayName": "DOC-EXAMPLE-ACCOUNT-OWNER",
                "ID":
 "852b113e7a2f25102679df27bb0ae12b3f85be6BucketOwnerCanonicalUserID",
                "Type": "CanonicalUser"
            },
            "Permission": "FULL_CONTROL"
        },
        {
            "Grantee": {
                "Type": "Group",
                "URI": "http://acs.amazonaws.com/groups/global/AllUsers"
            },
            "Permission": "READ"
        }
    ]
}
```

Para migrar permissões públicas de ACL de leitura para uma política de bucket

1. Para conceder acesso público de leitura a todos os objetos do bucket, adicione a política de bucket a seguir, substituindo os valores de exemplo.

```
aws s3api put-bucket-policy --bucket amzn-s3-demo-bucket --policy
 file://policy.json

policy.json:
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PublicReadGetObject",
            "Effect": "Allow",
            "Principal": "*",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ]
        }
    ]
}
```

   Para conceder acesso público a um objeto específico de uma política de bucket, use o seguinte formato para o elemento `Resource`.

```
"Resource": "arn:aws:s3:::amzn-s3-demo-bucket/OBJECT-KEY"
```

   Para conceder acesso público a todos os objetos com um prefixo específico, use o seguinte formato para o elemento `Resource`.

```
"Resource": "arn:aws:s3:::amzn-s3-demo-bucket/PREFIX/*"
```

2. Adote a configuração Imposto pelo proprietário do bucket em Propriedade de objeto.

Conceder ao Amazon ElastiCache (Redis OSS) acesso ao bucket do S3

É possível exportar o backup do ElastiCache (Redis OSS) para um bucket do S3, o que concede a você acesso ao backup de fora do ElastiCache. Para exportar o backup para um bucket do S3, é necessário conceder permissões do ElastiCache para copiar um snapshot para o bucket. Se você concedeu permissões ao ElastiCache em uma ACL de bucket, será necessário migrar essas permissões para uma política de bucket antes de adotar a configuração Imposto pelo proprietário do bucket para desabilitar ACLs. Para obter mais informações, consulte Conceder acesso do ElastiCache ao bucket do Amazon S3 no Guia do usuário do Amazon ElastiCache.

O exemplo a seguir mostra as permissões de ACL de bucket que concedem permissões ao ElastiCache.

```
{
    "Owner": {
        "DisplayName": "DOC-EXAMPLE-ACCOUNT-OWNER",
        "ID": "852b113e7a2f25102679df27bb0ae12b3f85be6BucketOwnerCanonicalUserID"
    },
    "Grants": [
        {
            "Grantee": {
                "DisplayName": "DOC-EXAMPLE-ACCOUNT-OWNER",
                "ID":
 "852b113e7a2f25102679df27bb0ae12b3f85be6BucketOwnerCanonicalUserID",
                "Type": "CanonicalUser"
            },
            "Permission": "FULL_CONTROL"
        },
        {
            "Grantee": {
                "DisplayName": "aws-scs-s3-readonly",
                "ID":
 "540804c33a284a299d2547575ce1010f2312ef3da9b3a053c8bc45bf233e4353",
                "Type": "CanonicalUser"
            },
            "Permission": "READ"
        },
        {
            "Grantee": {
                "DisplayName": "aws-scs-s3-readonly",
                "ID":
 "540804c33a284a299d2547575ce1010f2312ef3da9b3a053c8bc45bf233e4353",
```

```
                "Type": "CanonicalUser"
            },
            "Permission": "WRITE"
        },
        {
            "Grantee": {
                "DisplayName": "aws-scs-s3-readonly",
                "ID":
 "540804c33a284a299d2547575ce1010f2312ef3da9b3a053c8bc45bf233e4353",
                "Type": "CanonicalUser"
            },
            "Permission": "READ_ACP"
        }
    ]
}
```

Como migrar permissões de ACL de bucket ao ElastiCache (Redis OSS) para uma política de bucket

1. Adicione a política de bucket a seguir ao bucket, substituindo os valores de exemplo.

```
aws s3api put-bucket-policy --bucket amzn-s3-demo-bucket --policy
 file://policy.json

policy.json:
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt15399483",
            "Effect": "Allow",
            "Principal": {
                "Service": "Region.elasticache-snapshot.amazonaws.com"
            },
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:GetBucketAcl",
                "s3:ListMultipartUploadParts",
                "s3:ListBucketMultipartUploads"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket",
```

```
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ]
        }
    ]
}
```

2. Redefina a ACL de bucket para a ACL padrão:

```
aws s3api put-bucket-acl --bucket amzn-s3-demo-bucket --acl private
```

3. Adote a configuração Imposto pelo proprietário do bucket em Propriedade de objeto.

Configurar Object Ownership ao criar um bucket

Ao criar um bucket, você pode configurar o S3 Object Ownership. Para definir o Object Ownership para um bucket existente, consulte Configurar propriedade de objeto em um bucket existente.

O S3 Object Ownership é uma configuração no nível do bucket do Amazon S3 que você pode usar para desabilitar as listas de controle de acesso (ACLs) e assumir a propriedade de cada objeto em seu bucket, simplificando o gerenciamento de acesso para dados armazenados no Amazon S3. Por padrão, a Propriedade de Objetos do S3 é definida como a configuração Imposto pelo proprietário do bucket e as ACLs são desabilitadas para novos buckets. Com as ACLs desabilitadas, o proprietário do bucket possui cada objeto no bucket e gerencia o acesso aos dados exclusivamente usando políticas de gerenciamento de acesso. Recomendamos manter as ACLs desabilitadas, exceto em circunstâncias incomuns em que seja necessário controlar o acesso para cada objeto individualmente.

Há três configurações em Object Ownership que podem ser usadas para controlar a propriedade de objetos carregados no bucket e para desabilitar ou habilitar ACLs:

ACLs desabilitadas

- Imposto pelo proprietário do bucket (padrão): as ACLs são desabilitadas e o proprietário do bucket automaticamente tem a propriedade e o controle total sobre todos os objetos do bucket. As ACLs não afetam mais as permissões nos dados no bucket do S3. O bucket usa políticas para definir o controle de acesso.

ACLs habilitadas

- Bucket owner preferred (Preferencial do proprietário do bucket): o proprietário do bucket tem a propriedade e o controle total sobre novos objetos que outras contas gravam no bucket com a ACL `bucket-owner-full-control` pré-configurada.
- Object writer (Gravador de objetos): a Conta da AWS que carrega um objeto é a proprietária do objeto, tem controle total sobre ele e pode conceder acesso a outros usuários por meio de ACLs.

Permissões: para aplicar a configuração Bucket owner enforced (Imposto pelo proprietário do bucket) ou Bucket owner preferred (Proprietário do bucket preferido), é necessário ter as seguintes permissões: `s3:CreateBucket` e `s3:PutBucketOwnershipControls`. Nenhuma permissão adicional é necessária ao criar um bucket com a configuração Object writer (Autor do objeto). Consulte mais informações sobre as permissões do Amazon S3 em Actions, resources, and condition keys for Amazon S3 na Referência de autorização do serviço.

Para ter mais informações sobre as permissões referentes a operações de API do S3 de acordo com os tipos de recurso do S3, consulte Permissões obrigatórias para operações de API do Amazon S3.

> **Important**
>
> A maioria dos casos de uso modernos no Amazon S3 não requer mais o uso de ACLs, e recomendamos desabilitar as ACLs, exceto em circunstâncias incomuns em que seja necessário controlar o acesso para cada objeto individualmente. Com Object Ownership, é possível desabilitar ACLs e confiar em políticas para controle de acesso. Ao desabilitar ACLs, você pode facilmente manter um bucket com objetos carregados por diferentes contas da AWS. Como proprietário do bucket, você possui todos os objetos do bucket e pode gerenciar o acesso a eles usando políticas.

Usar o console do S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Na barra de navegação na parte superior da página, escolha o nome da Região da AWS exibida no momento. Em seguida, escolha a região na qual você deseja criar um bucket.

> **Note**
>
> - Depois de criar um bucket, você não pode mudar sua região.
> - Para reduzir a latência e os custos e atender aos requisitos regulatórios, selecione uma região perto de você. Os objetos armazenados em uma região nunca saem dessa região, a menos que você os transfira para outra região. Para obter uma lista de Regiões da AWS do Amazon S3, consulte Endpoints de AWS service (Serviço da AWS) no Referência geral da Amazon Web Services.

3. No painel de navegação à esquerda, escolha Buckets de uso geral.
4. Selecione Create bucket (Criar bucket). A página Create bucket (Criar bucket) é aberta.
5. Para Nome do bucket, insira um nome para o bucket.

   O nome do bucket deve:

   - Ser exclusivo em uma partição. Uma partição é um agrupamento de regiões. No momento, a AWS tem três partições: `aws` (regiões comerciais), `aws-cn` (regiões da China) e `aws-us-gov` (AWS GovCloud (US) Regions).
   - Ter entre 3 e 63 caracteres.
   - Consistir em apenas letras minúsculas, números, pontos (`.`) e hifens (`-`). Para obter a melhor compatibilidade, recomendamos evitar o uso de pontos (`.`) em nomes de bucket, exceto em buckets usados apenas para hospedagem de sites estáticos.
   - Inicie e termine com uma letra ou um número.
   - Para obter uma lista completa de regras de nomenclatura de buckets, consulte Regras de nomenclatura de buckets de uso geral.

   > **Important**
   >
   > - Depois de criado o bucket, você não pode mudar seu nome.
   > - Não inclua informações confidenciais no nome do bucket. O nome do bucket é visível nos URLs que apontam para os objetos no bucket.

6. (Opcional) Em Configuração geral, você pode optar por copiar as configurações de um bucket existente para seu novo bucket. Prossiga·para·a·próxima·etapa·se você não quiser copiar as configurações de um bucket existente.

   > **Note**
   >
   > Essa opção:
   >
   > - Não está disponível na AWS CLI, mas apenas no console do Amazon S3.
   > - Não copia a política de bucket existente para o novo bucket.

   Para copiar as configurações de um bucket existente, em Copiar configurações do bucket existente, selecione Escolher bucket. A janela Escolher bucket é aberta. Encontre o bucket com as configurações que você quer copiar e selecione Escolher bucket. A janela Escolher bucket é fechada e a janela Criar bucket é reaberta.

   Agora, em Copiar configurações do bucket existente, você vê o nome do bucket selecionado. As configurações do novo bucket agora correspondem às configurações do bucket que você selecionou. Se você quiser remover as configurações copiadas, escolha Restaurar padrões. Revise as configurações restantes do bucket na página Criar bucket. Se não quiser fazer nenhuma alteração, você poderá pular para a etapa final.

7. Em Object Ownership, para desabilitar ou habilitar ACLs e controlar a propriedade de objetos carregados em seu bucket, escolha uma das seguintes configurações:

   ACLs desabilitadas

   - Imposto pelo proprietário do bucket (padrão): as ACLs são desabilitadas e o proprietário do bucket automaticamente tem propriedade e controle total sobre todos os objetos do bucket de uso geral. As ACLs não afetam mais as permissões de acesso aos dados no bucket de uso geral do S3. O bucket usa políticas exclusivamente para definir o controle de acesso.

     Por padrão, as ACLs estão desabilitadas. A maioria dos casos de uso modernos no Amazon S3 não exige mais o uso de ACLs. Recomendamos manter as ACLs desabilitadas, exceto em circunstâncias incomuns em que seja necessário controlar o acesso para cada objeto individualmente. Para obter mais informações, consulte Controlar a propriedade de objetos e desabilitar ACLs para seu bucket.

ACLs habilitadas

- Bucket owner preferred (Preferencial do proprietário do bucket): o proprietário do bucket tem a propriedade e o controle total sobre novos objetos que outras contas gravam no bucket com a ACL `bucket-owner-full-control` pré-configurada.

  Se você aplicar a configuração Proprietário do bucket preferido para exigir que todos os uploads do Amazon S3 incluam a ACL `bucket-owner-full-control` pré-configurada, será possível adicionar uma política de bucket que só permita uploads de objetos que usem essa ACL.

- Object writer (Gravador de objetos): a Conta da AWS que carrega um objeto é a proprietária do objeto, tem controle total sobre ele e pode conceder acesso a outros usuários por meio de ACLs.

> **Note**
>
> A configuração padrão é Imposto pelo proprietário do Bucket. Para aplicar a configuração padrão e manter as ACLs desabilitadas, somente a permissão `s3:CreateBucket` é necessária. Para habilitar ACLs, é necessário ter a permissão `s3:PutBucketOwnershipControls`.

8. Em Configurações de bloqueio de acesso público para este bucket, selecione as configurações de bloqueio de acesso público que deseja aplicar ao bucket.

   Por padrão, todas as quatro configurações do Bloqueio de Acesso Público são habilitadas. Recomendamos que você mantenha todas as configurações habilitadas, a menos que precise desativar uma ou mais delas para seu caso de uso específico. Para obter mais informações sobre como bloquear o acesso público, consulte Bloquear o acesso público ao armazenamento do Amazon S3.

   > **Note**
   >
   > Para habilitar todas as configurações do Bloqueio de Acesso Público, somente a permissão `s3:CreateBucket` é necessária. Para desabilitar qualquer

configuração do Bloqueio de Acesso Público, é necessário ter a permissão `s3:PutBucketPublicAccessBlock`.

9. (Opcional) Por padrão, Versionamento de bucket está desabilitado. Versionamento é um meio de manter diversas variantes de um objeto no mesmo bucket. O versionamento pode ser usado para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do . Com o versionamento, você pode se recuperar mais facilmente de ações não intencionais do usuário e de falhas da aplicação. Para obter mais informações sobre versionamento, consulte Reter várias versões de objetos com o Versionamento do S3.

   Para habilitar o versionamento no bucket, escolha Habilitar.

10. (Opcional) Em Tags (Etiquetas), você pode optar por adicionar etiquetas ao seu bucket. Com a alocação de custos da AWS, você pode usar tags de bucket para anotar o faturamento referente ao uso de um bucket. Uma tag é um par chave-valor que representa uma etiqueta que você atribui a um bucket. Para obter mais informações, consulte the section called “Usar tags de alocação de custos”.

    Para adicionar uma etiqueta, escolha Add Tag (Adicionar etiqueta) e insira uma chave e um valor para cada etiqueta.

11. Para configurar Criptografia padrão, em Tipo de criptografia, selecione uma das seguintes opções:

    - Criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3)
    - Criptografia no lado do servidor com chaves do AWS Key Management Service (SSE-KMS)
    - Criptografia de camada dupla do lado do servidor com chaves do AWS Key Management Service (AWS KMS) (DSSE-KMS)

    > **Important**
    >
    > Se você usar a opção SSE-KMS ou a DSSE-KMS em sua configuração de criptografia padrão, poderão ser cobradas cotas de solicitações por segundo (RPS) do AWS KMS. Para obter mais informações sobre as cotas do AWS KMS e como solicitar um aumento de cota, consulte Cotas no Guia do desenvolvedor do AWS Key Management Service.

Buckets e novos objetos são criptografados por meio da criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3) como o nível básico da configuração de criptografia. Para obter mais informações sobre criptografia padrão, consulte Definir o comportamento padrão da criptografia para os buckets do Amazon S3. Para ter mais informações sobre SSE-S3, consulte Usar a criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3).

Para obter mais informações sobre como usar a criptografia no lado do servidor para criptografar seus dados, consulte the section called “Criptografia de dados”.

12. Se você escolheu Criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3) ou Criptografia de camada dupla do lado do servidor com chaves do AWS Key Management Service (AWS KMS) (DSSE-KMS), faça o seguinte:

    a. Em Chave do AWS KMS, especifique sua chave do KMS de uma das seguintes maneiras:

    - Para escolher entre uma lista de chaves do KMS disponíveis, selecione Escolher entre suas AWS KMS keys e escolha sua chave do KMS na lista de chaves disponíveis.

      As chaves Chave gerenciada pela AWS (`aws/s3`) e as chaves gerenciadas pelo cliente são exibidas nessa lista. Para ter mais informações sobre chaves gerenciadas pelo cliente, consulte Chaves de clientes e chaves da AWS no Guia do desenvolvedor do AWS Key Management Service.
    - Para inserir o ARN da chave do KMS, escolha Inserir ARN da AWS KMS key e insira o ARN da chave do KMS no campo exibido.
    - Para criar uma chave gerenciada pelo cliente no console do AWS KMS, selecione Criar uma chave do KMS.

      Para ter mais informações sobre como criar uma AWS KMS key, consulte Criação de chaves no Guia do desenvolvedor do AWS Key Management Service.

> **Important**
>
> Você só pode usar chaves do KMS disponíveis na mesma Região da AWS que o bucket. O console do Amazon S3 lista somente as primeiras 100 chaves do KMS na mesma região que o bucket. Para usar uma chave do KMS que não esteja listada, você deve inserir o respectivo ARN. Se quiser usar uma chave do KMS

pertencente a outra conta, primeiro você deverá ter permissão para usar a chave e, depois, inserir o respectivo ARN. Para obter mais informações sobre permissões entre contas referentes a chaves do KMS, consulte Creating KMS keys that other accounts can use no Guia do desenvolvedor do AWS Key Management Service. Para obter mais informações sobre SSE-KMS, consulte Especificando criptografia no lado do servidor com o AWS KMS (SSE-KMS). Para ter mais informações sobre DSSE-KMS, consulte the section called “Criptografia de camada dupla do lado do servidor (DSSE-KMS)”.

Ao usar uma AWS KMS key para criptografia no lado do servidor no Amazon S3, você deve escolher uma chave de criptografia do KMS simétrica. O Amazon S3 só é compatível com chaves do KMS de criptografia simétrica, e não com chaves assimétricas do KMS. Para ter mais informações, consulte Identificar chaves do KMS simétricas e assimétricas no Guia do desenvolvedor do AWS Key Management Service.

b. Ao configurar o bucket para usar a criptografia padrão com SSE-KMS, você também pode usar as chaves de bucket do S3. As chaves de bucket do S3 diminuem o custo de criptografia reduzindo o tráfego de solicitações do Amazon S3 para o AWS KMS. Para obter mais informações, consulte Redução do custo do SSE-KMS com chaves de bucket do Amazon S3. As chaves de bucket do S3 não comportam DSSE-KMS.

   Por padrão, as chaves de bucket do S3 estão habilitadas no console do Amazon S3. Recomendamos deixá-las habilitadas para reduzir os custos. Para desabilitar as chaves de bucket do S3 do seu bucket, em Chave de bucket, escolha Desabilitar.

13. (Opcional) O Bloqueio de Objetos do S3 ajuda a proteger novos objetos contra exclusão ou substituição. Para obter mais informações, consulte Bloquear objetos com o Bloqueio de Objetos. Se você quiser habilitar o Bloqueio de Objetos do S3, faça o seguinte:

    a. Selecione Advanced settings (Configurações avançadas).

> **Important**
>
> A habilitação do Bloqueio de Objetos habilita automaticamente o versionamento do bucket. Depois de habilitar e criar o bucket com sucesso, você também deverá definir as configurações de retenção padrão e de retenção jurídica do Bloqueio de Objetos na guia Propriedades do bucket.

b. Se quiser habilitar o bloqueio de objetos, escolha Enable (Habilitar), leia o aviso que aparece e confirme-o.

> **Note**
>
> Para criar um bucket com o Bloqueio de Objetos habilitado, você deve ter as seguintes permissões: `s3:CreateBucket`, `s3:PutBucketVersioning` e `s3:PutBucketObjectLockConfiguration`.

14. Escolha Criar bucket.

Como usar o AWS CLI

Para definir Object Ownership ao criar um novo bucket, use o comando `create-bucket` da AWS CLI com o parâmetro `--object-ownership`.

Este exemplo aplica a configuração Imposto pelo proprietário do bucket para um novo bucket usando a AWS CLI:

```
aws s3api create-bucket --bucket  amzn-s3-demo-bucket --region us-east-1 --object-
ownership BucketOwnerEnforced
```

> **Important**
>
> Se você não definir a Propriedade de objeto ao criar um bucket usando a AWS CLI, a configuração padrão será `ObjectWriter` (ACLs habilitadas).

Usar o AWS SDK para Java

Este exemplo define a configuração Imposto pelo proprietário do bucket para um novo bucket usando o AWS SDK para Java:

```
    // Build the ObjectOwnership for CreateBucket
    CreateBucketRequest createBucketRequest = CreateBucketRequest.builder()
            .bucket(bucketName)
            .objectOwnership(ObjectOwnership.BucketOwnerEnforced)
            .build()
```

```
// Send the request to Amazon S3
s3client.createBucket(createBucketRequest);
```

Usar o AWS CloudFormation

Para usar o recurso `AWS::S3::Bucket` do AWS CloudFormation para definir a Propriedade de Objeto ao criar um bucket, consulte OwnershipControls em AWS::S3::Bucket no Guia do usuário do AWS CloudFormation.

Uso da API REST

Para adotar a configuração Imposto pelo proprietário do bucket para Propriedade de objeto do S3, use a operação de API `CreateBucket` com o cabeçalho da solicitação `x-amz-object-ownership` definido como `BucketOwnerEnforced`. Para obter informações e exemplos, consulte CreateBucket na Referência da API do Amazon Simple Storage Service.

Próximas etapas: depois de adotar as configurações Imposto pelo proprietário do bucket ou Proprietário do bucket preferido para a Propriedade de Objetos, você poderá seguir estas etapas:

- Bucket owner enforced (Aplicada pelo proprietário do bucket): exija que todos os novos buckets sejam criados com ACLs desabilitadas usando uma política do IAM ou do Organizations.
- Bucket owner preferred (Preferencial do proprietário do bucket): adicione uma política de bucket do S3 para exigir a ACL `bucket-owner-full-control` pré-configurada para todos os carregamentos de objetos para o bucket.

Configurar propriedade de objeto em um bucket existente

Você pode configurar S3 Object Ownership em um bucket do S3 existente. Para aplicar o Object Ownership ao criar um bucket, consulte Configurar Object Ownership ao criar um bucket.

O S3 Object Ownership é uma configuração no nível do bucket do Amazon S3 que você pode usar para desabilitar as listas de controle de acesso (ACLs) e assumir a propriedade de cada objeto em seu bucket, simplificando o gerenciamento de acesso para dados armazenados no Amazon S3. Por padrão, a Propriedade de Objetos do S3 é definida como a configuração Imposto pelo proprietário do bucket e as ACLs são desabilitadas para novos buckets. Com as ACLs desabilitadas, o proprietário do bucket possui cada objeto no bucket e gerencia o acesso aos dados exclusivamente

usando políticas de gerenciamento de acesso. Recomendamos manter as ACLs desabilitadas, exceto em circunstâncias incomuns em que seja necessário controlar o acesso para cada objeto individualmente.

Há três configurações em Object Ownership que podem ser usadas para controlar a propriedade de objetos carregados no bucket e para desabilitar ou habilitar ACLs:

ACLs desabilitadas

- Imposto pelo proprietário do bucket (padrão): as ACLs são desabilitadas e o proprietário do bucket automaticamente tem a propriedade e o controle total sobre todos os objetos do bucket. As ACLs não afetam mais as permissões nos dados no bucket do S3. O bucket usa políticas para definir o controle de acesso.

ACLs habilitadas

- Bucket owner preferred (Preferencial do proprietário do bucket): o proprietário do bucket tem a propriedade e o controle total sobre novos objetos que outras contas gravam no bucket com a ACL `bucket-owner-full-control` pré-configurada.
- Object writer (Gravador de objetos): a Conta da AWS que carrega um objeto é a proprietária do objeto, tem controle total sobre ele e pode conceder acesso a outros usuários por meio de ACLs.

Pré-requisitos: antes de adotar a configuração Imposto pelo proprietário do bucket para desabilitar ACLs, você deve migrar permissões de ACL de bucket para políticas de bucket e redefinir suas ACLs de bucket para a ACL privada padrão. Também recomendamos migrar permissões de ACL de objeto para políticas de bucket e editar políticas de bucket que exigem ACLs que não sejam ACLs de controle total do proprietário do bucket. Para obter mais informações, consulte Pré-requisitos para desabilitar ACLs.

Permissions (Permissões): para usar essa operação, é necessário ter a permissão `s3:PutBucketOwnershipControls`. Consulte mais informações sobre as permissões do Amazon S3 em Actions, resources, and condition keys for Amazon S3 na Referência de autorização do serviço.

Para ter mais informações sobre as permissões referentes a operações de API do S3 de acordo com os tipos de recurso do S3, consulte Permissões obrigatórias para operações de API do Amazon S3.

Usar o console do S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Na lista Buckets, escolha o nome do bucket para o qual você deseja aplicar uma configuração S3 Object Ownership.
3. Escolha a aba Permissões.
4. Em Object Ownership, escolha Edit (Editar).
5. Em Object Ownership, para desabilitar ou habilitar ACLs e controlar a propriedade de objetos carregados em seu bucket, escolha uma das seguintes configurações:

   ACLs desabilitadas

   - Bucket owner enforced (Aplicada pelo proprietário do bucket) (recomendado): as ACLs são desabilitadas e o proprietário do bucket automaticamente tem a propriedade e o controle total sobre todos os objetos do bucket. As ACLs não afetam mais as permissões nos dados no bucket do S3. O bucket usa políticas para definir o controle de acesso.

     Para exigir que todos os novos buckets sejam criados com ACLs desabilitadas usando IAM ou políticas do AWS Organizations, consulteDesabilitar ACLs para todos os novos buckets (aplicada pelo proprietário do bucket).

   ACLs habilitadas

   - Bucket owner preferred (Preferencial do proprietário do bucket): o proprietário do bucket tem a propriedade e o controle total sobre novos objetos que outras contas gravam no bucket com a ACL `bucket-owner-full-control` pré-configurada.

     Se você aplicar a configuração preferencial do proprietário do bucket para exigir que todos os carregamentos do Amazon S3 incluam a ACL `bucket-owner-full-control` pré-configurada, será possível adicionar uma política de bucket que só permita carregamentos de objetos que usam essa ACL.
   - Object writer (Gravador de objetos): a Conta da AWS que carrega um objeto é a proprietária do objeto, tem controle total sobre ele e pode conceder acesso a outros usuários por meio de ACLs.
6. Escolha Salvar.

Como usar o AWS CLI

Para aplicar uma configuração do Object Ownership a um bucket existente, use o comando `put-bucket-ownership-controls` com o parâmetro `--ownership-controls`. Os valores válidos de propriedade são `BucketOwnerEnforced`, `BucketOwnerPreferred` ou `ObjectWriter`.

Este exemplo aplica a configuração Imposto pelo proprietário do bucket para um bucket existente usando a AWS CLI:

```
aws s3api put-bucket-ownership-controls --bucket amzn-s3-demo-bucket --ownership-
controls="Rules=[{ObjectOwnership=BucketOwnerEnforced}]"
```

Para obter informações sobre `put-bucket-ownership-controls`, consulte put-bucket-ownership-controls no Guia do usuário do AWS Command Line Interface.

Usar o AWS SDK para Java

Este exemplo aplica a configuração `BucketOwnerEnforced` à Propriedade de objeto em um bucket existente usando o AWS SDK para Java:

```
        // Build the ObjectOwnership for BucketOwnerEnforced
        OwnershipControlsRule rule = OwnershipControlsRule.builder()
               .objectOwnership(ObjectOwnership.BucketOwnerEnforced)
               .build();

        OwnershipControls ownershipControls = OwnershipControls.builder()
                  .rules(rule)
                  .build()

         // Build the PutBucketOwnershipControlsRequest
         PutBucketOwnershipControlsRequest putBucketOwnershipControlsRequest =
               PutBucketOwnershipControlsRequest.builder()
                       .bucket(BUCKET_NAME)
                       .ownershipControls(ownershipControls)
                       .build();

         // Send the request to Amazon S3
         s3client.putBucketOwnershipControls(putBucketOwnershipControlsRequest);
```

Usar o AWS CloudFormation

Para usar o AWS CloudFormation para aplicar uma configuração de Propriedade de Objeto a um bucket existente, consulte AWS::S3::Bucket OwnershipControls no Guia do usuário do AWS CloudFormation.

Uso da API REST

Para usar a API REST para aplicar uma configuração do Object Ownership a um bucket do S3 existente, use `PutBucketOwnershipControls`. Para obter mais informações, consulte PutBucketOwnershipControls na Referência da API do Amazon Simple Storage Service.

Próximas etapas: depois de adotar as configurações Imposto pelo proprietário do bucket ou Proprietário do bucket preferido para a Propriedade de Objetos, você poderá seguir estas etapas:

- Bucket owner enforced (Aplicada pelo proprietário do bucket): exija que todos os novos buckets sejam criados com ACLs desabilitadas usando uma política do IAM ou do Organizations.
- Bucket owner preferred (Preferencial do proprietário do bucket): adicione uma política de bucket do S3 para exigir a ACL `bucket-owner-full-control` pré-configurada para todos os carregamentos de objetos para o bucket.

Visualizar a configuração do Object Ownership de um bucket do Amazon S3

O S3 Object Ownership é uma configuração no nível do bucket do Amazon S3 que você pode usar para desabilitar as listas de controle de acesso (ACLs) e assumir a propriedade de cada objeto em seu bucket, simplificando o gerenciamento de acesso para dados armazenados no Amazon S3. Por padrão, a Propriedade de Objetos do S3 é definida como a configuração Imposto pelo proprietário do bucket e as ACLs são desabilitadas para novos buckets. Com as ACLs desabilitadas, o proprietário do bucket possui cada objeto no bucket e gerencia o acesso aos dados exclusivamente usando políticas de gerenciamento de acesso. Recomendamos manter as ACLs desabilitadas, exceto em circunstâncias incomuns em que seja necessário controlar o acesso para cada objeto individualmente.

Há três configurações em Object Ownership que podem ser usadas para controlar a propriedade de objetos carregados no bucket e para desabilitar ou habilitar ACLs:

ACLs desabilitadas

- Imposto pelo proprietário do bucket (padrão): as ACLs são desabilitadas e o proprietário do bucket automaticamente tem a propriedade e o controle total sobre todos os objetos do bucket. As ACLs não afetam mais as permissões nos dados no bucket do S3. O bucket usa políticas para definir o controle de acesso.

ACLs habilitadas

- Bucket owner preferred (Preferencial do proprietário do bucket): o proprietário do bucket tem a propriedade e o controle total sobre novos objetos que outras contas gravam no bucket com a ACL `bucket-owner-full-control` pré-configurada.
- Object writer (Gravador de objetos): a Conta da AWS que carrega um objeto é a proprietária do objeto, tem controle total sobre ele e pode conceder acesso a outros usuários por meio de ACLs.

É possível ver as configurações do S3 Object Ownership de um bucket do Amazon S3. Para definir o Object Ownership para um novo bucket, consulte Configurar Object Ownership ao criar um bucket. Para definir o Object Ownership para um bucket existente, consulte Configurar propriedade de objeto em um bucket existente.

Permissões (Permissões): para usar essa operação, é necessário ter a permissão `s3:GetBucketOwnershipControls`. Consulte mais informações sobre as permissões do Amazon S3 em Actions, resources, and condition keys for Amazon S3 na Referência de autorização do serviço.

Para ter mais informações sobre as permissões referentes a operações de API do S3 de acordo com os tipos de recurso do S3, consulte Permissões obrigatórias para operações de API do Amazon S3.

Usar o console do S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Na lista Buckets, escolha o nome do bucket para o qual você deseja aplicar uma configuração do Object Ownership.
3. Escolha a aba Permissões.
4. Em Object Ownership, você pode ver as configurações de Object Ownership do bucket.

Como usar o AWS CLI

Para recuperar a configuração da Propriedade de objeto do S3 para um bucket do S3, use o comando get-bucket-ownership-controls da AWS CLI.

```
aws s3api get-bucket-ownership-controls --bucket amzn-s3-demo-bucket
```

Uso da API REST

Para recuperar a configuração de Object Ownership para um bucket do S3, use a operação de API `GetBucketOwnershipControls`. Para obter mais informações, consulte GetBucketOwnershipControls.

Desabilitar ACLs de todos os novos buckets e aplicar Object Ownership

Recomendamos desabilitar ACLs nos buckets do Amazon S3. Faça isso aplicando a configuração Imposto pelo proprietário do bucket para Propriedade de objeto do S3. Quando você aplica essa configuração, as ACLs são desabilitadas, e você automaticamente tem a propriedade e o controle total sobre todos os objetos de seu bucket. Para exigir que todos os novos buckets sejam criados com ACLs desabilitadas usando políticas do AWS Identity and Access Management (IAM) ou políticas de controle de serviços (SCPs) do AWS Organizations, conforme descrito na próxima seção.

Para aplicar a propriedade do objeto a novos objetos sem desabilitar ACLs, aplique a configuração preferencial do proprietário do bucket. Quando você aplica essa configuração, é altamente recomendável atualizar a política de bucket para exigir a ACL `bucket-owner-full-control` pré-configurada para todas as solicitações PUT para o bucket. Atualize também os clientes para enviar a ACL `bucket-owner-full-control` pré-configurada de outras contas para o bucket.

Tópicos

- Desabilitar ACLs para todos os novos buckets (aplicada pelo proprietário do bucket)
- Exigir a ACL pré-configurada bucket-owner-full-control para operações PUT do Amazon S3 (preferencial do proprietário do bucket)

Desabilitar ACLs para todos os novos buckets (aplicada pelo proprietário do bucket)

O exemplo a seguir de política do IAM nega a permissão `s3:CreateBucket` para um usuário ou um perfil do IAM específico, a menos que a configuração Imposto pelo proprietário do bucket seja adotada em Propriedade de objeto. O par de chave-valor no bloco `Condition` especifica a

chave `s3:x-amz-object-ownership` e a configuração `BucketOwnerEnforced` como valor. Em outras palavras, o usuário do IAM pode criar buckets somente se definir a configuração Imposto pelo proprietário do bucket para Propriedade de objeto e desabilitar ACLs. Também é possível usar essa política como um SCP de limite para sua organização da AWS.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "RequireBucketOwnerFullControl",
            "Action": "s3:CreateBucket",
            "Effect": "Deny",
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "s3:x-amz-object-ownership": "BucketOwnerEnforced"
                }
            }
        }
    ]
}
```

Exigir a ACL pré-configurada bucket-owner-full-control para operações **PUT** do Amazon S3 (preferencial do proprietário do bucket)

Com a configuração preferencial do proprietário do bucket para Propriedade de objeto, como proprietário do bucket, você tem a propriedade e o controle total sobre novos objetos que outras contas gravam em seu bucket com a ACL `bucket-owner-full-control` pré-configurada. Porém, se outras contas gravarem objetos em seu bucket sem a ACL `bucket-owner-full-control` pré-configurada, o gravador de objetos manterá o acesso de controle total. Como proprietário do bucket, você pode implementar uma política de bucket que permita gravações somente se especificarem a ACL `bucket-owner-full-control` pré-configurada.

> **Note**
>
> Caso tenha ACLs desabilitadas com a configuração Imposto pelo proprietário do bucket, como proprietário do bucket, você automaticamente terá propriedade e controle total sobre todos os objetos do bucket. Não é necessário usar esta seção para atualizar sua política de bucket a fim de aplicar a propriedade do objeto para o proprietário do bucket.

A política de bucket a seguir especifica que a conta *111122223333* pode fazer upload de objetos *amzn-s3-demo-bucket* somente quando a ACL do objeto estiver definida como `bucket-owner-full-control`. Substitua *111122223333* por uma conta real e *amzn-s3-demo-bucket* pelo nome de seu bucket.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "Only allow writes to my bucket with bucket owner full control",
         "Effect": "Allow",
         "Principal": {
            "AWS": [
               "arn:aws:iam::111122223333:user/ExampleUser"
            ]
         },
         "Action": [
            "s3:PutObject"
         ],
         "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
         "Condition": {
            "StringEquals": {
               "s3:x-amz-acl": "bucket-owner-full-control"
            }
         }
      }
   ]
}
```

Veja a seguir um exemplo de operação de cópia que inclui a ACL pré-configurada `bucket-owner-full-control` usando a AWS Command Line Interface (AWS CLI).

```
aws s3 cp file.txt s3://amzn-s3-demo-bucket --acl bucket-owner-full-control
```

Depois que a política de bucket entrar em vigor, se o cliente não incluir a ACL pré-configurada `bucket-owner-full-control`, a operação falhará, e quem carregar receberá o seguinte erro:

An error occurred (AccessDenied) when calling the PutObject operation: Access Denied (Ocorreu um erro (AccessDenied) ao chamar a operação PutObject: acesso negado.

> **Note**
>
> Se os clientes precisarem de acesso a objetos após o upload, será necessário conceder permissões adicionais à conta de upload. Para obter informações sobre como conceder a contas acesso aos seus recursos, consulte Demonstrações que usam políticas para gerenciar o acesso a recursos do Amazon S3.

Solução de problemas

Ao adotar a configuração Imposto pelo proprietário do bucket para a Propriedade de Objetos do S3, as listas de controle de acesso (ACLs) serão desabilitadas e, como proprietário do bucket, você assumirá a propriedade de todos os objetos no bucket. As ACLs não afetam mais as permissões dos objetos do bucket. Você pode usar políticas para conceder permissões. Todas as solicitações PUT do S3 devem especificar a ACL predefinida `bucket-owner-full-control` ou não especificar uma ACL, senão essas solicitações falharão. Para obter mais informações, consulte Controlar a propriedade de objetos e desabilitar ACLs para seu bucket.

Se uma ACL inválida for especificada ou se as permissões de ACL de bucket concederem acesso fora de sua Conta da AWS, você poderá ver as respostas de erro a seguir.

AccessControlListNotSupported

Ao adotar a configuração Imposto pelo proprietário do bucket em Propriedade de objeto, as ACLs são desabilitadas. Solicitações para definir ACLs ou atualizar ACLs falham com um erro `400` e retornam o código de erro AccessControlListNotSupported. Ainda há suporte para solicitações de leitura de ACLs. As solicitações de leitura para ACLs sempre retornam uma resposta que mostra controle total para o proprietário do bucket. Nas operações PUT, é necessário especificar ACLs de controle total do proprietário do bucket ou não especificar uma ACL. Caso contrário, as operações PUT falharão.

O exemplo de comando `put-object` da AWS CLI a seguir inclui a ACL `public-read` predefinida.

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key object-key-name --body doc-example-body --acl public-read
```

Se o bucket usar a configuração Imposto pelo proprietário do bucket para desabilitar ACLs, essa operação falhará, e a pessoa que carregar receberá esta mensagem de erro:

An error occurred (AccessControlListNotSupported) when calling the PutObject operation: The bucket does not allow ACLs (Ocorreu um erro [AccessControlListNotSupported] ao chamar a operação PutObject: o bucket não permite ACLs)

InvalidBucketAclWithObjectOwnership

Para adotar a configuração Imposto pelo proprietário do bucket para desabilitar ACLs, a ACL do bucket deverá dar controle total somente ao proprietário do bucket. Sua ACL de bucket não pode dar acesso a uma Conta da AWS externa ou a qualquer outro grupo. Por exemplo, se a solicitação `CreateBucket` definir a configuração aplicada pelo proprietário do bucket e especificar uma ACL de bucket que fornece acesso a uma Conta da AWS externa, a solicitação apresentará o erro `400` e retornará o código de erro InvalidBucketAclWithObjectOwnership. Da mesma forma, se a solicitação `PutBucketOwnershipControls` definir a configuração aplicada pelo proprietário do bucket em um bucket que tem uma ACL de bucket que concede permissões a outros, a solicitação falhará.

Example : ACL de bucket existente concede acesso público de leitura

Por exemplo, se uma ACL de bucket existente conceder acesso público de leitura, não será possível adotar a configuração Imposto pelo proprietário do bucket para Propriedade de objeto enquanto essas permissões de ACL não forem migradas para uma política de bucket e sua ACL de bucket não for redefinida para a ACL privada padrão. Para obter mais informações, consulte Pré-requisitos para desabilitar ACLs.

Este exemplo de ACL de bucket concede acesso público de leitura:

```
{
    "Owner": {
        "ID": "852b113e7a2f25102679df27bb0ae12b3f85be6BucketOwnerCanonicalUserID"
    },
    "Grants": [
        {
            "Grantee": {
                "ID":
 "852b113e7a2f25102679df27bb0ae12b3f85be6BucketOwnerCanonicalUserID",
                "Type": "CanonicalUser"
            },
            "Permission": "FULL_CONTROL"
        },
        {
            "Grantee": {
```

```
                "Type": "Group",
                "URI": "http://acs.amazonaws.com/groups/global/AllUsers"
            },
            "Permission": "READ"
        }
    ]
}
```

O exemplo a seguir do comando `put-bucket-ownership-controls` da AWS CLI adota a configuração Imposto pelo proprietário do bucket para Propriedade de objeto:

```
aws s3api put-bucket-ownership-controls --bucket amzn-s3-demo-bucket --ownership-
controls Rules=[{ObjectOwnership=BucketOwnerEnforced}]
```

Como a ACL de bucket concede acesso público de leitura, a solicitação falha e retorna o seguinte código de erro:

An error occurred (InvalidBucketAclWithObjectOwnership) when calling the PutBucketOwnershipControls operation: Bucket cannot have ACLs set with ObjectOwnership's BucketOwnerEnforced setting (Ocorreu um erro [InvalidBucketAclWithObjectOwnership] ao chamar a operação PutBucketOwnershipControls: o bucket não pode ter ACLs definidas com a configuração BucketOwnerEnforced do ObjectOwnership

Segurança no Amazon S3

A segurança na nuvem da AWS é nossa maior prioridade. Como cliente da AWS, você se beneficiará de um data center e de uma arquitetura de rede criados para atender aos requisitos das empresas com as maiores exigências de segurança.

A segurança é uma responsabilidade compartilhada entre a AWS e você. O modelo de responsabilidade compartilhada descreve isto como segurança da nuvem e segurança na nuvem:

Segurança da nuvem

A AWS é responsável pela proteção da infraestrutura que executa serviços da AWS na Nuvem AWS. A AWS também fornece a você serviços que podem ser usados com segurança. A eficácia da nossa segurança é regularmente testada e verificada por auditores de terceiros como parte dos Programas de conformidade da AWS. Para saber mais sobre os programas de conformidade que se aplicam ao Amazon S3, consulte Serviços da AWS no escopo pelo programa de conformidade.

Segurança na nuvem

Sua responsabilidade é determinada pelo serviço da AWS que você usa. Também existe a responsabilidade por outros fatores, incluindo a confidencialidade de dados, os requisitos da organização e as leis e regulamentos aplicáveis. Para o Amazon S3, sua responsabilidade inclui as seguintes áreas:

- Gerenciar seus dados, incluindo propriedade de objetos e criptografia.
- Classificar seus ativos.
- Gerenciar o acesso a seus dados usando as funções do IAM e outras configurações de serviço para aplicar as permissões apropriadas.
- Habilitar controles de detecção, como AWS CloudTrail ou Amazon GuardDutypara o Amazon S3.

Esta documentação ajudará você a entender como aplicar o modelo de responsabilidade compartilhada ao usar o Amazon S3. Os tópicos a seguir mostram como configurar o Amazon S3 para atender aos seus objetivos de segurança e de conformidade. Você também aprenderá como usar outros produtos da AWS que podem ajudar a monitorar e proteger seus recursos do Amazon S3.

> **Note**
>
> Para obter mais informações sobre o uso da classe de armazenamento Amazon S3 Express One Zone com buckets de diretório, consulte S3 Express One Zone e Trabalhar com buckets de diretório.

Tópicos

- Práticas recomendadas de segurança para o Amazon S3
- Proteção de dados no Amazon S3
- Proteger dados com criptografia
- Privacidade do tráfego entre redes
- Validação de conformidade para o Amazon S3
- Resiliência no Amazon S3
- Segurança da infraestrutura no Amazon S3
- Análise de configuração e vulnerabilidade no Amazon S3
- Gerenciamento de acesso

Práticas recomendadas de segurança para o Amazon S3

O Amazon S3 fornece uma série de recursos de segurança a serem considerados no desenvolvimento e na implementação das suas próprias políticas de segurança. As melhores práticas a seguir são diretrizes gerais e não representam uma solução completa de segurança. Como essas práticas recomendadas podem não ser adequadas ou suficientes para o seu ambiente, trate-as como recomendações úteis em vez de requisitos.

Tópicos

- Práticas recomendadas de segurança para o Amazon S3
- Práticas recomendadas de auditoria e monitoramento do Amazon S3
- Monitorar a segurança dos dados com serviços de segurança gerenciados da AWS

Práticas recomendadas de segurança para o Amazon S3

As seguintes práticas recomendadas do Amazon S3 podem ajudar a evitar incidentes de segurança.

Desativar listas de controle de acesso (ACLs)

A Propriedade de objeto do S3 é uma configuração no nível do bucket do Amazon S3 que você pode usar para controlar a propriedade de objetos carregados no bucket e para desabilitar ou habilitar as ACLs. Por padrão, a Propriedade de objeto está definida com a configuração Imposto pelo proprietário do bucket e todas as ACLs estão desabilitadas. Quando as ACLs são desabilitadas, o proprietário do bucket possui todos os objetos do bucket e gerencia o acesso aos dados usando políticas de gerenciamento de acesso.

A maioria dos casos de uso no Amazon S3 não exige mais o uso de listas de controle de acesso (ACLs). Recomendamos desabilitar as ACLs, exceto em circunstâncias incomuns em que seja necessário controlar o acesso para cada objeto individualmente. Para desativar as ACLs e assumir a propriedade de cada objeto de seu bucket, aplique a configuração Imposto pelo proprietário do bucket para a Propriedade de objeto do S3. Ao desabilitar ACLs, você pode facilmente manter um bucket com objetos carregados por diferentes Contas da AWS.

Quando as ACLs são desabilitadas, o controle de acesso para os dados é baseado em políticas, como as seguintes:

- Políticas de usuário do AWS Identity and Access Management (IAM)
- Políticas de bucket do S3

- Políticas de endpoint de nuvem privada virtual (VPC)
- Políticas de controle de serviço (SCPs) do AWS Organizations
- Políticas de controle de recursos (RCPs) do AWS Organizations

A desativação das ACLs simplifica o gerenciamento e a auditoria de permissões. Por padrão, as ACLs estão desabilitadas para novos buckets. Também é possível desabilitar ACLs para buckets existentes. Se você tiver um bucket existente que já contenha objetos, depois de desabilitar ACLs, as ACLs de objeto e bucket não farão mais parte do processo de avaliação de acesso. Em vez disso, o acesso é concedido ou negado com base nas políticas.

Antes de desabilitar as ACLs, faça o seguinte:

- Revise sua política de bucket para garantir que ela abranja todas as maneiras pelas quais você pretende conceder acesso ao bucket fora da conta.
- Redefina a ACL do bucket para o padrão (controle total para o proprietário do bucket).

Ao desabilitar as ACLs, os seguintes comportamentos ocorrem:

- O bucket aceita somente solicitações PUT que não especificam uma ACL ou solicitações PUT com ACLs de controle total do proprietário do bucket. Essas ACLs incluem a ACL predefinida `bucket-owner-full-control` ou formas equivalentes dessa ACL que são expressas em XML.
- Aplicações existentes compatíveis com ACLs de controle total do proprietário do bucket não são afetadas.
- Solicitações PUT que contêm outras ACLs (por exemplo, concessões personalizadas para determinadas Contas da AWS) falham e retornam um código de status de HTTP de `400 (Bad Request)` com o código de erro `AccessControlListNotSupported`.

Para obter mais informações, consulte Controlar a propriedade de objetos e desabilitar ACLs para seu bucket.

Garantir que seus buckets do Amazon S3 utilizem as políticas corretas e não sejam acessados publicamente

A não ser que seja absolutamente necessário que alguém na internet possa ler ou gravar no seu bucket do S3, ele não deve ser público. Veja abaixo algumas etapas que você pode seguir para bloquear o acesso público:

- Use o Bloqueio de Acesso Público do S3. Com o Bloqueio de Acesso Público do S3, é possível configurar facilmente os controles centralizados impostos para limitar o acesso público aos recursos do Amazon S3. Esses controles centralizados são aplicados independentemente de como os recursos são criados. Para obter mais informações, consulte Bloquear o acesso público ao armazenamento do Amazon S3.
- Identifique as políticas de bucket do Amazon S3 que permitam uma identidade curinga, como `"Principal": "*"` (que efetivamente significa “qualquer pessoa”). Procure também políticas que permitem uma ação curinga `"*"` (que efetivamente permite que o usuário realize qualquer ação no bucket do Amazon S3).
- Da mesma forma, procure as listas de controle de acesso (ACLs) do bucket do Amazon S3 que fornecem acesso de leitura, gravação, ou total a “Todos” ou a “Qualquer usuário autenticado da AWS”.
- Use a operação de API `ListBuckets` para verificar todos os buckets do Amazon S3. Depois, use `GetBucketAcl`, `GetBucketWebsite` e `GetBucketPolicy` para determinar se cada bucket tem controles de acesso de conformidade e uma configuração de conformidade.
- Use o AWS Trusted Advisor para inspecionar sua implementação do Amazon S3.
- Considere a implementação de controles contínuos de detecção usando o Regras do AWS Config gerenciado s3-bucket-public-read-prohibited e s3-bucket-public-write-prohibited.

Para obter mais informações, consulte Gerenciamento de identidade e acesso para o Amazon S3.

Implementar o acesso de privilégio mínimo

Ao conceder permissões, você decide quem receberá quais permissões para quais recursos do Amazon S3. Você habilita ações específicas que quer permitir nesses recursos. Portanto, recomendamos conceder apenas as permissões necessárias para executar uma tarefa. A implementação do acesso de privilégio mínimo é fundamental para reduzir o risco de segurança e o impacto que pode resultar de erros ou usuários mal-intencionados.

As ferramentas a seguir estão disponíveis para implementar o privilégio de acesso mínimo:

- Ações de políticas para o Amazon S3 e Limites de permissões para entidades do IAM
- Como o Amazon S3 funciona com o IAM
- Visão geral da lista de controle de acesso (ACL)

Para obter orientação sobre o que considerar ao escolher um ou mais mecanismos precedentes, consulte Gerenciamento de identidade e acesso para o Amazon S3.

Usar perfis do IAM para aplicações e Serviços da AWS que exigem acesso ao Amazon S3

Para que aplicações em execução no Amazon EC2 ou outros Serviços da AWS acessem recursos do Amazon S3, eles devem incluir credenciais válidas da AWS em suas solicitações de API da AWS. Recomendamos não armazenar credenciais da AWS diretamente na aplicação ou na instância do Amazon EC2. Essas são credenciais de longo prazo que não são automaticamente alternadas e podem ter um impacto comercial significativo se forem comprometidas.

Em vez disso, use um perfil do IAM para gerenciar credenciais temporárias para aplicações ou serviços que precisam de acesso ao Amazon S3. Quando você usa um perfil, não é necessário distribuir credenciais de longo prazo (como um nome de usuário e uma senha ou chaves de acesso) para uma instância do Amazon EC2 ou um AWS service (Serviço da AWS) como o AWS Lambda. Em vez disso, a função fornece permissões temporárias que os aplicativos podem usar ao fazer chamadas para outros recursos da AWS.

Para obter mais informações, consulte os seguintes tópicos no Manual do usuário do IAM:

- Perfis do IAM
- Cenários comuns para perfis: usuários, aplicações e serviços

Considerar a criptografia de dados em repouso

Você tem as seguintes opções de proteção de dados em repouso no Amazon S3:

- Criptografia do lado do servidor: todos os buckets do Amazon S3 têm criptografia configurada por padrão e todos os novos objetos que são carregados em um bucket do S3 são automaticamente criptografados em repouso. A criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3) é a configuração de criptografia padrão para todos os buckets no Amazon S3. Para usar um tipo diferente de criptografia, você pode especificar a criptografia do lado do servidor a ser usada nas solicitações PUT do S3 ou definir a configuração de criptografia padrão no bucket de destino.

  O Amazon S3 também fornece as seguintes opções de criptografia do lado do servidor:

  - Criptografia no lado do servidor com chaves do AWS Key Management Service (AWS KMS) (SSE-KMS)
  - Criptografia de camada dupla do lado do servidor com chaves do AWS Key Management Service (AWS KMS) (DSSE-KMS)
  - Criptografia do lado do servidor com chaves fornecidas pelo cliente (SSE-C)

Para obter mais informações, consulte Proteger os dados usando criptografia do lado do servidor.

- Criptografia do lado do cliente: criptografe dados do lado do cliente e carregue os dados criptografados no Amazon S3. Nesse caso, você gerencia o processo de criptografia, as chaves de criptografia e as ferramentas relacionadas. Assim como na criptografia no lado do servidor, a criptografia no lado do cliente pode ajudar a reduzir o risco criptografando os dados com uma chave armazenada em um mecanismo diferente do mecanismo que armazena os próprios dados.

  O Amazon S3 fornece muitas opções de criptografia no lado do cliente. Para obter mais informações, consulte Proteger dados usando a criptografia do lado do cliente.

Aplicar a criptografia de dados em trânsito

É possível usar HTTPS (TLS) para ajudar a evitar que invasores espionem ou manipulem tráfego de rede usando ataques person-in-the-middle (intermediários) ou similares. Recomendamos permitir apenas conexões criptografadas por HTTPS (TLS) usando a condição aws:SecureTransport nas políticas de bucket do Amazon S3. Para ter mais informações, consulte o exemplo de política de bucket do S3 em Gerenciar o acesso com base em solicitações HTTP ou HTTPS. Além de negar solicitações HTTP, recomendamos que configure alarmes do Amazon CloudWatch em `tlsDetails.tlsVersion NOT EXISTS` que alertem você em caso de tentativa de acesso HTTP ao seu conteúdo. Para ter mais informações sobre como configurar os alarmes do Amazon CloudWatch, consulte Creating CloudWatch alarms for CloudTrail events: examples e CloudTrail record contents no Guia do usuário do AWS CloudTrail.

> **Important**
>
> Recomendamos que sua aplicação não fixe certificados TLS do Amazon S3, pois a AWS não permite a fixação de certificados publicamente confiáveis. O S3 renova automaticamente os certificados, o que pode ocorrer a qualquer momento antes da expiração do certificado. Renovar um certificado gera um novo par de chaves pública-privada. Se você fixou um certificado do S3 que foi renovado recentemente com uma nova chave pública, não poderá se conectar ao S3 enquanto a aplicação não usar o novo certificado.

Considere também implementar controles de detecção contínuos usando a regra gerenciada s3-bucket-ssl-requests-only de AWS Config.

Considerar o uso do Bloqueio de objetos do S3

Com o Bloqueio de objetos do S3, é possível armazenar objetos usando um modelo “gravação única e várias leituras” (WORM). O bloqueio de objetos do S3 pode ajudar a evitar a exclusão acidental ou inadequada de dados. Por exemplo, você pode usar o Bloqueio de objetos do S3 para ajudar a proteger os logs do AWS CloudTrail.

Para obter mais informações, consulte Bloquear objetos com o Bloqueio de Objetos.

Habilitar o versionamento do S3

O versionamento do S3 é um meio de manter diversas variantes de um objeto no mesmo bucket. O versionamento pode ser usado para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do . Com o versionamento, você pode se recuperar, facilmente, de ações não intencionais do usuário e de falhas de aplicativo.

Considere também implementar controles de detecção contínuos usando a regra gerenciada s3-bucket-versioning-enabled de AWS Config.

Para obter mais informações, consulte Reter várias versões de objetos com o Versionamento do S3.

Considerar o uso da Replicação do S3 Entre Regiões Diferentes

Embora o Amazon S3 armazene seus dados em diversas zonas de disponibilidade geograficamente distantes por padrão, requisitos de conformidade podem ditar que você armazene os dados em distâncias ainda maiores. Com a Replicação do S3 Entre Regiões Diferentes (CRR), é possível replicar dados entre Regiões da AWS distantes para ajudar a cumprir esses requisitos. A CRR permite a cópia assíncrona automática de objetos em buckets, em diferentes Regiões da AWS. Para obter mais informações, consulte Replicar objetos dentro de uma região e entre regiões.

> **Note**
>
> A CRR requer que tanto o bucket de origem quanto o de destino do S3 tenham o versionamento habilitado.

Considere também implementar controles de detecção contínuos usando a regra gerenciada s3-bucket-replication-enabled de AWS Config.

Considerar o uso dos endpoints da VPC para acesso ao Amazon S3

Um endpoint da Virtual Private Cloud (VPC) para Amazon S3 é uma entidade lógica dentro de uma VPC que permite conectividade apenas com o Amazon S3. Os endpoints da VPC podem ajudar a impedir que o tráfego atravesse a internet aberta.

Os VPC endpoints para Amazon S3 fornecem várias maneiras de controlar o acesso aos dados do Amazon S3:

- É possível controlar as solicitações, os usuários ou os grupos permitidos por um endpoint da VPC específico usando políticas de bucket do S3.
- Você pode controlar quais VPCs ou VPC endpoints têm acesso a seus buckets do S3 usando as políticas de bucket do S3.
- Você pode ajudar a evitar a exfiltração de dados usando uma VPC que não tenha um internet gateway.

Para obter mais informações, consulte Controlar o acesso a partir de VPC endpoints com políticas de bucket.

Use serviços de segurança gerenciados da AWS para monitorar a segurança dos dados

Vários serviços gerenciados de segurança da AWS podem ajudar a identificar, avaliar e monitorar os riscos de segurança e conformidade dos dados do Amazon S3. Esses serviços também podem ajudar você a proteger seus dados contra esses riscos. Esses serviços incluem recursos automatizados de detecção, monitoramento e proteção que são projetados para escalar desde recursos do Amazon S3 para uma única Conta da AWS até recursos para organizações que abrangem milhares de contas.

Para obter mais informações, consulte Monitorar a segurança dos dados com serviços de segurança gerenciados da AWS.

Práticas recomendadas de auditoria e monitoramento do Amazon S3

As práticas recomendadas a seguir para o Amazon S3 podem ajudar a detectar pontos fracos e incidentes potenciais de segurança.

Identificar e auditar todos os buckets do Amazon S3

A identificação de seus ativos de TI é um aspecto essencial de governança e segurança. É necessário ter visibilidade de seus recursos do Amazon S3 para avaliar sua postura de

segurança e agir em possíveis áreas de fraqueza. Para auditar seus recursos, recomendamos fazer o seguinte:

- Use o Editor de tags para identificar e marcar recursos sensíveis quanto a segurança ou auditoria; depois, use essas tags quando precisar procurar esses recursos. Para obter mais informações, consulte Pesquisa de recursos para marcar no Guia do usuário de recursos da AWS.
- Use o S3 Inventory para auditar e gerar relatórios sobre o status da replicação e criptografia de seus objetos para necessidades empresariais, regulatórias e de conformidade. Para obter mais informações, consulte Catalogar e analisar seus dados com o Inventário S3.
- Crie grupos de recursos para seus recursos do Amazon S3. Para obter mais informações, consulte O que são grupos de atributos? no Guia do usuário do AWS Resource Groups.

Implementar o monitoramento usando ferramentas de monitoramento da AWS

O monitoramento é uma parte importante para manter a confiabilidade, segurança, disponibilidade e performance do Amazon S3 e suas soluções da AWS. A AWS fornece várias ferramentas e serviços para ajudar a monitorar o Amazon S3 e outros Serviços da AWS. Por exemplo, é possível monitorar métricas do Amazon CloudWatch para o Amazon S3, particularmente as métricas `PutRequests`, `GetRequests`, `4xxErrors` e `DeleteRequests`. Para obter mais informações, consulte Monitoramento de métricas com o Amazon CloudWatch e Registrar em log e monitorar no Amazon S3.

Para obter um segundo exemplo, consulte, Exemplo: atividade do bucket do Amazon S3. Este exemplo descreve como criar um alarme do CloudWatch que é ativado quando uma chamada de API do Amazon S3 é feita para `PUT` ou `DELETE` uma política do bucket, um ciclo de vida do bucket ou uma configuração de replicação do bucket ou para `PUT` uma ACL do bucket.

Habilitar o registro em log de acesso ao servidor do Amazon S3

O registro em log de acesso ao servidor fornece detalhes sobre as solicitações que são feitas a um bucket. Os logs de acesso ao servidor podem ajudar na auditoria de segurança e acesso, a saber mais sobre a base de clientes e entender sua fatura do Amazon S3. Para obter informações sobre como habilitar o registro em log de acesso ao servidor, consulte Registrar em log as solicitações com registro em log de acesso ao servidor.

Considere também implementar controles de detecção contínuos usando a regra gerenciada s3-bucket-logging-enabled.

Usar o AWS CloudTrail

O AWS CloudTrail fornece um registro das ações executadas por um usuário, uma função ou um AWS service (Serviço da AWS) no Amazon S3. É possível usar as informações coletadas pelo CloudTrail para determinar o seguinte:

- A solicitação feita ao Amazon S3
- O endereço IP do qual a solicitação foi feita.
- Quem fez a solicitação.
- Quando a solicitação foi feita
- Detalhes adicionais sobre a solicitação

Por exemplo, é possível identificar entradas do CloudTrail para ações PUT que afetam o acesso a dados, em particular `PutBucketAcl`, `PutObjectAcl`, `PutBucketPolicy` e `PutBucketWebsite`.

Quando você configura sua Conta da AWS, o CloudTrail é habilitado por padrão. Você pode visualizar eventos recentes no console do CloudTrail. Para criar um registro contínuo de atividades e eventos para os buckets do Amazon S3, você pode criar uma trilha no console do CloudTrail. Para obter mais informações, consulte Registrar eventos de dados, no Guia do usuário do AWS CloudTrail.

Ao criar uma trilha, você pode configurar o CloudTrail para registrar em log eventos de dados. Eventos de dados são registros de operações de recurso executadas no recurso ou dentro de um recurso. No Amazon S3, os eventos de dados registram a atividade da API no nível do objeto para buckets individuais. O CloudTrail é compatível com um subconjunto de operações de API no nível do objeto do Amazon S3 como `GetObject`, `DeleteObject` e `PutObject`. Para obter mais informações sobre como o CloudTrail funciona com o Amazon S3, consulte Registrar chamadas de API do Amazon S3 em log usando AWS CloudTrail. No console do Amazon S3, você também pode configurar seus buckets do S3 para Habilitar o log de eventos do CloudTrail para buckets e objetos do S3.

O AWS Config fornece uma regra gerenciada (`cloudtrail-s3-dataevents-enabled`) que você pode usar para confirmar que pelo menos uma trilha do CloudTrail está registrando eventos de dados para seus buckets do S3. Para obter mais informações, consulte cloudtrail-s3-dataevents-enabled no Guia do desenvolvedor do AWS Config.

Habilitar AWS Config

Muitas das práticas recomendadas listadas neste tópico sugerem criar regras do AWS Config. O AWS Config ajuda a avaliar, fazer auditoria e analisar as configurações de seus recursos da AWS. O AWS Config monitora as configurações de recurso, para que seja possível avaliar as configurações gravadas com relação às configurações seguras desejadas. Com o AWS Config, você pode fazer o seguinte:

- Revisar as alterações nas configurações e nas relações entre recursos da AWS
- Investigar históricos detalhados de configurações de recursos
- Determinar sua conformidade geral com relação às configurações especificadas nas diretrizes internas.

O uso do AWS Config pode ajudar a simplificar a auditoria de conformidade, a análise de segurança, o gerenciamento de alterações e a solução de problemas operacionais. Para obter mais informações, consulte Configuração do AWS Config com o console no Guia do desenvolvedor do AWS Config. Ao especificar os tipos de recurso que devem ser registrados, inclua os recursos do Amazon S3.

> **Important**
>
> As regras gerenciadas do AWS Config só oferecem suporte a buckets de uso geral ao avaliar os recursos do Amazon S3. O AWS Config não registra alterações de configuração em buckets de diretório. Para obter mais informações, consulte AWS Config Managed Rules e List of AWS Config Managed Rules no Guia do desenvolvedor do AWS Config.

Para obter um exemplo de como usar o AWS Config, consulte Como usar o AWS Config para monitorar e responder a buckets do Amazon S3 que permitem acesso público no Blog de segurança da AWS.

Uso da Lente de Armazenamento do S3

A Lente de Armazenamento do S3 é um recurso de análise de armazenamento em nuvem que você pode usar para obter visibilidade em toda a organização sobre o uso e a atividade do armazenamento de objetos. A Lente de Armazenamento do S3 também analisa as métricas para fornecer recomendações contextuais que você pode usar para otimizar os custos de armazenamento e aplicar as práticas recomendadas de proteção de dados.

Com a Lente de Armazenamento do S3, é possível usar métricas para gerar insights resumidos, como descobrir quanto armazenamento você tem em toda a organização ou quais são os buckets e prefixos que mais crescem. Você também pode usar as métricas da Lente de Armazenamento do S3 para identificar oportunidades de otimização de custos, implementar práticas recomendadas de proteção de dados e gerenciamento de acesso, e melhorar a performance das workloads de aplicações.

Por exemplo, você pode identificar buckets que não têm regras de ciclo de vida do S3 para interromper carregamentos fracionados que estão incompletos há mais de sete dias. Você também pode identificar buckets que não estão seguindo as práticas recomendadas de proteção de dados, como usar a Replicação do S3 ou o Versionamento do S3. Para obter mais informações, consulte Noções básicas do Amazon S3 Storage Lens.

Monitorar as recomendações de segurança da AWS

Recomendamos verificar regularmente as recomendações de segurança publicadas no Trusted Advisor para sua Conta da AWS. Especificamente, procure avisos sobre buckets do Amazon S3 com “permissões de acesso em aberto”. É possível fazer isso de maneira programática usando describe-trusted-advisor-checks.

Além disso, monitore ativamente o endereço de e-mail registrado como principal para cada uma de suas Contas da AWS. A AWS usa esse endereço de e-mail para entrar em contato sobre problemas de segurança emergentes que poderiam afetar você.

Problemas operacionais da AWS com grande impacto são publicados no AWS Health Dashboard Service Health. Eles também são publicados em contas individuais por meio do AWS Health Dashboard. Para obter mais informações, consulte a documentação do AWS Health.

Monitorar a segurança dos dados com serviços de segurança gerenciados da AWS

Vários serviços gerenciados de segurança da AWS podem ajudar a identificar, avaliar e monitorar os riscos de segurança e conformidade dos dados do Amazon S3. Esses serviços também podem ajudar você a proteger seus dados contra esses riscos. Esses serviços incluem recursos automatizados de detecção, monitoramento e proteção que são projetados para escalar desde recursos do Amazon S3 para uma única Conta da AWS até recursos para organizações que abrangem milhares de Contas da AWS.

Os serviços de detecção e resposta da AWS podem ajudar a identificar possíveis configurações incorretas de segurança, ameaças ou comportamentos inesperados, para que você possa responder rapidamente a atividades possivelmente não autorizadas ou mal-intencionadas em seu ambiente. Os serviços de proteção de dados da AWS podem ajudar a monitorar e proteger seus dados, contas e workloads contra o acesso não autorizado. Eles também podem ajudar a descobrir dados sigilosos, como informações de identificação pessoal (PII), em seu conjunto de dados do Amazon S3.

Para ajudar a identificar e avaliar riscos de segurança e conformidade de dados, os serviços de segurança gerenciados da AWS geram descobertas para notificar você sobre possíveis eventos ou problemas de segurança com os dados do Amazon S3. As descobertas fornecem detalhes relevantes que você pode usar para investigar, avaliar e tomar medidas com relação a esses riscos de acordo com seus fluxos de trabalho e políticas de resposta a incidentes. É possível acessar os dados das descobertas diretamente usando cada serviço. Também é possível enviar os dados para outras aplicações, serviços e sistemas, como o sistema de gerenciamento de incidentes e eventos de segurança (SIEM).

Para monitorar a segurança dos dados do Amazon S3, considere usar estes serviços de segurança gerenciados da AWS.

Amazon GuardDuty

O Amazon GuardDuty é um serviço de detecção de ameaças que monitora continuamente suas Contas da AWS e workloads em busca de atividades mal-intencionadas e fornece descobertas de segurança detalhadas para visibilidade e correção.

Com o recurso de proteção do S3 no GuardDuty, é possível configurar o GuardDuty para analisar eventos de gerenciamento e de dados do AWS CloudTrail para os recursos do Amazon S3. Depois, o GuardDuty monitora esses eventos em busca de atividades mal-intencionadas e suspeitas. Para fundamentar a análise e identificar possíveis riscos de segurança, o GuardDuty usa feeds de inteligência de ameaças e machine learning.

O GuardDuty pode monitorar diferentes tipos de atividade para os recursos do Amazon S3. Por exemplo, os eventos de gerenciamento do CloudTrail para o Amazon S3 incluem operações em nível de bucket, como `ListBuckets`, `DeleteBucket` e `PutBucketReplication`. Os eventos de dados do CloudTrail para o Amazon S3 incluem operações em nível de objeto, como `GetObject`, `ListObjects` e `PutObject`. Se o GuardDuty detectar atividades anômalas ou possivelmente mal-intencionadas, ele gerará uma descoberta para notificar você.

Para obter mais informações, consulte Proteção do Amazon S3 no Amazon GuardDuty no Guia do usuário do Amazon GuardDuty.

Amazon Detective

O Amazon Detective simplifica o processo investigativo e ajuda você a conduzir investigações de segurança mais rápidas e eficazes. O Detective fornece agregações de dados, resumos e contexto predefinidos que podem ajudar a analisar e avaliar a natureza e a extensão dos possíveis problemas de segurança.

O Detective extrai automaticamente eventos baseados em tempo, como chamadas de API do AWS CloudTrail e logs de fluxo da Amazon VPC para os recursos da AWS. Ele também ingere descobertas geradas pelo Amazon GuardDuty. Depois, o Detective usa machine learning, análise estatística e teoria de grafos para gerar visualizações que ajudam você a conduzir investigações de segurança eficazes com maior rapidez.

Essas visualizações fornecem uma visão unificada e interativa dos comportamentos dos recursos e das interações entre eles ao longo do tempo. É possível explorar esse grafo de comportamento para examinar ações possivelmente mal-intencionadas, como tentativas malsucedidas de login ou chamadas de API suspeitas. Também é possível ver como essas ações afetam recursos, como buckets e objetos do S3.

Para obter mais informações, consulte o Guia de administração do Amazon Detective.

IAM Access Analyzer

O AWS Identity and Access Management Access Analyzer (IAM Access Analyzer) pode ajudar a identificar os recursos compartilhados com uma entidade externa. Também é possível usar o IAM Access Analyzer para validar as políticas do IAM em relação à gramática de políticas e às práticas recomendadas, além de gerar políticas do IAM com base na atividade de acesso nos logs do AWS CloudTrail.

O IAM Access Analyzer usa raciocínio baseado em lógica para analisar políticas de recursos em seu ambiente da AWS, como políticas de bucket. Com o IAM Access Analyzer para S3, você recebe alertas quando um bucket do S3 é configurado para permitir o acesso a qualquer pessoa na internet ou a outras Contas da AWS, incluindo contas fora da organização. Por exemplo, o IAM Access Analyzer para S3 pode relatar que um bucket tem acesso de leitura ou gravação fornecido por meio de uma lista de controle de acesso (ACL) de bucket, uma política de bucket, uma política de ponto de acesso multirregional ou uma política de ponto de acesso. Para cada bucket público ou compartilhado, você recebe descobertas que indicam a origem e o nível de acesso público ou compartilhado. Com essas descobertas, você pode tomar medidas corretivas imediatas e precisas para restaurar o acesso ao bucket da forma desejada.

Para obter mais informações, consulte Revisar o acesso de bucket usando o IAM Access Analyzer para S3.

Amazon Macie

O Amazon Macie é um serviço de segurança que descobre dados sigilosos usando machine learning e correspondência entre padrões. O Macie fornece visibilidade sobre os riscos de segurança de dados e permite a proteção automatizada contra esses riscos. Com o Macie, é possível automatizar a descoberta e a emissão de relatórios de dados sigilosos em seu patrimônio de dados do Amazon S3 para compreender melhor os dados armazenados pela organização no S3.

Para detectar dados sigilosos com o Macie, é possível usar técnicas e critérios incorporados projetados para detectar uma lista grande e crescente de tipos de dados sigilosos para muitos países e regiões. Esses tipos de dados sigilosos incluem vários tipos de informações de identificação pessoal (PII), dados financeiros e dados de credenciais. Também é possível usar critérios personalizados definidos por você: expressões regulares que definem padrões de texto com os quais deve haver correspondência e, opcionalmente, sequências de caracteres e regras de proximidade que refinam os resultados.

Se o Macie detectar dados sigilosos em um objeto do S3, ele gerará uma descoberta de segurança para notificar você. Essa descoberta fornece informações sobre o objeto afetado, os tipos e o número de ocorrências dos dados sigilosos encontrados pelo Macie e detalhes adicionais para ajudar você a investigar o bucket e o objeto do S3 afetados. Para obter mais informações, consulte o Guia do usuário da Amazon Macie.

AWS Security Hub

O AWS Security Hub é um serviço de gerenciamento de procedimento de segurança que realiza verificações de práticas recomendadas de segurança, agrega alertas e descobertas de várias fontes em um único formato e permite a correção automatizada.

O Security Hub coleta e fornece dados de descobertas de segurança de Serviços da AWS e soluções de segurança do AWS Partner Network integradas, como Amazon Detective, Amazon GuardDuty, IAM Access Analyzer e Amazon Macie. Ele também gera suas próprias descobertas executando verificações de segurança automatizadas e contínuas com base nas práticas recomendadas da AWS e em padrões compatíveis do setor.

Depois, o Security Hub correlaciona e consolida as descobertas nos provedores para ajudar a priorizar as mais significativas. Ele também aceita ações personalizadas, que você pode usar para invocar respostas ou ações de correção para classes específicas de descobertas.

Com o Security Hub, é possível avaliar o status de segurança e conformidade dos recursos do Amazon S3 e fazer isso como parte de uma análise mais ampla do procedimento de segurança da organização em Regiões da AWS individuais e em várias regiões. Isso inclui analisar as tendências de segurança e identificar os problemas de segurança de maior prioridade. Também é possível agregar descobertas de várias Regiões da AWS e monitorar e processar dados de descobertas agregadas de uma única região.

Para obter mais informações, acesse Controles do Amazon Simple Storage Service no Guia do usuário do AWS Security Hub.

Proteção de dados no Amazon S3

O Amazon S3 fornece uma infraestrutura de armazenamento resiliente projetada para armazenamento de dados de missão crítica e primários. S3 Standard, S3 Intelligent-Tiering, S3 Standard – IA, S3 Glacier Instant Retrieval, S3 Glacier Flexieval Retrieval e S3 Glacier Deep Archive armazenam objetos redundantemente em vários dispositivos em um mínimo de três zonas de disponibilidade de uma Região da AWS. Uma zona de disponibilidade é um ou mais datacenters discretos com energia, redes e conectividade redundantes em uma Região da AWS. As zonas de disponibilidade são fisicamente separadas por uma distância considerável, de muitos quilômetros, de qualquer outra zona de disponibilidade, embora todas estejam a até 100 quilômetros de distância uma da outra. A classe de armazenamento S3 One Zone – IA armazena dados de forma redundante em vários dispositivos dentro de uma única zona de disponibilidade. Esses serviços são projetados para lidar com falhas simultâneas de dispositivos, detectando e reparando rapidamente qualquer redundância perdida, além de verificar regularmente a integridade dos dados usando somas de verificação.

O armazenamento Amazon S3 Standard oferece os seguintes recursos:

- Respaldado pelo Acordo de Nível de Serviço do Amazon S3.
- Projetado para fornecer 99,999999999% de durabilidade e 99,99% de disponibilidade dos objetos em determinado ano.
- S3 Standard, S3 Intelligent-Tiering, S3 Standard – IA, S3 Glacier Instant Retrieval, S3 Glacier Flexible Retrieval e S3 Glacier Deep Archive foram projetados para sustentar dados em caso de perda de uma zona de disponibilidade do Amazon S3 inteira.

O Amazon S3 protege ainda mais seus dados usando o versionamento. O versionamento pode ser usado para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no

bucket do Amazon S3. Com o versionamento, você pode se recuperar, facilmente, de ações não intencionais do usuário e de falhas de aplicativo. Por padrão, as solicitações recuperam a versão gravada mais recente. Você pode recuperar as versões mais antigas de um objeto, especificando uma versão do objeto em uma solicitação.

Além do Versionamento do S3, você também pode usar o Bloqueio de Objeto do Amazon S3 e a Replicação do S3 para proteger seus dados. Para obter mais informações, consulte Proteção de dados no Amazon S3.

Para fins de proteção de dados, recomendamos que você proteja as credenciais da sua Conta da AWS e configure contas de usuário individuais com o AWS Identity and Access Management de modo que cada usuário receba somente as permissões necessárias para cumprir suas funções.

Se você precisar de módulos criptográficos validados pelo FIPS 140-2 ao acessar AWS por meio de uma interface de linha de comando ou uma API, use um endpoint FIPS. Para obter mais informações sobre endpoints do FIPS, consulte Federal Information Processing Standard (FIPS) 140-2.

As melhores práticas de segurança a seguir também abordam a proteção de dados no Amazon S3:

- Implement server-side encryption
- Enforce encryption of data in transit
- Consider using Macie with Amazon S3
- Identify and audit all your Amazon S3 buckets
- Monitor Amazon Web Services security advisories

Proteger dados com criptografia

> **Important**
>
> O Amazon S3 agora aplica criptografia do lado do servidor com chaves gerenciadas do Amazon S3 (SSE-S3) como nível básico de criptografia para cada bucket no Amazon S3. Desde 5 de janeiro de 2023, todos os novos uploads de objetos para o Amazon S3 são automaticamente criptografados sem custo adicional e sem impacto na performance. O status de criptografia automática para a configuração de criptografia padrão do bucket do S3 e para novos uploads de objetos está disponível em logs do AWS CloudTrail, no Inventário do S3, na Lente de Armazenamento do S3, no console do Amazon S3 e como cabeçalho adicional de resposta da API do Amazon S3 na AWS Command Line Interface e em AWS

SDKs. Para obter mais informações, consulte Perguntas frequentes sobre criptografia padrão.

A proteção de dados refere-se à proteção enquanto eles estão em trânsito (à medida que são transferidos para e do Amazon S3) e em repouso (enquanto estão armazenados em discos em datacenters do Amazon S3). É possível proteger dados em trânsito usando SSL/TLS (Secure Socket Layer/Transport Layer Security) ou criptografia do lado do cliente. Para proteger dados em repouso no Amazon S3, você tem as seguintes opções:

- Criptografia do lado do servidor: o Amazon S3 criptografa os objetos antes de salvá-los em discos em seus datacenters da AWS e descriptografa-os quando você os baixa.

  Todos os buckets do Amazon S3 têm criptografia configurada por padrão e todos os novos objetos que são carregados em um bucket do S3 são automaticamente criptografados em repouso. A criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3) é a configuração de criptografia padrão para todos os buckets no Amazon S3. Para usar um tipo diferente de criptografia, você pode especificar a criptografia do lado do servidor a ser usada nas solicitações PUT do S3 ou atualizar a configuração de criptografia padrão no bucket de destino.

  Se quiser especificar um tipo de criptografia diferente nas solicitações PUT, você pode usar a criptografia do lado do servidor com chaves do AWS Key Management Service (AWS KMS) (SSE-KMS), criptografia de camada dupla do lado do servidor com chaves do AWS KMS (DSSE-KMS) ou criptografia do lado do servidor com chaves fornecidas pelo cliente (SSE-C). Se quiser definir uma configuração de criptografia padrão diferente no bucket de destino, você pode usar SSE-KMS ou DSSE-KMS.

  Para ter mais informações sobre a alteração da configuração padrão de criptografia para buckets de uso geral, consulte Configurar a criptografia padrão.

  Quando você altera a configuração de criptografia padrão do bucket para SSE-KMS, o tipo de criptografia dos objetos do Amazon S3 existentes no bucket não é alterado. Para alterar o tipo de criptografia de objetos preexistentes depois de atualizar a configuração padrão de criptografia para SSE-KMS, use o recurso Operações em Lote do Amazon S3. Basta fornecer uma lista de objetos ao recurso Operações em Lote do S3 para que ele chame a respectiva operação de API. É possível usar a ação Copiar objetos para copiar objetos existentes, gravando-os de volta no mesmo bucket que os objetos criptografados por SSE-KMS. Um único trabalho do Batch Operations pode realizar a operação especificada em bilhões de objetos. Para ter mais

informações, consulte Executar operações de objetos em massa com o Operações em Lote e a publicação How to retroactively encrypt existing objects in Amazon S3 using S3 Inventory, Amazon Athena, and S3 Batch Operations do Blog do AWS Storage.

Para obter mais informações sobre cada opção de criptografia do lado do servidor, consulte Proteger os dados usando criptografia do lado do servidor.

Para configurar a criptografia do lado do servidor, consulte:

- Especificar a criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3)
- Especificando criptografia no lado do servidor com o AWS KMS (SSE-KMS)
- the section called “Especificar a DSSE-KMS”
- Especificação de criptografia no lado do servidor com chaves fornecidas pelo cliente (SSE-C).

- Criptografia do lado do cliente: você criptografa dados do lado do cliente e faz upload dos dados criptografados no Amazon S3. Nesse caso, você gerencia o processo de criptografia, as chaves de criptografia e as ferramentas relacionadas.

  Para configurar a criptografia do lado do cliente, consulte Proteger dados usando a criptografia do lado do cliente.

Para ver qual porcentagem dos seus bytes de armazenamento estão criptografados, você pode usar as métricas da Lente de Armazenamento do Amazon S3. A Lente de Armazenamento do S3 é um recurso de análise de armazenamento em nuvem que você pode usar para obter visibilidade em toda a organização sobre o uso e a atividade do armazenamento de objetos. Para obter mais informações, consulte Avaliar a atividade e o uso do armazenamento com o S3 Storage Lens. Para obter uma lista completa de métricas, consulte o Glossário de métricas da Lente de Armazenamento do S3.

Para obter mais informações sobre criptografia do lado do servidor e criptografia do lado do cliente, consulte os tópicos a seguir.

Tópicos

- Proteger os dados usando criptografia do lado do servidor
- Proteger dados usando a criptografia do lado do cliente

Proteger os dados usando criptografia do lado do servidor

> **Important**
>
> O Amazon S3 agora aplica criptografia do lado do servidor com chaves gerenciadas do Amazon S3 (SSE-S3) como nível básico de criptografia para cada bucket no Amazon S3. Desde 5 de janeiro de 2023, todos os novos uploads de objetos para o Amazon S3 são automaticamente criptografados sem custo adicional e sem impacto na performance. O status de criptografia automática para a configuração de criptografia padrão do bucket do S3 e para novos uploads de objetos está disponível em logs do AWS CloudTrail, no Inventário do S3, na Lente de Armazenamento do S3, no console do Amazon S3 e como cabeçalho adicional de resposta da API do Amazon S3 na AWS Command Line Interface e em AWS SDKs. Para obter mais informações, consulte Perguntas frequentes sobre criptografia padrão.

A criptografia do lado do servidor é a criptografia de dados em seu destino pela aplicação ou serviço que os recebe. O Amazon S3 criptografa os dados no nível do objeto no momento em que os grava em discos nos datacenters da AWS e descriptografa-os quando você os acessa. Contanto que você autentique sua solicitação e tenha permissões de acesso, não há diferença na forma de acesso aos objetos criptografados ou não criptografados. Por exemplo, se você compartilhar seus objetos usando um URL pré-assinado, esse URL funcionará da mesma forma para objetos criptografados e não criptografados. Além disso, quando você lista objetos no bucket, as operações de API de lista retornam uma lista de todos os objetos, independentemente de estarem ou não criptografados.

Todos os buckets do Amazon S3 têm criptografia configurada por padrão e todos os novos objetos que são carregados em um bucket do S3 são automaticamente criptografados em repouso. A criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3) é a configuração de criptografia padrão para todos os buckets no Amazon S3. Para usar um tipo diferente de criptografia, você pode especificar a criptografia do lado do servidor a ser usada nas solicitações PUT do S3 ou atualizar a configuração de criptografia padrão no bucket de destino.

Se quiser especificar um tipo de criptografia diferente nas solicitações PUT, você pode usar a criptografia do lado do servidor com chaves do AWS Key Management Service (AWS KMS) (SSE-KMS), criptografia de camada dupla do lado do servidor com chaves do AWS KMS (DSSE-KMS) ou criptografia do lado do servidor com chaves fornecidas pelo cliente (SSE-C). Se quiser definir uma configuração de criptografia padrão diferente no bucket de destino, você pode usar SSE-KMS ou DSSE-KMS.

Para ter mais informações sobre a alteração da configuração padrão de criptografia para buckets de uso geral, consulte Configurar a criptografia padrão.

Quando você altera a configuração de criptografia padrão do bucket para SSE-KMS, o tipo de criptografia dos objetos do Amazon S3 existentes no bucket não é alterado. Para alterar o tipo de criptografia de objetos preexistentes depois de atualizar a configuração padrão de criptografia para SSE-KMS, use o recurso Operações em Lote do Amazon S3. Basta fornecer uma lista de objetos ao recurso Operações em Lote do S3 para que ele chame a respectiva operação de API. É possível usar a ação Copiar objetos para copiar objetos existentes, gravando-os de volta no mesmo bucket que os objetos criptografados por SSE-KMS. Um único trabalho do Batch Operations pode realizar a operação especificada em bilhões de objetos. Para ter mais informações, consulte Executar operações de objetos em massa com o Operações em Lote e a publicação How to retroactively encrypt existing objects in Amazon S3 using S3 Inventory, Amazon Athena, and S3 Batch Operations do Blog do AWS Storage.

> **Note**
>
> Não é possível aplicar diferentes tipos de criptografia de servidor ao mesmo objeto simultaneamente.

Se você precisar criptografar os objetos existentes, use as operações em lote do S3 e o inventário do S3. Para obter mais informações, consulte Criptografar objetos com as operações em lote do Amazon S3 e Executar operações de objetos em massa com o Operações em Lote.

Ao armazenar dados no Amazon S3, há quatro opções mutuamente excludentes de criptografia do lado do servidor, dependendo de como você opta por gerenciar as chaves de criptografia e do número de camadas de criptografia que deseja aplicar.

Criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3)

Todos os buckets do Amazon S3 têm criptografia configurada por padrão. A opção padrão para a criptografia do lado do servidor é com as chaves gerenciadas pelo Amazon S3 (SSE-S3). Cada objeto é criptografado com uma chave exclusiva. Como uma proteção adicional, a SSE-S3 criptografa a própria chave com uma chave-raiz que alterna regularmente. A SSE-S3 usa uma das cifras de bloco mais fortes disponíveis, o padrão de criptografia avançada de 256 bits (AES-256), para criptografar os dados. Para obter mais informações, consulte Usar a criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3).

Criptografia no lado do servidor com chaves do AWS Key Management Service (AWS KMS) (SSE-KMS)

A criptografia do lado do servidor com o AWS KMS keys (SSE-KMS) é fornecida por meio de uma integração do serviço AWS KMS com o Amazon S3. Com o AWS KMS, você tem mais controle sobre suas chaves. Por exemplo, você pode visualizar chaves separadas, editar políticas de controle e seguir as chaves no AWS CloudTrail. Além disso, é possível criar e gerenciar chaves gerenciadas pelo cliente ou usar Chaves gerenciadas pela AWS que são exclusivas para você, para o seu serviço e para a sua região. Para obter mais informações, consulte Usar criptografia do lado do servidor com o AWS KMS (SSE-KMS).

Criptografia de camada dupla do lado do servidor com chaves do AWS Key Management Service (AWS KMS) (DSSE-KMS)

A criptografia de camada dupla do lado do servidor com AWS KMS keys (DSSE-KMS) é semelhante à SSE-KMS, mas a DSSE-KMS aplica duas camadas individuais de criptografia em nível de objeto em vez apenas uma. Como as duas camadas de criptografia são aplicadas a um objeto do lado do servidor, você pode usar uma grande variedade de ferramentas e Serviços da AWS para analisar dados no S3 enquanto usa um método de criptografia capaz de atender aos seus requisitos de conformidade. Para obter mais informações, consulte Usar criptografia de camada dupla do lado do servidor com chaves do AWS KMS (DSSE-KMS).

Criptografia do lado do servidor com chaves fornecidas pelo cliente (SSE-C)

Com a criptografia do lado do servidor com chaves fornecidas pelo cliente (SSE-C), você gerencia as chaves de criptografia e o Amazon S3 gerencia a criptografia, ao gravar em discos, e a descriptografia, quando você acessa os objetos. Para obter mais informações, consulte Como usar criptografia do lado do servidor com chaves fornecidas pelo cliente (SSE-C).

> **Note**
>
> Ao usar pontos de acesso para sistemas de arquivos do Amazon FSx utilizando o recurso Pontos de Acesso S3, você tem uma opção para criptografia do lado do servidor.
>
> Criptografia do lado do servidor com o Amazon FSx (SSE-FSX)
>
> Todos os sistemas de arquivos do Amazon FSx têm criptografia configurada por padrão e são criptografados em repouso com chaves gerenciadas por meio do AWS Key Management Service. Os dados são automaticamente criptografados e descriptografados pelo sistema de

arquivos à medida que são gravados e lidos no sistema de arquivos. Esses processos são tratados de maneira transparente pelo Amazon FSx.

Definir o comportamento padrão da criptografia para os buckets do Amazon S3

Important

O Amazon S3 agora aplica criptografia do lado do servidor com chaves gerenciadas do Amazon S3 (SSE-S3) como nível básico de criptografia para cada bucket no Amazon S3. Desde 5 de janeiro de 2023, todos os novos uploads de objetos para o Amazon S3 são automaticamente criptografados sem custo adicional e sem impacto na performance. O status de criptografia automática para a configuração de criptografia padrão do bucket do S3 e para novos uploads de objetos está disponível em logs do AWS CloudTrail, no Inventário do S3, na Lente de Armazenamento do S3, no console do Amazon S3 e como cabeçalho adicional de resposta da API do Amazon S3 na AWS Command Line Interface e em AWS SDKs. Para obter mais informações, consulte Perguntas frequentes sobre criptografia padrão.

Todos os buckets do Amazon S3 têm a criptografia configurada por padrão, e os objetos são automaticamente criptografados usando criptografia do lado do servidor, com chaves gerenciadas do Amazon S3 (SSE-S3). Essa configuração de criptografia se aplica a todos os objetos em seus buckets do Amazon S3.

Se você precisar de maior controle sobre suas chaves, como gerenciar a alternância de chaves e as concessões de políticas de acesso, poderá optar por usar a criptografia do lado do servidor chaves do AWS Key Management Service (AWS KMS) (SSE-KMS) ou a criptografia de camada dupla do lado do servidor com chaves do AWS KMS (DSSE-KMS). Para ter mais informações sobre edição de chaves do KMS, consulte Editar chaves no Guia do desenvolvedor do AWS Key Management Service.

Note

Alteramos os buckets para criptografar automaticamente uploads de novos objetos. Se você criou anteriormente um bucket sem criptografia padrão, o Amazon S3 ativará a criptografia por padrão para o bucket usando SSE-S3. Não haverá nenhuma alteração na configuração de criptografia padrão para um bucket existente que já tenha a criptografia SSE-S3 ou SSE-

KMS configurada. Se quiser criptografar seus objetos com a SSE-KMS, deverá alterar o tipo de criptografia nas configurações do bucket. Para obter mais informações, consulte Usar criptografia do lado do servidor com o AWS KMS (SSE-KMS).

Ao configurar seu bucket para usar criptografia padrão com a SSE-KMS, você também pode ativar o recurso de chaves de bucket do S3 para diminuir o tráfego de solicitações do Amazon S3 para o AWS KMS e reduzir o custo de criptografia. Para obter mais informações, consulte Redução do custo do SSE-KMS com chaves de bucket do Amazon S3.

Para identificar buckets que têm SSE-KMS habilitada como criptografia padrão, você pode usar as métricas da Lente de Armazenamento do Amazon S3. A Lente de Armazenamento do S3 é um recurso de análise de armazenamento em nuvem que você pode usar para obter visibilidade em toda a organização sobre o uso e a atividade do armazenamento de objetos. Para obter mais informações, consulte Como usar a Lente de Armazenamento do S3 para proteger seus dados.

Quando você usa a criptografia no lado do servidor, o Amazon S3 criptografa um objeto antes de salvá-lo no disco e o descriptografa quando você o baixa. Para ter mais informações sobre como proteger dados usando a criptografia no lado do servidor e o gerenciamento de chaves de criptografia, consulte Proteger os dados usando criptografia do lado do servidor.

Para ter mais informações sobre permissões necessárias para criptografia padrão, consulte PutBucketEncryption na Referência da API do Amazon Simple Storage Service.

Você pode configurar o comportamento da criptografia padrão do Amazon S3 para um bucket do S3 usando o console do Amazon S3, os AWS SDKs, a API REST do Amazon S3 e a AWS Command Line Interface (AWS CLI).

Criptografar objetos existentes

Para criptografar objetos existentes não criptografados do Amazon S3, você pode usar Operações em Lote do Amazon S3. Você fornece uma lista de objetos às operações em lote do S3 que, por sua vez, chamam a respectiva API para realizar a operação especificada. É possível usar a operação Copy do Batch Operations para copiar objetos não criptografados existentes e gravá-los de volta no mesmo bucket que os objetos criptografados. Um único trabalho do Batch Operations pode realizar a operação especificada em bilhões de objetos. Para obter mais informações, consulte Executar operações de objetos em massa com o Operações em Lote e a publicação do Blog de armazenamento da AWS Criptografia de objetos existentes com o Amazon S3 Batch Operations.

Você também pode criptografar objetos existentes usando a operação de API `CopyObject` ou o comando `copy-object` da AWS CLI. Para obter mais informações, consulte a publicação do Blog de armazenamento da AWS Criptografia de objetos existentes do Amazon S3 com a AWS CLI.

> **Note**
>
> Os buckets do Amazon S3 com criptografia definida como SSE-KMS não podem ser usados como buckets de destino para the section called “Registrando acesso ao servidor”. Somente a criptografia padrão SSE-S3 é suportada para buckets de destino do log de acesso do servidor.

Usar criptografia SSE-KMS para operações entre contas

Ao utilizar a criptografia para operações entre contas, esteja ciente do seguinte:

- Se o nome do recurso da Amazon (ARN) da AWS KMS key ou alias não for fornecido no momento da solicitação nem por meio da configuração de criptografia padrão do bucket, a Chave gerenciada pela AWS (`aws/s3`) será utilizada.
- Se você estiver fazendo upload ou acessando objetos do S3 usando entidades principais do AWS Identity and Access Management (IAM) que estão na mesma Conta da AWS que a sua chave do KMS, poderá usar a Chave gerenciada pela AWS (`aws/s3`).
- Se quiser conceder acesso entre contas aos seus objetos do S3, use uma chave gerenciada pelo cliente. Você pode configurar a política de uma chave gerenciada pelo cliente para permitir o acesso de outra conta.
- Se estiver especificando uma chave do KMS gerenciada pelo cliente, recomendamos usar um ARN de chave do KMS totalmente qualificado. Se você usar um alias da chave do KMS, o AWS KMS resolverá a chave na conta do solicitante. Isso pode resultar em dados criptografados com uma chave do KMS pertencente ao solicitante, e não ao proprietário do bucket.
- É necessário especificar uma chave para a qual você (o solicitante) recebeu a permissão `Encrypt`. Para ter mais informações, consulte Permitir que os usuários da chave usem uma chave do KMS para operações criptográficas no Guia do desenvolvedor do AWS Key Management Service.

Para ter mais informações sobre quando usar as chaves gerenciadas pelo cliente e as chaves do KMS gerenciadas pela AWS, consulte Devo usar uma Chave gerenciada pela AWS ou uma chave pelo cliente para criptografar meus objetos no Amazon S3?

Como usar a criptografia padrão com a replicação

Ao habilitar a criptografia padrão para um bucket de destino de replicação, o seguinte comportamento de criptografia será aplicado:

- Se os objetos no bucket de origem não estiverem criptografados, os objetos de réplica no bucket de destino serão criptografados usando as configurações de criptografia padrão do bucket de destino. Como resultado, as tags de entidade (ETags) dos objetos de origem diferem dos ETags dos objetos de réplica. Se você tiver aplicações que usam ETags, será necessário atualizar essas aplicações para considerar essa diferença.
- Se os objetos no bucket de origem forem criptografados usando a criptografia do lado do servidor com chaves gerenciadas do Amazon S3 (SSE-S3), a criptografia do lado do servidor com chaves do AWS Key Management Service (AWS KMS) (SSE-KMS) ou a criptografia de camada dupla do lado do servidor com chaves do AWS KMS (DSSE-KMS), os objetos de réplica no bucket de destino usarão o mesmo tipo de criptografia que os objetos de origem. As configurações de criptografia padrão do bucket de destino não são usadas.

Para obter mais informações sobre como usar a criptografia padrão com SSE-KMS, consulte Replicar objetos criptografados.

Usar Chaves de bucket do Amazon S3 com criptografia padrão

Quando você configura seu bucket para usar a SSE-KMS como o comportamento de criptografia padrão para novos objetos, você também pode configurar chaves de bucket do S3. As chaves de bucket do S3 diminuem o número de transações do Amazon S3 para o AWS KMS a fim de reduzir o custo da SSE-KMS.

Quando você configura seu bucket para usar chaves de bucket do S3 para SSE-KMS em novos objetos, o AWS KMS gera uma chave no nível de bucket usada para criar uma chave de dados exclusiva para objetos no bucket. Essa chave de bucket do S3 é usada por um período limitado no Amazon S3, reduzindo a necessidade do Amazon S3 fazer solicitações ao AWS KMS para concluir operações de criptografia.

Para obter mais informações sobre como usar Chaves de bucket do S3, consulte Uso de chaves de bucket do Amazon S3.

Configurar a criptografia padrão

> **Important**
>
> O Amazon S3 agora aplica criptografia do lado do servidor com chaves gerenciadas do Amazon S3 (SSE-S3) como nível básico de criptografia para cada bucket no Amazon S3. Desde 5 de janeiro de 2023, todos os novos uploads de objetos para o Amazon S3 são automaticamente criptografados sem custo adicional e sem impacto na performance. O status de criptografia automática para a configuração de criptografia padrão do bucket do S3 e para novos uploads de objetos está disponível em logs do AWS CloudTrail, no Inventário do S3, na Lente de Armazenamento do S3, no console do Amazon S3 e como cabeçalho adicional de resposta da API do Amazon S3 na AWS Command Line Interface e em AWS SDKs. Para obter mais informações, consulte Perguntas frequentes sobre criptografia padrão.

Os buckets do Amazon S3 têm a criptografia configurada por padrão, e os novos objetos são automaticamente criptografados usando criptografia do lado do servidor, com chaves gerenciadas do Amazon S3 (SSE-S3). Essa criptografia se aplica a todos os novos objetos em seus buckets do Amazon S3 e não tem nenhum custo para você.

Se você precisar de maior controle sobre suas chaves de criptografia, como gerenciar a alternância de chaves e as concessões de políticas de acesso, poderá optar por usar a criptografia do lado do servidor com chaves do AWS Key Management Service (AWS KMS) (SSE-KMS) ou a criptografia de camada dupla do lado do servidor com chaves do AWS KMS (DSSE-KMS). Para obter mais informações sobre SSE-KMS, consulte Especificando criptografia no lado do servidor com o AWS KMS (SSE-KMS). Para ter mais informações sobre DSSE-KMS, consulte the section called “Criptografia de camada dupla do lado do servidor (DSSE-KMS)”.

Se quiser usar uma chave do KMS que seja de propriedade de outra conta, você deverá ter permissão para usar a chave. Para obter mais informações sobre permissões entre contas para chaves do KMS, consulte Criar chaves do KMS que outras contas podem usar no Guia do desenvolvedor do AWS Key Management Service.

Ao definir a criptografia do bucket padrão como SSE-KMS, você também pode configurar uma chave de bucket do S3 para reduzir os custos de solicitação do AWS KMS. Para obter mais informações, consulte Redução do custo do SSE-KMS com chaves de bucket do Amazon S3.

> **Note**
>
> Se você usa PutBucketEncryption para definir a criptografia de bucket padrão como SSE-KMS, é necessário verificar se o ID da chave do KMS está correto. O Amazon S3 não valida o ID da chave do KMS fornecido nas solicitações PutBucketEncryption.

Não há cobranças adicionais para usar a criptografia padrão para buckets do S3. As solicitações para configurar o comportamento de criptografia padrão geram cobranças padrão de solicitação do Amazon S3. Para obter mais informações sobre preços, consulte Preços do Amazon S3. Para a SSE-KMS e DSSE-KMS, tarifas do AWS KMS podem ser aplicadas. Elas estão listadas em Preços do AWS KMS.

A criptografia no lado do servidor com chaves fornecidas pelo cliente (SSE-C) não é compatível para criptografia padrão.

Você pode configurar a criptografia padrão do Amazon S3 para um bucket do S3 usando o console do Amazon S3, os AWS SDKs, a API REST do Amazon S3 e a AWS Command Line Interface (AWS CLI).

Alterações feitas às observações antes de habilitar a criptografia padrão

Depois de habilitar a criptografia padrão para um bucket, o seguinte comportamento de criptografia será aplicado:

- Não há alteração na criptografia dos objetos que existiam no bucket antes da ativação da criptografia padrão.
- Quando você faz upload de objetos após a ativação da criptografia padrão:
  - Se seus cabeçalhos de solicitação PUT não incluírem informações de criptografia, o Amazon S3 usará as configurações de criptografia padrão do bucket para criptografar os objetos.
  - Se seus cabeçalhos de solicitação PUT incluírem informações de criptografia, o Amazon S3 usará as informações de criptografia da solicitação PUT para criptografar objetos antes de armazená-los no Amazon S3.
- Se você usar a opção SSE-KMS ou a DSSE-KMS em sua configuração de criptografia padrão, poderão ser cobradas cotas de solicitações por segundo (RPS) do AWS KMS. Para ter mais informações sobre as cotas do AWS KMS e como solicitar um aumento de cota, consulte Cotas no Guia do desenvolvedor do AWS Key Management Service.

> **Note**
>
> Os objetos carregados antes da ativação da criptografia padrão não serão criptografados. Para ter informações sobre criptografia de objetos existentes, consulte the section called "Definir criptografia de bucket padrão".

Usar o console do S3

Como configurar a criptografia padrão em um bucket do Amazon S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets.
3. Na lista de Buckets, escolha o nome do bucket desejado.
4. Escolha a guia Properties (Propriedades).
5. Em Default encryption (Criptografia padrão), escolha Edit (Editar).
6. Para configurar a criptografia padrão, em Tipo de criptografia, selecione uma das seguintes opções:

   - Criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3)
   - Criptografia no lado do servidor com chaves do AWS Key Management Service (SSE-KMS)
   - Criptografia de camada dupla do lado do servidor com chaves do AWS Key Management Service (DSSE-KMS)

   > **Important**
   >
   > Se você usar a opção SSE-KMS ou a DSSE-KMS em sua configuração de criptografia padrão, poderão ser cobradas cotas de solicitações por segundo (RPS) do AWS KMS. Para obter mais informações sobre as cotas do AWS KMS e como solicitar um aumento de cota, consulte Cotas no Guia do desenvolvedor do AWS Key Management Service.

   Os buckets e novos objetos são criptografados por padrão com o SSE-S3, a menos que você especifique outro tipo de criptografia padrão para eles. Para obter mais informações sobre

criptografia padrão, consulte Definir o comportamento padrão da criptografia para os buckets do Amazon S3.

Para obter mais informações sobre como usar a criptografia no lado do servidor do Amazon S3 para criptografar seus dados, consulte Usar a criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3).

7. Se você escolheu Criptografia do lado do servidor com chaves do AWS Key Management Service (SSE-KMS) ou Criptografia de camada dupla do lado do servidor com chaves do AWS Key Management Service (DSSE-KMS), faça o seguinte:

   a. Em Chave do AWS KMS, especifique sua chave do KMS de uma das seguintes maneiras:

      - Para escolher entre uma lista de chaves do KMS disponíveis, selecione Escolher entre suas AWS KMS keys e escolha sua chave do KMS na lista de chaves disponíveis.

        As chaves Chave gerenciada pela AWS (`aws/s3`) e as chaves gerenciadas pelo cliente são exibidas nessa lista. Para ter mais informações sobre chaves gerenciadas pelo cliente, consulte Chaves de clientes e chaves da AWS no Guia do desenvolvedor do AWS Key Management Service.

      - Para inserir o ARN da chave do KMS, escolha Inserir ARN da AWS KMS key e insira o ARN da chave do KMS no campo exibido.

      - Para criar uma chave gerenciada pelo cliente no console do AWS KMS, selecione Criar uma chave do KMS.

        Para ter mais informações sobre como criar uma AWS KMS key, consulte Criação de chaves no Guia do desenvolvedor do AWS Key Management Service.

> **Important**
>
> Você só pode usar chaves do KMS habilitadas na mesma Região da AWS que o bucket. Quando você seleciona Choose from your KMS keys , (Escolher de suas chaves do KMS), o console do S3 lista somente 100 chaves do KMS por região. Se você tiver mais de 100 chaves do KMS na mesma região, será possível ver somente as primeiras 100 chaves do KMS no console do S3. Para usar uma chave do KMS que não esteja listada no console, escolha Inserir o ARN da AWS KMS key e insira o ARN da chave do KMS.

Ao usar uma AWS KMS key para criptografia no lado do servidor no Amazon S3, você deve escolher uma chave de criptografia do KMS simétrica. O Amazon S3 só é compatível com chaves do KMS de criptografia simétrica. Para obter mais informações sobre essas chaves, consulte Chaves do KMS de criptografia simétrica no Guia do desenvolvedor do AWS Key Management Service.

Para ter mais informações sobre como usar a SSE-KMS com o Amazon S3, consulte Usar criptografia do lado do servidor com o AWS KMS (SSE-KMS). Para ter mais informações sobre como usar a DSSE-KMS, consulte the section called “Criptografia de camada dupla do lado do servidor (DSSE-KMS)”.

b. Ao configurar seu bucket para usar a criptografia padrão com a SSE-KMS, você também pode ativar a chave de bucket do S3. As chaves de bucket do S3 diminuem o custo de criptografia reduzindo o tráfego de solicitações do Amazon S3 para o AWS KMS. Para obter mais informações, consulte Redução do custo do SSE-KMS com chaves de bucket do Amazon S3.

   Para usar Chaves de bucket do S3, em Bucket Key (Chave de bucket), escolha Enable (Habilitar).

   > **Note**
   >
   > As chaves de bucket do S3 não comportam DSSE-KMS.

8. Escolha Salvar alterações.

Como usar o AWS CLI

Esses exemplos mostram como configurar a criptografia padrão usando SSE-S3 ou usando a SSE-KMS com uma chave de bucket do S3.

Para obter mais informações sobre criptografia padrão, consulte Definir o comportamento padrão da criptografia para os buckets do Amazon S3. Para obter mais informações sobre o uso da AWS CLI para configurar a criptografia padrão, consulte put-bucket-encryption.

Example – Criptografia padrão com SSE-S3

Esse exemplo configura a criptografia de bucket padrão com chaves gerenciadas pelo Amazon S3.

```
aws s3api put-bucket-encryption --bucket amzn-s3-demo-bucket --server-side-encryption-
configuration '{
    "Rules": [
        {
            "ApplyServerSideEncryptionByDefault": {
                "SSEAlgorithm": "AES256"
            }
        }
    ]
}'
```

Example – Criptografia padrão com SSE-KMS usando uma chave de bucket do S3

Esse exemplo configura a criptografia de bucket padrão com o SSE-KMS usando uma chave de bucket do S3.

```
aws s3api put-bucket-encryption --bucket amzn-s3-demo-bucket --server-side-encryption-
configuration '{
    "Rules": [
            {
                "ApplyServerSideEncryptionByDefault": {
                    "SSEAlgorithm": "aws:kms",
                    "KMSMasterKeyID": "KMS-Key-ARN"
                },
                "BucketKeyEnabled": true
            }
        ]
    }'
```

Uso da API REST

Use a operação `PutBucketEncryption` da API REST para habilitar a criptografia padrão e definir o tipo de criptografia do lado do servidor a ser utilizado, ou seja, SSE-S3, SSE-KMS ou DSSE-KMS.

Para obter mais informações, consulte PutBucketEncryption na Referência da API do Amazon Simple Storage Service.

Monitorar a criptografia padrão com o AWS CloudTrail e o Amazon EventBridge

> **Important**
>
> O Amazon S3 agora aplica criptografia do lado do servidor com chaves gerenciadas do Amazon S3 (SSE-S3) como nível básico de criptografia para cada bucket no Amazon S3. Desde 5 de janeiro de 2023, todos os novos uploads de objetos para o Amazon S3 são automaticamente criptografados sem custo adicional e sem impacto na performance. O status de criptografia automática para a configuração de criptografia padrão do bucket do S3 e para novos uploads de objetos está disponível em logs do AWS CloudTrail, no Inventário do S3, na Lente de Armazenamento do S3, no console do Amazon S3 e como cabeçalho adicional de resposta da API do Amazon S3 na AWS Command Line Interface e em AWS SDKs. Para obter mais informações, consulte Perguntas frequentes sobre criptografia padrão.

Você pode rastrear solicitações de configuração de criptografia padrão para buckets do Amazon S3 usando eventos do AWS CloudTrail. Os seguintes nomes de eventos de API são usados nos logs do CloudTrail:

- `PutBucketEncryption`
- `GetBucketEncryption`
- `DeleteBucketEncryption`

Você também pode criar regras do EventBridge que correspondam aos eventos do CloudTrail para essas chamadas de API. Para obter mais informações sobre eventos do CloudTrail, consulte Habilitar o registro em log de objetos em um bucket usando o console. Para ter mais informações sobre eventos do EventBridge, consulte Eventos de Serviços da AWS.

Você pode usar logs do CloudTrail para ações do Amazon S3 no nível de objeto a fim de rastrear solicitações PUT e POST para o Amazon S3. Você pode usar essas ações para verificar se a criptografia padrão está sendo usada para criptografar objetos quando as solicitações PUT recebidas não têm cabeçalhos de criptografia.

Quando o Amazon S3 criptografa um objeto usando as configurações de criptografia padrão, o log inclui um dos seguintes campos como o par de nome-valor: `"SSEApplied":"Default_SSE_S3"`, `"SSEApplied":"Default_SSE_KMS"` ou `"SSEApplied":"Default_DSSE_KMS"`.

Quando o Amazon S3 criptografa um objeto usando os cabeçalhos de criptografia PUT, o log inclui um dos seguintes campos como par de nome-valor: `"SSEApplied":"SSE_S3"`, `"SSEApplied":"SSE_KMS"`, `"SSEApplied":"DSSE_KMS"` ou `"SSEApplied":"SSE_C"`.

Para multipart uploads, essas informações estão incluídas nas solicitações de operação de API `InitiateMultipartUpload`. Para obter mais informações sobre como usar o CloudTrail e o CloudWatch, consulte Registrar em log e monitorar no Amazon S3.

Perguntas frequentes sobre criptografia padrão

O Amazon S3 agora aplica criptografia do lado do servidor com chaves gerenciadas do Amazon S3 (SSE-S3) como nível básico de criptografia para cada bucket no Amazon S3. Desde 5 de janeiro de 2023, todos os novos uploads de objetos para o Amazon S3 são automaticamente criptografados sem custo adicional e sem impacto na performance. A SSE-S3, que usa criptografia AES-256 (Advanced Encryption Standard de 256 bits), é aplicada automaticamente a todos os novos buckets e a todos os buckets do S3 existentes que ainda não tenham a criptografia padrão configurada. O status de criptografia automática para a configuração de criptografia padrão do bucket do S3 e para novos uploads de objetos está disponível em logs do AWS CloudTrail, no Inventário do S3, na Lente de Armazenamento do S3, no console do Amazon S3 e como cabeçalho adicional de resposta da API do Amazon S3 na AWS Command Line Interface (AWS CLI) e nos AWS SDKs.

As seções a seguir respondem a perguntas sobre essa atualização.

O Amazon S3 altera as configurações de criptografia padrão para meus buckets existentes que já têm a criptografia padrão configurada?

Não. Não há nenhuma alteração na configuração de criptografia padrão para um bucket existente que já tenha a criptografia SSE-S3 ou a criptografia do lado do servidor com chaves do AWS Key Management Service (AWS KMS) (SSE-KMS) configuradas. Para obter mais informações sobre como definir o comportamento de criptografia padrão para buckets, consulte Definir o comportamento padrão da criptografia para os buckets do Amazon S3. Para obter mais informações sobre configurações de criptografia SSE-S3 e SSE-KMS, consulte Proteger os dados usando criptografia do lado do servidor.

A criptografia padrão é ativada em meus buckets existentes que não têm a criptografia padrão configurada?

Sim. O Amazon S3 agora configura a criptografia padrão em todos os buckets não criptografados para aplicar a criptografia do lado do servidor com chaves gerenciadas do S3 (SSE-S3) como o nível

básico de criptografia para novos objetos carregados nesses buckets. Objetos que já estão em um bucket não criptografado existente não serão criptografados automaticamente.

Como posso ver o status de criptografia padrão de novos uploads de objetos?

Atualmente, é possível visualizar o status de criptografia padrão de novos uploads de objetos em logs do AWS CloudTrail, no Inventário do S3, na Lente de Armazenamento do S3, no console do Amazon S3 e como cabeçalho adicional de resposta da API do Amazon S3 na AWS Command Line Interface (AWS CLI) e em AWS SDKs.

- Para ver seus eventos do CloudTrail, consulte Visualizar eventos do CloudTrail no console do CloudTrail no Guia do usuário do AWS CloudTrail. Os logs do CloudTrail fornecem monitoramento de API para solicitações `PUT` e `POST` para o Amazon S3. Quando a criptografia padrão está sendo usada para criptografar objetos nos buckets, os logs do CloudTrail para solicitações de API `PUT` e `POST` incluem o seguinte campo como o par de nome-valor: `"SSEApplied":"Default_SSE_S3"`.
- Para visualizar o status de criptografia automática de novos uploads de objetos no Inventário do S3, configure um relatório do Inventário do S3 para incluir o campo de metadados Encryption (Criptografia), depois veja o status de criptografia de cada novo objeto no relatório. Para obter mais informações, consulte Configurar o Inventário do Amazon S3.
- Para ver o status de criptografia automática de novos uploads de objetos na Lente de Armazenamento do S3, configure um painel da Lente de Armazenamento do S3 e veja as métricas Encrypted bytes (Bytes criptografados) Encrypted object count (Contagem de objetos criptografados) na categoria Data protection (Proteção de dados) do painel. Para obter mais informações, consulte Usar o console do S3 e Exibição das métricas da lente de armazenamento do S3 nos painéis.
- Para ver o status da criptografia automática no nível do bucket no console do Amazon S3, verifique a criptografia padrão dos buckets do Amazon S3 no console do Amazon S3. Para obter mais informações, consulte Configurar a criptografia padrão.
- Para ver o status de criptografia automática como cabeçalho adicional de resposta da API do Amazon S3 na AWS Command Line Interface (AWS CLI) e em AWS SDKs, verifique o cabeçalho de resposta `x-amz-server-side-encryption` ao usar APIs de ação do objeto, como PutObject e GetObject.

O que preciso fazer para aproveitar essa mudança?

Você não precisa fazer nenhuma alteração em suas aplicações existentes. Como a criptografia padrão está habilitada para todos os seus buckets, todos os novos objetos enviados para o Amazon S3 serão criptografados automaticamente.

Posso desativar a criptografia para os novos objetos que serão gravados no meu bucket?

Não. A SSE-S3 é o novo nível básico de criptografia aplicado a todos os novos objetos que são enviados para o bucket. Não é mais possível desativar a criptografia para novos uploads de objetos.

Minhas cobranças serão afetadas?

Não. A criptografia padrão com SSE-S3 está disponível sem nenhum custo adicional. Serão cobrados o armazenamento, as solicitações e outros recursos do S3, como de costume. Para obter informações sobre preços, consulte Definição de preços do Amazon S3.

O Amazon S3 vai criptografar meus objetos existentes que não estão criptografados?

Não. A partir de 5 de janeiro de 2023, o Amazon S3 criptografa automaticamente somente novos uploads de objetos. Para criptografar objetos existentes, você pode usar o recurso Operações em Lote do S3 para criar cópias criptografadas de seus objetos. Essas cópias criptografadas reterão os dados e o nome do objeto existente e serão criptografadas usando as chaves de criptografia que você especificar. Para obter mais detalhes, consulte Criptografia de objetos com o recurso Operações em Lote do Amazon S3 no blog de armazenamento da AWS.

Eu não habilitei a criptografia para meus buckets antes desse lançamento. Preciso mudar a forma como acesso os objetos?

Não. A criptografia padrão com SSE-S3 criptografa automaticamente seus dados à medida que são gravados no Amazon S3 e os descriptografa para você quando os acessa. Não há nenhuma alteração na forma como você acessa objetos que são criptografados automaticamente.

Preciso mudar a forma como acesso meus objetos com criptografia do lado do cliente?

Não. Todos os objetos criptografados do lado do cliente antes de serem carregados no Amazon S3 chegam como objetos de texto cifrado criptografados no Amazon S3. Esses objetos agora terão uma camada adicional de criptografia SSE-S3. Suas workloads que usam objetos criptografados do lado do cliente não exigirão nenhuma alteração nos serviços do cliente ou nas configurações de autorização.

> **Note**
>
> Os usuários da Terraform da HashiCorp que não usam uma versão atualizada do AWS Provider talvez vejam uma mudança inesperada depois de criar buckets do S3 sem nenhuma configuração de criptografia definida pelo cliente. Para evitar esse desvio, atualize sua versão do AWS Provider para Terraform para uma das seguintes versões: qualquer versão 4.x, 3.76.1 ou 2.70.4.

Usar a criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3)

> **Important**
>
> O Amazon S3 agora aplica criptografia do lado do servidor com chaves gerenciadas do Amazon S3 (SSE-S3) como nível básico de criptografia para cada bucket no Amazon S3. Desde 5 de janeiro de 2023, todos os novos uploads de objetos para o Amazon S3 são automaticamente criptografados sem custo adicional e sem impacto na performance. O status de criptografia automática para a configuração de criptografia padrão do bucket do S3 e para novos uploads de objetos está disponível em logs do AWS CloudTrail, no Inventário do S3, na Lente de Armazenamento do S3, no console do Amazon S3 e como cabeçalho adicional de resposta da API do Amazon S3 na AWS Command Line Interface e em AWS SDKs. Para obter mais informações, consulte Perguntas frequentes sobre criptografia padrão.

Todos os uploads de novos objetos para buckets do Amazon S3 são criptografados por padrão com criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3).

A criptografia no lado do servidor protege dados em repouso. O Amazon S3 criptografa cada objeto com uma chave exclusiva. Como uma proteção adicional, ela criptografa a si mesma utilizando uma chave que alterna regularmente. A criptografia do lado do servidor do Amazon S3 usa o Advanced Encryption Standard Galois/Counter Mode (AES-GCM) de 256 bits para criptografar todos os objetos carregados.

Não existem taxas adicionais pelo uso da criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3). Mas, as solicitações de configuração do recurso de criptografia padrão

geram os encargos de solicitação padrão do Amazon S3. Para obter mais informações sobre preços, consulte Preços do Amazon S3.

Se você precisar que os uploads de dados sejam criptografados usando somente chaves gerenciadas pelo Amazon S3, poderá usar a política de bucket a seguir. Por exemplo, a política de bucket a seguir negará permissões para fazer upload de um objeto, a menos que a solicitação não inclua o cabeçalho `x-amz-server-side-encryption` a fim de solicitar criptografia no lado do servidor:

```
{
  "Version": "2012-10-17",
  "Id": "PutObjectPolicy",
  "Statement": [
    {
      "Sid": "DenyObjectsThatAreNotSSES3",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
      "Condition": {
        "StringNotEquals": {
          "s3:x-amz-server-side-encryption": "AES256"
        }
      }
    }
  ]
}
```

> **Note**
>
> A criptografia no lado do servidor criptografa somente os dados de objeto, não os metadados de objeto.

Suporte de API para criptografia do lado do servidor

Todos os buckets do Amazon S3 têm criptografia configurada por padrão e todos os novos objetos que são carregados em um bucket do S3 são automaticamente criptografados em repouso. A criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3) é a configuração de criptografia padrão para todos os buckets no Amazon S3. Para usar um tipo

diferente de criptografia, você pode especificar a criptografia do lado do servidor a ser usada nas solicitações PUT do S3 ou atualizar a configuração de criptografia padrão no bucket de destino.

Se quiser especificar um tipo de criptografia diferente nas solicitações PUT, você pode usar a criptografia do lado do servidor com chaves do AWS Key Management Service (AWS KMS) (SSE-KMS), criptografia de camada dupla do lado do servidor com chaves do AWS KMS (DSSE-KMS) ou criptografia do lado do servidor com chaves fornecidas pelo cliente (SSE-C). Se quiser definir uma configuração de criptografia padrão diferente no bucket de destino, você pode usar SSE-KMS ou DSSE-KMS.

Para ter mais informações sobre a alteração da configuração padrão de criptografia para buckets de uso geral, consulte Configurar a criptografia padrão.

Quando você altera a configuração de criptografia padrão do bucket para SSE-KMS, o tipo de criptografia dos objetos do Amazon S3 existentes no bucket não é alterado. Para alterar o tipo de criptografia de objetos preexistentes depois de atualizar a configuração padrão de criptografia para SSE-KMS, use o recurso Operações em Lote do Amazon S3. Basta fornecer uma lista de objetos ao recurso Operações em Lote do S3 para que ele chame a respectiva operação de API. É possível usar a ação Copiar objetos para copiar objetos existentes, gravando-os de volta no mesmo bucket que os objetos criptografados por SSE-KMS. Um único trabalho do Batch Operations pode realizar a operação especificada em bilhões de objetos. Para ter mais informações, consulte Executar operações de objetos em massa com o Operações em Lote e a publicação How to retroactively encrypt existing objects in Amazon S3 using S3 Inventory, Amazon Athena, and S3 Batch Operations do Blog do AWS Storage.

Para configurar a criptografia do lado do servidor usando as APIs REST de criação de objetos, é necessário fornecer o cabeçalho de solicitação `x-amz-server-side-encryption`. Para obter informações sobre as APIs REST, consulte Uso da API REST.

As APIs do Amazon S3 a seguir são compatíveis com este cabeçalho:

- Operações PUT: especifique o cabeçalho de solicitação ao fazer upload de dados usando a API PUT. Para obter mais informações, consulte Objeto PUT.
- Iniciar upload de várias partes: especifique o cabeçalho na solicitação de inicialização ao fazer upload de objetos grandes usando a operação de API de upload de várias partes. Para obter mais informações, consulte Iniciar Multipart Upload.
- Operações COPY: quando você copia um objeto, tem um objeto de origem e um objeto de destino. Para obter mais informações, consulte Objeto PUT - Copiar.

> **Note**
>
> Ao usar uma operação POST para fazer upload de um objeto, em vez de fornecer o cabeçalho de solicitação, você fornece as mesmas informações nos campos de formulário. Para obter mais informações, consulte Objeto POST.

Os AWS SDKs também fornecem APIs de wrapper que você pode usar para solicitar criptografia no lado do servidor. Você também pode usar o AWS Management Console para fazer upload de objetos e solicitar a criptografia no lado do servidor.

Para obter mais informações gerais, consulte Conceitos do AWS KMS no Guia do desenvolvedor do AWS Key Management Service.

Tópicos

- Especificar a criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3)

Especificar a criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3)

Todos os buckets do Amazon S3 têm criptografia configurada por padrão e todos os novos objetos que são carregados em um bucket do S3 são automaticamente criptografados em repouso. A criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3) é a configuração de criptografia padrão para todos os buckets no Amazon S3. Para usar um tipo diferente de criptografia, você pode especificar a criptografia do lado do servidor a ser usada nas solicitações PUT do S3 ou atualizar a configuração de criptografia padrão no bucket de destino.

Se quiser especificar um tipo de criptografia diferente nas solicitações PUT, você pode usar a criptografia do lado do servidor com chaves do AWS Key Management Service (AWS KMS) (SSE-KMS), criptografia de camada dupla do lado do servidor com chaves do AWS KMS (DSSE-KMS) ou criptografia do lado do servidor com chaves fornecidas pelo cliente (SSE-C). Se quiser definir uma configuração de criptografia padrão diferente no bucket de destino, você pode usar SSE-KMS ou DSSE-KMS.

Para ter mais informações sobre a alteração da configuração padrão de criptografia para buckets de uso geral, consulte Configurar a criptografia padrão.

Quando você altera a configuração de criptografia padrão do bucket para SSE-KMS, o tipo de criptografia dos objetos do Amazon S3 existentes no bucket não é alterado. Para alterar o tipo de

criptografia de objetos preexistentes depois de atualizar a configuração padrão de criptografia para SSE-KMS, use o recurso Operações em Lote do Amazon S3. Basta fornecer uma lista de objetos ao recurso Operações em Lote do S3 para que ele chame a respectiva operação de API. É possível usar a ação Copiar objetos para copiar objetos existentes, gravando-os de volta no mesmo bucket que os objetos criptografados por SSE-KMS. Um único trabalho do Batch Operations pode realizar a operação especificada em bilhões de objetos. Para ter mais informações, consulte Executar operações de objetos em massa com o Operações em Lote e a publicação How to retroactively encrypt existing objects in Amazon S3 using S3 Inventory, Amazon Athena, and S3 Batch Operations do Blog do AWS Storage.

Você pode especificar o SSE-S3 usando o console do S3, APIs REST, AWS SDKs e a AWS Command Line Interface (AWS CLI). Para obter mais informações, consulte Definir o comportamento padrão da criptografia para os buckets do Amazon S3.

Usar o console do S3

Este tópico descreve como definir ou alterar o tipo de criptografia de um objeto usando o AWS Management Console. Ao copiar um objeto usando o console, o Amazon S3 copia o objeto como está. Isso significa que se o objeto de origem é criptografado, o objeto de destino também será criptografado. É possível usar o console para adicionar ou alterar a criptografia para um objeto.

> **Note**
>
> - Você pode alterar a criptografia de um objeto se ele tiver menos de 5 GB. Se o objeto tiver mais de 5 GB, você deve usar a AWS CLI ou SDKs da AWS para alterar a criptografia de um objeto.
> - Para obter uma lista das permissões adicionais necessárias para alterar a criptografia de um objeto, consulte the section called “Permissões obrigatórias para operações de API do S3”. Para ver exemplos das políticas que concedem essas permissões, consulte the section called “Exemplos de políticas baseadas em identidade”.
> - Se você alterar a criptografia de um objeto, um novo objeto será criado para substituir o antigo. Se o versionamento do S3 estiver habilitado, uma nova versão do objeto será criada e o objeto existente se tornará uma versão mais antiga. O perfil que altera a propriedade também se torna o proprietário do novo objeto (ou versão do objeto).

Para alterar a criptografia de um objeto

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação, escolha Buckets e selecione a guia Buckets de uso geral. Acesse o bucket ou pasta do Amazon S3 que contém os objetos que você quer alterar.
3. Marque a caixa de seleção referente aos objetos que você quer alterar.
4. No menu Ações, escolha Editar criptografia no lado do servidor na lista de opções exibida.
5. Role até a seção Criptografia do lado do servidor.
6. Em Configurações de criptografia, escolha Usar configurações de bucket para criptografia padrão ou Substituir configurações de bucket para criptografia padrão.
7. Se você escolher Substituir configurações do bucket para criptografia padrão, defina as configurações de criptografia a seguir.
   - Em Tipo de criptografia, escolha Criptografia do lado do servidor com chaves de criptografia gerenciadas pelo Amazon S3 (SSE-S3). A SSE-S3 usa uma das criptografias de bloco mais fortes: o padrão de criptografia avançada de 256 bits (AES-256) para criptografar cada objeto. Para obter mais informações, consulte Usar a criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3).
8. Em Configurações adicionais de cópia, escolha se você quer Copiar configurações de origem, Não especificar configurações ou Especificar configurações. Copiar configurações de origem é a opção padrão. Se você quiser copiar o objeto somente sem os atributos das configurações de origem, escolha Não especificar configurações. Escolha Especificar configurações para especificar configurações referentes a classes de armazenamento, ACLs, tags de objeto, metadados, criptografia do lado do servidor e somas de verificação adicionais.
9. Escolha Salvar alterações.

> **Note**
>
> Essa ação aplica criptografia a todos os objetos especificados. Ao criptografar pastas, aguarde a conclusão da operação de salvamento antes de adicionar novos objetos à pasta.

Uso da API REST

No momento da criação do objeto (quando você faz upload de um objeto novo ou faz uma cópia de um objeto existente), é possível especificar se deseja que o Amazon S3 criptografe seus dados com as chaves gerenciadas pelo Amazon S3 (SSE-S3) adicionando o cabeçalho `x-amz-server-side-encryption` à solicitação. Defina o valor do cabeçalho como o algoritmo de criptografia `AES256`, que é compatível com o Amazon S3. O Amazon S3 confirma que o objeto foi armazenado com SSE-S3 retornando o cabeçalho de resposta `x-amz-server-side-encryption`.

As seguintes operações de APIs de upload REST aceitam o cabeçalho de solicitação `x-amz-server-side-encryption`.

- Objeto PUT
- Objeto PUT - Copiar
- Objeto POST
- Iniciar multipart upload

Ao fazer upload de objetos grandes usando a operação de API de upload de várias partes, você pode especificar a criptografia do lado do servidor adicionando o cabeçalho `x-amz-server-side-encryption` à solicitação Iniciar upload de várias partes. Ao copiar um objeto existente, independentemente de o objeto de origem ser criptografado ou não, o objeto de destino não é criptografado, a menos que você solicite explicitamente a criptografia do lado do servidor.

Os cabeçalhos de resposta das operações de API REST a seguir retornam o cabeçalho `x-amz-server-side-encryption` quando um objeto é armazenado usando SSE-S3.

- Objeto PUT
- Objeto PUT - Copiar
- Objeto POST
- Iniciar multipart upload
- Carregar parte
- Carregamento de parte: copiar
- Concluir carregamento fracionado
- Objeto Get
- Objeto Head

> **Note**
>
> Não envie cabeçalhos de solicitação de criptografia para solicitações `GET` e `HEAD` se o objeto usa SSE-S3, ou você receberá um erro 400 (Solicitação inválida) de status HTTP.

Uso dos SDKs da AWS

Ao usar AWS SDKs, é possível solicitar que o Amazon S3 use criptografia do lado do servidor com chaves de criptografia gerenciadas pelo Amazon S3 (SSE-S3). Esta seção fornece exemplos de uso dos AWS SDKs em várias linguagens. Para obter informações sobre outros SDKs, consulte Código de exemplo e bibliotecas.

Java

Ao usar o AWS SDK para Java para fazer upload de um objeto, você pode usar SSE-S3 para criptografá-lo. Para solicitar a criptografia no lado do servidor, use a propriedade `ObjectMetadata` da `PutObjectRequest` para configurar o cabeçalho da solicitação `x-amz-server-side-encryption`. Ao chamar o método `putObject()` do `AmazonS3Client`, o Amazon S3 criptografa e salva os dados.

Você também pode solicitar a criptografia SSE-S3 ao fazer upload de objetos com a operação de API de upload de várias partes:

- Ao usar a operação de API de alto nível de upload de várias partes, você usa os métodos `TransferManager` para aplicar criptografia no lado do servidor aos objetos conforme faz upload desses objetos. Você pode usar qualquer um dos métodos de upload que assumem `ObjectMetadata` como um parâmetro. Para obter mais informações, consulte Fazer upload de um objeto usando multipart upload.
- Ao usar a operação de API de upload de várias partes de baixo nível, você especifica a criptografia de servidor ao iniciar o upload de várias partes. Você adiciona a propriedade `ObjectMetadata` chamando o método `InitiateMultipartUploadRequest.setObjectMetadata()`. Para obter mais informações, consulte Usar os AWS SDKs (API de baixo nível).

Você não poderá alterar diretamente o estado de criptografia de um objeto (criptografando um objeto não criptografado ou descriptografando um objeto criptografado). Para alterar o estado de criptografia de um objeto, faça uma cópia do objeto, especificando o estado

desejado de criptografia para a cópia e, em seguida, exclua o objeto original. O Amazon S3 criptografa o objeto copiado somente se você solicitar explicitamente criptografia no lado do servidor. Para solicitar a criptografia do objeto copiado por meio da API Java, use a propriedade `ObjectMetadata` para especificar a criptografia no lado do servidor na `CopyObjectRequest`.

Example Exemplo

O exemplo a seguir mostra como definir a criptografia do lado do servidor usando o AWS SDK para Java. Ele mostra como executar as seguintes tarefas:

- Faça upload de um novo objeto usando SSE-S3.
- Alterar o estado de criptografia de um objeto (neste exemplo, criptografar um objeto anteriormente não criptografado) fazendo uma cópia do objeto.
- Verificar o estado de criptografia do objeto.

Para obter mais informações sobre criptografia no lado do servidor, consulte Uso da API REST. Consulte instruções sobre como criar e testar uma amostra funcional em Getting Started no Guia do desenvolvedor do AWS SDK para Java.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.internal.SSEResultBase;
import com.amazonaws.services.s3.model.*;

import java.io.ByteArrayInputStream;

public class SpecifyServerSideEncryption {

    public static void main(String[] args) {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "*** Bucket name ***";
        String keyNameToEncrypt = "*** Key name for an object to upload and encrypt
 ***";
        String keyNameToCopyAndEncrypt = "*** Key name for an unencrypted object to
 be encrypted by copying ***";
```

```
        String copiedObjectKeyName = "*** Key name for the encrypted copy of the
unencrypted object ***";

        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withRegion(clientRegion)
                    .withCredentials(new ProfileCredentialsProvider())
                    .build();

            // Upload an object and encrypt it with SSE.
            uploadObjectWithSSEEncryption(s3Client, bucketName, keyNameToEncrypt);

            // Upload a new unencrypted object, then change its encryption state
            // to encrypted by making a copy.
            changeSSEEncryptionStatusByCopying(s3Client,
                    bucketName,
                    keyNameToCopyAndEncrypt,
                    copiedObjectKeyName);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }

    private static void uploadObjectWithSSEEncryption(AmazonS3 s3Client, String
bucketName, String keyName) {
        String objectContent = "Test object encrypted with SSE";
        byte[] objectBytes = objectContent.getBytes();

        // Specify server-side encryption.
        ObjectMetadata objectMetadata = new ObjectMetadata();
        objectMetadata.setContentLength(objectBytes.length);

objectMetadata.setSSEAlgorithm(ObjectMetadata.AES_256_SERVER_SIDE_ENCRYPTION);
        PutObjectRequest putRequest = new PutObjectRequest(bucketName,
                keyName,
                new ByteArrayInputStream(objectBytes),
                objectMetadata);
```

```
        // Upload the object and check its encryption status.
        PutObjectResult putResult = s3Client.putObject(putRequest);
        System.out.println("Object \"" + keyName + "\" uploaded with SSE.");
        printEncryptionStatus(putResult);
    }

    private static void changeSSEEncryptionStatusByCopying(AmazonS3 s3Client,
            String bucketName,
            String sourceKey,
            String destKey) {
        // Upload a new, unencrypted object.
        PutObjectResult putResult = s3Client.putObject(bucketName, sourceKey,
"Object example to encrypt by copying");
        System.out.println("Unencrypted object \"" + sourceKey + "\" uploaded.");
        printEncryptionStatus(putResult);

        // Make a copy of the object and use server-side encryption when storing the
        // copy.
        CopyObjectRequest request = new CopyObjectRequest(bucketName,
                sourceKey,
                bucketName,
                destKey);
        ObjectMetadata objectMetadata = new ObjectMetadata();

objectMetadata.setSSEAlgorithm(ObjectMetadata.AES_256_SERVER_SIDE_ENCRYPTION);
        request.setNewObjectMetadata(objectMetadata);

        // Perform the copy operation and display the copy's encryption status.
        CopyObjectResult response = s3Client.copyObject(request);
        System.out.println("Object \"" + destKey + "\" uploaded with SSE.");
        printEncryptionStatus(response);

        // Delete the original, unencrypted object, leaving only the encrypted copy
in
        // Amazon S3.
        s3Client.deleteObject(bucketName, sourceKey);
        System.out.println("Unencrypted object \"" + sourceKey + "\" deleted.");
    }

    private static void printEncryptionStatus(SSEResultBase response) {
        String encryptionStatus = response.getSSEAlgorithm();
        if (encryptionStatus == null) {
            encryptionStatus = "Not encrypted with SSE";
        }
```

```
        System.out.println("Object encryption status is: " + encryptionStatus);
    }
}
```

.NET

Ao fazer upload de um objeto, você pode instruir o Amazon S3 a criptografar esse objeto. Para alterar o estado de criptografia de um objeto existente, faça uma cópia do objeto e exclua o objeto de origem. Por padrão, a operação de cópia criptografa o destino somente se você solicitar explicitamente a criptografia no lado do servidor do objeto de destino. Para especificar a SSE-S3 no `CopyObjectRequest`, adicione o seguinte:

```
ServerSideEncryptionMethod = ServerSideEncryptionMethod.AES256
```

Para obter uma amostra funcional de como copiar um objeto, consulte Uso dos SDKs da AWS.

O exemplo a seguir faz upload de um objeto. Na solicitação, o exemplo instrui o Amazon S3 a criptografar o objeto. O exemplo então recupera metadados do objeto e verifica o método de criptografia que foi usado. Para obter informações sobre como configurar e executar exemplos de código, consulte Conceitos básicos do AWS SDK for .NET no Guia do desenvolvedor do AWS SDK for .NET.

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class SpecifyServerSideEncryptionTest
    {
        private const string bucketName = "*** bucket name ***";
        private const string keyName = "*** key name for object created ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 client;

        public static void Main()
        {
```

```
            client = new AmazonS3Client(bucketRegion);
            WritingAnObjectAsync().Wait();
        }

        static async Task WritingAnObjectAsync()
        {
            try
            {
                var putRequest = new PutObjectRequest
                {
                    BucketName = bucketName,
                    Key = keyName,
                    ContentBody = "sample text",
                    ServerSideEncryptionMethod = ServerSideEncryptionMethod.AES256
                };

                var putResponse = await client.PutObjectAsync(putRequest);

                // Determine the encryption state of an object.
                GetObjectMetadataRequest metadataRequest = new
GetObjectMetadataRequest
                {
                    BucketName = bucketName,
                    Key = keyName
                };
                GetObjectMetadataResponse response = await
client.GetObjectMetadataAsync(metadataRequest);
                ServerSideEncryptionMethod objectEncryption =
response.ServerSideEncryptionMethod;

                Console.WriteLine("Encryption method used: {0}",
objectEncryption.ToString());
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered ***. Message:'{0}' when writing
an object", e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
writing an object", e.Message);
            }
        }
```

```
    }
}
```

PHP

Este tópico mostra como usar classes da versão 3 do AWS SDK para PHP para adicionar SSE-S3 a objetos que você carrega no Amazon S3. Para obter mais informações sobre a API do AWS SDK for Ruby, acesse AWS SDK for Ruby Version 2.

Para fazer upload de um objeto no Amazon S3, use o método Aws\S3\S3Client::putObject(). Para adicionar o cabeçalho de solicitação `x-amz-server-side-encryption` à sua solicitação de upload, especifique o parâmetro `ServerSideEncryption` com o valor `AES256`, conforme exibido no seguinte exemplo de código. Para obter informações sobre solicitações de criptografia no lado do servidor, consulte Uso da API REST.

```
 require 'vendor/autoload.php';

use Aws\S3\S3Client;

$bucket = '*** Your Bucket Name ***';
$keyname = '*** Your Object Key ***';

// $filepath should be an absolute path to a file on disk.
$filepath = '*** Your File Path ***';

$s3 = new S3Client([
    'version' => 'latest',
    'region'  => 'us-east-1'
]);

// Upload a file with server-side encryption.
$result = $s3->putObject([
    'Bucket'               => $bucket,
    'Key'                  => $keyname,
    'SourceFile'           => $filepath,
    'ServerSideEncryption' => 'AES256',
]);
```

Em resposta, o Amazon S3 retorna o cabeçalho `x-amz-server-side-encryption` com o valor do algoritmo de criptografia que foi usado para criptografar os dados de objeto.

Ao fazer upload de objetos grandes usando a operação de API de upload de várias partes, você pode especificar a SSE-S3 para os objetos que estiver carregando, conforme segue:

- Ao usar a operação de API de upload de várias partes de baixo nível, especifique a criptografia do lado do servidor ao chamar o método Aws\S3\S3Client::createMultipartUpload(). Para adicionar o cabeçalho de solicitação `x-amz-server-side-encryption` à sua solicitação, especifique a chave `array` do parâmetro `ServerSideEncryption` com o valor `AES256`. Para obter mais informações sobre a operação de API de upload de várias partes de baixo nível, consulte Usar os AWS SDKs (API de baixo nível).
- Ao usar a operação de API de upload de várias partes de alto nível, especifique a criptografia do lado do servidor usando o parâmetro `ServerSideEncryption` da operação de API CreateMultipartUpload. Para ver um exemplo de uso do método `setOption()` com a operação de API de upload de várias partes de alto nível, consulte Fazer upload de um objeto usando multipart upload.

Para determinar o estado de criptografia de um objeto existente, recupere os metadados de objeto chamando o método Aws\S3\S3Client::headObject() conforme exibido no seguinte exemplo de código PHP.

```
 require 'vendor/autoload.php';

use Aws\S3\S3Client;

$bucket = '*** Your Bucket Name ***';
$keyname = '*** Your Object Key ***';

$s3 = new S3Client([
    'version' => 'latest',
    'region'  => 'us-east-1'
]);

// Check which server-side encryption algorithm is used.
$result = $s3->headObject([
    'Bucket' => $bucket,
    'Key'    => $keyname,
]);
echo $result['ServerSideEncryption'];
```

Para alterar o estado de criptografia de um objeto existente, faça uma cópia do objeto usando o método Aws\S3\S3Client::copyObject() e exclua o objeto de origem. Por padrão, o `copyObject()` não criptografará o destino, a menos que você solicite explicitamente a criptografia do lado do servidor do objeto de destino usando o parâmetro `ServerSideEncryption` com o valor `AES256`. O exemplo de código PHP a seguir faz uma cópia de um objeto e adiciona a criptografia no lado do servidor ao objeto copiado.

```
 require 'vendor/autoload.php';

use Aws\S3\S3Client;

$sourceBucket = '*** Your Source Bucket Name ***';
$sourceKeyname = '*** Your Source Object Key ***';

$targetBucket = '*** Your Target Bucket Name ***';
$targetKeyname = '*** Your Target Object Key ***';

$s3 = new S3Client([
    'version' => 'latest',
    'region'  => 'us-east-1'
]);

// Copy an object and add server-side encryption.
$s3->copyObject([
    'Bucket'               => $targetBucket,
    'Key'                  => $targetKeyname,
    'CopySource'           => "$sourceBucket/$sourceKeyname",
    'ServerSideEncryption' => 'AES256',
]);
```

Para obter mais informações, consulte os tópicos a seguir.

- AWS SDK para PHP for Amazon S3, classe Aws\S3\S3Client
- Documentação do AWS SDK para PHP

Ruby

Ao usar o AWS SDK para Ruby para fazer upload de um objeto, você pode especificar que o objeto seja armazenado criptografado em repouso com a SSE-S3. Ao ler o objeto de volta, ele é descriptografado automaticamente.

O exemplo do AWS SDK para Ruby versão 3 a seguir demonstra como especificar que um arquivo carregado no Amazon S3 seja criptografado em repouso.

```
require 'aws-sdk-s3'

# Wraps Amazon S3 object actions.
class ObjectPutSseWrapper
  attr_reader :object

  # @param object [Aws::S3::Object] An existing Amazon S3 object.
  def initialize(object)
    @object = object
  end

  def put_object_encrypted(object_content, encryption)
    @object.put(body: object_content, server_side_encryption: encryption)
    true
  rescue Aws::Errors::ServiceError => e
    puts "Couldn't put your content to #{object.key}. Here's why: #{e.message}"
    false
  end
end

# Example usage:
def run_demo
  bucket_name = "amzn-s3-demo-bucket"
  object_key = "my-encrypted-content"
  object_content = "This is my super-secret content."
  encryption = "AES256"

  wrapper = ObjectPutSseWrapper.new(Aws::S3::Object.new(bucket_name,
 object_content))
  return unless wrapper.put_object_encrypted(object_content, encryption)

  puts "Put your content into #{bucket_name}:#{object_key} and encrypted it with
 #{encryption}."
end

run_demo if $PROGRAM_NAME == __FILE__
```

O exemplo de código a seguir demonstra como determinar o estado de criptografia de um objeto existente.

```
require 'aws-sdk-s3'

# Wraps Amazon S3 object actions.
class ObjectGetEncryptionWrapper
  attr_reader :object

  # @param object [Aws::S3::Object] An existing Amazon S3 object.
  def initialize(object)
    @object = object
  end

  # Gets the object into memory.
  #
  # @return [Aws::S3::Types::GetObjectOutput, nil] The retrieved object data if
 successful; otherwise nil.
  def object
    @object.get
  rescue Aws::Errors::ServiceError => e
    puts "Couldn't get object #{@object.key}. Here's why: #{e.message}"
  end
end

# Example usage:
def run_demo
  bucket_name = "amzn-s3-demo-bucket"
  object_key = "my-object.txt"

  wrapper = ObjectGetEncryptionWrapper.new(Aws::S3::Object.new(bucket_name,
 object_key))
  obj_data = wrapper.get_object
  return unless obj_data

  encryption = obj_data.server_side_encryption.nil? ? 'no' :
 obj_data.server_side_encryption
  puts "Object #{object_key} uses #{encryption} encryption."
end

run_demo if $PROGRAM_NAME == __FILE__
```

Se a criptografia do lado do servidor não for usada para o objeto que é armazenado no Amazon S3, o método retornará `null`.

Para alterar o estado de criptografia de um objeto existente, faça uma cópia do objeto e exclua o objeto de origem. Por padrão, os métodos de cópia não criptografam o destino, a menos que você solicite explicitamente a criptografia no lado do servidor. Você pode solicitar a criptografia do objeto de destino especificando o valor `server_side_encryption` no argumento de hash de opções conforme mostrado no seguinte exemplo de código Ruby. O exemplo de código demonstra como copiar um objeto e criptografar a cópia com SSE-S3.

```
require 'aws-sdk-s3'

# Wraps Amazon S3 object actions.
class ObjectCopyEncryptWrapper
  attr_reader :source_object

  # @param source_object [Aws::S3::Object] An existing Amazon S3 object. This is
 used as the source object for
  #                                        copy actions.
  def initialize(source_object)
    @source_object = source_object
  end

  # Copy the source object to the specified target bucket, rename it with the target
 key, and encrypt it.
  #
  # @param target_bucket [Aws::S3::Bucket] An existing Amazon S3 bucket where the
 object is copied.
  # @param target_object_key [String] The key to give the copy of the object.
  # @return [Aws::S3::Object, nil] The copied object when successful; otherwise,
 nil.
  def copy_object(target_bucket, target_object_key, encryption)
    @source_object.copy_to(bucket: target_bucket.name, key: target_object_key,
 server_side_encryption: encryption)
    target_bucket.object(target_object_key)
  rescue Aws::Errors::ServiceError => e
    puts "Couldn't copy #{@source_object.key} to #{target_object_key}. Here's why:
 #{e.message}"
  end
end

# Example usage:
def run_demo
  source_bucket_name = "amzn-s3-demo-bucket1"
  source_key = "my-source-file.txt"
  target_bucket_name = "amzn-s3-demo-bucket2"
```

```
  target_key = "my-target-file.txt"
  target_encryption = "AES256"

  source_bucket = Aws::S3::Bucket.new(source_bucket_name)
  wrapper = ObjectCopyEncryptWrapper.new(source_bucket.object(source_key))
  target_bucket = Aws::S3::Bucket.new(target_bucket_name)
  target_object = wrapper.copy_object(target_bucket, target_key, target_encryption)
  return unless target_object

  puts "Copied #{source_key} from #{source_bucket_name} to
 #{target_object.bucket_name}:#{target_object.key} and "\
       "encrypted the target with #{target_object.server_side_encryption}
 encryption."
end

run_demo if $PROGRAM_NAME == __FILE__
```

Como usar o AWS CLI

Para especificar a SSE-S3 ao carregar um objeto usando a AWS CLI, use o exemplo a seguir.

```
aws s3api put-object --bucket amzn-s3-demo-bucket1 --key object-key-name --server-side-
encryption AES256  --body file path
```

Para obter mais informações, consulte put-object na referência da AWS CLI. Para especificar a SSE-S3 ao copiar um objeto usando a AWS CLI, consulte copy-object.

Usar o AWS CloudFormation

Para obter exemplos de configuração de criptografia usando o AWS CloudFormation, consulte os exemplos Criar um bucket com criptografia padrão e Criar um bucket usando criptografia do lado do servidor do AWS KMS com uma Chave de bucket do S3 no tópico `AWS::S3::Bucket ServerSideEncryptionRule` do Guia do usuário do AWS CloudFormation.

Usar criptografia do lado do servidor com o AWS KMS (SSE-KMS)

> **Important**
>
> O Amazon S3 agora aplica criptografia do lado do servidor com chaves gerenciadas do Amazon S3 (SSE-S3) como nível básico de criptografia para cada bucket no Amazon S3.

Desde 5 de janeiro de 2023, todos os novos uploads de objetos para o Amazon S3 são automaticamente criptografados sem custo adicional e sem impacto na performance. O status de criptografia automática para a configuração de criptografia padrão do bucket do S3 e para novos uploads de objetos está disponível em logs do AWS CloudTrail, no Inventário do S3, na Lente de Armazenamento do S3, no console do Amazon S3 e como cabeçalho adicional de resposta da API do Amazon S3 na AWS Command Line Interface e em AWS SDKs. Para obter mais informações, consulte Perguntas frequentes sobre criptografia padrão.

A criptografia do lado do servidor é a criptografia de dados em seu destino pela aplicação ou serviço que os recebe.

O Amazon S3 ativa automaticamente a criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3) para uploads de novos objetos.

A menos que você especifique o contrário, os buckets usam SSE-S3 por padrão para criptografar objetos. No entanto, você pode optar por configurar buckets para usar a criptografia do lado do servidor com chaves do AWS Key Management Service (AWS KMS) (SSE-KMS) em vez disso. Para obter mais informações, consulte Especificando criptografia no lado do servidor com o AWS KMS (SSE-KMS).

O AWS KMS é um serviço que combina hardware e software seguros e altamente disponíveis para fornecer um sistema de gerenciamento de chaves escalado para a nuvem. O Amazon S3 usa criptografia do lado do servidor com AWS KMS (SSE-KMS) para criptografar os dados do objeto do S3. Além disso, quando a SSE-KMS é solicitada para o objeto, a soma de verificação do S3 (como parte dos metadados do objeto) é armazenada em formato criptografado. Para obter mais informações sobre a soma de verificação, consulte Verificar a integridade do objeto no Amazon S3.

Se você usar chaves do KMS, poderá usar o AWS KMS por meio do AWS Management Console ou da API do AWS KMS para fazer o seguinte:

- Criar, visualizar, editar, monitorar, ativar/desativar, rotacionar e programar a exclusão de chaves KMS, tudo de forma centralizada.
- Definir políticas que controlam como e por quem as chaves do KMS podem ser usadas.
- Audite o uso da chave do KMS para verificar se ela está sendo usada corretamente. A auditoria é compatível com a API do AWS KMS, não com o console do AWS KMS.

Os controles de segurança do AWS KMS podem ajudá-lo a satisfazer os requisitos de conformidade relacionados à criptografia. Você pode usar essas chaves do KMS para proteger seus dados em buckets do Amazon S3. Ao usar a criptografia SSE-KMS com um bucket do S3, as AWS KMS keys devem estar na mesma região que o bucket.

Não há custos adicionais por usar o AWS KMS keys. Para obter mais informações, consulte Conceitos de AWS KMS key no Guia do desenvolvedor do AWS Key Management Service e Preços do AWS KMS.

Para obter instruções sobre como permitir que os usuários do IAM acessem os buckets criptografados do KMS, consulte Meu bucket do Amazon S3 tem criptografia padrão usando uma chave personalizada do AWSAWS KMS. Como permitir que os usuários façam download pelo bucket e upload para o bucket? no Centro de Conhecimento do AWS re:Post.

Permissões

Para fazer uma solicitação `PutObject` bem-sucedida para criptografar um objeto com uma chave do AWS KMS ao Amazon S3, você precisa de permissões `kms:GenerateDataKey` na chave. Para fazer download de um objeto criptografado com uma AWS KMS key, você precisa de permissões `kms:Decrypt` para a chave. Para realizar um upload fracionado a fim de criptografar um objeto com uma AWS KMS key, você precisa das permissões `kms:GenerateDataKey` e `kms:Decrypt` para a chave.

> **Important**
>
> Analise cuidadosamente as permissões concedidas em suas políticas de chave do KMS. Restrinja sempre as permissões de política de chave do KMS gerenciada pelo cliente somente às entidades principais do IAM e a serviços da AWS que precisam acessar a ação de chave do AWS KMS pertinente. Para obter mais informações, consulte Usar políticas de chaves no AWS KMS.

Tópicos

- AWS KMS keys
- Amazon S3 Bucket Keys
- Exigir a criptografia no lado do servidor
- Contexto de criptografia

- Enviar solicitações para objetos criptografados do AWS KMS
- Especificando criptografia no lado do servidor com o AWS KMS (SSE-KMS)
- Redução do custo do SSE-KMS com chaves de bucket do Amazon S3

AWS KMS keys

Ao usar criptografia do lado do servidor com o AWS KMS (SSE-KMS), você pode usar a chave gerenciada pela AWS padrão ou especificar uma chave gerenciada pelo cliente que você já tenha criado. O AWS KMS é compatível com criptografia envelopada. O S3 usa os recursos do AWS KMS de criptografia envelopada para proteger ainda mais seus dados. Criptografia envelopada é a prática de criptografar dados de texto simples com uma chave de dados, depois criptografar essa chave de dados com uma chave do KMS. Para ter mais informações sobre a criptografia de envelope, consulte Criptografia de envelope no Guia do desenvolvedor do AWS Key Management Service.

Se você não especificar uma chave gerenciada pelo cliente, o Amazon S3 criará automaticamente uma Chave gerenciada pela AWS em sua Conta da AWS na primeira vez que você adicionar um objeto criptografado com SSE-KMS a um bucket. Por padrão, o Amazon S3 usa essa chave do KMS para SSE-KMS.

> **Note**
>
> Objetos criptografados usando SSE-KMS com Chaves gerenciadas pela AWS não podem ser compartilhados entre contas. Se você precisar replicar dados de SSE-KMS entre contas, será necessário usar uma chave gerenciada pelo cliente do AWS KMS.

Se você quiser usar uma chave gerenciada pelo cliente para SSE-KMS, crie uma chave de criptografia simétrica gerenciada pelo cliente antes de configurar a SSE-KMS. Depois, ao configurar o SSE-KMS para seu bucket, especifique a chave gerenciada pelo cliente existente. Para obter mais informações sobre chaves de criptografia simétrica, consulte Chaves do KMS de criptografia simétrica, no Guia do desenvolvedor do AWS Key Management Service.

A criação de uma chave gerenciada pelo cliente oferece a você mais flexibilidade e controle. Por exemplo, você pode criar, alternar e desabilitar chaves gerenciadas pelo cliente. Você também pode definir controles de acesso e auditar a chave gerenciada pelo cliente que você usa para proteger seus dados. Para obter mais informações sobre chaves gerenciadas pelo cliente e pela AWS, consulte Chaves de clientes e chaves da AWS no Guia do desenvolvedor do AWS Key Management Service.

> **Note**
>
> Ao usar a criptografia do lado do servidor com uma chave gerenciada pelo cliente que é armazenada em um armazenamento de chaves externo, ao contrário das chaves do KMS padrão, você é responsável por garantir a disponibilidade e a durabilidade do seu material de chaves. Para obter mais informações sobre armazenamentos de chaves externos e como eles mudam o modelo de responsabilidade compartilhada, consulte Armazenamentos de chaves externos no Guia do desenvolvedor do AWS Key Management Service.

Usar criptografia SSE-KMS para operações entre contas

Ao utilizar a criptografia para operações entre contas, esteja ciente do seguinte:

- Se o nome do recurso da Amazon (ARN) da AWS KMS key ou alias não for fornecido no momento da solicitação nem por meio da configuração de criptografia padrão do bucket, a Chave gerenciada pela AWS (`aws/s3`) será utilizada.
- Se você estiver fazendo upload ou acessando objetos do S3 usando entidades principais do AWS Identity and Access Management (IAM) que estão na mesma Conta da AWS que a sua chave do KMS, poderá usar a Chave gerenciada pela AWS (`aws/s3`).
- Se quiser conceder acesso entre contas aos seus objetos do S3, use uma chave gerenciada pelo cliente. Você pode configurar a política de uma chave gerenciada pelo cliente para permitir o acesso de outra conta.
- Se estiver especificando uma chave do KMS gerenciada pelo cliente, recomendamos usar um ARN de chave do KMS totalmente qualificado. Se você usar um alias da chave do KMS, o AWS KMS resolverá a chave na conta do solicitante. Isso pode resultar em dados criptografados com uma chave do KMS pertencente ao solicitante, e não ao proprietário do bucket.
- É necessário especificar uma chave para a qual você (o solicitante) recebeu a permissão `Encrypt`. Para ter mais informações, consulte Permitir que os usuários da chave usem uma chave do KMS para operações criptográficas no Guia do desenvolvedor do AWS Key Management Service.

Para ter mais informações sobre quando usar as chaves gerenciadas pelo cliente e as chaves do KMS gerenciadas pela AWS, consulte Devo usar uma Chave gerenciada pela AWS ou uma chave pelo cliente para criptografar meus objetos no Amazon S3?

Fluxo de trabalho de criptografia SSE-KMS

Se você optar por criptografar seus dados usando uma Chave gerenciada pela AWS ou uma chave gerenciada pelo cliente, o AWS KMS e o Amazon S3 realizarão as seguintes ações de criptografia envelopada:

1. O Amazon S3 solicitará uma chave de dados em texto simples e uma cópia da chave criptografada na chave do KMS especificada.
2. O AWS KMS gera uma chave de dados, criptografa-a com a chave do KMS e envia a chave de dados em texto simples e a chave de dados criptografada ao Amazon S3.
3. O Amazon S3 criptografa os dados usando a chave de dados e remove a chave de texto não criptografado da memória assim que possível, após o uso.
4. O Amazon S3 armazena a chave de dados criptografada como metadados com os dados criptografados.

Quando você solicitar que os dados sejam descriptografados, o Amazon S3 e o AWS KMS farão o seguinte:

1. O Amazon S3 envia a chave de dados criptografada ao AWS KMS em uma solicitação `Decrypt`.
2. O AWS KMS descriptografa a chave dos dados criptografados usando a mesma chave do KMS e retorna a chave de dados de texto simples para o Amazon S3.
3. O Amazon S3 descriptografa os dados criptografados usando a chave de dados de texto simples e remove a chave de dados de texto simples da memória o quanto antes.

> **Important**
>
> Ao usar uma AWS KMS key para criptografia no lado do servidor no Amazon S3, você deve escolher uma chave de criptografia do KMS simétrica. O Amazon S3 só é compatível com chaves do KMS de criptografia simétrica. Para obter mais informações sobre essas chaves, consulte Chaves do KMS de criptografia simétrica no Guia do desenvolvedor do AWS Key Management Service.

Auditoria da criptografia SSE-KMS

Para identificar solicitações que especificam SSE-KMS, você pode usar as métricas All SSE-KMS requests (Todas as solicitações de SSE-KMS) e % all SSE-KMS requests (% de todas as

solicitações de SSE-KMS) da Lente de Armazenamento do Amazon S3. A Lente de Armazenamento do S3 é um recurso de análise de armazenamento em nuvem que você pode usar para obter visibilidade em toda a organização sobre o uso e a atividade do armazenamento de objetos. Você também pode usar a contagem de buckets habilitada para SSE-KMS e a porcentagem de buckets habilitados para (SSE-KMS) para a criptografia de bucket padrão. Para obter mais informações, consulte Avaliar a atividade e o uso do armazenamento com o S3 Storage Lens. Para obter uma lista completa de métricas, consulte o Glossário de métricas da Lente de Armazenamento do S3.

Para auditar o uso das chaves do AWS KMS para seus dados criptografados por SSE-KMS, você pode usar logs do AWS CloudTrail. Você pode obter informações sobre suas operações criptográficas, como GenerateDataKey e Decrypt. O CloudTrail oferece suporte a vários valores de atributos para filtrar a pesquisa, como nome do evento, nome de usuário e origem do evento.

Amazon S3 Bucket Keys

Ao configurar a criptografia do lado do servidor usando o AWS KMS (SSE-KMS), você pode configurar os buckets para usar chaves de bucket do S3 para SSE-KMS. Usar uma chave em nível de bucket para SSE-KMS pode reduzir os custos de solicitação do AWS KMS em até 99% ao reduzir o tráfego de solicitação do Amazon S3 para o AWS KMS.

Quando você configura o bucket para usar uma chave de bucket do S3 para SSE-KMS em novos objetos, o AWS KMS gera uma chave no nível de bucket usada para criar chaves de dados exclusivas para objetos no bucket. Essa chave de bucket do S3 é usada por um período limitado no Amazon S3, reduzindo ainda mais a necessidade do Amazon S3 fazer solicitações ao AWS KMS para concluir operações de criptografia. Para obter mais informações sobre como usar Chaves de bucket do S3, consulte Redução do custo do SSE-KMS com chaves de bucket do Amazon S3.

Exigir a criptografia no lado do servidor

Para exigir criptografia do lado do servidor de todos os objetos em um bucket específico do Amazon S3, é possível usar uma política de bucket. Por exemplo, a política de bucket a seguir negará permissão de upload de objeto (`s3:PutObject`) para todos se a solicitação não incluir um cabeçalho `x-amz-server-side-encryption-aws-kms-key-id` que solicita criptografia do lado do servidor com a SSE-KMS.

```
{
   "Version":"2012-10-17",
   "Id":"PutObjectPolicy",
   "Statement":[{
         "Sid":"DenyObjectsThatAreNotSSEKMS",
```

```
         "Effect":"Deny",
         "Principal":"*",
         "Action":"s3:PutObject",
         "Resource":"arn:aws:s3:::amzn-s3-demo-bucket1/*",
         "Condition":{
            "Null":{
               "s3:x-amz-server-side-encryption-aws-kms-key-id":"true"
            }
         }
      }
   ]
}
```

Para exigir que uma AWS KMS key específica seja usada para criptografar os objetos em um bucket, use a chave de condição `s3:x-amz-server-side-encryption-aws-kms-key-id`. Para especificar a chave do KMS, é necessário usar um nome do recurso da Amazon (ARN) da chave no formato `arn:aws:kms:region:acct-id:key/key-id`. O AWS Identity and Access Management não validará se a string para `s3:x-amz-server-side-encryption-aws-kms-key-id` existe.

> **Note**
>
> Ao fazer upload de um objeto, é possível especificar a chave do KMS usando o cabeçalho `x-amz-server-side-encryption-aws-kms-key-id` ou confiar na configuração de criptografia de bucket padrão. Se sua solicitação PutObject especificar `aws:kms` no cabeçalho `x-amz-server-side-encryption`, mas não especificar o cabeçalho `x-amz-server-side-encryption-aws-kms-key-id`, o Amazon S3 presumirá que você deseja usar o Chave gerenciada pela AWS. No entanto, o ID de chave do AWS KMS que o Amazon S3 usa para a criptografia de objeto deve corresponder ao ID de chave do AWS KMS na política. Caso contrário, o Amazon S3 negará a solicitação.

Consulte uma lista completa de chaves de condição específicas do Amazon S3 em Condition keys for Amazon S3 na Referência de autorização do serviço.

Contexto de criptografia

Um contexto de criptografia é um conjunto de pares chave-valor que contém informações contextuais adicionais sobre os dados. O contexto de criptografia não é criptografado. Quando um contexto de

criptografia é especificado para uma operação criptográfica, o Amazon S3 deve especificar o mesmo contexto de criptografia da operação de descriptografia. Caso contrário, a descriptografia falhará. O AWS KMS usa o contexto de criptografia como dados autenticados adicionais (AAD) para oferecer suporte à criptografia autenticada. Para obter mais informações sobre o contexto de criptografia, consulte Contexto de criptografia no Guia do desenvolvedor do AWS Key Management Service.

Por padrão, o Amazon S3 usa o nome do recurso da Amazon (ARN) do objeto ou do bucket como o par de contexto de criptografia:

- Se você usar o SSE-KMS sem habilitar uma chave de bucket do S3, o ARN do objeto será usado como o contexto de criptografia.

```
arn:aws:s3:::object_ARN
```

- Se você usar o SSE-KMS e habilitar uma chave de bucket do S3, o ARN do bucket será usado como o contexto de criptografia. Para obter mais informações sobre chaves de buckets do S3, consulte Redução do custo do SSE-KMS com chaves de bucket do Amazon S3.

```
arn:aws:s3:::bucket_ARN
```

Opcionalmente, você pode fornecer um par de contexto de criptografia adicional usando o cabeçalho `x-amz-server-side-encryption-context` em uma solicitação s3:PutObject. No entanto, como o contexto de criptografia não é criptografado, ele não deve incluir informações sigilosas. O Amazon S3 armazena esse par de chaves adicional junto com o contexto de criptografia padrão. Ao processar sua solicitação PUT, o Amazon S3 acrescenta o contexto de criptografia padrão de `aws:s3:arn` àquele fornecido por você.

É possível usar o contexto de criptografia para identificar e categorizar suas operações de criptografia. Você também pode usar o valor do ARN do contexto de criptografia padrão para rastrear solicitações relevantes no AWS CloudTrail visualizando qual ARN do Amazon S3 foi usado com qual chave de criptografia.

No campo `requestParameters` de um arquivo de log do CloudTrail, o contexto de criptografia é parecido com este.

```
"encryptionContext": {
    "aws:s3:arn": "arn:aws:s3:::amzn-s3-demo-bucket1/file_name"
}
```

Quando você usa o SSE-KMS com o recurso opcional S3 Bucket Keys, o valor do contexto de criptografia é o ARN do bucket.

```
"encryptionContext": {
    "aws:s3:arn": "arn:aws:s3:::amzn-s3-demo-bucket1"
}
```

Enviar solicitações para objetos criptografados do AWS KMS

> **Important**
>
> Todas as solicitações GET e PUT para objetos criptografados do AWS KMS devem ser criadas usando Secure Sockets Layer (SSL) ou Transport Layer Security (TLS). As solicitações também devem ser assinadas usando credenciais válidas, como AWS Signature Version 4 (ou AWS Signature Version 2).

O AWS Signature Version 4 é o processo de adicionar informações de autenticação às solicitações da AWS enviadas por HTTP. Por segurança, a maioria das solicitações para AWS deve ser assinada com uma chave de acesso, que consiste em um ID de chave de acesso e na chave de acesso secreta. Essas duas chaves são comumente conhecidas como suas credenciais de segurança. Para obter mais informações, consulte Autenticação de solicitações (AWS Signature Version 4) e Processo de assinatura do Signature Version 4.

> **Important**
>
> Se o objeto usar SSE-KMS, não envie cabeçalhos de solicitação de criptografia para solicitações GET e solicitações HEAD. Caso contrário, você receberá um erro HTTP 400 Solicitação Inválida.

Tópicos

- Especificando criptografia no lado do servidor com o AWS KMS (SSE-KMS)
- Redução do custo do SSE-KMS com chaves de bucket do Amazon S3

Especificando criptografia no lado do servidor com o AWS KMS (SSE-KMS)

Todos os buckets do Amazon S3 têm criptografia configurada por padrão e todos os novos objetos que são carregados em um bucket do S3 são automaticamente criptografados em repouso. A criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3) é a configuração de criptografia padrão para todos os buckets no Amazon S3. Para usar um tipo diferente de criptografia, você pode especificar a criptografia do lado do servidor a ser usada nas solicitações PUT do S3 ou atualizar a configuração de criptografia padrão no bucket de destino.

Se quiser especificar um tipo de criptografia diferente nas solicitações PUT, você pode usar a criptografia do lado do servidor com chaves do AWS Key Management Service (AWS KMS) (SSE-KMS), criptografia de camada dupla do lado do servidor com chaves do AWS KMS (DSSE-KMS) ou criptografia do lado do servidor com chaves fornecidas pelo cliente (SSE-C). Se quiser definir uma configuração de criptografia padrão diferente no bucket de destino, você pode usar SSE-KMS ou DSSE-KMS.

Para ter mais informações sobre a alteração da configuração padrão de criptografia para buckets de uso geral, consulte Configurar a criptografia padrão.

Quando você altera a configuração de criptografia padrão do bucket para SSE-KMS, o tipo de criptografia dos objetos do Amazon S3 existentes no bucket não é alterado. Para alterar o tipo de criptografia de objetos preexistentes depois de atualizar a configuração padrão de criptografia para SSE-KMS, use o recurso Operações em Lote do Amazon S3. Basta fornecer uma lista de objetos ao recurso Operações em Lote do S3 para que ele chame a respectiva operação de API. É possível usar a ação Copiar objetos para copiar objetos existentes, gravando-os de volta no mesmo bucket que os objetos criptografados por SSE-KMS. Um único trabalho do Batch Operations pode realizar a operação especificada em bilhões de objetos. Para ter mais informações, consulte Executar operações de objetos em massa com o Operações em Lote e a publicação How to retroactively encrypt existing objects in Amazon S3 using S3 Inventory, Amazon Athena, and S3 Batch Operations do Blog do AWS Storage.

Você pode especificar a SSE-KMS usando o console do Amazon S3, operações da API REST, AWS SDKs e a AWS Command Line Interface (AWS CLI). Para obter mais informações, consulte os tópicos a seguir.

> **Note**
>
> Você pode usar uma AWS KMS keys de várias regiões no Amazon S3. No entanto, o Amazon S3 trata no momento as chaves de várias regiões como se fossem chaves de região

única e não usa os recursos de várias regiões da chave. Consulte mais informações em Using multi-Region keys no Guia do desenvolvedor do AWS Key Management Service.

> **Note**
>
> Se quiser usar uma chave do KMS que seja de propriedade de outra conta, você deverá ter permissão para usar a chave. Para obter mais informações sobre permissões entre contas para chaves do KMS, consulte Criar chaves do KMS que outras contas podem usar no Guia do desenvolvedor do AWS Key Management Service.

Usar o console do S3

Este tópico descreve como definir ou alterar o tipo de criptografia de um objeto para usar criptografia do lado do servidor com chaves do AWS Key Management Service (AWS KMS) (SSE-KMS) usando o console do Amazon S3.

> **Note**
>
> - Você pode alterar a criptografia de um objeto se ele tiver menos de 5 GB. Se o objeto tiver mais de 5 GB, você deve usar a AWS CLI ou SDKs da AWS para alterar a criptografia de um objeto.
> - Para obter uma lista das permissões adicionais necessárias para alterar a criptografia de um objeto, consulte the section called “Permissões obrigatórias para operações de API do S3”. Para ver exemplos das políticas que concedem essas permissões, consulte the section called “Exemplos de políticas baseadas em identidade”.
> - Se você alterar a criptografia de um objeto, um novo objeto será criado para substituir o antigo. Se o versionamento do S3 estiver habilitado, uma nova versão do objeto será criada e o objeto existente se tornará uma versão mais antiga. O perfil que altera a propriedade também se torna o proprietário do novo objeto (ou versão do objeto).

Como adicionar ou alterar a criptografia de um objeto

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.

2. No painel de navegação, escolha Buckets e selecione a guia Buckets de uso geral. Acesse o bucket ou pasta do Amazon S3 que contém os objetos que você quer alterar.
3. Marque a caixa de seleção referente aos objetos que você quer alterar.
4. No menu Ações, escolha Editar criptografia no lado do servidor na lista de opções exibida.
5. Role até a seção Criptografia do lado do servidor.
6. Em Configurações de criptografia, escolha Usar configurações de bucket para criptografia padrão ou Substituir configurações de bucket para criptografia padrão.

> **Important**
>
> Se você usar a opção SSE-KMS em sua configuração de criptografia padrão, estará sujeito às cotas de solicitações por segundo (RPS) do AWS KMS. Para obter mais informações sobre as cotas do AWS KMS e como solicitar um aumento de cota, consulte Cotas no Guia do desenvolvedor do AWS Key Management Service.

7. Se você escolher Substituir configurações do bucket para criptografia padrão, defina as configurações de criptografia a seguir.

   a. Em Tipo de criptografia, escolha Criptografia do lado do servidor com chaves do AWS Key Management Service (SSE-KMS).

   b. Em Chave do AWS KMS, realize um dos seguintes procedimentos para escolher sua chave do KMS:

      - Para escolher entre uma lista de chaves do KMS disponíveis, selecione Escolher de sua AWS KMS keys e escolha a chave do KMS na lista de chaves disponíveis.

        As chaves Chave gerenciada pela AWS (`aws/s3`) e as chaves gerenciadas pelo cliente são exibidas nessa lista. Para ter mais informações sobre chaves gerenciadas pelo cliente, consulte Chaves de clientes e chaves da AWS no Guia do desenvolvedor do AWS Key Management Service.
      - Para inserir o ARN da chave do KMS, selecione Inserir ARN da AWS KMS key e insira o ARN da chave do KMS no campo exibido.
      - Para criar uma chave gerenciada pelo cliente no console do AWS KMS, selecione Criar uma chave do KMS.

        Para ter mais informações sobre como criar uma AWS KMS key, consulte Criação de chaves no Guia do desenvolvedor do AWS Key Management Service.

> **Important**
>
> Você só pode usar chaves do KMS disponíveis na mesma Região da AWS que o bucket. O console do Amazon S3 lista somente as primeiras 100 chaves do KMS na mesma região que o bucket. Para usar uma chave do KMS que não esteja listada, você deve inserir o ARN da chave do KMS. Se quiser usar uma chave do KMS que seja de propriedade de outra conta, primeiro você deverá ter permissão para usar a chave e, depois, inserir o ARN da chave do KMS.
>
> O Amazon S3 só é compatível com chaves do KMS de criptografia simétrica, e não com chaves assimétricas do KMS. Para ter mais informações, consulte Identificar chaves do KMS simétricas e assimétricas no Guia do desenvolvedor do AWS Key Management Service.

8. Em Configurações adicionais de cópia, escolha se você quer Copiar configurações de origem, Não especificar configurações ou Especificar configurações. Copiar configurações de origem é a opção padrão. Se você quiser copiar o objeto somente sem os atributos das configurações de origem, escolha Não especificar configurações. Escolha Especificar configurações para especificar configurações referentes a classes de armazenamento, ACLs, tags de objeto, metadados, criptografia do lado do servidor e somas de verificação adicionais.
9. Escolha Salvar alterações.

> **Note**
>
> Essa ação aplica criptografia a todos os objetos especificados. Ao criptografar pastas, aguarde a conclusão da operação de salvamento antes de adicionar novos objetos à pasta.

Uso da API REST

Quando você cria um objeto, ou seja, quando você faz upload de um novo objeto ou copia um objeto existente, é possível especificar a utilização de criptografia do lado do servidor com AWS KMS keys (SSE-KMS) para criptografar os dados. Para fazer isso, adicione o cabeçalho `x-amz-server-side-encryption` à solicitação. Defina o valor do cabeçalho como o algoritmo de criptografia `aws:kms`. O Amazon S3 confirma que o objeto foi armazenado usando SSE-KMS retornando o cabeçalho de resposta `x-amz-server-side-encryption`.

Se você especificar o cabeçalho `x-amz-server-side-encryption` com um valor de `aws:kms`, também poderá usar os seguintes cabeçalhos de solicitação:

- `x-amz-server-side-encryption-aws-kms-key-id`
- `x-amz-server-side-encryption-context`
- `x-amz-server-side-encryption-bucket-key-enabled`

Tópicos

- Operações da API REST do Amazon S3 compatíveis com SSE-KMS
- Contexto de criptografia (x-amz-server-side-encryption-context)
- ID da chave do AWS KMS (x-amz-server-side-encryption-aws-kms-key-id)
- Chaves de bucket do S3 (x-amz-server-side-encryption-aws-bucket-key-enabled)

Operações da API REST do Amazon S3 compatíveis com SSE-KMS

As seguintes operações da API REST aceitam os cabeçalhos de solicitação `x-amz-server-side-encryption`, `x-amz-server-side-encryption-aws-kms-key-id`, e `x-amz-server-side-encryption-context`.

- PutObject: ao carregar dados usando a operação de APIPUT, é possível especificar esses cabeçalhos de solicitação.
- CopyObject: quando você copia um objeto, há um objeto de origem e um objeto de destino. Ao transmitir cabeçalhos de SSE-KMS com a operação `CopyObject`, eles são aplicados somente ao objeto de destino. Ao copiar um objeto existente, independentemente de o objeto de origem ser criptografado ou não, o objeto de destino não é criptografado, a menos que você solicite explicitamente a criptografia do lado do servidor.
- POST Object: ao usar uma operação `POST` para fazer upload de um objeto, em vez dos cabeçalhos de solicitação, você fornece as mesmas informações nos campos de formulário.
- CreateMultipartUpload: ao fazer upload de objetos grandes usando a operação de API de upload multiparte, você pode especificar esses cabeçalhos. Esses cabeçalhos são especificados na solicitação `CreateMultipartUpload`.

Os cabeçalhos de resposta das operações de API REST a seguir retornam o cabeçalho `x-amz-server-side-encryption` quando um objeto é armazenado usando criptografia de servidor.

- PutObject
- CopyObject
- POST Object
- CreateMultipartUpload
- UploadPart
- UploadPartCopy
- CompleteMultipartUpload
- GetObject
- HeadObject

> **Important**
>
> - Todas as solicitações `GET` e `PUT` para um objeto protegido por AWS KMS falharão se elas não forem feitas usando Secure Sockets Layer (SSL), Transport Layer Security (TLS) ou Signature Version 4.
> - Se o objeto usar SSE-KMS, os cabeçalhos de solicitação de criptografia não deverão ser enviados para solicitações `GET` e solicitações `HEAD`,ou um erro HTTP 400 BadRequest será exibido.

Contexto de criptografia (**`x-amz-server-side-encryption-context`**)

Se você especificar `x-amz-server-side-encryption:aws:kms`, a API do Amazon S3 oferece suporte a um contexto de criptografia com o cabeçalho `x-amz-server-side-encryption-context`. Um contexto de criptografia é um conjunto de pares chave-valor que contém informações contextuais adicionais sobre os dados.

O Amazon S3 usa automaticamente o nome do recurso da Amazon (ARN) do objeto ou bucket como o par de contexto de criptografia. Se você usar o SSE-KMS sem habilitar uma chave de bucket do S3, você usará o ARN de objeto como seu contexto de criptografia, por exemplo, `arn:aws:s3:::`*`object_ARN`*. No entanto, se você usar o SSE-KMS e habilitar uma chave de bucket do S3, use o ARN do bucket para o contexto de criptografia, por exemplo, `arn:aws:s3:::`*`bucket_ARN`*.

Você também pode fornecer um par adicional de contexto de criptografia usando o cabeçalho `x-amz-server-side-encryption-context`. No entanto, como o contexto de criptografia não é criptografado, ele não deve incluir informações sigilosas. O Amazon S3 armazena esse par de chaves adicional junto com o contexto de criptografia padrão.

Para obter informações sobre o contexto de criptografia no Amazon S3, consulte Contexto de criptografia. Para obter informações gerais sobre o contexto de criptografia, consulte Conceitos do AWS Key Management Service: contexto de criptografia no Guia do desenvolvedor do AWS Key Management Service.

ID da chave do AWS KMS (**`x-amz-server-side-encryption-aws-kms-key-id`**)

Você pode usar o cabeçalho `x-amz-server-side-encryption-aws-kms-key-id` para especificar o ID da chave gerenciada pelo cliente usada para proteger os dados. Se você especificar o cabeçalho `x-amz-server-side-encryption:aws:kms`, mas não fornecer o cabeçalho `x-amz-server-side-encryption-aws-kms-key-id`, o Amazon S3 usará a Chave gerenciada pela AWS (`aws/s3`) para proteger os dados. Se desejar usar uma chave gerenciada pelo cliente, você deve fornecer o cabeçalho `x-amz-server-side-encryption-aws-kms-key-id` da chave gerenciada pelo cliente.

> **Important**
>
> Ao usar uma AWS KMS key para criptografia no lado do servidor no Amazon S3, você deve escolher uma chave de criptografia do KMS simétrica. O Amazon S3 só é compatível com chaves do KMS de criptografia simétrica. Para obter mais informações sobre essas chaves, consulte Chaves do KMS de criptografia simétrica no Guia do desenvolvedor do AWS Key Management Service.

Chaves de bucket do S3 (**`x-amz-server-side-encryption-aws-bucket-key-enabled`**)

Você pode usar o cabeçalho da solicitação `x-amz-server-side-encryption-aws-bucket-key-enabled` para habilitar ou desabilitar uma chave de bucket do S3 ao nível do objeto. As chaves de bucket do S3 podem reduzir os custos de solicitação do AWS KMS diminuindo o tráfego de solicitação do Amazon S3 para o AWS KMS. Para obter mais informações, consulte Redução do custo do SSE-KMS com chaves de bucket do Amazon S3.

Se você especificar o cabeçalho `x-amz-server-side-encryption:aws:kms`, mas não fornecer o cabeçalho `x-amz-server-side-encryption-aws-bucket-key-enabled`, o objeto usará as

configurações da chave de bucket do S3 para o bucket de destino para criptografar seu objeto. Para obter mais informações, consulte Configurar uma chave de bucket do S3 no nível de objeto.

Usar a AWS CLI

Para usar os exemplos de comandos da AWS CLI a seguir, substitua os *user input placeholders* por suas próprias informações.

Ao fazer upload de um novo objeto ou copiar um objeto existente, ou seja, você pode especificar a utilização de criptografia do lado do servidor com chaves do AWS KMS para criptografar seus dados. Para fazer isso, adicione o cabeçalho `--server-side-encryption aws:kms` à solicitação. Use `--ssekms-key-id` *example-key-id* para adicionar a chave do AWS KMS gerenciada pelo cliente que você criou. Se você especificar `--server-side-encryption aws:kms`, mas não fornecer um ID de chave do AWS KMS, o Amazon S3 usará uma chave gerenciada pela AWS.

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key example-object-key --server-
side-encryption aws:kms --ssekms-key-id example-key-id --body filepath
```

Além disso, você pode ativar ou desativar as chaves de bucket do Amazon S3 nas operações PUT ou COPY adicionando `--bucket-key-enabled` ou `--no-bucket-key-enabled`. As chaves de bucket do Amazon S3 podem reduzir os custos de solicitação do AWS KMS diminuindo o tráfego de solicitação do Amazon S3 para o AWS KMS. Para obter mais informações, consulte Reduzir o custo da SSE-KMS usando chaves de bucket do Amazon S3.

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key example-object-key --server-
side-encryption aws:kms --bucket-key-enabled --body filepath
```

Você pode criptografar um objeto não criptografado para usar a SSE-KMS copiando o objeto de volta no lugar.

```
aws s3api copy-object --bucket amzn-s3-demo-bucket --key example-object-key --
body filepath --bucket amzn-s3-demo-bucket --key example-object-key --sse aws:kms --
sse-kms-key-id example-key-id --body filepath
```

Uso dos SDKs da AWS

Ao usar AWS SDKs, é possível solicitar que o Amazon S3 use AWS KMS keys para criptografia do lado do servidor. Os exemplos a seguir mostram como usar a SSE-KMS com os AWS SDKs para Java e .NET. Para obter informações sobre outros SDKs, consulte Código de exemplo e bibliotecas no Centro do desenvolvedor da AWS.

> **Important**
>
> Ao usar uma AWS KMS key para criptografia no lado do servidor no Amazon S3, você deve escolher uma chave de criptografia do KMS simétrica. O Amazon S3 só é compatível com chaves do KMS de criptografia simétrica. Para obter mais informações sobre essas chaves, consulte Chaves do KMS de criptografia simétrica no Guia do desenvolvedor do AWS Key Management Service.

Operação do **`CopyObject`**

Ao copiar objetos, você adiciona as mesmas propriedades de solicitação (`ServerSideEncryptionMethod` e `ServerSideEncryptionKeyManagementServiceKeyId`) para solicitar ao Amazon S3 que utilize uma AWS KMS key. Para obter mais informações sobre cópia de objetos, consulte Copiar, mover e renomear objetos.

Operação do **`PUT`**

Java

Ao fazer upload de um objeto usando o AWS SDK para Java, você pode solicitar que o Amazon S3 use uma AWS KMS key adicionando a propriedade `SSEAwsKeyManagementParams`, conforme exibido na seguinte solicitação:

```
PutObjectRequest putRequest = new PutObjectRequest(bucketName,
   keyName, file).withSSEAwsKeyManagementParams(new SSEAwsKeyManagementParams());
```

Nesse caso, o Amazon S3 usa a Chave gerenciada pela AWS (`aws/s3`). Para obter mais informações, consulte Usar criptografia do lado do servidor com o AWS KMS (SSE-KMS). Como opção, é possível criar uma chave de criptografia simétrica do KMS e especificar isso na solicitação, conforme mostrado no seguinte exemplo:

```
PutObjectRequest putRequest = new PutObjectRequest(bucketName,
   keyName, file).withSSEAwsKeyManagementParams(new
 SSEAwsKeyManagementParams(keyID));
```

Para obter mais informações sobre como criar chaves gerenciadas pelo cliente, consulte Programação da API do AWS KMS no Guia do desenvolvedor do AWS Key Management Service.

Para ver exemplos de código funcionais de upload de um objeto, consulte os seguintes tópicos. Para usar esses exemplos, é necessário atualizar os exemplos de código e fornecer informações de criptografia, conforme exibido no fragmento de código anterior.

- Para fazer upload de um objeto em uma única operação, consulte Fazer upload de objetos.
- Para uploads multiparte que usam as operações de API de upload multiparte de alto ou baixo nível, consulte Fazer upload de um objeto usando multipart upload.

.NET

Ao fazer upload de um objeto usando o AWS SDK para .NET, você pode solicitar que o Amazon S3 use uma AWS KMS key adicionando a propriedade `ServerSideEncryptionMethod`, conforme exibido na seguinte solicitação:

```
PutObjectRequest putRequest = new PutObjectRequest
 {
     BucketName = amzn-s3-demo-bucket,
     Key = keyName,
     // other properties
     ServerSideEncryptionMethod = ServerSideEncryptionMethod.AWSKMS
 };
```

Nesse caso, o Amazon S3 usa a Chave gerenciada pela AWS. Para obter mais informações, consulte Usar criptografia do lado do servidor com o AWS KMS (SSE-KMS). Como opção, você pode criar sua própria chave de criptografia simétrica do KMS gerenciada pelo cliente e especificar isso na solicitação, conforme mostrado no seguinte exemplo:

```
PutObjectRequest putRequest1 = new PutObjectRequest
{
  BucketName = amzn-s3-demo-bucket,
  Key = keyName,
  // other properties
  ServerSideEncryptionMethod = ServerSideEncryptionMethod.AWSKMS,
  ServerSideEncryptionKeyManagementServiceKeyId = keyId
};
```

Para obter mais informações sobre como criar chaves gerenciadas pelo cliente, consulte Programação da API do AWS KMS no Guia do desenvolvedor do AWS Key Management Service.

Para ver exemplos de código funcionais de upload de um objeto, consulte os seguintes tópicos. Para usar esses exemplos, é necessário atualizar os exemplos de código e fornecer informações de criptografia, conforme exibido no fragmento de código anterior.

- Para fazer upload de um objeto em uma única operação, consulte Fazer upload de objetos.
- Para uploads multiparte que usam as operações de API de upload multiparte de alto ou baixo nível, consulte Fazer upload de um objeto usando multipart upload.

Pre-signed URLs

Java

Ao criar um URL pré-assinado para um objeto criptografado com uma AWS KMS key, você deverá especificar explicitamente o Signature Version 4, conforme mostrado no seguinte exemplo:

```
ClientConfiguration clientConfiguration = new ClientConfiguration();
clientConfiguration.setSignerOverride("AWSS3V4SignerType");
AmazonS3Client s3client = new AmazonS3Client(
        new ProfileCredentialsProvider(), clientConfiguration);
...
```

Para ver um exemplo de código, consulte Compartilhar objetos com URLs pré-assinados.

.NET

Ao criar um URL pré-assinado para um objeto criptografado com uma AWS KMS key, você deverá especificar explicitamente o Signature Version 4, conforme mostrado no seguinte exemplo:

```
AWSConfigs.S3Config.UseSignatureVersion4 = true;
```

Para ver um exemplo de código, consulte Compartilhar objetos com URLs pré-assinados.

Redução do custo do SSE-KMS com chaves de bucket do Amazon S3

As chaves de bucket do Amazon S3 reduzem o custo da criptografia do lado do servidor do Amazon S3 com chaves do AWS Key Management Service (AWS KMS) (SSE-KMS). Usar uma chave no nível de bucket para SSE-KMS pode reduzir os custos de solicitação do AWS KMS em até 99% ao reduzir o tráfego de solicitação do Amazon S3 para o AWS KMS. Com alguns cliques no AWS

Management Console e sem alterações em aplicações do cliente, você pode configurar o bucket para usar uma chave de bucket do S3 para criptografia SSE-KMS em novos objetos.

> **Note**
>
> As chaves de bucket do S3 não comportam criptografia de camada dupla do lado do servidor com chaves do AWS Key Management Service (AWS KMS) (DSSE-KMS).

Chaves de bucket S3 para SSE-KMS

Cargas de trabalho que acessam milhões ou bilhões de objetos criptografados com o SSE-KMS podem gerar grandes volumes de solicitações para o AWS KMS. Quando você usa o SSE-KMS para proteger seus dados sem uma chave de bucket do S3, o Amazon S3 usa uma chave de dados individual do AWS KMS para cada objeto. Nesse caso, o Amazon S3 faz uma chamada para o AWS KMS sempre que uma solicitação é feita contra um objeto criptografado pelo KMS. Para obter informações sobre como o SSE-KMS funciona, consulte Usar criptografia do lado do servidor com o AWS KMS (SSE-KMS).

Quando você configura um bucket para usar uma chave de bucket do S3 para SSE-KMS, a AWS gera uma chave de bucket de curta duração do AWS KMS e a mantém temporariamente no S3. Essa chave de bucket criará chaves de dados para novos objetos durante seu ciclo de vida. As chaves de bucket do S3 são usadas por um período limitado no Amazon S3, reduzindo a necessidade de o Amazon S3 fazer solicitações ao AWS KMS para concluir operações de criptografia. Isso reduz o tráfego do S3 para o AWS KMS, permitindo que você acesse objetos criptografados pelo AWS KMS no Amazon S3 por uma fração do custo anterior.

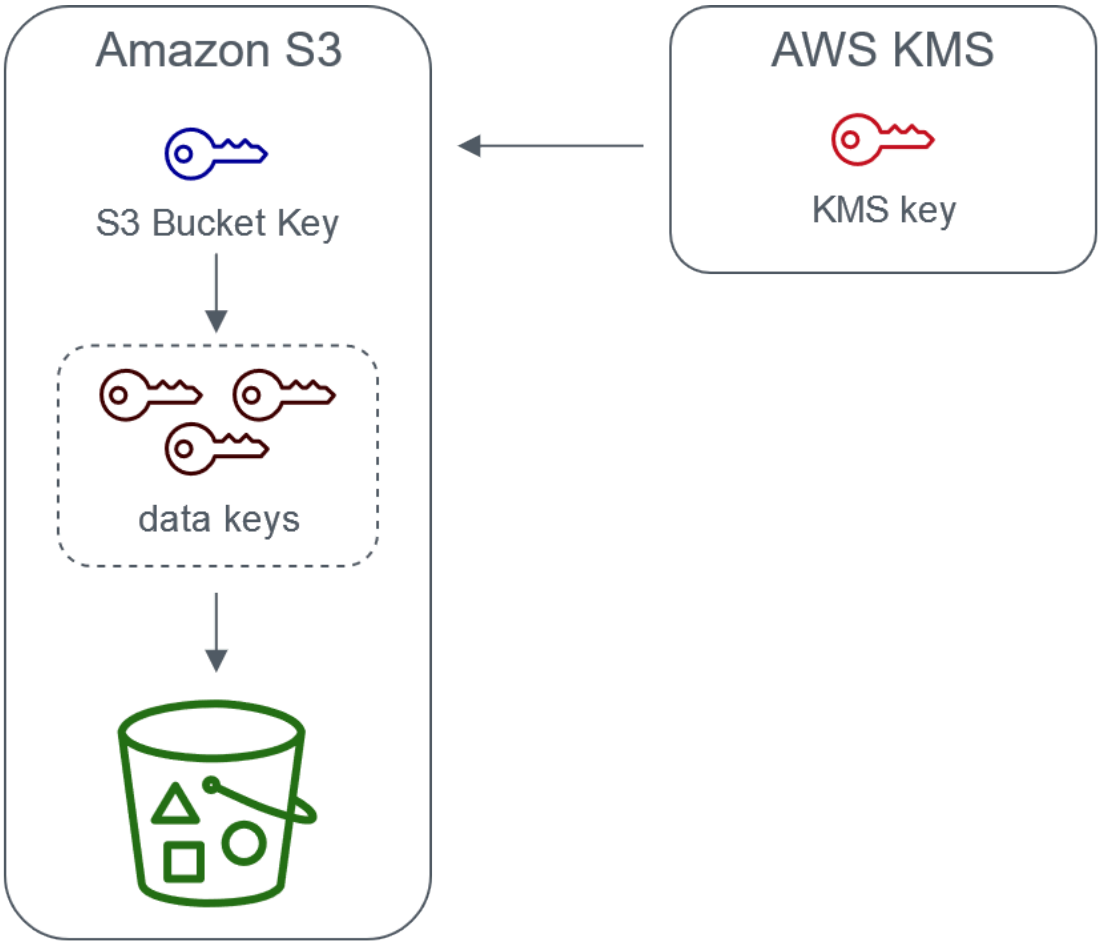
Chaves exclusivas em nível de bucket são buscadas pelo menos uma vez por solicitante para garantir que o acesso do solicitante à chave seja capturado em um evento do CloudTrail no AWS KMS. O Amazon S3 trata os chamadores como solicitantes diferentes quando usam perfis ou contas diferentes, ou o mesmo perfil com políticas de escopo diferentes. A economia de solicitações do AWS KMS reflete o número de solicitantes, os padrões de solicitação e a idade relativa dos objetos solicitados. Por exemplo, um número menor de solicitantes, solicitando vários objetos em um período limitado e criptografados com a mesma chave de bucket, resultará em maior economia.

> **Note**
>
> O uso de chaves de bucket do S3 permite que você reduza os custos de solicitações do AWS KMS ao diminuir as solicitações ao AWS KMS para operações `Encrypt`,

`GenerateDataKey` e `Decrypt` por meio do uso de uma chave em nível de bucket. Por definição, as solicitações subsequentes que aproveitam essa chave em nível de bucket não resultam em solicitações de API do AWS KMS nem validam o acesso em relação à política de chave AWS KMS.

Quando você configura uma chave de bucket do S3, os objetos que já estão no bucket não usam a chave do bucket do S3. Para configurar uma chave de bucket do S3 para objetos existentes, você pode usar uma operação `CopyObject`. Para obter mais informações, consulte Configurar uma chave de bucket do S3 no nível de objeto.

O Amazon S3 compartilhará apenas uma chave de bucket do S3 para objetos criptografados pela mesma AWS KMS key. As chaves de bucket do S3 são compatíveis com chaves do KMS criadas pelo AWS KMS, material de chave importado e material chave baseado em armazenamentos de chaves personalizados.



Server-side encryption with AWS Key Management service using an S3 Bucket Key

Configurando chaves de bucket do S3

Você pode configurar seu bucket para usar uma chave de bucket do S3 para SSE-KMS em novos objetos por meio do console do Amazon S3, dos AWS SDKs, da AWS CLI ou da API REST. Com as chaves de bucket do S3 habilitadas em seu bucket, os objetos carregados com outra chave de SSE-KMS especificada usarão suas próprias chaves de bucket do S3. Independentemente da configuração de chave de bucket do S3, você pode incluir o cabeçalho `x-amz-server-side-encryption-bucket-key-enabled` com um valor `true` ou `false` em sua solicitação para substituir a configuração do bucket.

Antes de configurar seu bucket para usar uma chave de bucket do S3, revise Alterações na observação antes de habilitar uma chave de bucket do S3.

Configuração de uma chave de bucket do S3 usando o console do Amazon S3

Ao criar um novo bucket, você pode configurar seu bucket para usar uma Chave de bucket do S3 para SSE-KMS em novos objetos. Você também pode configurar um bucket existente para usar uma Chave de bucket do S3 para SSE-KMS em novos objetos atualizando suas propriedades do bucket.

Para obter mais informações, consulte Configurando seu bucket para usar uma chave de bucket do S3 com SSE-KMS para novos objetos.

Compatibilidade da API REST, da AWS CLI e do AWS SDK com chaves de bucket do S3

Você pode usar a API REST, a AWS CLI ou o AWS SDK para configurar seu bucket para usar uma chave de bucket do S3 para SSE-KMS em novos objetos. Você também pode habilitar uma chave de bucket do S3 no nível do objeto.

Para obter mais informações, consulte:

- Configurar uma chave de bucket do S3 no nível de objeto
- Configurando seu bucket para usar uma chave de bucket do S3 com SSE-KMS para novos objetos

As seguintes operações de API são compatíveis com chaves de bucket do S3 para SSE-KMS:

- PutBucketEncryption
  - `ServerSideEncryptionRule` aceita o parâmetro `BucketKeyEnabled` para habilitar e desabilitar uma chave de bucket do S3.
- GetBucketEncryption

  - `ServerSideEncryptionRule` retorna as configurações para `BucketKeyEnabled`.
- PutObject, CopyObject, CreateMultipartUpload, e POST Object
  - O cabeçalho de solicitação `x-amz-server-side-encryption-bucket-key-enabled` ativa ou desativa uma chave de bucket do S3 no nível do objeto.
- HeadObject, GetObject, UploadPartCopy, UploadPart e CompleteMultipartUpload
  - O cabeçalho de resposta `x-amz-server-side-encryption-bucket-key-enabled` indica se uma chave de bucket do S3 está ativada ou desativada para um objeto.

Trabalhar com o AWS CloudFormation

No AWS CloudFormation, o recurso `AWS::S3::Bucket` inclui uma propriedade de criptografia chamada `BucketKeyEnabled` que você pode usar para ativar ou desativar uma chave de bucket do S3.

Para obter mais informações, consulte Usar o AWS CloudFormation.

Alterações na observação antes de habilitar uma chave de bucket do S3

Antes de ativar uma chave de bucket do S3, observe as seguintes alterações relacionadas:

Políticas de chave do IAM ou do AWS KMS

Se suas políticas do AWS Identity and Access Management (IAM) ou políticas de chave do AWS KMS usarem seu objeto do nome do recurso da Amazon (ARN) como contexto de criptografia para refinar ou limitar o acesso à chave do KMS, essas políticas não funcionarão com uma chave de bucket do S3. As Chaves de bucket do S3 usam o ARN do bucket como contexto de criptografia. Antes de ativar uma chave de bucket do S3, atualize suas políticas do IAM ou políticas de chave do AWS KMS para usar o ARN do bucket como contexto de criptografia.

Para obter mais informações sobre contexto de criptografia e chaves de bucket do S3, consulte Contexto de criptografia.

Eventos do CloudTrail para o AWS KMS

Depois de habilitar uma chave de bucket do S3, seus eventos do AWS KMS CloudTrail registram em log o ARN do bucket em vez do ARN do objeto. Além disso, você vê menos eventos do KMS CloudTrail para objetos SSE-KMS em seus logs. Como o material de chave tem uma limitação de tempo no Amazon S3, menos solicitações são feitas ao AWS KMS.

Uso de uma chave de bucket do S3 com replicação

Você pode usar chaves de bucket do S3 com SRR (Same-Region Replication, replicação entre regiões) e CRR (Cross-Region Replication, replicação entre regiões).

Quando o Amazon S3 replica um objeto criptografado, ele geralmente preserva as configurações de criptografia do objeto de réplica no bucket de destino. No entanto, se o objeto de origem não for criptografado e seu bucket de destino usar criptografia padrão ou uma chave de bucket do S3, o Amazon S3 criptografa o objeto com a configuração do bucket de destino.

Os exemplos a seguir ilustram como uma chave de bucket do S3 funciona com a replicação. Para obter mais informações, consulte Replicar objetos criptografados (SSE-S3, SSE-KMS, DSSE-KMS, SSE-C).

Example Exemplo 1 – O objeto de origem usa chaves de bucket do S3; o bucket de destino usa criptografia padrão

Se o objeto de origem usa uma Chave de bucket do S3, mas seu bucket de destino usa criptografia padrão com o SSE-KMS, o objeto de réplica manterá suas configurações de criptografia S3 Bucket Key no bucket de destino. O bucket de destino ainda usa criptografia padrão com SSE-KMS.

Example Exemplo 2 – O objeto de origem não é criptografado; o bucket de destino usa uma chave de bucket do S3 com SSE-KMS

Se o objeto de origem não estiver criptografado e o bucket de destino usar uma chave de bucket S3 com SSE-KMS, o objeto de réplica será criptografado usando uma chave de bucket S3 com a SSE-KMS no bucket de destino. Isso faz com que a `ETag` do objeto de origem seja diferente da `ETag` do objeto de réplica. Você precisa atualizar os aplicativos que usam a `ETag` para acomodar essa diferença.

Como trabalhar com chaves de bucket do S3

Para obter mais informações sobre como ativar e trabalhar com chaves de bucket do S3, consulte as seguintes seções:

- Configurando seu bucket para usar uma chave de bucket do S3 com SSE-KMS para novos objetos
- Configurar uma chave de bucket do S3 no nível de objeto
- Visualizar as configurações para uma chave de bucket do S3

Configurando seu bucket para usar uma chave de bucket do S3 com SSE-KMS para novos objetos

Ao configurar a criptografia do lado do servidor com chaves do AWS Key Management Service (AWS KMS) (SSE-KMS), você pode configurar seu bucket para usar uma chave de bucket do S3 para SSE-KMS em novos objetos. As chaves de bucket do S3 diminuem o tráfego de solicitações do Amazon S3 para o AWS KMS e reduzem o custo do SSE-KMS. Para obter mais informações, consulte Redução do custo do SSE-KMS com chaves de bucket do Amazon S3.

Você pode configurar seu bucket para usar uma chave de bucket do S3 para SSE-KMS em novos objetos usando o console do Amazon S3, a API REST, AWS SDKs, a AWS Command Line Interface (AWS CLI) ou o AWS CloudFormation. Se você quiser habilitar ou desabilitar uma chave de bucket do S3 para objetos existentes, poderá usar uma operação `CopyObject`. Para obter mais informações, consulte Configurar uma chave de bucket do S3 no nível de objeto e Usar o Operações em Lote para habilitar chaves de bucket do S3 para SSE-KMS.

Quando uma chave de bucket do S3 estiver habilitada para o bucket de origem ou de destino, o contexto de criptografia será o Amazon Resource Name (ARN) do bucket e não o ARN do objeto, por exemplo, `arn:aws:s3:::`*`bucket_ARN`*. Você precisa atualizar suas políticas do IAM a fim de usar o ARN de bucket para o contexto de criptografia. Para obter mais informações, consulte Chaves de bucket do S3 e replicação.

Os exemplos a seguir ilustram como uma chave de bucket do S3 funciona com a replicação. Para obter mais informações, consulte Replicar objetos criptografados (SSE-S3, SSE-KMS, DSSE-KMS, SSE-C).

Pré-requisitos

Antes de configurar seu bucket para usar uma chave de bucket do S3, revise Alterações na observação antes de habilitar uma chave de bucket do S3.

Uso do console do S3

No console do S3, você pode ativar ou desativar uma chave de bucket do S3 para um bucket novo ou existente. Os objetos no console do S3 herdam sua configuração de chave de bucket do S3 da configuração do bucket. Quando você habilita uma chave de bucket do S3 para seu bucket, novos objetos que você envia para o bucket usam uma chave de bucket do S3 para SSE-KMS.

Carregando, copiando ou modificando objetos em buckets que tenham uma chave de bucket S3 ativada

Se você carregar, modificar ou copiar um objeto em um bucket que tenha uma chave de bucket S3 ativada, as configurações da chave de bucket do S3 para esse objeto poderão ser atualizadas para alinhar com a configuração do bucket.

Se um objeto já tiver uma chave de bucket S3 ativada, as configurações da chave de bucket do S3 para esse objeto não serão alteradas quando você copia ou modifica o objeto. No entanto, se você modificar ou copiar um objeto que não tenha uma chave de bucket S3 ativada e o bucket de destino tiver uma configuração de chave de bucket S3, o objeto herdará as configurações da chave de bucket S3 do bucket de destino. Por exemplo, se o objeto de origem não tiver uma chave de bucket do S3 ativada, mas o bucket de destino tiver a chave de bucket do S3 ativada, uma chave de bucket do S3 será habilitada para o objeto.

Para habilitar uma chave de bucket do S3 ao criar um novo bucket

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets.
3. Selecione Create bucket (Criar bucket).
4. Insira o nome do bucket e escolha sua Região da AWS.
5. Em Criptografia padrão, para Tipo de chave de criptografia, escolha Chave do AWS Key Management Service (SSE-KMS).
6. Em Chave do AWS KMS, realize um dos seguintes procedimentos para escolher sua chave do KMS:

   - Para escolher entre uma lista de chaves do KMS disponíveis, selecione Escolher de sua AWS KMS keys e escolha a chave do KMS na lista de chaves disponíveis.

     As chaves Chave gerenciada pela AWS (`aws/s3`) e as chaves gerenciadas pelo cliente são exibidas nessa lista. Para ter mais informações sobre chaves gerenciadas pelo cliente, consulte Chaves de clientes e chaves da AWS no Guia do desenvolvedor do AWS Key Management Service.
   - Para inserir o ARN da chave do KMS, escolha Inserir ARN da AWS KMS key e insira o ARN da chave do KMS no campo exibido.
   - Para criar uma chave gerenciada pelo cliente no console do AWS KMS, selecione Criar uma chave do KMS.

Para obter mais informações sobre como criar uma AWS KMS key, consulte Criação de chaves no Guia do desenvolvedor do AWS Key Management Service.

7. Em Bucket key (Chave do bucket), escolha Enable (Ativar).
8. Selecione Create bucket (Criar bucket).

   O Amazon S3 cria seu bucket com uma chave de bucket do S3 ativada. Novos objetos que você carregar no bucket usarão uma chave de bucket do S3.

   Para desativar uma chave de bucket do S3, siga as etapas anteriores e escolha Disable (Desativar).

Para habilitar uma chave de bucket do S3 para um bucket existente

1. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets.
3. Na lista Buckets (Buckets), escolha o bucket para o qual você deseja habilitar uma chave de bucket do S3.
4. Escolha a guia Properties (Propriedades).
5. Em Default encryption (Criptografia padrão), escolha Edit (Editar).
6. Em Criptografia padrão, para Tipo de chave de criptografia, escolha Chave do AWS Key Management Service (SSE-KMS).
7. Em Chave do AWS KMS, realize um dos seguintes procedimentos para escolher sua chave do KMS:

   - Para escolher entre uma lista de chaves do KMS disponíveis, selecione Escolher de sua AWS KMS keys e escolha a chave do KMS na lista de chaves disponíveis.

     As chaves Chave gerenciada pela AWS (`aws/s3`) e as chaves gerenciadas pelo cliente são exibidas nessa lista. Para ter mais informações sobre chaves gerenciadas pelo cliente, consulte Chaves de clientes e chaves da AWS no Guia do desenvolvedor do AWS Key Management Service.
   - Para inserir o ARN da chave do KMS, escolha Inserir ARN da AWS KMS key e insira o ARN da chave do KMS no campo exibido.
   - Para criar uma chave gerenciada pelo cliente no console do AWS KMS, selecione Criar uma chave do KMS.

Para obter mais informações sobre como criar uma AWS KMS key, consulte Criação de chaves no Guia do desenvolvedor do AWS Key Management Service.

8. Em Bucket key (Chave do bucket), escolha Enable (Ativar).
9. Selecione Save changes.

O Amazon S3 habilita uma chave de bucket do S3 para novos objetos adicionados ao seu bucket. Os objetos existentes não usam a chave de bucket do S3. Para configurar uma chave de bucket do S3 para objetos existentes, você pode usar uma operação `CopyObject`. Para obter mais informações, consulte Configurar uma chave de bucket do S3 no nível de objeto.

Para desativar uma chave de bucket do S3, siga as etapas anteriores e escolha Disable (Desativar).

Uso dos REST API

Você pode usar PutBucketEncryption para habilitar ou desabilitar uma chave de bucket do S3 para o bucket. Para configurar uma chave de bucket do S3 com `PutBucketEncryption`, use o tipo de dados ServerSideEncryptionRule, que inclui criptografia padrão com SSE-KMS. Você também pode usar opcionalmente uma chave gerenciada pelo cliente especificando o ID da chave do KMS para a chave gerenciada pelo cliente.

Para obter mais informações e sintaxe de exemplo, consulte PutBucketenCryption.

Usar o AWS SDK para Java

O exemplo a seguir habilita a criptografia de bucket padrão com SSE-KMS e uma chave de bucket do S3 usando o AWS SDK para Java.

Java

```
AmazonS3 s3client = AmazonS3ClientBuilder.standard()
    .withRegion(Regions.DEFAULT_REGION)
    .build();

ServerSideEncryptionByDefault serverSideEncryptionByDefault = new
 ServerSideEncryptionByDefault()
    .withSSEAlgorithm(SSEAlgorithm.KMS);
ServerSideEncryptionRule rule = new ServerSideEncryptionRule()
    .withApplyServerSideEncryptionByDefault(serverSideEncryptionByDefault)
```

```
    .withBucketKeyEnabled(true);
ServerSideEncryptionConfiguration serverSideEncryptionConfiguration =
    new ServerSideEncryptionConfiguration().withRules(Collections.singleton(rule));

SetBucketEncryptionRequest setBucketEncryptionRequest = new
 SetBucketEncryptionRequest()
    .withServerSideEncryptionConfiguration(serverSideEncryptionConfiguration)
    .withBucketName(bucketName);

s3client.setBucketEncryption(setBucketEncryptionRequest);
```

Como usar o AWS CLI

O exemplo a seguir habilita a criptografia de bucket padrão com SSE-KMS e uma chave de bucket do S3 usando o AWS CLI. Substitua os *`user input placeholders`* por suas próprias informações.

```
aws s3api put-bucket-encryption --bucket amzn-s3-demo-bucket --server-side-encryption-
configuration '{
        "Rules": [
            {
                "ApplyServerSideEncryptionByDefault": {
                    "SSEAlgorithm": "aws:kms",
                    "KMSMasterKeyID": "KMS-Key-ARN"
                },
                "BucketKeyEnabled": true
            }
        ]
    }'
```

Usar o AWS CloudFormation

Para obter mais informações sobre como configurar uma chave de bucket do S3 com AWS CloudFormation, consulte AWS::S3::Bucket ServerSideEncryptionRule no Guia do usuário do AWS CloudFormation.

Configurar uma chave de bucket do S3 no nível de objeto

Ao executar uma operação PUT ou COPY usando a API REST, os AWS SDKs ou a AWS CLI, você pode habilitar ou desabilitar uma chave de bucket do S3 para o objeto adicionando o cabeçalho de solicitação `x-amz-server-side-encryption-bucket-key-enabled` com um valor `true` ou

`false`. As chaves de bucket do S3 reduzem o custo da criptografia do lado do servidor usando o AWS Key Management Service (AWS KMS) (SSE-KMS), diminuindo assim o tráfego de solicitações do Amazon S3 para o AWS KMS. Para obter mais informações, consulte Redução do custo do SSE-KMS com chaves de bucket do Amazon S3.

Quando você configura uma chave de bucket do S3 para um objeto usando uma operação PUT ou COPY, o Amazon S3 atualiza somente as configurações desse objeto. As configurações da chave de bucket S3 para o bucket de destino não são alteradas. Se você enviar uma solicitação PUT ou COPY para um objeto criptografado pelo KMS em um bucket com as chaves de bucket do S3 habilitadas, suas operações no objeto vão usar automaticamente as chaves de bucket do S3, a menos que você desabilite as chaves no cabeçalho da solicitação. Se você não especificar uma chave de bucket do S3 para seu objeto, o Amazon S3 aplicará as configurações da chave de bucket do S3 para o bucket de destino ao objeto.

Pré-requisito:

Antes de configurar seu objeto para usar uma chave de bucket do S3, revise Alterações na observação antes de habilitar uma chave de bucket do S3.

Tópicos

- Amazon S3 Batch Operations
- Uso da API REST
- Usar o AWSSDK Java (PutObject)
- Como usar a AWS CLI (PutObject)

Amazon S3 Batch Operations

Para criptografar objetos existentes do Amazon S3 com uma única solicitação, você pode usar o Amazon S3 Batch Operations. Você fornece uma lista de objetos às operações em lote do S3 que, por sua vez, chamam a respectiva API para realizar a operação especificada.

É possível usar a operação Copy do S3 Batch Operations para copiar objetos não criptografados existentes e gravá-los de volta no mesmo bucket que os objetos criptografados. Um único trabalho do Batch Operations pode realizar a operação especificada em bilhões de objetos. Para obter mais informações, consulte Executar operações de objetos em massa com o Operações em Lote e Criptografia de objetos existentes com o Amazon S3 Batch Operations.

Uso da API REST

Ao usar a SSE-KMS, você pode habilitar uma chave de bucket do S3 para um objeto usando as seguintes operações de API:

- PutObject — Ao fazer upload de um objeto, você pode especificar o cabeçalho da `x-amz-server-side-encryption-bucket-key-enabled` solicitação para ativar ou desativar uma chave de bucket do S3 no nível do objeto.
- CopyObject (Copiar objeto) — Quando você copia um objeto e configura o SSE-KMS, você pode especificar o cabeçalho da solicitação `x-amz-server-side-encryption-bucket-key-enabled` para ativar ou desativar uma chave de bucket do S3 para seu objeto.
- POST Object: quando você usa uma operação `POST` para fazer upload de um objeto e configurar a SSE-KMS, você pode usar o campo do formulário `x-amz-server-side-encryption-bucket-key-enabled` para ativar ou desativar uma chave de bucket S3 para o objeto.
- CreateMultipartUpload: ao fazer upload de objetos grandes usando a operação de API de `CreateMultipartUpload` e configurar a SSE-KMS, você pode usar o cabeçalho de solicitação `x-amz-server-side-encryption-bucket-key-enabled` para habilitar ou desabilitar uma chave de bucket do S3 para o objeto.

Para habilitar uma chave de bucket do S3 no nível do objeto, inclua o cabeçalho da solicitação `x-amz-server-side-encryption-bucket-key-enabled`. Para obter mais informações sobre o SSE-KMS e a API REST, consulte Uso da API REST.

Usar o AWSSDK Java (PutObject)

Você pode usar o exemplo a seguir para configurar uma chave de bucket do S3 no nível de objeto usando o AWS SDK para Java.

Java

```
AmazonS3 s3client = AmazonS3ClientBuilder.standard()
    .withRegion(Regions.DEFAULT_REGION)
    .build();

String bucketName = "amzn-s3-demo-bucket1";
String keyName = "key name for object";
String contents = "file contents";
```

```
PutObjectRequest putObjectRequest = new PutObjectRequest(bucketName, keyName,
 contents)
    .withBucketKeyEnabled(true);

s3client.putObject(putObjectRequest);
```

Como usar a AWS CLI (PutObject)

Você pode usar o seguinte exemplo da AWS CLI para configurar uma chave de bucket do S3 no nível de objeto como parte de uma solicitação `PutObject`.

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key object key name --server-side-
encryption aws:kms --bucket-key-enabled --body filepath
```

Visualizar as configurações para uma chave de bucket do S3

Você pode visualizar as configurações de uma chave de bucket do S3 no nível de bucket ou objeto usando o console do Amazon S3, a API REST, a AWS Command Line Interface (AWS CLI) ou os AWS SDKs.

As chaves de bucket do S3 diminuem o tráfego de solicitações do Amazon S3 para o AWS KMS e reduzem o custo da criptografia do lado do servidor usando o AWS Key Management Service (SSE-KMS). Para obter mais informações, consulte Redução do custo do SSE-KMS com chaves de bucket do Amazon S3.

Para exibir as configurações da chave de bucket do S3 para um bucket ou um objeto que herdou as configurações da chave de bucket S3 da configuração do bucket, você precisa de permissão para executar a ação `s3:GetEncryptionConfiguration`. Para obter mais informações, consulteGetBucketEncryption na Referência da API do Amazon Simple Storage Service.

Uso do console do S3

No console do S3, você pode visualizar as configurações da chave de bucket do S3 para seu bucket ou objeto. As configurações da chave de bucket do S3 são herdadas da configuração do bucket, a menos que os objetos de origem já tenham uma chave de bucket S3 configurada.

Objetos e pastas no mesmo bucket podem ter configurações diferentes da chave de bucket do S3. Por exemplo, se você fizer upload de um objeto usando a API REST e habilitar uma chave de bucket S3 para o objeto, o objeto manterá sua configuração da chave de bucket de S3 no bucket de destino,

mesmo que a chave de bucket S3 esteja desativada no bucket de destino. Como outro exemplo, se você habilitar uma chave de bucket S3 para um bucket existente, os objetos que já estão no bucket não usarão uma chave de bucket do S3. No entanto, novos objetos têm uma chave de bucket S3 ativada.

Para visualizar a configuração da chave de bucket do S3 para o bucket

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets.
3. Na lista Buckets (Buckets), escolha o bucket para o qual você deseja habilitar uma chave de bucket do S3.
4. Escolha Properties (Propriedades).
5. Na seção Default encryption (Criptografia padrão), em Bucket Key (Chave do bucket), você verá a configuração da chave de bucket do S3 para seu bucket.

   Se você não conseguir ver a configuração da chave de bucket do S3, talvez não tenha permissão para executar a ação `s3:GetEncryptionConfiguration`. Para obter mais informações, consulte GetBucketEncryption na Referência da API do Amazon Simple Storage Service.

Para exibir a configuração da chave de bucket do S3 para seu objeto

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Na lista Buckets (Buckets), escolha o bucket para o qual você deseja habilitar uma chave de bucket do S3.
3. Na lista Objects (Objetos), escolha o nome do objeto.
4. Na guia Details (Detalhes), em Server-side encryption settings (Configurações de criptografia do lado do servidor), escolha Edit (Editar).

   Em Chave de bucket, você vê a configuração da chave de bucket do S3 para o objeto. Você não pode editar essa configuração.

Como usar o AWS CLI

Para retornar as configurações da chave de bucket do S3 no nível de bucket

Para usar esse exemplo, substitua cada *user input placeholder* por suas próprias informações.

```
aws s3api get-bucket-encryption --bucket amzn-s3-demo-bucket1
```

Para obter mais informações, consulte get-bucket-encryption na Referência de comandos da AWS CLI.

Como retornar configurações de chave de bucket do S3 para objetos

Para usar esse exemplo, substitua cada *user input placeholder* por suas próprias informações.

```
aws s3api head-object --bucket amzn-s3-demo-bucket1 --key my_images.tar.bz2
```

Para obter mais informações, consulte head-object na Referência de comandos da AWS CLI.

Uso da API REST

Para retornar as configurações da chave de bucket do S3 no nível de bucket

Para retornar informações de criptografia de um bucket, incluindo configurações para uma chave de bucket do S3, use a operação `GetBucketEncryption`. As configurações da chave de bucket do S3 são retornadas no corpo da resposta no elemento `ServerSideEncryptionConfiguration` com a configuração `BucketKeyEnabled`. Para obter mais informações, consulte GetBucketenCryption na Referência da API do Amazon S3.

Para retornar configurações de nível de objeto para uma chave de bucket do S3

Para retornar o status da chave de bucket S3 para um objeto, use a operação `HeadObject`. O `HeadObject` retorna o cabeçalho de resposta de `x-amz-server-side-encryption-bucket-key-enabled` para mostrar se uma chave de bucket de S3 está ativada ou desativada para o objeto. Para obter mais informações, consulte HeadObject (Objeto do cabeçalho) na Referência da API do Amazon S3.

As seguintes operações de API também retornam o cabeçalho de resposta `x-amz-server-side-encryption-bucket-key-enabled` se uma chave de bucket de S3 estiver configurada para um objeto:

- PutObject

- PostObject
- CopyObject
- CreateMultipartUpload
- UploadPartCopy
- UploadPart
- CompleteMultipartUpload
- GetObject

Usar criptografia de camada dupla do lado do servidor com chaves do AWS KMS (DSSE-KMS)

O uso da criptografia de camada dupla do lado do servidor com chaves do AWS Key Management Service (AWS KMS) (DSSE-KMS) aplica duas camadas de criptografia aos objetos quando eles são carregados no Amazon S3. A DSSE-KMS ajuda a cumprir mais facilmente os padrões de conformidade que exigem que você aplique a criptografia de várias camadas aos dados e tenha controle total das chaves de criptografia.

Ao usar a criptografia DSSE-KMS com um bucket do Amazon S3, as chaves do AWS KMS devem estar na mesma região que o bucket. Além disso, quando a DSSE-KMS é solicitada para o objeto, a soma de verificação do S3 que faz parte dos metadados do objeto é armazenada em formato criptografado. Para ter mais informações sobre somas de verificação, consulte Verificar a integridade do objeto no Amazon S3.

Há custos adicionais para usar a DSSE-KMS e as AWS KMS keys. Para ter mais informações sobre o preço da DSSE-KMS, consulte Conceitos do AWS KMS key no Guia do desenvolvedor do AWS Key Management Service e Preços do AWS KMS.

> **Note**
>
> As chaves de bucket do S3 não comportam DSSE-KMS.

Exigir criptografia de camada dupla do lado do servidor com chaves do AWS KMS keys (DSSE-KMS)

Para exigir criptografia de camada dupla do lado do servidor de todos os objetos em um bucket específico do Amazon S3, é possível usar uma política de bucket. Por exemplo, a política de bucket a seguir negará permissão de carregamento de objeto (`s3:PutObject`) para todos se a solicitação

não incluir um cabeçalho `x-amz-server-side-encryption` que solicita criptografia do lado do servidor com a DSSE-KMS.

```
{
            "Version":"2012-10-17",
            "Id":"PutObjectPolicy",
            "Statement":[{
                  "Sid":"DenyUnEncryptedObjectUploads",
                  "Effect":"Deny",
                  "Principal":"*",
                  "Action":"s3:PutObject",
                  "Resource":"arn:aws:s3:::amzn-s3-demo-bucket/*",
                  "Condition":{
                     "StringNotEquals":{
                        "s3:x-amz-server-side-encryption":"aws:kms:dsse"
                     }
                  }
               }
            ]
         }
```

Tópicos

- Especificar criptografia de camada dupla do lado do servidor com chaves do AWS KMS (DSSE-KMS)

Especificar criptografia de camada dupla do lado do servidor com chaves do AWS KMS (DSSE-KMS)

É possível aplicar criptografia durante o upload de um novo objeto ou ao copiar um objeto existente.

Você pode especificar a DSSE-KMS usando o console do Amazon S3, a API REST do Amazon S3 e a AWS Command Line Interface (AWS CLI). Para obter mais informações, consulte os tópicos a seguir.

> **Note**
>
> Você pode usar uma AWS KMS keys de várias regiões no Amazon S3. No entanto, o Amazon S3 trata no momento as chaves de várias regiões como se fossem chaves de região única e não usa os recursos de várias regiões da chave. Consulte mais informações em Using multi-Region keys no Guia do desenvolvedor do AWS Key Management Service.

> **Note**
>
> Se quiser usar uma chave do KMS que seja de propriedade de outra conta, você deverá ter permissão para usar a chave. Para obter mais informações sobre permissões entre contas para chaves do KMS, consulte Criar chaves do KMS que outras contas podem usar no Guia do desenvolvedor do AWS Key Management Service.

Usar o console do S3

Esta seção descreve como definir ou alterar o tipo de criptografia de um objeto para usar criptografia de camada dupla do lado do servidor com chaves do AWS Key Management Service (AWS KMS) (DSSE-KMS) por meio do console do Amazon S3.

> **Note**
>
> - Você pode alterar a criptografia de um objeto se ele tiver menos de 5 GB. Se o objeto tiver mais de 5 GB, você deve usar a AWS CLI ou SDKs da AWS para alterar a criptografia de um objeto.
> - Para obter uma lista das permissões adicionais necessárias para alterar a criptografia de um objeto, consulte the section called “Permissões obrigatórias para operações de API do S3”. Para ver exemplos das políticas que concedem essas permissões, consulte the section called “Exemplos de políticas baseadas em identidade”.
> - Se você alterar a criptografia de um objeto, um novo objeto será criado para substituir o antigo. Se o versionamento do S3 estiver habilitado, uma nova versão do objeto será criada e o objeto existente se tornará uma versão mais antiga. O perfil que altera a propriedade também se torna o proprietário do novo objeto (ou versão do objeto).

Como adicionar ou alterar a criptografia de um objeto

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação, escolha Buckets e selecione a guia Buckets de uso geral. Acesse o bucket ou pasta do Amazon S3 que contém os objetos que você quer alterar.
3. Marque a caixa de seleção referente aos objetos que você quer alterar.
4. No menu Ações, escolha Editar criptografia no lado do servidor na lista de opções exibida.

5. Role até a seção Criptografia do lado do servidor.
6. Em Configurações de criptografia, escolha Usar configurações de bucket para criptografia padrão ou Substituir configurações de bucket para criptografia padrão.
7. Se você escolher Substituir configurações do bucket para criptografia padrão, defina as configurações de criptografia a seguir.

   a. Em Tipo de criptografia, escolha Criptografia de camada dupla do lado do servidor com chaves do AWS Key Management Service (DSSE-KMS).

   b. Em Chave do AWS KMS, realize um dos seguintes procedimentos para escolher sua chave do KMS:

      - Para escolher entre uma lista de chaves do KMS disponíveis, selecione Escolher de sua AWS KMS keys e escolha a chave do KMS na lista de chaves disponíveis.

        As chaves Chave gerenciada pela AWS (`aws/s3`) e as chaves gerenciadas pelo cliente são exibidas nessa lista. Para ter mais informações sobre chaves gerenciadas pelo cliente, consulte Chaves de clientes e chaves da AWS no Guia do desenvolvedor do AWS Key Management Service.
      - Para inserir o ARN da chave do KMS, selecione Inserir ARN da AWS KMS key e insira o ARN da chave do KMS no campo exibido.
      - Para criar uma chave gerenciada pelo cliente no console do AWS KMS, selecione Criar uma chave do KMS.

        Para ter mais informações sobre como criar uma AWS KMS key, consulte Criação de chaves no Guia do desenvolvedor do AWS Key Management Service.

> **Important**
>
> Você só pode usar chaves do KMS disponíveis na mesma Região da AWS que o bucket. O console do Amazon S3 lista somente as primeiras 100 chaves do KMS na mesma região que o bucket. Para usar uma chave do KMS que não esteja listada, você deve inserir o ARN da chave do KMS. Se quiser usar uma chave do KMS que seja de propriedade de outra conta, primeiro você deverá ter permissão para usar a chave e, depois, inserir o ARN da chave do KMS.
> O Amazon S3 só é compatível com chaves do KMS de criptografia simétrica, e não com chaves assimétricas do KMS. Para ter mais informações, consulte Identificar

chaves do KMS assimétricas no Guia do desenvolvedor do AWS Key Management Service.

8. Para Chave do bucket, escolha Desabilitar. As chaves de bucket do S3 não comportam DSSE-KMS.
9. Em Configurações adicionais de cópia, escolha se você quer Copiar configurações de origem, Não especificar configurações ou Especificar configurações. Copiar configurações de origem é a opção padrão. Se você quiser copiar o objeto somente sem os atributos das configurações de origem, escolha Não especificar configurações. Escolha Especificar configurações para especificar configurações referentes a classes de armazenamento, ACLs, tags de objeto, metadados, criptografia do lado do servidor e somas de verificação adicionais.
10. Escolha Salvar alterações.

> **Note**
>
> Essa ação aplica criptografia a todos os objetos especificados. Ao criptografar pastas, aguarde a conclusão da operação de salvamento antes de adicionar novos objetos à pasta.

Uso da API REST

Quando você cria um objeto, ou seja, quando você carrega um novo objeto ou copia um objeto, é possível especificar a utilização de criptografia de camada dupla do lado do servidor com AWS KMS keys (DSSE-KMS) para criptografar os dados. Para fazer isso, adicione o cabeçalho `x-amz-server-side-encryption` à solicitação. Defina o valor do cabeçalho como o algoritmo de criptografia `aws:kms:dsse`. O Amazon S3 confirma que o objeto foi armazenado com a criptografia DSSE-S3 retornando o cabeçalho de resposta `x-amz-server-side-encryption`.

Se você especificar o cabeçalho `x-amz-server-side-encryption` com um valor de `aws:kms:dsse`, também poderá usar os seguintes cabeçalhos de solicitação:

- `x-amz-server-side-encryption-aws-kms-key-id: SSEKMSKeyId`
- `x-amz-server-side-encryption-context: SSEKMSEncryptionContext`

Tópicos

- Operações da API REST do Amazon S3 compatíveis com DSSE-KMS

- Contexto de criptografia (x-amz-server-side-encryption-context)
- ID da chave do AWS KMS (x-amz-server-side-encryption-aws-kms-key-id)

Operações da API REST do Amazon S3 compatíveis com DSSE-KMS

As seguintes operações da API REST aceitam os cabeçalhos de solicitação `x-amz-server-side-encryption`, `x-amz-server-side-encryption-aws-kms-key-id`, e `x-amz-server-side-encryption-context`.

- PutObject: ao carregar dados usando a operação de APIPUT, é possível especificar esses cabeçalhos de solicitação.
- CopyObject: quando você copia um objeto, há um objeto de origem e um objeto de destino. Ao transmitir cabeçalhos de DSSE-KMS com a operação `CopyObject`, eles são aplicados somente ao objeto de destino. Ao copiar um objeto existente, independentemente de o objeto de origem ser criptografado ou não, o objeto de destino não é criptografado, a menos que você solicite explicitamente a criptografia do lado do servidor.
- Objeto POST: ao usar uma operação `POST` para fazer upload de um objeto, em vez dos cabeçalhos de solicitação, você fornece as mesmas informações nos campos de formulário.
- CreateMultipartUpload: ao carregar objetos grandes usando a operação de API de carregamento fracionado, você pode especificar esses cabeçalhos na solicitação `CreateMultipartUpload`.

Os cabeçalhos de resposta das operações da API REST a seguir retornam o cabeçalho `x-amz-server-side-encryption` quando um objeto é armazenado com criptografia do lado do servidor.

- PutObject
- CopyObject
- Objeto POST
- CreateMultipartUpload
- UploadPart
- UploadPartCopy
- CompleteMultipartUpload
- GetObject
- HeadObject

> **Important**
>
> - Todas as solicitações `GET` e `PUT` para um objeto protegido por AWS KMS falharão se elas não forem feitas usando Secure Sockets Layer (SSL), Transport Layer Security (TLS) ou Signature versão 4.
> - Se o objeto usar DSSE-KMS, os cabeçalhos de solicitação de criptografia não deverão ser enviados para solicitações `GET` e `HEAD`; do contrário, será exibido um erro HTTP 400 (BadRequest).

Contexto de criptografia (**`x-amz-server-side-encryption-context`**)

Se você especificar `x-amz-server-side-encryption:aws:kms:dsse`, a API do Amazon S3 oferece suporte a um contexto de criptografia com o cabeçalho `x-amz-server-side-encryption-context`. Um contexto de criptografia é um conjunto de pares chave-valor que contém informações contextuais adicionais sobre os dados.

O Amazon S3 usa automaticamente o nome do recurso da Amazon (ARN) do objeto como o par de contexto de criptografia, por exemplo `arn:aws:s3:::`*`object_ARN`*.

Você também pode fornecer um par adicional de contexto de criptografia usando o cabeçalho `x-amz-server-side-encryption-context`. No entanto, como o contexto de criptografia não é criptografado, ele não deve incluir informações sigilosas. O Amazon S3 armazena esse par de chaves adicional junto com o contexto de criptografia padrão.

Para obter informações sobre o contexto de criptografia no Amazon S3, consulte Contexto de criptografia. Para obter informações gerais sobre o contexto de criptografia, consulte Conceitos do AWS Key Management Service: contexto de criptografia no Guia do desenvolvedor do AWS Key Management Service.

ID da chave do AWS KMS (**`x-amz-server-side-encryption-aws-kms-key-id`**)

Você pode usar o cabeçalho `x-amz-server-side-encryption-aws-kms-key-id` para especificar o ID da chave gerenciada pelo cliente usada para proteger os dados. Se você especificar o cabeçalho `x-amz-server-side-encryption:aws:kms:dsse`, mas não fornecer o cabeçalho `x-amz-server-side-encryption-aws-kms-key-id`, o Amazon S3 usará a Chave gerenciada pela AWS (`aws/s3`) para proteger os dados. Se desejar usar uma chave gerenciada pelo cliente, você deve fornecer o cabeçalho `x-amz-server-side-encryption-aws-kms-key-id` da chave gerenciada pelo cliente.

> **Important**
>
> Ao usar uma AWS KMS key para criptografia no lado do servidor no Amazon S3, você deve escolher uma chave de criptografia do KMS simétrica. O Amazon S3 só é compatível com chaves do KMS de criptografia simétrica. Para obter mais informações sobre essas chaves, consulte Chaves do KMS de criptografia simétrica no Guia do desenvolvedor do AWS Key Management Service.

Como usar o AWS CLI

Ao carregar um novo objeto ou copiar um objeto, é possível especificar a utilização de criptografia de DSSE-KMS para criptografar os dados. Para isso, adicione o parâmetro `--server-side-encryption aws:kms:dsse` à solicitação. Use o parâmetro `--ssekms-key-id` *`example-key-id`* para adicionar a chave do AWS KMS gerenciada pelo cliente que você criou. Se você especificar `--server-side-encryption aws:kms:dsse`, mas não fornecer um ID de chave do AWS KMS, o Amazon S3 usará a chave gerenciada pela AWS (`aws/s3`).

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key example-object-key --server-
side-encryption aws:kms:dsse --ssekms-key-id example-key-id --body filepath
```

Você pode criptografar um objeto não criptografado para usar a DSSE-KMS copiando o objeto de volta no lugar.

```
aws s3api copy-object --bucket amzn-s3-demo-bucket --key example-object-key --copy-
source amzn-s3-demo-bucket/example-object-key --server-side-encryption aws:kms:dsse --
ssekms-key-id example-key-id
```

Como usar criptografia do lado do servidor com chaves fornecidas pelo cliente (SSE-C)

A criptografia de servidor envolve a proteção de dados em repouso. A criptografia no lado do servidor criptografa somente os dados de objeto, não os metadados de objeto. Ao usar a criptografia do lado do servidor com chaves fornecidas pelo cliente (SSE-C), você pode armazenar dados criptografados com suas próprias chaves de criptografia. Com a chave de criptografia que você fornece como parte de sua solicitação, o Amazon S3 gerencia a criptografia de dados ao gravar em discos, e a descriptografia dos dados quando você acessa seus objetos. Portanto, você não precisa manter

um código para executar a criptografia e a descriptografia de dados. A única coisa que você precisa fazer é gerenciar as chaves de criptografia fornecidas.

Quando você faz upload de um objeto, o Amazon S3 usa a chave de criptografia fornecida para aplicar a criptografia AES-256 aos seus dados. Depois, o Amazon S3 remove a chave de criptografia da memória. Quando você recupera um objeto, deve fornecer a mesma chave de criptografia como parte de sua solicitação. O Amazon S3 primeiro verifica se a chave de criptografia fornecida é correspondente, depois decifra o objeto antes de retornar os dados de objeto.

Não há cobranças adicionais pelo uso de SSE-C. No entanto, as solicitações para configurar e usar SSE-C incorrem em cobranças padrão de solicitação do Amazon S3. Para obter mais informações sobre preços, consulte Preços do Amazon S3.

> **Note**
>
> O Amazon S3 não armazena a chave de criptografia que você fornece. Em vez disso, ele armazena um valor de código de autenticação de mensagens por hash (HMAC) com salt aleatório da chave de criptografia para validar solicitações futuras. O valor de HMAC com salt não pode ser usado para derivar o valor da chave de criptografia ou para decifrar o conteúdo do objeto criptografado. Isso significa que, se você perder a chave de criptografia, perderá o objeto.

A replicação do S3 oferece suporte a objetos que são criptografados com SSE-C. Para obter mais informações sobre replicação de objetos criptografados, consulte the section called “Replicar objetos criptografados”.

Para obter mais informações sobre SSE-C, consulte os tópicos a seguir.

Tópicos

- Visão geral do SSE-C
- Exigência e restrição de SSE-C
- Pre-signed URLs e SSE-C
- Especificação de criptografia no lado do servidor com chaves fornecidas pelo cliente (SSE-C).

Visão geral do SSE-C

Esta seção fornece uma visão geral da SSE-C. Ao usar SSE-C, tenha as seguintes considerações em mente:

- Você deve usar HTTPS.

  > **Important**
  >
  > O Amazon S3 rejeitará todas as solicitações feitas por HTTP ao usar SSE-C. Por questões de segurança, recomendamos considerar que todas as chaves enviadas erroneamente por HTTP estão comprometidas. Descarte a chave e alterne conforme apropriado.

- A etiqueta de entidade (ETag) na resposta não é o hash MD5 dos dados de objeto.
- Você gerencia um mapeamento cuja chave de criptografia foi usada para criptografar objetos. O Amazon S3 não armazena chaves de criptografia. Você é responsável por acompanhar a chave de criptografia que forneceu para um objeto.
  - Se seu bucket tiver versionamento habilitado, cada versão de objeto carregada usando esse recurso poderá ter sua própria chave de criptografia. Você é responsável por acompanhar a chave de criptografia usada para uma versão de objeto.
  - Como gerencia chaves de criptografia no lado do cliente, você gerencia todas as proteções adicionais, como a alternância de chave, no lado do cliente.

  > **Warning**
  >
  > Se você perder a chave de criptografia, qualquer solicitação `GET` de um objeto sem chave de criptografia falhará e você perderá o objeto.

Exigência e restrição de SSE-C

Para exigir SSE-C de todos os objetos em um bucket específico do Amazon S3, use uma política de bucket.

Por exemplo, a política de bucket a seguir nega permissões para upload de objeto (`s3:PutObject`) a todas as solicitações que não incluam o cabeçalho `x-amz-server-side-encryption-customer-algorithm` que solicita SSE-C.

```
{
```

```
    "Version": "2012-10-17",
    "Id": "PutObjectPolicy",
    "Statement": [
        {
            "Sid": "RequireSSECObjectUploads",
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
            "Condition": {
                "Null": {
                    "s3:x-amz-server-side-encryption-customer-algorithm": "true"
                }
            }
        }
    ]
}
```

Você também pode usar uma política para restringir a criptografia do lado do servidor de todos os objetos em um bucket específico do Amazon S3. Por exemplo, a política de bucket a seguir nega permissão de upload de objeto (`s3:PutObject`) para todos se a solicitação inclui o cabeçalho `x-amz-server-side-encryption-customer-algorithm` solicitando SSE-C.

```
{
    "Version": "2012-10-17",
    "Id": "PutObjectPolicy",
    "Statement": [
        {
            "Sid": "RestrictSSECObjectUploads",
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
            "Condition": {
                "Null": {
                    "s3:x-amz-server-side-encryption-customer-algorithm": "false"
                }
            }
        }
    ]
}
```

> **Important**
>
> Se você usar uma política de bucket para exigir SSE-C em `s3:PutObject`, deverá incluir o cabeçalho `x-amz-server-side-encryption-customer-algorithm` em todas as solicitações de carregamento fracionado (CreateMultipartUpload, UploadPart e CompleteMultipartUpload).

Pre-signed URLs e SSE-C

Você pode gerar um URL pré-assinado que pode ser usado para operações, como fazer upload de um objeto novo, recuperar um objeto existente ou recuperar metadados de objeto. Os URLs pré-assinados oferecem suporte a SSE-C da seguinte maneira:

- Ao criar um URL pré-assinado, você deve especificar o algoritmo usando o cabeçalho `x-amz-server-side-encryption-customer-algorithm` no cálculo de assinatura.
- Ao usar o URL pré-assinado para fazer upload de um objeto novo, recuperar um objeto existente ou recuperar somente metadados de objeto, você deve fornecer todos os cabeçalhos de criptografia na solicitação de aplicação cliente.

> **Note**
>
> Para objetos que não usam SSE-C, é possível gerar um URL pré-assinado e colá-lo diretamente em um navegador para acessar os dados.
> No entanto, não é possível fazer isso para objetos SSE-C porque, além do URL pré-assinado, você também precisa incluir cabeçalhos HTTP específicos para objetos SSE-C. Dessa forma, é possível usar URLs pré-assinados para objetos SSE-C somente de maneira programática.

Para obter mais informações sobre pre-signed URLs, consulte the section called “Usar URLs pré-assinados para baixar e fazer upload de objetos”.

Especificação de criptografia no lado do servidor com chaves fornecidas pelo cliente (SSE-C).

No momento da criação do objeto com a API REST, você pode especificar a criptografia do lado do servidor com chaves fornecidas pelo cliente (SSE-C). Ao usar o SSE-C, você deve fornecer informações da chave de encriptação utilizando os cabeçalhos de pedido a seguir.

Nome	Descrição
`x-amz-server-side-encryption-customer-algorithm`	Use esse cabeçalho para especificar o algoritmo de criptografia. O valor do cabeçalho deve ser `AES256`.
`x-amz-server-side-encryption-customer-key`	Use esse cabeçalho para fornecer a chave de criptografia com codificação base64 de 256 bits para o Amazon S3 a ser usada para criptografar ou descriptografar seus dados.
`x-amz-server-side-encryption-customer-key-MD5`	Use esse cabeçalho para fornecer o resumo MD5 com codificação base64 de 128 bits da chave de criptografia de acordo com RFC 1321. O Amazon S3 usa esse cabeçalho para fazer uma verificação de integridade de mensagens e conferir se a chave de criptografia foi transmitida sem erros.

Você pode usar bibliotecas de wrapper do AWS SDK para adicionar esses cabeçalhos à sua solicitação. Se precisar, você pode fazer com que a API REST do Amazon S3 seja chamada diretamente na aplicação.

> **Note**
>
> Não é possível usar o console do Amazon S3 para fazer upload de um objeto e solicitar SSE-C. Também não é possível usar o console para atualizar (por exemplo, alterar a classe de armazenamento ou adicionar metadados) um objeto armazenado com o SSE-C.

Uso da API REST

APIs REST do Amazon S3 que oferecem suporte ao SSE-C

As APIs do Amazon S3 a seguir oferecem suporte à criptografia pelo servidor com chaves de criptografia fornecidas pelo cliente (SSE-C).

- Operação GET: ao recuperar objetos usando a API GET (consulte GET Object), você pode especificar os cabeçalhos da solicitação.

- Operação HEAD: para recuperar metadados de objeto usando a API HEAD (consulte HEAD Object), você pode especificar esses cabeçalhos de solicitação.
- Operação PUT: ao fazer upload de dados usando a API PUT (consulte PUT Object), você pode especificar esses cabeçalhos de solicitação.
- Carregamento fracionado: ao fazer upload de objetos grandes usando a API de carregamentos fracionados, você pode especificar esses cabeçalhos. Especifique esses cabeçalhos na solicitação de inicialização (consulte Iniciar carregamento fracionado) e em cada solicitação de upload de parte subsequente (consulte Fazer upload de parte ou Fazer upload de parte: cópia). Para cada solicitação de upload de parte, as informações de criptografia devem ser as mesmas que você forneceu na solicitação iniciada do multipart upload.
- Operação POST: ao usar uma operação POST para fazer upload de um objeto (consulte Objeto POST), em vez dos cabeçalhos de solicitação, você fornece as mesmas informações nos campos de formulário.
- Operação de cópia: quando você copia um objeto (consulte Objeto PUT - Copiar), tem um objeto de origem e um objeto de destino.
  - Se você quiser que o objeto de destino seja criptografado usando criptografia de servidor com chaves gerenciadas pela AWS, forneça o cabeçalho de solicitação `x-amz-server-side-encryption`.
  - Se você quiser que o objeto de destino seja criptografado usando SSE-C, forneça informações de criptografia usando os três cabeçalhos descritos na tabela anterior.
  - Se o objeto de origem for criptografado usando SSE-C, você deverá fornecer informações de chave de criptografia usando os seguintes cabeçalhos para que o Amazon S3 possa descriptografar o objeto para cópia.

Nome	Descrição
`x-amz-copy-source-server-side-encryption-customer-algorithm`	Inclua esse cabeçalho para especificar o algoritmo que o Amazon S3 deve usar para decifrar o objeto de origem. Esse valor deve ser `AES256`.
`x-amz-copy-source-server-s`	Inclua esse cabeçalho para fornecer a chave de criptografia com codificação base64 para o Amazon S3 a ser usada para descripto grafar o objeto de origem. Essa chave de criptografia deve ser

Nome	Descrição
`ide-encryption-customer-key`	a que você forneceu ao Amazon S3 quando criou o objeto de origem. Caso contrário, o Amazon S3 não pode descriptografar o objeto.
`x-amz-copy-source-server-side-encryption-customer-key-MD5`	Inclua esse cabeçalho para fornecer o resumo MD5 com codificação base64 de 128 bits da chave de criptografia, de acordo com RFC 1321.

Uso dos AWS SDKs para especificar SSE-C para operações PUT, GET, Head e Copy

O exemplo a seguir mostra como solicitar a criptografia de servidor com chaves fornecidas pelo cliente (SSE-C) para objetos. Os exemplos executam as seguintes operações. Cada operação mostra como especificar cabeçalhos relacionados a SSE-C na solicitação:

- Colocar objeto: faz upload de um objeto e solicita a criptografia de servidor, usando uma chave de criptografia fornecida pelo cliente.
- Obter objeto: faz download do objeto carregado na etapa anterior. Na solicitação, você fornece as mesmas informações de criptografia fornecidas quando o objeto foi carregado. O Amazon S3 precisa dessas informações para descriptografar o objeto e para que ele possa ser devolvido a você.
- Obter metadados do objeto: recupera os metadados do objeto. Você fornece as mesmas informações de criptografia usadas quando o objeto foi criado.
- Copiar objeto: faz uma cópia de um objeto carregado anteriormente. Como o objeto de origem é armazenado usando SSE-C, você deve fornecer suas informações de criptografia na solicitação de cópia. Por padrão, o Amazon S3 criptografa a cópia do objeto somente se você solicitar explicitamente. Esse exemplo direciona o Amazon S3 a armazenar uma cópia criptografada do objeto.

Java

> **Note**
>
> Este exemplo mostra como fazer upload de um objeto em uma única operação. Ao usar a API de Multipart Upload para fazer upload de objetos grandes, você fornece informações de criptografia da mesma maneira que exibidas nesse exemplo. Para exemplos de carregamentos fracionados usando o AWS SDK para Java, consulte Fazer upload de um objeto usando multipart upload.

Para adicionar informações necessárias de criptografia, inclua uma `SSECustomerKey` na solicitação. Para obter mais informações sobre a classe `SSECustomerKey`, consulte a seção REST API.

Para obter informações sobre SSE-C, consulte Como usar criptografia do lado do servidor com chaves fornecidas pelo cliente (SSE-C). Consulte instruções sobre como criar e testar uma amostra funcional em Getting Started no Guia do desenvolvedor do AWS SDK para Java.

Example

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.*;

import javax.crypto.KeyGenerator;
import java.io.BufferedReader;
import java.io.File;
import java.io.IOException;
import java.io.InputStreamReader;
import java.security.NoSuchAlgorithmException;
import java.security.SecureRandom;

public class ServerSideEncryptionUsingClientSideEncryptionKey {
    private static SSECustomerKey SSE_KEY;
    private static AmazonS3 S3_CLIENT;
    private static KeyGenerator KEY_GENERATOR;
```

```
   public static void main(String[] args) throws IOException,
NoSuchAlgorithmException {
       Regions clientRegion = Regions.DEFAULT_REGION;
       String bucketName = "*** Bucket name ***";
       String keyName = "*** Key name ***";
       String uploadFileName = "*** File path ***";
       String targetKeyName = "*** Target key name ***";

       // Create an encryption key.
       KEY_GENERATOR = KeyGenerator.getInstance("AES");
       KEY_GENERATOR.init(256, new SecureRandom());
       SSE_KEY = new SSECustomerKey(KEY_GENERATOR.generateKey());

       try {
           S3_CLIENT = AmazonS3ClientBuilder.standard()
                   .withCredentials(new ProfileCredentialsProvider())
                   .withRegion(clientRegion)
                   .build();

           // Upload an object.
           uploadObject(bucketName, keyName, new File(uploadFileName));

           // Download the object.
           downloadObject(bucketName, keyName);

           // Verify that the object is properly encrypted by attempting to
retrieve it
           // using the encryption key.
           retrieveObjectMetadata(bucketName, keyName);

           // Copy the object into a new object that also uses SSE-C.
           copyObject(bucketName, keyName, targetKeyName);
       } catch (AmazonServiceException e) {
           // The call was transmitted successfully, but Amazon S3 couldn't process
           // it, so it returned an error response.
           e.printStackTrace();
       } catch (SdkClientException e) {
           // Amazon S3 couldn't be contacted for a response, or the client
           // couldn't parse the response from Amazon S3.
           e.printStackTrace();
       }
   }
```

```
   private static void uploadObject(String bucketName, String keyName, File file) {
       PutObjectRequest putRequest = new PutObjectRequest(bucketName, keyName,
file).withSSECustomerKey(SSE_KEY);
       S3_CLIENT.putObject(putRequest);
       System.out.println("Object uploaded");
   }

   private static void downloadObject(String bucketName, String keyName) throws
IOException {
       GetObjectRequest getObjectRequest = new GetObjectRequest(bucketName,
keyName).withSSECustomerKey(SSE_KEY);
       S3Object object = S3_CLIENT.getObject(getObjectRequest);

       System.out.println("Object content: ");
       displayTextInputStream(object.getObjectContent());
   }

   private static void retrieveObjectMetadata(String bucketName, String keyName) {
       GetObjectMetadataRequest getMetadataRequest = new
GetObjectMetadataRequest(bucketName, keyName)
               .withSSECustomerKey(SSE_KEY);
       ObjectMetadata objectMetadata =
S3_CLIENT.getObjectMetadata(getMetadataRequest);
       System.out.println("Metadata retrieved. Object size: " +
objectMetadata.getContentLength());
   }

   private static void copyObject(String bucketName, String keyName, String
targetKeyName)
           throws NoSuchAlgorithmException {
       // Create a new encryption key for target so that the target is saved using
       // SSE-C.
       SSECustomerKey newSSEKey = new SSECustomerKey(KEY_GENERATOR.generateKey());

       CopyObjectRequest copyRequest = new CopyObjectRequest(bucketName, keyName,
bucketName, targetKeyName)
               .withSourceSSECustomerKey(SSE_KEY)
               .withDestinationSSECustomerKey(newSSEKey);

       S3_CLIENT.copyObject(copyRequest);
       System.out.println("Object copied");
   }
```

```
    private static void displayTextInputStream(S3ObjectInputStream input) throws
 IOException {
        // Read one line at a time from the input stream and display each line.
        BufferedReader reader = new BufferedReader(new InputStreamReader(input));
        String line;
        while ((line = reader.readLine()) != null) {
            System.out.println(line);
        }
        System.out.println();
    }
}
```

.NET

> **Note**
>
> Para exemplos de upload de objetos grandes usando a API multipart upload, consulte Fazer upload de um objeto usando multipart upload e Usar os AWS SDKs (API de baixo nível).

Para obter informações sobre SSE-C, consulte Como usar criptografia do lado do servidor com chaves fornecidas pelo cliente (SSE-C). Para obter informações sobre como configurar e executar exemplos de código, consulte Conceitos básicos do AWS SDK for .NET no Guia do desenvolvedor do AWS SDK for .NET.

Example

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.IO;
using System.Security.Cryptography;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class SSEClientEncryptionKeyObjectOperationsTest
    {
        private const string bucketName = "*** bucket name ***";
```

```
        private const string keyName = "*** key name for new object created ***";
        private const string copyTargetKeyName = "*** key name for object copy ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
RegionEndpoint.USWest2;
        private static IAmazonS3 client;

        public static void Main()
        {
            client = new AmazonS3Client(bucketRegion);
            ObjectOpsUsingClientEncryptionKeyAsync().Wait();
        }
        private static async Task ObjectOpsUsingClientEncryptionKeyAsync()
        {
            try
            {
                // Create an encryption key.
                Aes aesEncryption = Aes.Create();
                aesEncryption.KeySize = 256;
                aesEncryption.GenerateKey();
                string base64Key = Convert.ToBase64String(aesEncryption.Key);

                // 1. Upload the object.
                PutObjectRequest putObjectRequest = await
UploadObjectAsync(base64Key);
                // 2. Download the object and verify that its contents matches what
you uploaded.
                await DownloadObjectAsync(base64Key, putObjectRequest);
                // 3. Get object metadata and verify that the object uses AES-256
encryption.
                await GetObjectMetadataAsync(base64Key);
                // 4. Copy both the source and target objects using server-side
encryption with
                //    a customer-provided encryption key.
                await CopyObjectAsync(aesEncryption, base64Key);
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered ***. Message:'{0}' when writing
an object", e.Message);
            }
            catch (Exception e)
            {
```

```
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
writing an object", e.Message);
            }
        }

        private static async Task<PutObjectRequest> UploadObjectAsync(string
base64Key)
        {
            PutObjectRequest putObjectRequest = new PutObjectRequest
            {
                BucketName = bucketName,
                Key = keyName,
                ContentBody = "sample text",
                ServerSideEncryptionCustomerMethod =
ServerSideEncryptionCustomerMethod.AES256,
                ServerSideEncryptionCustomerProvidedKey = base64Key
            };
            PutObjectResponse putObjectResponse = await
client.PutObjectAsync(putObjectRequest);
            return putObjectRequest;
        }
        private static async Task DownloadObjectAsync(string base64Key,
PutObjectRequest putObjectRequest)
        {
            GetObjectRequest getObjectRequest = new GetObjectRequest
            {
                BucketName = bucketName,
                Key = keyName,
                // Provide encryption information for the object stored in Amazon
S3.
                ServerSideEncryptionCustomerMethod =
ServerSideEncryptionCustomerMethod.AES256,
                ServerSideEncryptionCustomerProvidedKey = base64Key
            };

            using (GetObjectResponse getResponse = await
client.GetObjectAsync(getObjectRequest))
            using (StreamReader reader = new
StreamReader(getResponse.ResponseStream))
            {
                string content = reader.ReadToEnd();
                if (String.Compare(putObjectRequest.ContentBody, content) == 0)
                    Console.WriteLine("Object content is same as we uploaded");
                else
```

```
                    Console.WriteLine("Error...Object content is not same.");

                if (getResponse.ServerSideEncryptionCustomerMethod ==
ServerSideEncryptionCustomerMethod.AES256)
                    Console.WriteLine("Object encryption method is AES256, same as
we set");
                else
                    Console.WriteLine("Error...Object encryption method is not the
same as AES256 we set");

                // Assert.AreEqual(putObjectRequest.ContentBody, content);
                // Assert.AreEqual(ServerSideEncryptionCustomerMethod.AES256,
getResponse.ServerSideEncryptionCustomerMethod);
            }
        }
        private static async Task GetObjectMetadataAsync(string base64Key)
        {
            GetObjectMetadataRequest getObjectMetadataRequest = new
GetObjectMetadataRequest
            {
                BucketName = bucketName,
                Key = keyName,

                // The object stored in Amazon S3 is encrypted, so provide the
necessary encryption information.
                ServerSideEncryptionCustomerMethod =
ServerSideEncryptionCustomerMethod.AES256,
                ServerSideEncryptionCustomerProvidedKey = base64Key
            };

            GetObjectMetadataResponse getObjectMetadataResponse = await
client.GetObjectMetadataAsync(getObjectMetadataRequest);
            Console.WriteLine("The object metadata show encryption method used is:
{0}", getObjectMetadataResponse.ServerSideEncryptionCustomerMethod);
            // Assert.AreEqual(ServerSideEncryptionCustomerMethod.AES256,
getObjectMetadataResponse.ServerSideEncryptionCustomerMethod);
        }
        private static async Task CopyObjectAsync(Aes aesEncryption, string
base64Key)
        {
            aesEncryption.GenerateKey();
            string copyBase64Key = Convert.ToBase64String(aesEncryption.Key);

            CopyObjectRequest copyRequest = new CopyObjectRequest
```

```
            {
                SourceBucket = bucketName,
                SourceKey = keyName,
                DestinationBucket = bucketName,
                DestinationKey = copyTargetKeyName,
                // Information about the source object's encryption.
                CopySourceServerSideEncryptionCustomerMethod =
 ServerSideEncryptionCustomerMethod.AES256,
                CopySourceServerSideEncryptionCustomerProvidedKey = base64Key,
                // Information about the target object's encryption.
                ServerSideEncryptionCustomerMethod =
 ServerSideEncryptionCustomerMethod.AES256,
                ServerSideEncryptionCustomerProvidedKey = copyBase64Key
            };
            await client.CopyObjectAsync(copyRequest);
        }
    }
}
```

Usar AWS SDKs para especificar SSE-C para uploads fracionados

O exemplo da seção anterior mostra como solicitar a criptografia de servidor com a chave fornecida pelo cliente (SSE-C) nas operações PUT, GET, Head e Copy. Esta seção descreve outras APIs do Amazon S3 que oferecem suporte para SSE-C.

Java

Para carregar objetos grandes, você pode usar a API de carregamento fracionado (consulte Carregar e copiar objetos usando upload fracionado no Amazon S3). Você pode usar APIs de alto ou baixo nível para fazer upload de objetos grandes. Essas APIs oferecem suporte para cabeçalhos relacionados à criptografia na solicitação.

- Ao usar a API do `TransferManager` de alto nível, você fornece os cabeçalhos específicos de criptografia na `PutObjectRequest` (consulte Fazer upload de um objeto usando multipart upload).
- Ao usar a API de baixo nível, você fornece informações relacionadas à criptografia na `InitiateMultipartUploadRequest`, seguidas por informações de criptografia idênticas em cada `UploadPartRequest`. Você não precisa fornecer cabeçalhos específicos de criptografia na `CompleteMultipartUploadRequest`. Para obter exemplos, consulte Usar os AWS SDKs (API de baixo nível).

O exemplo a seguir usa `TransferManager` para criar objetos e mostra como fornecer informações relacionadas a SSE-C. O exemplo faz o seguinte:

- Cria um objeto usando o método `TransferManager.upload()`. Na instância `PutObjectRequest`, você fornece informações de chave de criptografia para solicitar. O Amazon S3 criptografa o objeto usando a chave fornecida pelo cliente.
- Faz uma cópia do objeto, chamando o método `TransferManager.copy()`. O exemplo instrui o Amazon S3 a criptografar a cópia do objeto usando um novo `SSECustomerKey`. Como o objeto de origem é criptografado usando SSE-C, o `CopyObjectRequest` também fornece a chave de criptografia do objeto de origem para que o Amazon S3 possa descriptografar o objeto antes de copiá-lo.

Example

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.CopyObjectRequest;
import com.amazonaws.services.s3.model.PutObjectRequest;
import com.amazonaws.services.s3.model.SSECustomerKey;
import com.amazonaws.services.s3.transfer.Copy;
import com.amazonaws.services.s3.transfer.TransferManager;
import com.amazonaws.services.s3.transfer.TransferManagerBuilder;
import com.amazonaws.services.s3.transfer.Upload;

import javax.crypto.KeyGenerator;
import java.io.File;
import java.security.SecureRandom;

public class ServerSideEncryptionCopyObjectUsingHLwithSSEC {

    public static void main(String[] args) throws Exception {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "*** Bucket name ***";
        String fileToUpload = "*** File path ***";
        String keyName = "*** New object key name ***";
        String targetKeyName = "*** Key name for object copy ***";
```

```
        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withRegion(clientRegion)
                    .withCredentials(new ProfileCredentialsProvider())
                    .build();
            TransferManager tm = TransferManagerBuilder.standard()
                    .withS3Client(s3Client)
                    .build();

            // Create an object from a file.
            PutObjectRequest putObjectRequest = new PutObjectRequest(bucketName,
keyName, new File(fileToUpload));

            // Create an encryption key.
            KeyGenerator keyGenerator = KeyGenerator.getInstance("AES");
            keyGenerator.init(256, new SecureRandom());
            SSECustomerKey sseCustomerEncryptionKey = new
SSECustomerKey(keyGenerator.generateKey());

            // Upload the object. TransferManager uploads asynchronously, so this
call
            // returns immediately.
            putObjectRequest.setSSECustomerKey(sseCustomerEncryptionKey);
            Upload upload = tm.upload(putObjectRequest);

            // Optionally, wait for the upload to finish before continuing.
            upload.waitForCompletion();
            System.out.println("Object created.");

            // Copy the object and store the copy using SSE-C with a new key.
            CopyObjectRequest copyObjectRequest = new CopyObjectRequest(bucketName,
keyName, bucketName, targetKeyName);
            SSECustomerKey sseTargetObjectEncryptionKey = new
SSECustomerKey(keyGenerator.generateKey());
            copyObjectRequest.setSourceSSECustomerKey(sseCustomerEncryptionKey);

copyObjectRequest.setDestinationSSECustomerKey(sseTargetObjectEncryptionKey);

            // Copy the object. TransferManager copies asynchronously, so this call
returns
            // immediately.
            Copy copy = tm.copy(copyObjectRequest);
```

```
            // Optionally, wait for the upload to finish before continuing.
            copy.waitForCompletion();
            System.out.println("Copy complete.");
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

.NET

Para carregar objetos grandes, você pode usar a API de carregamentos fracionados (consulte Carregar e copiar objetos usando upload fracionado no Amazon S3). AWS O SDK for .NET fornece APIs de alto ou baixo nível para fazer upload de objetos grandes. Essas APIs oferecem suporte para cabeçalhos relacionados à criptografia na solicitação.

- Ao usar a API do `Transfer-Utility` de alto nível, você fornece os cabeçalhos específicos de criptografia na `TransferUtilityUploadRequest`, conforme mostrado. Para obter exemplos de código, consulte Fazer upload de um objeto usando multipart upload.

```
TransferUtilityUploadRequest request = new TransferUtilityUploadRequest()
{
    FilePath = filePath,
    BucketName = existingBucketName,
    Key = keyName,
    // Provide encryption information.
    ServerSideEncryptionCustomerMethod =
 ServerSideEncryptionCustomerMethod.AES256,
    ServerSideEncryptionCustomerProvidedKey = base64Key,
};
```

- Ao usar a API de baixo nível, você fornece informações relacionadas à criptografia na solicitação para iniciar o multipart upload, seguidas por informações de criptografia idênticas nas solicitações subsequentes de upload de parte. Você não precisa fornecer cabeçalhos

específicos de criptografia na solicitação de multipart upload completo. Para obter exemplos, consulte Usar os AWS SDKs (API de baixo nível).

O seguinte é um exemplo de multipart upload de baixo nível que faz uma cópia de um objeto grande existente. No exemplo, o objeto a ser copiado é armazenado no Amazon S3 usando o SSE-C, e você deseja salvar o objeto de destino também usando o SSE-C. No exemplo, faça o seguinte:

- Inicie uma solicitação de multipart upload fornecendo uma chave de criptografia e as informações relacionadas.
- Forneça as chaves de criptografia de objeto de origem e de destino e as informações relacionadas na `CopyPartRequest`.
- Obtenha o tamanho do objeto de origem a ser copiado recuperando os metadados do objeto.
- Faça upload dos objetos em partes de 5 MB.

Example

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Collections.Generic;
using System.IO;
using System.Security.Cryptography;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class SSECLowLevelMPUcopyObjectTest
    {
        private const string existingBucketName = "*** bucket name ***";
        private const string sourceKeyName      = "*** source object key name
 ***";
        private const string targetKeyName      = "*** key name for the target
 object ***";
        private const string filePath           = @"*** file path ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 s3Client;
        static void Main()
```

```
        {
            s3Client = new AmazonS3Client(bucketRegion);
            CopyObjClientEncryptionKeyAsync().Wait();
        }

        private static async Task CopyObjClientEncryptionKeyAsync()
        {
            Aes aesEncryption = Aes.Create();
            aesEncryption.KeySize = 256;
            aesEncryption.GenerateKey();
            string base64Key = Convert.ToBase64String(aesEncryption.Key);

            await CreateSampleObjUsingClientEncryptionKeyAsync(base64Key,
s3Client);

            await CopyObjectAsync(s3Client, base64Key);
        }
        private static async Task CopyObjectAsync(IAmazonS3 s3Client, string
base64Key)
        {
            List<CopyPartResponse> uploadResponses = new List<CopyPartResponse>();

            // 1. Initialize.
            InitiateMultipartUploadRequest initiateRequest = new
InitiateMultipartUploadRequest
            {
                BucketName = existingBucketName,
                Key = targetKeyName,
                ServerSideEncryptionCustomerMethod =
ServerSideEncryptionCustomerMethod.AES256,
                ServerSideEncryptionCustomerProvidedKey = base64Key,
            };

            InitiateMultipartUploadResponse initResponse =
                await s3Client.InitiateMultipartUploadAsync(initiateRequest);

            // 2. Upload Parts.
            long partSize = 5 * (long)Math.Pow(2, 20); // 5 MB
            long firstByte = 0;
            long lastByte = partSize;

            try
            {
```

```
                // First find source object size. Because object is stored
encrypted with
                // customer provided key you need to provide encryption
information in your request.
                GetObjectMetadataRequest getObjectMetadataRequest = new
GetObjectMetadataRequest()
                {
                    BucketName = existingBucketName,
                    Key = sourceKeyName,
                    ServerSideEncryptionCustomerMethod =
ServerSideEncryptionCustomerMethod.AES256,
                    ServerSideEncryptionCustomerProvidedKey = base64Key // " *
**source object encryption key ***"
                };

                GetObjectMetadataResponse getObjectMetadataResponse = await
s3Client.GetObjectMetadataAsync(getObjectMetadataRequest);

                long filePosition = 0;
                for (int i = 1; filePosition <
getObjectMetadataResponse.ContentLength; i++)
                {
                    CopyPartRequest copyPartRequest = new CopyPartRequest
                    {
                        UploadId = initResponse.UploadId,
                        // Source.
                        SourceBucket = existingBucketName,
                        SourceKey = sourceKeyName,
                        // Source object is stored using SSE-C. Provide encryption
information.
                        CopySourceServerSideEncryptionCustomerMethod =
ServerSideEncryptionCustomerMethod.AES256,
                        CopySourceServerSideEncryptionCustomerProvidedKey =
base64Key, //"***source object encryption key ***",
                        FirstByte = firstByte,
                        // If the last part is smaller then our normal part size
then use the remaining size.
                        LastByte = lastByte >
getObjectMetadataResponse.ContentLength ?
                            getObjectMetadataResponse.ContentLength - 1 :
lastByte,

                        // Target.
                        DestinationBucket = existingBucketName,
```

```
                        DestinationKey = targetKeyName,
                        PartNumber = i,
                        // Encryption information for the target object.
                        ServerSideEncryptionCustomerMethod =
ServerSideEncryptionCustomerMethod.AES256,
                        ServerSideEncryptionCustomerProvidedKey = base64Key
                    };
                    uploadResponses.Add(await
s3Client.CopyPartAsync(copyPartRequest));
                    filePosition += partSize;
                    firstByte += partSize;
                    lastByte += partSize;
                }

                // Step 3: complete.
                CompleteMultipartUploadRequest completeRequest = new
CompleteMultipartUploadRequest
                {
                    BucketName = existingBucketName,
                    Key = targetKeyName,
                    UploadId = initResponse.UploadId,
                };
                completeRequest.AddPartETags(uploadResponses);

                CompleteMultipartUploadResponse completeUploadResponse =
                    await s3Client.CompleteMultipartUploadAsync(completeRequest);
            }
            catch (Exception exception)
            {
                Console.WriteLine("Exception occurred: {0}", exception.Message);
                AbortMultipartUploadRequest abortMPURequest = new
AbortMultipartUploadRequest
                {
                    BucketName = existingBucketName,
                    Key = targetKeyName,
                    UploadId = initResponse.UploadId
                };
                s3Client.AbortMultipartUpload(abortMPURequest);
            }
        }
        private static async Task
CreateSampleObjUsingClientEncryptionKeyAsync(string base64Key, IAmazonS3
s3Client)
        {
```

```
            // List to store upload part responses.
            List<UploadPartResponse> uploadResponses = new
List<UploadPartResponse>();

            // 1. Initialize.
            InitiateMultipartUploadRequest initiateRequest = new
InitiateMultipartUploadRequest
            {
                BucketName = existingBucketName,
                Key = sourceKeyName,
                ServerSideEncryptionCustomerMethod =
ServerSideEncryptionCustomerMethod.AES256,
                ServerSideEncryptionCustomerProvidedKey = base64Key
            };

            InitiateMultipartUploadResponse initResponse =
               await s3Client.InitiateMultipartUploadAsync(initiateRequest);

            // 2. Upload Parts.
            long contentLength = new FileInfo(filePath).Length;
            long partSize = 5 * (long)Math.Pow(2, 20); // 5 MB

            try
            {
                long filePosition = 0;
                for (int i = 1; filePosition < contentLength; i++)
                {
                    UploadPartRequest uploadRequest = new UploadPartRequest
                    {
                        BucketName = existingBucketName,
                        Key = sourceKeyName,
                        UploadId = initResponse.UploadId,
                        PartNumber = i,
                        PartSize = partSize,
                        FilePosition = filePosition,
                        FilePath = filePath,
                        ServerSideEncryptionCustomerMethod =
ServerSideEncryptionCustomerMethod.AES256,
                        ServerSideEncryptionCustomerProvidedKey = base64Key
                    };

                    // Upload part and add response to our list.
                    uploadResponses.Add(await
s3Client.UploadPartAsync(uploadRequest));
```

```
                    filePosition += partSize;
                }

                // Step 3: complete.
                CompleteMultipartUploadRequest completeRequest = new
 CompleteMultipartUploadRequest
                {
                    BucketName = existingBucketName,
                    Key = sourceKeyName,
                    UploadId = initResponse.UploadId,
                    //PartETags = new List<PartETag>(uploadResponses)

                };
                completeRequest.AddPartETags(uploadResponses);

                CompleteMultipartUploadResponse completeUploadResponse =
                    await s3Client.CompleteMultipartUploadAsync(completeRequest);

            }
            catch (Exception exception)
            {
                Console.WriteLine("Exception occurred: {0}", exception.Message);
                AbortMultipartUploadRequest abortMPURequest = new
 AbortMultipartUploadRequest
                {
                    BucketName = existingBucketName,
                    Key = sourceKeyName,
                    UploadId = initResponse.UploadId
                };
                await s3Client.AbortMultipartUploadAsync(abortMPURequest);
            }
        }
    }
}
```

Proteger dados usando a criptografia do lado do cliente

A criptografia do lado do cliente é o ato de criptografar dados localmente para ajudar a garantir sua segurança em trânsito e em repouso. Para criptografar os objetos antes de enviá-los ao Amazon S3, use o cliente de criptografia do Amazon S3. Quando os objetos são criptografados dessa maneira, eles não são expostos a terceiros, inclusive a AWS. O Amazon S3 recebe os objetos já

criptografados. O Amazon S3 não atua na criptografia ou descriptografia dos objetos. Você pode usar o cliente de criptografia do Amazon S3 e a criptografia do lado do servidor para criptografar os dados. Quando você envia objetos criptografados para o Amazon S3, o Amazon S3 não reconhece os objetos como sendo criptografados, ele detecta apenas objetos típicos.

O cliente de criptografia do Amazon S3 funciona como um intermediário entre você e o Amazon S3. Depois de instanciar o cliente de criptografia do Amazon S3, os objetos são automaticamente criptografados e descriptografados como parte do Amazon S3 e das solicitações `PutObject` e `GetObject`. Todos os objetos são criptografados com uma chave de dados exclusiva. O cliente de criptografia do Amazon S3 não usa nem interage com chaves de bucket, mesmo se você especificar uma chave do KMS como a chave de encapsulamento.

O Guia do desenvolvedor do cliente de criptografia do Amazon S3 concentra-se nas versões 3.0 e posteriores do cliente de criptografia do Amazon S3. Para obter mais informações, consulte Qual é o cliente de criptografia do Amazon S3? no Guia do desenvolvedor do cliente de criptografia do Amazon S3.

Para obter mais informações sobre versões anteriores do cliente de criptografia do Amazon S3, consulte o Guia do desenvolvedor do SDK AWS de acordo com a sua linguagem de programação.

- AWS SDK para Java
- AWS SDK para .NET
- AWS SDK para Go
- AWS SDK para PHP
- AWS SDK para Ruby
- AWS SDK para C++

Privacidade do tráfego entre redes

Este tópico descreve como o Amazon S3 protege conexões do serviço com outros locais.

Tráfego entre clientes de serviço e on-premises e os aplicativos

As seguintes conexões podem ser combinadas com o AWS PrivateLink para fornecer conectividade entre sua rede privada e a AWS:

- Uma conexão AWS Site-to-Site VPN. Para obter mais informações, consulte O que é o AWS Site-to-Site VPN?

- Uma conexão AWS Direct Connect. Para ter mais informações, consulte O que é o AWS Direct Connect?

O acesso ao Amazon S3 pela rede acontece por meio de APIs publicadas pela AWS. Os clientes devem ser compatíveis com o Transport Layer Security (TLS) 1.2. Recomendamos o TLS 1.3. Os clientes também devem ter suporte a pacotes de criptografia com sigilo de encaminhamento perfeito (PFS) como Ephemeral Diffie-Hellman (DHE) ou Ephemeral Elliptic Curve Diffie-Hellman (ECDHE). A maioria dos sistemas modernos como Java 7 e versões posteriores oferece suporte a esses modos. Além disso, você deve assinar solicitações usando um ID da chave de acesso e uma chave de acesso secreta associados a uma entidade principal do IAM. Ou você pode usar o AWS Security Token Service (STS) para gerar credenciais de segurança temporárias para assinar solicitações.

Tráfego entre recursos da AWS na mesma região

Um endpoint da Virtual Private Cloud (VPC) para Amazon S3 é uma entidade lógica dentro de uma VPC que permite conectividade apenas com o Amazon S3. A VPC roteia as solicitações para o Amazon S3 e as respostas de volta para a VPC. Para obter mais informações, consulte Endpoints da VPC no Guia do usuário da VPC. Para obter políticas de bucket de exemplo que podem ser usadas para controlar o acesso ao bucket do S3 de VPC endpoints, consulte Controlar o acesso a partir de VPC endpoints com políticas de bucket.

AWS PrivateLink for Amazon S3

Com o AWS PrivateLink para o Amazon S3, você pode provisionar endpoints da VPC de interface (endpoints de interface) em sua Virtual Private Cloud (VPC). Esses endpoints são diretamente acessíveis a partir de aplicações que estão no local por meio de VPN e AWS Direct Connect, ou em uma Região da AWS diferente por emparelhamento de VPC.

Os endpoints de interface são representados por uma ou mais interfaces de rede elástica (ENIs) que recebem endereços IP privados de sub-redes em sua VPC. As solicitações para o Amazon S3 por meio de endpoints de interface permanecem na rede da Amazon. Você também pode acessar endpoints de interface em sua VPC via aplicações on-premises por meio do AWS Direct Connect ou da AWS Virtual Private Network (AWS VPN). Para obter mais informações sobre como conectar sua VPC à rede on-premises, consulte o AWS Direct ConnectGuia do usuário do e o AWS Site-to-Site VPNGuia do usuário do .

Para obter informações gerais sobre endpoints de interface, consulte Endpoints da VPC de interface (AWS PrivateLink) no Manual do AWS PrivateLink.

Tópicos

- Tipos de VPC endpoints para o Amazon S3
- Restrições e limitações do AWS PrivateLink do Amazon S3
- Criar um endpoint da VPC
- Acessar endpoints da interface do Amazon S3
- DNS privado
- Acessar buckets, pontos de acesso e operações de API de controle do Amazon S3 de endpoints de interface do S3
- Atualizar uma configuração de DNS on-premises
- Criar uma política de VPC endpoint para o Amazon S3

Tipos de VPC endpoints para o Amazon S3

Você pode usar dois tipos de endpoints da VPC para acessar o Amazon S3: endpoints de gateway e endpoints de interface (usando o AWS PrivateLink). Um endpoint de gateway é um gateway que você especifica em sua tabela de rotas para acessar o Amazon S3 da sua VPC pela rede da AWS. Os endpoints de interface estendem a funcionalidade dos endpoints de gateway usando endereços IP privados para rotear solicitações para o Amazon S3 de dentro da sua VPC on-premises ou de uma PVC em outra Região da AWS usando emparelhamento da VPC ou o AWS Transit Gateway. Para obter mais informações, consulte O que é emparelhamento da VPC? em Transit Gateway vs. emparelhamento da VPC.

Os endpoints de interface são compatíveis com os endpoints de gateway. Se você tiver um endpoint de gateway existente na VPC, poderá usar ambos os tipos de endpoints na mesma VPC.

Endpoints de gateway para o Amazon S3	Endpoints de interface para o Amazon S3
Em ambos os casos, o tráfego de rede permanece na rede AWS.	
Usar endereços IP públicos do Amazon S3	Usar endereços IP privados da VPC para acessar o Amazon S3
Usar os mesmos nomes DNS do Amazon S3	Exigir nomes DNS do Amazon S3 específicos do endpoint

Endpoints de gateway para o Amazon S3	Endpoints de interface para o Amazon S3
Não permita o acesso pelo ambiente on-premises	Permitir acesso desde on-premises
Não permita o acesso por outra Região da AWS	Permitir acesso de uma VPC em outra Região da AWS usando emparelhamento da VPC ou AWS Transit Gateway
Não faturado	Faturado

Para obter mais informações sobre endpoints de gateway, consulte Endpoints da VPC de gateway no Guia do usuário do AWS PrivateLink.

Restrições e limitações do AWS PrivateLink do Amazon S3

As limitações da VPC aplicam-se ao AWS PrivateLink do Amazon S3. Para obter mais informações, consulte Considerações sobre o endpoint de interface e Cotas do AWS PrivateLink no Guia do usuário do AWS PrivateLink. Além disso, aplicam-se as restrições a seguir.

O AWS PrivateLink do Amazon S3 não é compatível com:

- Endpoints do Federal Information Processing Standard (FIPS – Padrões Federais de Processamento de Informações)
- Endpoints de site
- Endpoints globais herdados
- Endpoints do S3 traço região
- Endpoints de pilha dupla
- Usar CopyObject ou UploadPartCopy entre buckets em diferentes Regiões da AWS
- Transport Layer Security (TLS) 1.0
- Transport Layer Security (TLS) 1.1
- Transport Layer Security (TLS) 1.3

Criar um endpoint da VPC

Para criar um endpoint da VPC de interface, consulte Create a VPC endpoint (Criar um endpoint da VPC) no Guia do AWS PrivateLink.

Acessar endpoints da interface do Amazon S3

Quando você cria um endpoint de interface, o Amazon S3 gera dois tipos de nome de DNS do S3 específicos do endpoint: regional e zonal.

- Os nomes DNS regionais incluem um ID de endpoint da VPC exclusivo, um identificador de serviço, a Região da AWS e `vpce.amazonaws.com` em seu nome. Por exemplo, para o ID de VPC endpoint *`vpce-1a2b3c4d`*, o nome de DNS gerado pode ser semelhante a *`vpce-1a2b3c4d-5e6f`*`.s3.us-east-1.vpce.amazonaws.com`.
- Os nomes DNS zonais incluem a zona de disponibilidade. Por exemplo, *`vpce-1a2b3c4d-5e6f`***`-us-east-1a.`**`s3.us-east-1.vpce.amazonaws.com`. Você pode usar essa opção se sua arquitetura isola zonas de disponibilidade. Por exemplo, você pode usar para contenção de falhas ou para reduzir os custos regionais de transferência de dados.

Os nomes de DNS do S3 específicos do endpoint podem ser resolvidos a partir do domínio DNS público do S3.

DNS privado

As opções de DNS privado para endpoints da VPC de interface simplificam o roteamento do tráfego do S3 pelos endpoints da VPC e ajudam você a aproveitar o caminho de rede de menor custo disponível para a aplicação. Você pode usar opções de DNS privadas para rotear o tráfego regional do S3 sem atualizar seus clientes do S3 para usar os nomes DNS específicos dos endpoints de interface ou gerenciar a infraestrutura de DNS. Com os nomes DNS privados ativados, as consultas ao DNS regionais do S3 são resolvidas para os endereços IP privados de AWS PrivateLink dos seguintes endpoints:

- Endpoints regionais de bucket (por exemplo, `s3.us-east-1.amazonaws.com`)
- Endpoints de controle (por exemplo, `s3-control.us-east-1.amazonaws.com`)
- Endpoints de pontos de acesso (por exemplo, `s3-accesspoint.us-east-1.amazonaws.com`)

O AWS PrivateLink para Amazon S3 não permite usar endpoints de camada dupla do Amazon S3. Consulte Using Amazon S3 dual-stack endpoints. Se você usar um nome de DNS de pilha dupla do

S3 como nome de DNS privado, o tráfego IPv6 será descartado ou, se a nuvem privada virtual (VPC) tiver um gateway da internet, o tráfego IPv6 será direcionado pelo gateway da internet na VPC.

Se você tiver um endpoint de gateway na VPC, poderá rotear automaticamente as solicitações na VPC pelo endpoint do gateway do S3 existente e as solicitações on-premises pelo endpoint da interface. Essa abordagem permite que você otimize os custos da rede usando endpoints de gateway, que não são cobrados, para o tráfego na VPC. As aplicações on-premises podem usar AWS PrivateLink com a ajuda do endpoint de resolvedor de entrada. A Amazon fornece um servidor de DNS à VPC, o Route 53 Resolver. Um endpoint do Resolver de entrada encaminha consultas de DNS da rede on-premises para o Route 53 Resolver.

> **Important**
>
> Para aproveitar o caminho de rede de menor custo ao usar Habilitar DNS privado somente para endpoints de entrada, um endpoint de gateway deve estar presente na VPC. A presença de um endpoint de gateway ajuda a garantir que o tráfego na VPC sempre seja roteado pela rede privada da AWS quando a opção Habilitar DNS privado somente para endpoints de entrada é selecionada. Você deve manter esse endpoint de gateway enquanto estiver com a opção Habilitar DNS privado somente para endpoints de entrada selecionada. Se você quiser excluir o endpoint de gateway, primeiro desmarque Habilitar DNS privado somente para endpoints de entrada.
> Se você quiser atualizar um endpoint de interface existente para Habilitar DNS privado somente para endpoints de entrada, primeiro confirme se a VPC tem um endpoint de gateway do S3. Para obter mais informações sobre endpoints de gateway e gerenciamento de nomes DNS privados, consulte Gateway de endpoints da VPC e Gerenciar nomes DNS, respectivamente, no Guia do AWS PrivateLink.

A opção Habilitar DNS privado somente para endpoints de entrada está disponível somente para serviços compatíveis com endpoints de gateway.

Para obter mais informações sobre a criação de um endpoint da VPC que usa Habilitar DNS privado somente para endpoints de entrada, consulte Criar um endpoint de interface no Guia do AWS PrivateLink.

Usar o console da VPC

No console, você tem duas opções: Habilitar nome DNS e Habilitar DNS privado somente para endpoints de entrada. Habilitar nome DNS é uma opção compatível com AWS PrivateLink. Ao usar

a opção Habilitar nome de DNS, você pode usar a conectividade privada da Amazon com o Amazon S3, enquanto faz solicitações aos nomes DNS de endpoints públicos padrão. Quando essa opção é ativada, os clientes podem aproveitar o caminho de rede de menor custo disponível para a aplicação.

Quando você habilita nomes DNS privados em um endpoint da VPC de interface existente ou novo para o Amazon S3, a opção Habilitar DNS privado somente para endpoints de entrada é selecionada por padrão. Se essa opção for selecionada, as aplicações usarão somente endpoints de interface para o tráfego on-premises. Esse tráfego na VPC usa automaticamente os endpoints de gateway de menor custo. Como alternativa, você pode desmarcar Habilitar DNS privado somente para endpoints de entrada para rotear todas as solicitações do S3 pelo endpoint de interface.

Como usar a AWS CLI

Se você não especificar um valor para `PrivateDnsOnlyForInboundResolverEndpoint`, o padrão será `true`. No entanto, antes da VPC aplicar as configurações, ela realiza uma verificação para garantir que você tenha um endpoint de gateway presente na VPC. Se um endpoint de gateway estiver presente na VPC, a chamada será bem-sucedida. Caso contrário, você receberá a seguinte mensagem de erro:

Para definir PrivateDnsOnlyForInboundResolverEndpoint como verdadeiro, a VPC *`vpce_id`* deve ter um endpoint de gateway para o serviço.

Para um novo endpoint da VPC de interface

Use os atributos `private-dns-enabled` e `dns-options` para habilitar o DNS privado por meio da linha de comando. A opção `PrivateDnsOnlyForInboundResolverEndpoint` no atributo `dns-options` deve ser definida como `true`. Substitua os *`user input placeholders`* por suas próprias informações.

```
aws ec2 create-vpc-endpoint \
--region us-east-1 \
--service-name s3-service-name \
--vpc-id client-vpc-id \
--subnet-ids client-subnet-id \
--vpc-endpoint-type Interface  \
--private-dns-enabled  \
--ip-address-type ip-address-type \
--dns-options PrivateDnsOnlyForInboundResolverEndpoint=true \
--security-group-ids client-sg-id
```

Para um endpoint da VPC existente

Se você quiser usar o DNS privado para um endpoint da VPC existente, use o comando de exemplo a seguir e substitua *user input placeholders* por suas próprias informações.

```
aws ec2 modify-vpc-endpoint \
--region us-east-1 \
--vpc-endpoint-id client-vpc-id \
--private-dns-enabled \
--dns-options PrivateDnsOnlyForInboundResolverEndpoint=false
```

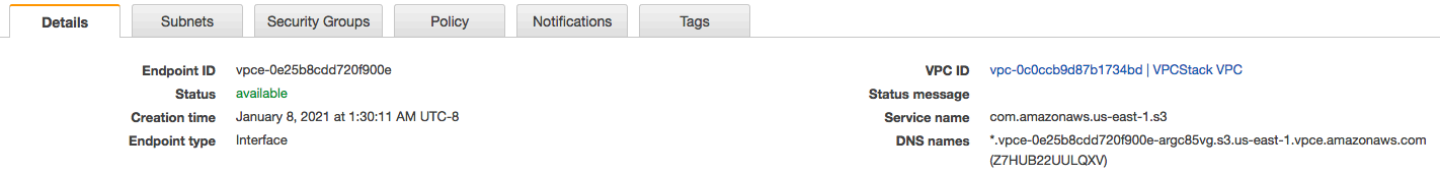
Se você quiser atualizar um endpoint da VPC existente para habilitar o DNS privado somente para o resolvedor de entrada, use o exemplo a seguir e substitua os valores de amostra pelos seus próprios valores.

```
aws ec2 modify-vpc-endpoint \
--region us-east-1 \
--vpc-endpoint-id client-vpc-id \
--private-dns-enabled \
--dns-options PrivateDnsOnlyForInboundResolverEndpoint=true
```

Acessar buckets, pontos de acesso e operações de API de controle do Amazon S3 de endpoints de interface do S3

Você pode usar a AWS CLI ou AWS SDKs para acessar buckets, pontos de acesso do S3 e operações de API de controle do Amazon S3 por meio de endpoints de interface do S3.

A imagem a seguir mostra a guia Detalhes do console da VPC, onde você pode encontrar o nome de DNS de um VPC endpoint. Neste exemplo, o ID do VPC endpoint (vpce-id) é `vpce-0e25b8cdd720f900e` e o nome de DNS é `*.vpce-0e25b8cdd720f900e-argc85vg.s3.us-east-1.vpce.amazonaws.com`.



Ao usar o nome DNS para acessar um recurso, substitua `*` pelo valor apropriado. Os valores apropriados a serem usados no lugar de `*` são os seguintes:

- `bucket`
- `accesspoint`
- `control`

Por exemplo, para acessar um bucket, use um nome DNS como este:

`bucket.vpce-0e25b8cdd720f900e-argc85vg.s3.us-east-1.vpce.amazonaws.com`

Para obter exemplos de como usar nomes DNS para acessar buckets, pontos de acesso e operações da API de controle do Amazon S3, consulte as seções a seguir de Exemplos do AWS CLI e Exemplos de AWS SDK.

Para obter mais informações sobre como visualizar os nomes de DNS específicos do endpoint, consulte Visualizar a configuração de nome de DNS privado do serviço de endpoint no Guia do usuário da VPC.

Exemplos do AWS CLI

Para acessar os buckets do S3, os pontos de acesso do S3 ou as operações de API de controle do Amazon S3 por meio de endpoints de interface do S3 em comandos AWS CLI, use os parâmetros `--region` e `--endpoint-url`.

Exemplo: usar um URL de endpoint para listar objetos no bucket

No exemplo a seguir, substitua o nome do bucket *`my-bucket`*, a região *`us-east-1`* e o nome de DNS do ID do endpoint da VPC *`vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com`* por suas próprias informações.

```
aws s3 ls s3://my-bucket/ --region us-east-1 --endpoint-url
 https://bucket.vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com
```

Exemplo: usar um URL de endpoint para listar objetos de um ponto de acesso

- Método 1: usar o nome do recurso da Amazon (ARN) do ponto de acesso com o endpoint do ponto de acesso

  Substitua o ARN *us-east-1:123456789012:accesspoint/accesspointexamplename*, a região *us-east-1* e o ID do endpoint da VPC *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* por suas próprias informações.

```
aws s3api list-objects-v2 --bucket arn:aws:s3:us-east-1:123456789012:accesspoint/
accesspointexamplename --region us-east-1 --endpoint-url
 https://accesspoint.vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com
```

  Se você não conseguir executar o comando com êxito, atualize a AWS CLI para a versão mais recente e tente novamente. Para obter mais informações sobre as instruções de atualização, consulte Instalar ou atualizar a versão mais recente da AWS CLI no Guia do usuário do AWS Command Line Interface.

- Método 2: usar o alias do ponto de acesso com o endpoint do bucket regional

  No exemplo a seguir, substitua o alias do ponto de acesso *accesspointexamplename-8tyekmigicmhun8n9kwpfur39dnw4use1a-s3alias*, a região *us-east-1* e o ID do endpoint da VPC *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* por suas próprias informações.

```
aws s3api list-objects-v2 --
bucket accesspointexamplename-8tyekmigicmhun8n9kwpfur39dnw4use1a-s3alias
 --region us-east-1 --endpoint-url https://bucket.vpce-1a2b3c4d-5e6f.s3.us-
east-1.vpce.amazonaws.com
```

- Método 3: usar o alias do ponto de acesso com o endpoint do ponto de acesso

  Primeiro, para construir um endpoint S3 com o bucket incluído como parte do nome do host, defina o estilo de endereçamento como `virtual` para `aws s3api` para uso. Para obter mais informações sobre `AWS configure`, consulte Arquivos de configuração e credencial no Guia do usuário do AWS Command Line Interface.

```
aws configure set default.s3.addressing_style virtual
```

  Depois, no exemplo a seguir, substitua o alias do ponto de acesso *accesspointexamplename-8tyekmigicmhun8n9kwpfur39dnw4use1a-s3alias*, a região *us-east-1* e o ID do endpoint da VPC *vpce-1a2b3c4d-5e6f.s3.us-*

east-1.vpce.amazonaws.com por suas próprias informações. Consulte mais informações sobre alias de ponto de acesso em Alias de ponto de acesso.

```
aws s3api list-objects-v2 --
bucket accesspointexamplename-8tyekmigicmhun8n9kwpfur39dnw4use1a-s3alias --
region us-east-1 --endpoint-url https://accesspoint.vpce-1a2b3c4d-5e6f.s3.us-
east-1.vpce.amazonaws.com
```

Exemplo: usar um URL de endpoint para listar trabalhos com uma operação de API de controle do S3

No exemplo a seguir, substitua a região *us-east-1*, o ID do endpoint da VPC *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* e o ID da conta *12345678* por suas próprias informações.

```
aws s3control --region us-east-1 --endpoint-url
 https://control.vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com list-jobs --
account-id 12345678
```

Exemplos de AWS SDK

Para acessar buckets do S3, pontos de acesso do S3 ou operações da API de controle do Amazon S3 por meio de endpoints de interface do S3 ao usar os AWS SDKs, atualize os SDKs para a versão mais recente. Depois, configure seus clientes para usar um URL de endpoint para acessar um bucket, ponto de acesso ou operações de API de controle do Amazon S3 por meio de endpoints de interface do S3.

SDK for Python (Boto3)

Exemplo: use um URL de endpoint para acessar um bucket do S3

No exemplo a seguir, substitua a região *us-east-1* e o ID do endpoint da VPC *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* por suas próprias informações.

```
s3_client = session.client(
service_name='s3',
region_name='us-east-1',
endpoint_url='https://bucket.vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com'
```

```
)
```

Exemplo: use um URL de endpoint para acessar um ponto de acesso do S3

No exemplo a seguir, substitua a região *us-east-1* e o ID do endpoint da VPC *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* por suas próprias informações.

```
ap_client = session.client(
service_name='s3',
region_name='us-east-1',
endpoint_url='https://accesspoint.vpce-1a2b3c4d-5e6f.s3.us-
east-1.vpce.amazonaws.com'
)
```

Exemplo: use um URL de endpoint para acessar a API de controle do Amazon S3

No exemplo a seguir, substitua a região *us-east-1* e o ID do endpoint da VPC *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* por suas próprias informações.

```
control_client = session.client(
service_name='s3control',
region_name='us-east-1',
endpoint_url='https://control.vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com'
)
```

SDK for Java 1.x

Exemplo: use um URL de endpoint para acessar um bucket do S3

No exemplo a seguir, substitua o ID do endpoint da VPC *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* por suas próprias informações.

```
// bucket client
final AmazonS3 s3 = AmazonS3ClientBuilder.standard().withEndpointConfiguration(
        new AwsClientBuilder.EndpointConfiguration(
                "https://bucket.vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com",
                Regions.DEFAULT_REGION.getName()
        )
).build();
List<Bucket> buckets = s3.listBuckets();
```

Exemplo: use um URL de endpoint para acessar um ponto de acesso do S3

No exemplo a seguir, substitua o ID do endpoint da VPC *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* e o ARN *us-east-1:123456789012:accesspoint/prod* por suas próprias informações.

```
// accesspoint client
final AmazonS3 s3accesspoint =
 AmazonS3ClientBuilder.standard().withEndpointConfiguration(
        new AwsClientBuilder.EndpointConfiguration(
                "https://accesspoint.vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com",
                Regions.DEFAULT_REGION.getName()
        )
).build();
ObjectListing objects = s3accesspoint.listObjects("arn:aws:s3:us-east-1:123456789012:accesspoint/prod");
```

Exemplo: usar um URL de endpoint para acessar uma operação de API de controle do Amazon S3

No exemplo a seguir, substitua o ID do endpoint da VPC *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* por suas próprias informações.

```
// control client
final AWSS3Control s3control =
 AWSS3ControlClient.builder().withEndpointConfiguration(
        new AwsClientBuilder.EndpointConfiguration(
                "https://control.vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com",
                Regions.DEFAULT_REGION.getName()
        )
).build();
final ListJobsResult jobs = s3control.listJobs(new ListJobsRequest());
```

SDK for Java 2.x

Exemplo: use um URL de endpoint para acessar um bucket do S3

No exemplo a seguir, substitua o ID do endpoint da VPC *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* e a região *Region.US_EAST_1* por suas próprias informações.

```
// bucket client
Region region = Region.US_EAST_1;
s3Client = S3Client.builder().region(region)

 .endpointOverride(URI.create("https://bucket.vpce-1a2b3c4d-5e6f.s3.us-
east-1.vpce.amazonaws.com"))
                   .build()
```

Exemplo: use um URL de endpoint para acessar um ponto de acesso do S3

No exemplo a seguir, substitua o ID do endpoint da VPC *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* e a região *Region.US_EAST_1* por suas próprias informações.

```
// accesspoint client
Region region = Region.US_EAST_1;
s3Client = S3Client.builder().region(region)

 .endpointOverride(URI.create("https://accesspoint.vpce-1a2b3c4d-5e6f.s3.us-
east-1.vpce.amazonaws.com"))
                   .build()
```

Exemplo: use um URL de endpoint para acessar a API de controle do Amazon S3

No exemplo a seguir, substitua o ID do endpoint da VPC *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* e a região *Region.US_EAST_1* por suas próprias informações.

```
// control client
Region region = Region.US_EAST_1;
s3ControlClient = S3ControlClient.builder().region(region)

 .endpointOverride(URI.create("https://control.vpce-1a2b3c4d-5e6f.s3.us-
east-1.vpce.amazonaws.com"))
                                  .build()
```

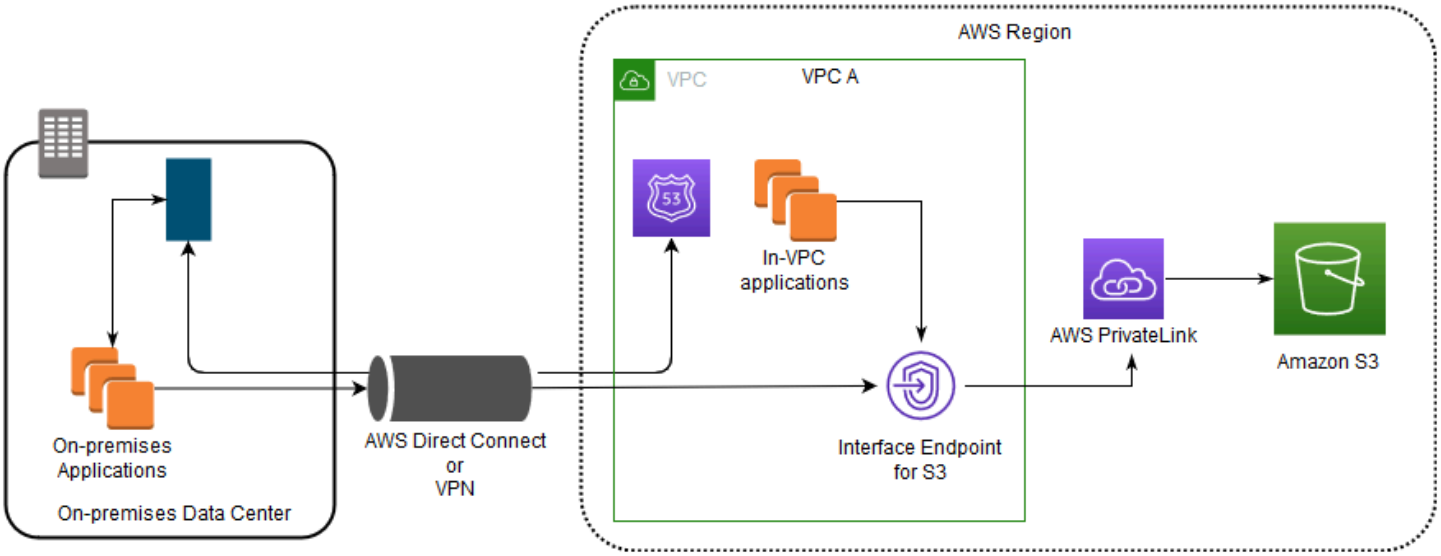
Atualizar uma configuração de DNS on-premises

Ao usar nomes de DNS específicos do endpoint para acessar os endpoints de interface do Amazon S3, você não precisa atualizar seu resolvedor de DNS on-premises. Você pode resolver o nome de

DNS específico do endpoint com o endereço IP privado do endpoint de interface do domínio DNS público do Amazon S3.

Usar endpoints de interface para acessar o Amazon S3 sem um endpoint de gateway ou um gateway da Internet na VPC

Os endpoints de interface na VPC podem rotear aplicativos na VPC e on-premises para o Amazon S3 pela rede da Amazon, conforme ilustrado no diagrama a seguir.



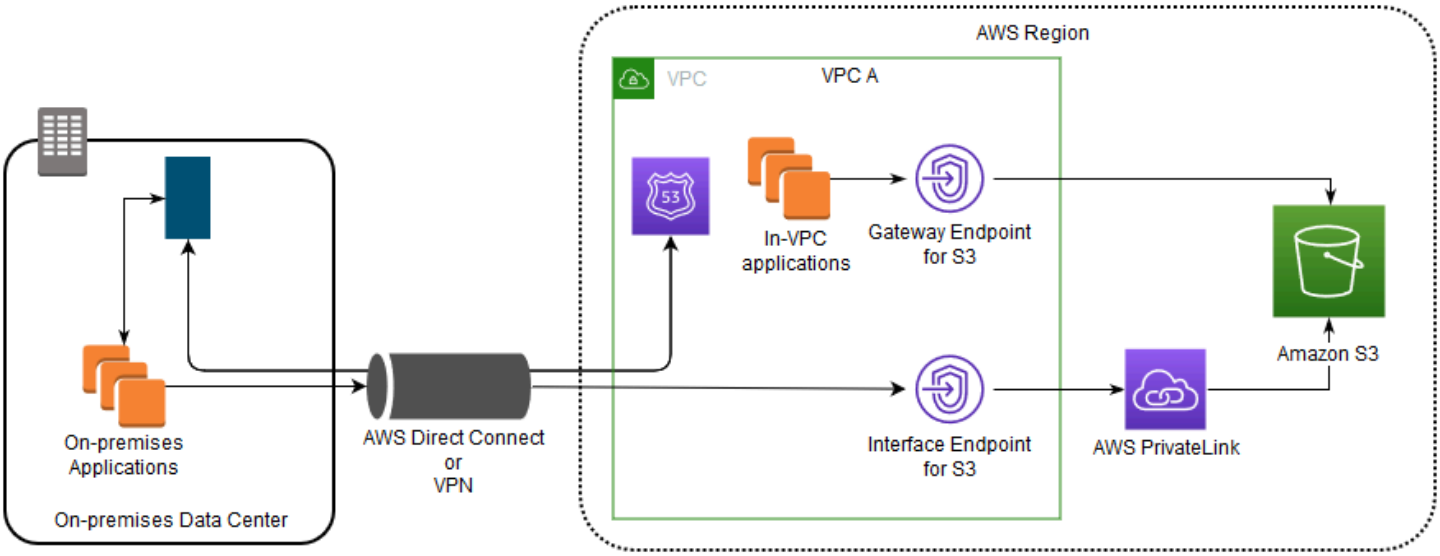
O diagrama ilustra o seguinte:

- Sua rede on-premises usa AWS Direct Connect ou AWS VPN para se conectar à VPC A.
- Seus aplicativos on-premises e na VPC A usam nomes de DNS específicos do endpoint para acessar o Amazon S3 por meio do endpoint de interface do S3.
- As aplicações on-premises enviam dados ao endpoint de interface na VPC via AWS Direct Connect (ou AWS VPN). O AWS PrivateLink move os dados do endpoint de interface para o Amazon S3 por meio da rede da AWS.
- As aplicações na VPC também enviam o tráfego ao endpoint de interface. O AWS PrivateLink move os dados do endpoint de interface para o Amazon S3 por meio da rede da AWS.

Usar endpoints de gateway e de interface juntos na mesma VPC para acessar o Amazon S3

Você pode criar endpoints de interface e reter o endpoint de gateway existente na mesma VPC, como mostra o diagrama a seguir. Ao adotar essa abordagem, você permite que as aplicações na VPC continuem acessando o Amazon S3 por meio do endpoint de gateway, que não é cobrado. Depois, apenas as aplicações on-premises usariam endpoints de interface para acessar o Amazon

S3. Para acessar o Amazon S3 dessa maneira, você deve atualizar as aplicações on-premises para usar nomes de DNS específicos do endpoint para Amazon S3.



O diagrama ilustra o seguinte:

- As aplicações on-premises usam nomes de DNS específicos do endpoint para enviar dados ao endpoint de interface dentro da VPC via AWS Direct Connect (ou AWS VPN). O AWS PrivateLink move os dados do endpoint de interface para o Amazon S3 por meio da rede da AWS.
- Usando nomes regionais padrão do Amazon S3, as aplicações na VPC enviam dados ao endpoint de gateway que se conecta ao Amazon S3 pela rede da AWS.

Para obter mais informações sobre endpoints de gateway, consulte Endpoints da VPC de gateway no Guia do usuário da VPC.

Criar uma política de VPC endpoint para o Amazon S3

É possível anexar uma política de endpoint ao VPC endpoint que controla o acesso ao Amazon S3. Essa política especifica as seguintes informações:

- A entidade principal do AWS Identity and Access Management (IAM) que pode executar ações
- As ações que podem ser executadas
- Os recursos nos quais as ações podem ser executadas

Você também pode usar políticas de bucket do Amazon S3 para restringir o acesso a buckets específicos de um endpoint da VPC específico usando a condição `aws:sourceVpce` na política

de bucket. Os exemplos a seguir mostram políticas que restringem o acesso a um bucket ou a um endpoint.

Tópicos

- Exemplo: restringir o acesso a um bucket específico a partir de um endpoint da VPC
- Exemplo: restringir o acesso a buckets em uma conta específica a partir de um endpoint da VPC
- Exemplo: restringir o acesso a um endpoint da VPC específico na política de bucket do S3

Exemplo: restringir o acesso a um bucket específico a partir de um endpoint da VPC

Você pode criar uma política de endpoint que restringe o acesso apenas a buckets específicos do Amazon S3. Esse tipo de política será útil se houver outros Serviços da AWS em sua VPC que usem buckets. A política de bucket a seguir restringe o acesso somente a *amzn-s3-demo-bucket1*. Para usar essa política de endpoint, substitua *amzn-s3-demo-bucket1* pelo nome do bucket.

```
{
  "Version": "2012-10-17",
  "Id": "Policy1415115909151",
  "Statement": [
    { "Sid": "Access-to-specific-bucket-only",
      "Principal": "*",
      "Action": [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Effect": "Allow",
      "Resource": ["arn:aws:s3:::amzn-s3-demo-bucket1",
                   "arn:aws:s3:::amzn-s3-demo-bucket1/*"]
    }
  ]
}
```

Exemplo: restringir o acesso a buckets em uma conta específica a partir de um endpoint da VPC

Você pode criar uma política de endpoint que restrinja o acesso apenas aos buckets do S3 em uma Conta da AWS específica. Para impedir que os clientes dentro da VPC acessem buckets que você não possui, use a declaração a seguir na política de endpoint. O exemplo a seguir cria uma política que restringe o acesso a recursos pertencentes a um único ID de Conta da AWS, *111122223333*.

```
{
```

```
  "Statement": [
    {
      "Sid": "Access-to-bucket-in-specific-account-only",
      "Principal": "*",
      "Action": [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Effect": "Deny",
      "Resource": "arn:aws:s3:::*",
      "Condition": {
        "StringNotEquals": {
          "aws:ResourceAccount": "111122223333"
        }
      }
    }
  ]
}
```

> **Note**
>
> Para especificar o ID da Conta da AWS do recurso que está sendo acessado, você pode usar a chave `aws:ResourceAccount` ou `s3:ResourceAccount` na política do IAM. No entanto, saiba que alguns Serviços da AWS dependem do acesso a buckets gerenciados pela AWS. Portanto, usar a chave `aws:ResourceAccount` ou `s3:ResourceAccount` em sua política do IAM também pode afetar o acesso a esses recursos.

Exemplo: restringir o acesso a um endpoint da VPC específico na política de bucket do S3

Exemplo: restringir o acesso a um endpoint da VPC específico na política de bucket do S3

A política de bucket do Amazon S3 a seguir permite o acesso a um bucket específico, *amzn-s3-demo-bucket2*, apenas pelo endpoint da VPC *vpce-1a2b3c4d*. Essa política negará todo acesso ao bucket se o endpoint especificado não estiver sendo usado. A condição `aws:sourceVpce` especifica o endpoint e não requer um nome do recurso da Amazon (ARN) para o recurso de endpoint da VPC, apenas o ID do endpoint. Para usar essa política de bucket, substitua *amzn-s3-demo-bucket2* e *vpce-1a2b3c4d* pelo nome e endpoint do bucket.

Important

- Ao aplicar as políticas de bucket do Amazon S3 a seguir para restringir o acesso somente a certos endpoints da VPC, você pode bloquear o acesso ao bucket inadvertidamente. As políticas de bucket destinadas especificamente a limitar o acesso do bucket às conexões originadas do endpoint da VPC podem bloquear todas as conexões ao bucket. Para obter informações sobre como corrigir esse problema, consulte Minha política de bucket tem o ID da VPC ou do endpoint da VPC incorreto. Como corrigir a política para que eu possa acessar o bucket? na Central de conhecimento do Suporte.
- Antes de usar a política de exemplo a seguir, substitua o ID do VPC endpoint por um valor apropriado para o caso de uso. Caso contrário, não será possível acessar o bucket.
- Essa política desabilita o acesso do console ao bucket especificado, pois as solicitações do console não se originam do VPC endpoint especificado.

```
{
  "Version": "2012-10-17",
  "Id": "Policy1415115909152",
  "Statement": [
    { "Sid": "Access-to-specific-VPCE-only",
      "Principal": "*",
      "Action": "s3:*",
      "Effect": "Deny",
      "Resource": ["arn:aws:s3:::amzn-s3-demo-bucket2",
                   "arn:aws:s3:::amzn-s3-demo-bucket2/*"],
      "Condition": {"StringNotEquals": {"aws:sourceVpce": "vpce-1a2b3c4d"}}
    }
  ]
}
```

Para obter mais exemplos de políticas, consulte Endpoints para o Amazon S3 no Guia do usuário da VPC.

Para obter mais informações sobre conectividade de VPC, consulte Network-to-VPC connectivity options (Opções de conectividade entre rede e VPC) no whitepaper da AWS Amazon Virtual Private Cloud Connectivity Options (Opções de conectividade do Amazon Virtual Private Cloud).

Validação de conformidade para o Amazon S3

Auditores terceiros avaliam a segurança e a conformidade do Amazon S3 como parte de vários programas de conformidade da AWS, incluindo o seguinte:

- Controles do Sistema e da Organização (CSO)
- Padrão de segurança de dados do setor de cartão de pagamento (PCI DSS – Payment Card Industry Data Security Standard)
- Federal Risk and Authorization Management Program (FedRAMP)
- Health Insurance Portability and Accountability Act (HIPAA)

A AWS fornece uma lista atualizada com frequência de serviços da AWS no escopo de programas de conformidade específicos em Serviços da AWS no escopo do programa de conformidade.

Os relatórios de auditoria de terceiros estão disponíveis para download por meio do AWS Artifact. Para obter mais informações, consulte Fazer o download de Relatórios no AWS Artifact.

Para obter mais informações sobre programas de conformidade da AWS, consulte Programas de conformidade da AWS.

Sua responsabilidade de conformidade ao usar o Amazon S3 é determinada pela confidencialidade de seus dados, pelas metas de conformidade da sua organização e pelas regulamentações e leis aplicáveis. Caso o uso do Amazon S3 esteja sujeito à conformidade com padrões como HIPAA, PCI ou FedRAMP, a AWS fornecerá os recursos para ajudar:

- Guias de início rápido de segurança e compatibilidade que discutem as considerações de arquitetura e fornecem etapas para a implantação de ambientes de linha de base focados em conformidade e segurança na AWS.
- O whitepaper Architecting for HIPAA Security and Compliance descreve como as empresas usam a AWS para ajudá-las a atender aos requisitos da HIPAA.
- Recursos de conformidade da AWS fornecem vários guias e manuais que podem se aplicar ao seu setor e local.
- AWS Config O pode ser usado para avaliar até que ponto suas configurações de recursos atendem adequadamente a práticas internas e a diretrizes e regulamentações do setor.
- O Security Hub da AWS fornece uma visão abrangente do seu estado de segurança na AWS que ajuda você a verificar a conformidade com os padrões e as melhores práticas do setor de segurança.

- O Bloquear objetos com o Bloqueio de Objetos pode ajudar a atender os requisitos de reguladores de serviços financeiros (como o SEC, FINRA e CFTC) que exigem armazenamento de dados WORM (Write Once, Read Many) para determinados tipos de informações gravadas.
- O Catalogar e analisar seus dados com o Inventário S3 pode ajudar você a auditar e gerar relatórios sobre o status da replicação e da criptografia de seus objetos para suas necessidades comerciais, de conformidade e regulatórias.

Resiliência no Amazon S3

A infraestrutura global da AWS é construída em torno de regiões e zonas de disponibilidade. As Regiões da AWS oferecem várias zonas de disponibilidade separadas e isoladas fisicamente que são conectadas com baixa latência, alto throughput e redes altamente redundantes. As zonas de disponibilidade oferecem a você uma forma eficiente para criar e operar aplicativos e bancos de dados. Elas são mais altamente disponíveis, tolerantes a falhas e escaláveis que infraestruturas com único data center ou infraestruturas com vários datacenters tradicionais. Se for necessário replicar seus dados especificamente em distâncias geográficas maiores, você poderá usar o Replicar objetos dentro de uma região e entre regiões, que permite a cópia automática e assíncrona de objetos entre buckets de diferentes Regiões da AWS.

Cada Região da AWS tem várias zonas de disponibilidade. Você pode implantar suas aplicações em diversas zonas de disponibilidade na mesma região para tolerância de falha e baixa latência. As zonas de disponibilidade são conectadas umas as outras com redes de fibra ótica rápidas e privadas, que permitem o desenvolvimento de aplicações submetidas a failover automaticamente entre as zonas de disponibilidade, sem interrupções.

Para obter mais informações sobre Regiões da AWS e zonas de disponibilidade, consulte Infraestrutura global da AWS.

Além da infraestrutura global da AWS, o Amazon S3 oferece vários recursos para oferecer suporte às suas necessidades de resiliência e backup de dados.

Configuração do ciclo de vida

> Uma configuração de ciclo de vida é um conjunto de regras que definem as ações aplicadas pelo Amazon S3 a um grupo de objetos. Com regras de configuração de ciclo de vida, é possível solicitar que o Amazon S3 faça a transição de objetos para classes de armazenamento menos caras, arquive-os ou exclua-os. Para obter mais informações, consulte Gerenciar o ciclo de vida dos objetos.

Versionamento

> Versionamento é um meio de manter diversas variantes de um objeto no mesmo bucket. O versionamento pode ser usado para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. Com o versionamento, você pode se recuperar, facilmente, de ações não intencionais do usuário e de falhas de aplicativo. Para obter mais informações, consulte Reter várias versões de objetos com o Versionamento do S3.

Bloqueio de objetos do S3

Você pode usar o bloqueio de objetos do S3 para armazenar objetos usando um modelo gravar uma vez, ler muitas (WORM, write once read many). Ao usar o bloqueio de objetos do S3, você pode evitar que um objeto seja excluído ou substituído por um período fixo ou indefinidamente. O bloqueio de objetos do S3 permite atender aos requisitos regulamentares que exigem armazenamento WORM, ou simplesmente adicionar uma camada extra de proteção contra alterações e exclusões de objetos. Para obter mais informações, consulte Bloquear objetos com o Bloqueio de Objetos.

Classes de armazenamento

O Amazon S3 oferece uma variedade de classes de armazenamento para escolher, de acordo com os requisitos da workload. As classes de armazenamento S3 Standard – IA e S3 One Zone – IA foram desenvolvidas para dados que você acessa cerca de uma vez por mês e precisam de acesso de milissegundos. A classe de armazenamento S3 Glacier Instant Retrieval foi projetada para dados de arquivo de longa duração com acesso de milissegundos que você acessa cerca de uma vez por trimestre. Para dados de arquivo que não necessitam de acesso imediato, como backups, use as classes de armazenamento S3 Glacier Flexieval ou S3 Glacier Deep Archive. Para obter mais informações, consulte Compreender e gerenciar classes de armazenamento do Amazon S3.

As melhores práticas de segurança a seguir também abordam resiliência:

- Enable versioning
- Consider Amazon S3 cross-region replication
- Identify and audit all your Amazon S3 buckets

Criptografia de backups do Amazon S3

Se estiver armazenando backups usando o Amazon S3, a criptografia dos backups dependerá da configuração desses buckets. O Amazon S3 fornece uma forma de configurar o comportamento de criptografia padrão para um bucket do S3. Você pode configurar a criptografia padrão em um bucket para que todos os objetos sejam criptografados quando forem armazenados nele. A criptografia padrão oferece suporte a chaves armazenadas no AWS KMS (SSE-KMS). Para obter mais informações, consulte Definir o comportamento padrão da criptografia para os buckets do Amazon S3.

Para obter mais informações sobre versionamento e bloqueio de objetos, consulte os seguintes tópicos: Reter várias versões de objetos com o Versionamento do S3 Bloquear objetos com o Bloqueio de Objetos

Segurança da infraestrutura no Amazon S3

Como um serviço gerenciado, o Amazon S3 é protegido pelo procedimento de segurança de redes global da AWS que são descritos no pilar de segurança do AWS Well-Architected Framework.

O acesso ao Amazon S3 pela rede acontece por meio de APIs publicadas pela AWS. Os clientes devem ser compatíveis com o Transport Layer Security (TLS) 1.2. Recomendamos também o suporte ao TLS 1.3. (Para obter mais informações sobre essa recomendação, consulte Conexões de nuvem AWS mais rápidas com TLS 1.3 no Blog de segurança da AWS.)

> **Note**
>
> O TLS 1.3 é compatível com todos os endpoints do S3, exceto no AWS PrivateLink para Amazon S3 e nos pontos de acesso multirregionais.

Os clientes também devem ter suporte a pacotes de criptografia com sigilo de encaminhamento perfeito (PFS) como Ephemeral Diffie-Hellman (DHE) ou Elliptic Curve Diffie-Hellman Encaminhamento (ECDHE). Além disso, as solicitações devem ser assinadas usando AWS Signature V4 ou AWS Signature V2, necessitando de credenciais válidas para o fornecimento.

Essas APIs podem ser chamadas de qualquer local da rede. No entanto, o Amazon S3 não oferece suporte a políticas de acesso com base em recursos, que podem incluir restrições com base no endereço IP de origem. Você também pode usar políticas de bucket do Amazon S3 para controlar o acesso a buckets a partir de endpoints específicos da virtual private cloud (VPC) ou de VPCs específicas. Efetivamente, isso isola o acesso à rede para um determinado bucket do Amazon S3 somente da VPC específica dentro da rede da AWS. Para obter mais informações, consulte Controlar o acesso a partir de VPC endpoints com políticas de bucket.

As melhores práticas de segurança a seguir também abordam a segurança de infraestrutura no Amazon S3:

- Consider VPC endpoints for Amazon S3 access
- Identify and audit all your Amazon S3 buckets

Análise de configuração e vulnerabilidade no Amazon S3

A AWS se encarrega das tarefas básicas de segurança, como aplicação de patches a bancos de dados e sistemas operacionais (SOs) convidados, configuração de firewalls e recuperação de desastres. Esses procedimentos foram revisados e certificados por terceiros certificados. Para obter mais detalhes, consulte os seguintes recursos da :

- Validação de conformidade para o Amazon S3
- Modelo de responsabilidade compartilhada
- Amazon Web Services: visão geral dos processos de segurança

As seguintes melhores práticas de segurança também abordam a análise de configuração e vulnerabilidade no Amazon S3:

- Identify and audit all your Amazon S3 buckets
- Habilitar AWS Config

Gerenciamento de acesso

O Amazon S3 fornece uma variedade de ferramentas de gerenciamento de acesso. Veja a seguir uma lista desses recursos e ferramentas. Você não precisa de todas essas ferramentas de gerenciamento de acesso, mas deve usar uma ou mais para conceder acesso a buckets e objetos do Amazon S3, além de outros Recursos do S3. A aplicação adequada dessas ferramentas pode ajudar a garantir que seus recursos só possam ser acessados pelos usuários pretendidos.

A ferramenta de gerenciamento de acesso mais usada é a política de acesso. Uma política de acesso pode ser uma política baseada em recurso vinculada a um recurso da AWS, como uma política de bucket para um bucket. Uma política de acesso também pode ser uma política baseada em identidade anexada a uma identidade do AWS Identity and Access Management (IAM), como um usuário, grupo ou perfil do IAM. A política de acesso descreve quem tem acesso a quê. Escreva uma política de acesso para conceder a Contas da AWS e usuários, grupos e perfis do IAM permissão para realizar operações em um recurso. Por exemplo, você pode conceder a permissão PUT `Object` para outra Conta da AWS de modo que o usuário possa fazer upload de objetos em seu bucket.

Veja a seguir as ferramentas de gerenciamento de acesso disponíveis no Amazon S3. Consulte um guia mais abrangente sobre o controle de acesso ao Amazon S3 em Controle de acesso no Amazon S3.

Política de bucket

Uma política de bucket do Amazon S3 é uma política baseada em recurso do AWS Identity and Access Management (IAM), formatada em JSON, que é anexada a determinado bucket. Use políticas de bucket para conceder a outras Contas da AWS ou identidades do IAM permissões de acesso ao bucket e aos objetos contidos nele. Muitos casos de uso de gerenciamento de acesso do S3 podem ser atendidos usando uma política de bucket. Com as políticas de bucket, é possível personalizar o acesso ao bucket para ajudar a garantir que somente as identidades que você aprovou possam acessar recursos e executar ações neles. Para obter mais informações, consulte Políticas de bucket para o Amazon S3.

Política baseada em identidade

Uma política de usuário do IAM ou baseada em identidade é um tipo de política do AWS Identity and Access Management(IAM). Uma política baseada em identidade é uma política em formato JSON anexada a usuários, grupos ou perfis do IAM em sua conta da AWS. Você pode usar políticas baseadas em identidade para conceder a uma identidade do IAM acesso a buckets ou objetos. É possível criar usuários, grupos e perfis do IAM em sua conta e anexar políticas de acesso a eles. Depois, você pode conceder acesso a recursos da AWS, incluindo recursos do Amazon S3. Para obter mais informações, consulte Políticas baseadas em identidade do Amazon S3.

Concessões de Acesso do S3

Use a funcionalidade Concessões de Acesso do S3 para criar concessões de acesso aos seus dados do Amazon S3 para identidades em diretórios de identidades corporativas, como Active Directory, e para identidades do AWS Identity and Access Management (IAM). A funcionalidade Concessões de Acesso do S3 ajuda você a gerenciar permissões de dados em grande escala. Além disso, a funcionalidade Concessões de Acesso do S3 registra a identidade do usuário final e a aplicação usada para acessar os dados do S3 em logs do AWS CloudTrail. Isso fornece um histórico de auditoria detalhado até a identidade do usuário final para todos os acessos aos dados em seus buckets do S3. Para obter mais informações, consulte Gerenciar o acesso com a funcionalidade Concessões de Acesso do S3.

Pontos de acesso

A funcionalidade Pontos de Acesso Amazon S3 simplifica o gerenciamento do acesso a dados em escala para aplicações que usam conjuntos de dados compartilhados no S3. Os pontos de acesso são endpoints de rede nomeados que são anexados a um bucket. Você pode usar os pontos de acesso para executar operações em objetos do S3 em grande escala, como fazer upload e recuperar objetos. Um bucket pode ter até 10.000 pontos de acesso anexados, e é possível impor permissões distintas e controles de rede a cada ponto de acesso para fornecer controle detalhado sobre o acesso aos objetos do S3. A funcionalidade Pontos de Acesso do S3 pode ser associada a buckets na mesma conta ou em outra conta confiável. As políticas de pontos de acesso são políticas baseadas em recurso que são avaliadas em conjunto com a política de bucket correspondente. Para obter mais informações, consulte Gerenciar o acesso a conjuntos de dados compartilhados com pontos de acesso.

Lista de controle de acesso (ACL)

Uma ACL é uma lista de concessões que identifica o concessionário e a permissão concedida. As ACLs concedem permissões básicas de leitura ou gravação a outras Contas da AWS. As ACLs usam um esquema XML específico do Amazon S3. Uma ACL é um tipo de política do AWS Identity and Access Management (IAM). Uma ACL de objeto é usada para gerenciar o acesso a um objeto, e uma ACL de bucket é usada para gerenciar o acesso a um bucket. No caso das políticas de bucket, há uma única política para o bucket todo, mas as ACLs de objeto são especificadas por objeto. Recomendamos manter as ACLs desativadas, exceto em circunstâncias incomuns em que seja necessário controlar o acesso para cada objeto individualmente. Para obter mais informações sobre como usar ACLs, consulte Controlar a propriedade de objetos e desabilitar ACLs para seu bucket.

> **Warning**
>
> A maioria dos casos de uso modernos no Amazon S3 não exige o uso de ACLs.

Propriedade de Objeto

Para gerenciar o acesso a um objeto, você precisa ser o proprietário desse objeto. Você pode usar a configuração Propriedade de Objeto ao nível do bucket para controlar a propriedade de objetos carregados no bucket. Além disso, use a Propriedade de Objeto para ativar as ACLs. Por padrão, a Propriedade de Objeto é definida como a configuração Imposto pelo proprietário do bucket e todas as ACLs estão desativadas. Quando as ACLs estão desativadas, o proprietário do bucket possui todos os objetos do bucket e gerencia exclusivamente o acesso aos dados. Para gerenciar o acesso, o proprietário do bucket usa políticas ou outra ferramenta de gerenciamento de acesso, excluindo as

ACLs. Para obter mais informações, consulte Controlar a propriedade de objetos e desabilitar ACLs para seu bucket.

Consulte um guia mais abrangente sobre o controle de acesso ao Amazon S3 e práticas recomendadas adicionais em Controle de acesso no Amazon S3.

Proteção de dados no Amazon S3

Além da resiliência oferecida pela infraestrutura global da AWS, o Amazon S3 oferece vários recursos para proteger os dados contra exclusões acidentais ou falhas regionais.

Replicação do S3

É possível usar a replicação em tempo real para habilitar a cópia automática e assíncrona de objetos nos buckets do Amazon S3. Os buckets configurados para replicação de objetos podem pertencer à mesma conta da Conta da AWS ou a contas diferentes. Os objetos podem ser replicados em um ou em vários buckets de destino. Os buckets de destino podem estar em Regiões da AWS diferentes ou na mesma região que o bucket de origem. Para habilitar os controles de failover, é possível configurar a replicação como bidirecional para que os buckets de origem e de destino possam ser mantidos sincronizados durante uma falha regional. Para obter mais informações, consulte the section called “Replicar objetos dentro de uma região e entre regiões”.

Pontos de Acesso Multirregionais e controles de failover

Os pontos de acesso multirregionais do Amazon S3 fornecem um endpoint global que as aplicações podem usar para atender a solicitações de buckets do S3 localizados em várias Regiões da AWS. Você pode usar pontos de acesso multirregionais para criar aplicações de várias regiões com a mesma arquitetura usada em uma única região, depois executar essas aplicações em qualquer lugar do mundo. Em vez de enviar solicitações pela Internet pública congestionada, os pontos de acesso multirregionais fornecem resiliência de rede integrada com aceleração de solicitações baseadas na Internet para o Amazon S3. Solicitações de aplicações feitas para um endpoint global de ponto de acesso multirregional usam o AWS Global Accelerator para rotear automaticamente pela rede global da AWS para o bucket do S3 mais próximo com status de roteamento ativo. Consulte mais informações sobre Pontos de Acesso Multirregionais em the section called “Gerenciar o tráfego multirregional ”.

Com os controles de failover para pontos de acesso multirregionais do Amazon S3, você pode manter a continuidade dos negócios durante interrupções no tráfego regional e, ao mesmo tempo, oferecer às aplicações uma arquitetura multirregional para atender às necessidades de conformidade e redundância. Se seu tráfego regional for interrompido, você poderá usar controles de failover para pontos de acesso multirregionais para selecionar quais Regiões da AWS por trás de um ponto de acesso multirregional do Amazon S3 vão processar as solicitações de acesso e armazenamento de dados.

Para oferecer suporte a failover, você pode configurar seu ponto de acesso multirregional em uma configuração ativa-passiva, com tráfego fluindo para a região ativa em condições normais e uma região passiva em espera para failover. Se você tiver a Replicação do S3 Entre Regiões Diferentes (CRR) habilitada com regras de replicação bidirecional, poderá manter seus buckets sincronizados durante um failover. Consulte mais informações sobre controles de failover em the section called “Configuração de failover”.

Versionamento do S3

Versionamento é um meio de manter diversas variantes de um objeto no mesmo bucket. O versionamento pode ser usado para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. Com o versionamento, você pode se recuperar, facilmente, de ações não intencionais do usuário e de falhas de aplicativo. Para obter mais informações, consulte Reter várias versões de objetos com o Versionamento do S3.

Bloqueio de objetos do S3

Você pode usar o bloqueio de objetos do S3 para armazenar objetos usando um modelo gravar uma vez, ler muitas (WORM, write once read many). Ao usar o bloqueio de objetos do S3, você pode evitar que um objeto seja excluído ou substituído por um período fixo ou indefinidamente. O bloqueio de objetos do S3 permite atender aos requisitos regulamentares que exigem armazenamento WORM, ou simplesmente adicionar uma camada extra de proteção contra alterações e exclusões de objetos. Para obter mais informações, consulte Bloquear objetos com o Bloqueio de Objetos.

AWS Backup

O Amazon S3 é integrado nativamente ao AWS Backup, um serviço totalmente gerenciado e baseado em políticas que você pode usar para definir políticas de backup centralmente e proteger dados do Amazon S3. Depois de definir suas políticas de backup e atribuir recursos do Amazon S3 às políticas, o AWS Backup automatiza a criação de backups do Amazon S3 e os armazena com segurança em um cofre de backup criptografado designado pelo seu plano de backup. Para obter mais informações, consulte the section called “Fazer backup de seus dados”.

Consulte um tutorial sobe como usar alguns desses recursos em conjunto para proteger seus dados em Tutorial: Proteja os dados no Amazon S3 contra exclusão acidental ou bugs de aplicativos que usam o versionamento do S3, o bloqueio de objetos do S3 e a replicação do S3.

> **Important**
>
> Além de usar os recursos anteriores para proteger seus dados, recomendamos que você consulte as recomendações em the section called “Práticas recomendadas de segurança”.

Tópicos

- Replicar objetos dentro de uma região e entre regiões
- Gerenciar o tráfego multirregional com Pontos de Acesso Multirregionais
- Reter várias versões de objetos com o Versionamento do S3
- Bloquear objetos com o Bloqueio de Objetos
- Fazer backup de dados do Amazon S3

Replicar objetos dentro de uma região e entre regiões

É possível usar a replicação para habilitar a cópia automática e assíncrona de objetos nos buckets do Amazon S3. Os buckets configurados para replicação de objetos podem pertencer à mesma conta da Conta da AWS ou a contas diferentes. Os objetos podem ser replicados em um ou em vários buckets de destino. Os buckets de destino podem estar em Regiões da AWS diferentes ou na mesma região que o bucket de origem.

Há dois tipos de replicação: replicação em tempo real e replicação sob demanda.

- Replicação em tempo real: para replicar automaticamente objetos novos e atualizados à medida que são gravados no bucket de origem, use a replicação em tempo real. A replicação em tempo real não replica nenhum objeto que já existia no bucket antes de você configurar a replicação. Para replicar objetos que já existiam antes de você configurar a replicação, use a replicação sob demanda.
- Replicação sob demanda: para replicar objetos existentes do bucket de origem para um ou mais buckets de destino sob demanda, use a Replicação em Lote do S3. Para obter mais informações sobre replicação de objetos existentes, consulte Quando usar S3 Batch Replication.

Há duas formas de replicação em tempo real: Replicação Entre Regiões Diferentes (CRR) e Replicação na Mesma Região (SRR).

- Replicação Entre Regiões Diferentes (CRR): é possível usar a CRR para replicar objetos entre buckets do Amazon S3 em Regiões da AWS diferentes. Para obter mais informações sobre CRR, consulte the section called “Quando usar a replicação entre regiões”.
- Replicação na Mesma Região (SRR): é possível usar a SRR para copiar objetos entre buckets do Amazon S3 na mesma Região da AWS. Consulte mais informações sobre SRR em the section called “Quando usar Replicação na mesma região”.

Tópicos

- Por que usar a replicação?
- Quando usar a replicação entre regiões
- Quando usar Replicação na mesma região
- Quando usar a replicação bidirecional
- Quando usar S3 Batch Replication
- Requisitos de workload e replicação em tempo real
- O que o Amazon S3 replica?
- Requisitos e considerações de replicação
- Visão geral da configuração da replicação em tempo real
- Gerenciar ou pausar a replicação em tempo real
- Replicar objetos existentes com o Replicação em Lote
- Solução de problemas de replicação
- Monitorar a replicação com métricas, notificações de eventos e status

Por que usar a replicação?

A replicação pode ajudar você a fazer o seguinte:

- Replicar objetos retendo os metadados: você pode usar a replicação para fazer cópias dos objetos retendo todos os metadados, como as horas de criação e os IDs de versão dos objetos originais. Esse recurso é importante se você precisar garantir que a réplica seja idêntica ao objeto original.
- Replicar objetos em diferentes classes de armazenamento: você pode usar a replicação para colocar objetos diretamente nas classes de armazenamento S3 Glacier Flexible Retrieval, S3 Glacier Deep Archive ou em outra classe de armazenamento no bucket de destino. Você também pode replicar seus dados para a mesma classe de armazenamento e usar configurações de ciclo

de vida nos buckets de destino para mover os objetos para uma classe de armazenamento “mais fria” à medida que eles forem ficando velhos.

- Manter cópias de objetos com proprietários diferentes: independentemente de quem seja o proprietário do objeto original, você pode instruir o Simple Storage Service (Amazon S3) a alterar o proprietário da réplica para a Conta da AWS que é proprietária do bucket de destino. Isso se chama opção de substituição do proprietário. Você pode usar esta opção para restringir acesso às replicas do objeto.
- Manter objetos armazenados em várias Regiões da AWS: para garantir diferenças geográficas em onde seus dados são mantidos, você pode definir vários buckets de destino em diferentes Regiões da AWS. Esse recurso pode ajudar a atender a determinados requisitos de conformidade.
- Replicar objetos dentro de 15 minutos: para replicar dados na mesma Região da AWS ou entre diferentes regiões dentro de um período previsível, você pode usar S3 Replication Time Control (S3 RTC - Controle de Horário de Replicação do S3). O S3 RTC replica 99,99 por cento dos novos objetos armazenados no Simple Storage Service (Amazon S3) em 15 minutos (baseado em um acordo de nível de serviço). Para obter mais informações, consulte the section called “Uso do Controle do tempo de replicação do S3”.

  > **Note**
  >
  > O S3 RTC não se aplica à replicação em lote. A replicação em lote é um trabalho de replicação sob demanda e pode ser rastreada com o recurso S3 Batch Operations. Para obter mais informações, consulte Monitoramento de relatórios de status e conclusão.

- Sincronizar buckets, replicar objetos existentes e replicar objetos cuja replicação falhou anteriormente: para sincronizar buckets e replicar objetos existentes, use a replicação em lote como uma ação de replicação sob demanda. Para obter mais informações sobre quando usar a replicação em lote, consulte Quando usar S3 Batch Replication.
- Replicar objetos e fazer failover para um bucket em outra Região da AWS: para manter todos os metadados e objetos sincronizados entre os buckets durante a replicação de dados, use regras de replicação bidirecional antes de configurar os controles de failover para pontos de acesso multirregionais do Amazon S3. As regras de replicação bidirecional ajudam a garantir que, quando os dados são gravados no bucket do S3 para o qual o tráfego faz failover, esses dados sejam replicados de volta para o bucket de origem.

Quando usar a replicação entre regiões

A replicação entre regiões (CRR) do S3 é usada para copiar objetos entre buckets do Amazon S3 em Regiões da AWS diferentes. As tags podem ajudar a fazer o seguinte:

- Atender aos requisitos de conformidade: embora o Simple Storage Service (Amazon S3), por padrão, armazene seus dados em diversas zonas de disponibilidade geograficamente distantes, requisitos de conformidade podem exigir que você armazene os dados a distâncias ainda maiores. Para atender a esses requisitos, use a Cross-Region Replication para replicar dados entre Regiões da AWS distantes.
- Minimizar a latência: se seus clientes estiverem em duas localizações geográficas diferentes, é possível minimizar a latência no acesso a objetos mantendo cópias dos objetos nas Regiões da AWS geograficamente mais próximas dos usuários.
- Aumentar a eficiência operacional: se tiver clusters de computação em duas Regiões da AWS diferentes que analisam o mesmo conjunto de objetos, talvez você prefira manter cópias dos objetos nessas regiões.

Quando usar Replicação na mesma região

A replicação para a mesma região (SRR) é usada para copiar objetos entre buckets do Amazon S3 na mesma Região da AWS. A SRR pode ajudar a fazer o seguinte:

- Agregar logs em um único bucket: se você armazenar os logs em vários buckets ou em várias contas, será possível replicar facilmente os logs em um único bucket na região. Isso permite processar os logs em um único local, o que é mais simples.
- Configurar replicação em tempo real entre contas de produção e teste: se você ou seus clientes tiverem contas de produção e de teste que usam os mesmos dados, será possível replicar objetos entre essas várias contas, mantendo os metadados dos objetos.
- Cumprir as leis de soberania de dados: pode ser necessário armazenar várias cópias dos dados em Contas da AWS separadas em uma determinada região. A replicação na mesma região pode ajudar a replicar automaticamente dados vitais quando os regulamentos de conformidade não permitirem que os dados saiam do país.

Quando usar a replicação bidirecional

- Criar conjuntos de dados compartilhados entre várias Regiões da AWS: com a sincronização de modificações da réplica, você pode replicar facilmente alterações de metadados, como listas de controle de acesso (ACLs) de objetos, etiquetas de objetos ou bloqueios de objetos, em objetos de replicação. Essa replicação bidirecional é importante se você quiser manter todos os objetos e alterações nos metadados dos objetos em sincronia. Você pode ativar a sincronização de modificações da réplica em uma regra de replicação nova ou existente ao realizar a replicação bidirecional entre dois ou mais buckets na mesma região ou em Regiões da AWS diferentes.
- Manter os dados sincronizados entre regiões durante o failover: você pode sincronizar dados em buckets entre Regiões da AWS configurando regras de replicação bidirecional com a Replicação do S3 Entre Regiões Diferentes (CRR) diretamente de um ponto de acesso multirregional. Para tomar uma decisão embasada sobre quando iniciar um failover, você também pode habilitar as métricas de replicação do S3 para monitorar a replicação no Amazon CloudWatch, no Controle de Tempo de Replicação do S3 (S3 RTC) ou no ponto de acesso multirregional.
- Tornar a aplicação altamente disponível: mesmo no caso de uma interrupção no tráfego regional, você pode usar regras de replicação bidirecional para manter todos os metadados e objetos sincronizados entre os buckets durante a replicação de dados.

Quando usar S3 Batch Replication

A replicação em lote replica objetos existentes em diferentes buckets como uma opção sob demanda. Ao contrário da replicação em tempo real, esses trabalhos podem ser executados conforme a necessidade. A replicação em lote pode ajudar você a fazer o seguinte:

- Replicar objetos existentes: você pode usar a replicação em lote para replicar objetos que foram adicionados ao bucket antes que a Same-Region Replication ou a Cross-Region Replication fossem configuradas.
- Replicar objetos cuja replicação falhou anteriormente: você pode filtrar um trabalho de replicação em lote para tentar replicar objetos com um status de replicação de FAILED (FALHOU).
- Replicar objetos que já foram replicados: pode ser necessário armazenar várias cópias dos dados em Contas da AWS ou Regiões da AWS separadas. A replicação em lote pode replicar objetos existentes em destinos recém-adicionados.
- Replicar réplicas de objetos que foram criadas segundo uma regra de replicação: as configurações de replicação criam réplicas de objetos em buckets de destino. As réplicas de objetos só podem ser replicadas com a replicação em lote.

Requisitos de workload e replicação em tempo real

Dependendo dos requisitos de workload, alguns tipos de replicação em tempo real serão mais adequados ao seu caso de uso do que outros. Use a tabela a seguir para determinar qual tipo de replicação usar para a sua situação e se você deve usar o Controle de Tempo de Replicação do S3 (S3 RTC) para sua workload. O S3 RTC replica 99,99% dos novos objetos armazenados no Amazon S3 em 15 minutos (baseado em um acordo de nível de serviço, ou SLA). Para obter mais informações, consulte the section called “Uso do Controle do tempo de replicação do S3”.

Requisito de workload	S3 RTC (SLA de 15 minutos)	Replicação Entre Regiões Diferentes (CRR)	Replicação na Mesma Região (SRR)
Replicar objetos entre Contas da AWS diferentes	Sim	Sim	Sim
Replicar objetos na mesma Região da AWS dentro de 24 a 48 horas (sem suporte de SLA)	Não	Não	Sim
Replicar objetos entre Regiões da AWS diferentes dentro de 24 a 48 horas (sem suporte de SLA)	Não	Sim	Não
Tempo de replicação previsível: apoiado pelo SLA para replicar 99,9% dos objetos em 15 minutos	Sim	Não	Não

O que o Amazon S3 replica?

O Amazon S3 replica somente itens específicos nos buckets que estão configurados para replicação.

Tópicos

- O que é replicado com as configurações de replicação?
- O que não é replicado com as configurações de replicação?

O que é replicado com as configurações de replicação?

Por padrão, o Simple Storage Service (Amazon S3) replica o seguinte:

- Objetos criados depois de adicionar uma configuração de replicação.
- Objetos não criptografados.
- Objetos criptografados usando chaves fornecidas pelo cliente (SSE-C), objetos criptografados em repouso por uma chave gerenciada pelo Amazon S3 (SSE-S3) ou uma chave do KMS armazenada no AWS Key Management Service (SSE-KMS). Para obter mais informações, consulte the section called “Replicar objetos criptografados”.
- Metadados de objeto dos objetos de origem para as réplicas. Para obter informações sobre como replicar metadados das réplicas para os objetos de origem, consulte Replicação de alterações de metadados com sincronização de modificação de réplica.
- Somente os objetos no bucket de origem para os quais o proprietário do bucket tenha permissões para ler objetos e listas de controle de acesso (ACLs).

  Para obter mais informações sobre propriedade de recurso, consulte Propriedade de bucket e objeto do Amazon S3.
- A ACL do objeto é atualizada, a menos que você oriente o Amazon S3 a alterar a propriedade da réplica quando os buckets de origem e de destino não forem de propriedade das mesmas contas.

  Para obter mais informações, consulte Alterar o proprietário da réplica.

  Pode levar um tempo até o Amazon S3 sincronizar as duas ACLs. Essa alteração de proprietário aplica-se apenas aos objetos criados depois que você adiciona uma configuração de replicação ao bucket.
- Tags de objeto, se houver.
- Informações de retenção de bloqueio de objetos do S3, se houver.

Quando o Amazon S3 replica objetos que tenham informações de retenção aplicadas, ele aplica esse mesmo controles de retenção à suas réplicas, substituindo o período de retenção padrão configurado nos buckets de destino. Se você não tiver controles de retenção aplicados aos objetos em seu bucket de origem e replicá-los em buckets de destino que tenham um período de retenção definido, o período de retenção padrão do bucket de destino será aplicado às réplicas de objeto. Para obter mais informações, consulte Bloquear objetos com o Bloqueio de Objetos.

Como a exclusão de operações afeta a replicação

Se você excluir um objeto do bucket de origem, as seguintes ações ocorrerão por padrão:

- Se você fizer uma solicitação DELETE sem especificar um ID de versão de objeto, o Amazon S3 adicionará um marcador de exclusão. O Amazon S3 lida com o marcador de exclusão da seguinte forma:
  - Se estiver usando a versão mais recente da configuração de replicação (ou seja, se você especificar o elemento `Filter` em uma regra de configuração da replicação), o Amazon S3 não replicará o marcador de exclusão, por padrão. Porém, você pode adicionar replicação de marcador de exclusão a regras não baseadas em etiquetas. Para obter mais informações, consulte Replicação de marcadores de exclusão entre intervalos.
  - Se você não especificar o elemento `Filter`, o Amazon S3 assumirá que a configuração de replicação é a versão V1 e replicará marcadores de exclusão resultantes de ações do usuário. No entanto, se o Amazon S3 excluir um objeto devido a uma ação de ciclo de vida, o marcador de exclusão não será replicado para os buckets de destino.
- Se você especificar um ID de versão do objeto para excluir na solicitação `DELETE`, o Amazon S3 excluirá essa versão do objeto no bucket de origem. Porém, ele não replica a exclusão no bucket de destino. Em outras palavras: ele não exclui a mesma versão do objeto dos buckets de destino. Isso protege os dados contra exclusões mal-intencionadas.

O que não é replicado com as configurações de replicação?

Por padrão, o Simple Storage Service (Amazon S3) não replica o seguinte:

- Objetos no bucket de origem que são réplicas criadas por outra regra de replicação. Por exemplo, se você configurar uma replicação em que o bucket A é a origem e o bucket B é o destino. Agora, suponha que você adicione outra configuração da replicação em que o bucket B é a origem e o

bucket C é o destino. Neste caso, os objetos no bucket B que são réplicas de objetos no bucket A não serão replicados para o bucket C.

Para replicar objetos que são réplicas, use a replicação em lote. Saiba mais sobre como configurar a replicação em lote em Replicar objetos existentes.

- Objetos no bucket de origem que já foram replicados para um destino diferente. Por exemplo, se você alterar o bucket de destino em uma configuração de replicação existente, o Simple Storage Service (Amazon S3) não replicará os objetos novamente.

  Para replicar objetos que já foram replicados anteriormente, use a replicação em lote. Saiba mais sobre como configurar a replicação em lote em Replicar objetos existentes.

- A replicação em lote não é compatível com a nova replicação de objetos que foram excluídos com o ID de versão do objeto do bucket de destino. Para replicar esses objetos novamente, copie os objetos de origem no local com um trabalho de cópia em lote. Copiar esses objetos no local criará versões dos objetos no bucket de origem e iniciará a replicação automaticamente para o destino. Para obter mais informações sobre como usar a cópia em lote, consulte Exemplos que usam o Batch Operations para copiar objetos.

- Por padrão, ao replicar de uma Conta da AWS diferente, os marcadores de exclusão adicionados ao bucket de origem não são replicados.

  Para obter mais informações sobre como os marcadores de exclusão funcionam, consulte Replicação de marcadores de exclusão entre intervalos.

- Objetos armazenados nas classes ou nos níveis de armazenamento S3 Glacier Flexible Retrieval, S3 Glacier Deep Archive, S3 Intelligent-Tiering Archive Access ou S3 Intelligent-Tiering Deep Archive Access. Não é possível replicar esses objetos enquanto eles não forem restaurados e copiados para uma classe de armazenamento diferente.

  Para saber mais sobre as classes S3 Glacier Flexible Retrieval e S3 Glacier Deep Archive, consulte Classes de armazenamento para objetos acessados raramente.

  Para saber mais sobre a classe S3 Intelligent-Tiering, consulte Gerenciar custos de armazenamento com o Amazon S3 Intelligent-Tiering.

- Objetos no bucket de origem que o proprietário do bucket não tem permissões suficientes para replicar.

Para obter informações sobre como o proprietário de um objeto pode conceder permissões ao proprietário do bucket, consulte Conceder permissões entre contas para fazer upload de objetos garantindo que o proprietário do bucket tenha controle total.

- Atualizações nos sub-recursos no nível do bucket.

  Por exemplo, se você alterar a configuração do ciclo de vida ou adicionar uma configuração de notificação ao bucket de origem, essas alterações não serão aplicadas ao bucket de destino. Esse recurso torna possível ter configurações diferentes no buckets de origem e de destino.

- Ações realizadas pela configuração do ciclo de vida.

  Por exemplo, se a configuração de ciclo de vida estiver habilitada apenas no seu bucket de origem, o Amazon S3 criará marcadores de exclusão para objetos expirados, mas não replicará esses marcadores. Se você quiser que a mesma configuração de ciclo de vida seja aplicada aos buckets de origem e de destino, habilite a mesma configuração de ciclo de vida em ambos. Para obter mais informações sobre a configuração do ciclo de vida, consulte Gerenciar o ciclo de vida dos objetos.

- Ao usar regras de replicação baseadas em etiquetas com replicação em tempo real, novos objetos precisam ser marcados com a etiqueta da regra de replicação correspondente na operação `PutObject`. Caso contrário, os objetos não serão replicados. Se os objetos forem marcados após a operação `PutObject`, esses objetos também não serão replicados.

  Para replicar objetos que foram marcados após a operação `PutObject`, use a funcionalidade Replicação em Lote do S3. Para obter mais informações sobre replicação em lote, consulte Replicar objetos existentes.

Requisitos e considerações de replicação

A replicação do Amazon S3 exige o seguinte:

- O proprietário do bucket de origem deve ter as Regiões da AWS de origem e de destino habilitadas para a conta. O proprietário do bucket de destino deve ter a região de destino habilitada para a conta.

  Consulte mais informações sobre como habilitar ou desabilitar uma Região da AWS em Specify which Regiões da AWS your account can use no Guia de referência do AWS Gerenciamento de contas.

- Tanto o bucket de origem quanto o de destino devem ter o versionamento habilitado. Para obter mais informações sobre versionamento, consulte Reter várias versões de objetos com o Versionamento do S3.
- O Amazon S3 deve ter permissões para replicar objetos do bucket de origem para o bucket de destino ou buckets em seu nome. Para obter mais informações sobre essas permissões, consulte Configurar permissões para replicação em tempo real.
- Se o proprietário do bucket de origem não for proprietário do objeto no bucket, o proprietário do objeto precisará conceder ao proprietário do bucket as permissões `READ` e `READ_ACP` com a lista de controle de acesso (ACL) do objeto. Para obter mais informações, consulte Visão geral da lista de controle de acesso (ACL).
- Se o bucket de origem tiver o Bloqueio de objetos do S3 habilitado, o bucket de destino também deverá ter o Bloqueio de objetos do S3 habilitado.

  Para habilitar a replicação em um bucket que tenha a funcionalidade Bloqueio de Objetos habilitada, você deve usar a AWS Command Line Interface, a API REST ou os AWS SDKs. Para obter mais informações gerais, consulte Bloquear objetos com o Bloqueio de Objetos.

  > **Note**
  >
  > É necessário conceder duas novas permissões no bucket de origem do S3 na função do AWS Identity and Access Management (IAM) usada para configurar a replicação. As duas novas permissões são `s3:GetObjectRetention` e `s3:GetObjectLegalHold`. Se a função tiver uma permissão `s3:Get*`, ela satisfaz os requisitos. Para obter mais informações, consulte Configurar permissões para replicação em tempo real.

Para obter mais informações, consulte Visão geral da configuração da replicação em tempo real.

Se você estiver definindo a configuração de replicação em um cenário entre contas, no qual os buckets de origem e de destino pertencem a diferentes Contas da AWS, o seguinte requisito adicional se aplicará:

- O proprietário dos buckets de destino precisa conceder ao proprietário do bucket de origem permissões para replicar objetos com uma política de bucket. Para obter mais informações, consulte Conceder permissões quando os buckets de origem e de destino pertencerem a Contas da AWS diferentes.

- O bucket de destino não pode ser configurado como um bucket de Pagamento pelo solicitante. Para obter mais informações, consulte Utilizar buckets de uso geral com pagamento pelo solicitante para transferência e uso de armazenamento.

Considerações de replicação

Antes de criar uma configuração de replicação, esteja ciente das considerações a seguir.

Tópicos

- Configuração de ciclo de vida e réplicas de objeto
- Configuração do versionamento e configuração de replicação
- Usar a replicação do S3 com o S3 Intelligent-Tiering
- Configuração de log e de replicação
- CRR e a região de destino
- Replicação em Lote do S3
- Controle do tempo de replicação do S3

Configuração de ciclo de vida e réplicas de objeto

O tempo que o Amazon S3 leva para replicar um objeto depende do tamanho do objeto. Para objetos grandes, pode levar várias horas. Embora possa demorar um pouco até a réplica ser disponibilizada no destino, demora o mesmo tempo para criar a réplica que demorou para criar o objeto correspondente no bucket de origem. Se uma configuração de ciclo de vida estiver ativada em um bucket de destino, as regras de ciclo de vida honrarão o tempo original de criação de objeto, não o momento em que a réplica foi disponibilizada no bucket de destino.

A configuração de replicação requer que o bucket seja ativado por versionamento. Ao habilitar o versionamento em um bucket, lembre-se de:

- Se você tiver uma configuração de ciclo de vida de expiração de um objeto, depois de ativar o versionamento, adicione uma política `NonCurrentVersionExpiration` para manter o mesmo comportamento de exclusão permanente de antes de ativar o versionamento.
- Se você tiver uma configuração de ciclo de vida de transição, depois de ativar o versionamento, considere adicionar uma política `NonCurrentVersionTransition`.

Configuração do versionamento e configuração de replicação

Os buckets de origem e de destino devem ter versionamento habilitado quando você configura replicação em um bucket. Depois que você habilitar o versionamento nos buckets de origem e de destino e configurar a replicação no bucket de origem, vai encontrar os seguintes problemas:

- Se você tentar desabilitar o versionamento do bucket de origem, o Amazon S3 retornará um erro. É necessário remover a configuração de replicação antes de desabilitar o versionamento o bucket de origem.
- Se você desabilitar o versionamento o bucket de destino, ocorrerá falha na replicação. O objeto de origem tem o status de replicação `FAILED`.

Usar a replicação do S3 com o S3 Intelligent-Tiering

A classe de armazenamento do S3 Intelligent-Tiering foi projetada para otimizar os custos de armazenamento, movendo automaticamente os dados para o nível de acesso mais econômico. Por uma cobrança pequena mensal de automação e monitoramento de objetos, o S3 Intelligent-Tiering monitora os padrões de acesso e move automaticamente os objetos que não foram acessados para níveis de acesso de baixo custo.

Replicação de objetos armazenados no S3 Intelligent-Tiering com replicação em lote do S3 ou invocação de CopyObject ou UploadPartCopy constitui acesso. Nesses casos, os objetos de origem das operações de cópia ou replicação são hierarquizados.

Para obter mais informações sobre o S3 Intelligent-Tiering, consulte Gerenciar custos de armazenamento com o Amazon S3 Intelligent-Tiering.

Configuração de log e de replicação

Se o Amazon S3 entregar logs em um bucket com a replicação habilitada, ele vai replicar os objetos do log.

Se os logs de acesso do servidor ou os logs do AWS CloudTrail estiverem habilitados no bucket de origem ou de destino, o Amazon S3 incluirá neles as solicitações relativas a replicação. Por exemplo, o Simple Storage Service (Amazon S3) registra cada objeto que ele replica.

CRR e a região de destino

A replicação entre regiões (CRR) do Amazon S3 é usada para copiar objetos entre buckets do S3 em Regiões da AWS diferentes. Você pode escolher a região do seu bucket de destino com base

nas suas necessidades comerciais ou nas considerações de custo. Por exemplo, as cobranças de transferência de dados entre regiões variam dependendo das regiões que você escolher.

Suponha que você escolheu Leste dos EUA (N. da Virgínia) (`us-east-1`) como a região do bucket de origem. Se escolher Oeste dos EUA (Oregon) (`us-west-2`) como a região dos buckets de destino, você pagará mais do que se escolher a região Leste dos EUA (Ohio) (`us-east-2`). Para obter informações sobre preços, consulte a seção "Definição de preço da transferência de dados" em Definição de preço do Amazon S3.

Não há cobranças de transferência de dados associadas à mesma região de replicação (SRR)

Replicação em Lote do S3

Consulte informações sobre considerações da Replicação em Lote em Considerações sobre o recurso S3 Batch Replication.

Controle do tempo de replicação do S3

Consulte informações sobre as considerações e as práticas recomendadas para o Controle de Tempo de Replicação do S3 (S3 RTC) em Melhores práticas e diretrizes do S3 RTC.

Visão geral da configuração da replicação em tempo real

> **Note**
>
> Objetos que já existiam antes de você configurar a replicação não são replicados automaticamente. Em outras palavras: o Amazon S3 não replica os objetos retroativamente. Para replicar objetos que foram criados antes da configuração de replicação, use S3 Batch Replication. Consulte mais informações sobre como configurar o Replicação em Lote em Replicar objetos existentes.

Adicione uma configuração de replicação ao bucket de origem para habilitar a replicação em tempo real: Replicação na Mesma Região (SRR) ou Replicação Entre Regiões Diferentes (CRR). Essa configuração instrui o Amazon S3 a replicar objetos conforme especificado. Na configuração de replicação, você deve fornecer o seguinte:

- Os buckets de destino: o bucket ou buckets onde você quer que o Simple Storage Service (Amazon S3) replique os objetos.

- Os objetos que você deseja replicar: é possível replicar todos os objetos no bucket de origem ou um subgrupo de objetos. Identifique um subgrupo fornecendo, na configuração, um prefixo do nome da chave, uma ou mais tags de objeto ou ambos.

  Por exemplo, se você configurar uma regra de replicação para replicar somente objetos com o prefixo de nome da chave `Tax/`, o Amazon S3 replicará objetos com chaves como `Tax/doc1` ou `Tax/doc2`. Porém, ele não replica objetos com a chave `Legal/doc3`. Se você especificar um prefixo e uma ou mais etiquetas, o Simple Storage Service (Amazon S3) replicará somente os objetos com o prefixo das chaves e as etiquetas específicas.
- Um perfil do AWS Identity and Access Management (IAM): o Amazon S3 assume esse perfil do IAM para replicar objetos em seu nome. Consulte mais informações sobre como criar esse perfil do IAM e gerenciar permissões em Configurar permissões para replicação em tempo real.

Além desses requisitos mínimos, você pode escolher as seguintes opções:

- Classe de armazenamento de réplicas: por padrão, o Simple Storage Service (Amazon S3) armazena réplicas de objetos usando a mesma classe de armazenamento do objeto de origem. Você pode especificar uma classe de armazenamento diferente para as réplicas.
- Propriedade da réplica: o Simple Storage Service (Amazon S3) pressupõe que a réplica de um objeto continue pertencendo ao proprietário do objeto de origem. Portanto, quando ele replica objetos, também replica a lista de controle de acesso (ACL) a objetos correspondente ou a configuração de propriedade de objetos do S3. Se os buckets de origem e destino pertencerem a Contas da AWS diferentes, você poderá configurar a replicação para alterar o proprietário de uma réplica para a Conta da AWS que é proprietária do bucket de destino. Para obter mais informações, consulte the section called “Alterar o proprietário da réplica”.

É possível configurar a replicação usando o console do Amazon S3, a AWS Command Line Interface (AWS CLI), SDKs da AWS ou a API REST do Amazon S3. Consulte demonstrações detalhadas de como configurar a replicação em the section called “Demonstrações de replicação”.

O Amazon S3 fornece operações da API REST para permitir a configuração das regras de replicação. Para obter mais informações, consulte os tópicos a seguir na Referência da API do Amazon Simple Storage Service:

- PutBucketReplication
- GetBucketReplication

- DeleteBucketReplication

Tópicos

- Elementos do arquivo de configuração de replicação
- Configurar permissões para replicação em tempo real
- Exemplos para configurar a replicação em tempo real

Elementos do arquivo de configuração de replicação

O Amazon S3 armazena uma configuração de replicação como XML. Se estiver configurando a replicação programaticamente por meio da API REST do Amazon S3, você especificará os vários elementos da configuração de replicação nesse arquivo XML. Se estiver configurando a replicação por meio da AWS Command Line Interface (AWS CLI), especifique a configuração de replicação usando o formato JSON. Com relação a exemplos de JSON, consulte as demonstrações em the section called “Demonstrações de replicação”.

> **Note**
>
> A versão mais recente do formato XML de configuração da replicação é V2. As configurações de replicação XML V2 são aquelas que contêm o elemento `<Filter>` para regras e regras que especificam o Controle do tempo de replicação do S3 (S3 RTC).
> Para ver a versão da configuração de replicação, você pode usar a operação de API `GetBucketReplication`. Para obter mais informações, consulte GetBucketReplication na Referência da API do Amazon Simple Storage Service.
> Para compatibilidade com versões anteriores, o Amazon S3 continua a permitir o formato de configuração de replicação XML V1. Se você usou o formato de configuração de replicação XML V1, consulte Considerações sobre a compatibilidade com versões anteriores para considerações sobre a compatibilidade com versões anteriores.

No arquivo XML de configuração de replicação, é necessário especificar um perfil do AWS Identity and Access Management (IAM) e uma ou mais regras, conforme mostrado no seguinte exemplo:

```
<ReplicationConfiguration>
    <Role>IAM-role-ARN</Role>
    <Rule>
```

```
        ...
    </Rule>
    <Rule>
         ...
    </Rule>
     ...
</ReplicationConfiguration>
```

O Amazon S3 não pode replicar objetos sem sua permissão. Você concede permissões ao Amazon S3 com o perfil do IAM especificado na configuração de replicação. O Amazon S3 assume esse perfil do IAM para replicar objetos em seu nome. Primeiro você precisa fornecer as permissões necessárias à função do IAM. Para obter mais informações sobre como gerenciar permissões, consulte Configurar permissões para replicação em tempo real.

Você adiciona apenas uma regra na configuração da replicação nos seguintes cenários:

- Você quer replicar todos os objetos.
- Você quer replicar apenas um subgrupo de objetos. Você identifica o subgrupo do objeto adicionando um filtro à regra. No filtro, você especifica um prefixo de chaves do objeto, tags ou uma combinação de ambos, de maneira a identificar o subgrupo de objetos aos quais a regra se aplica. Os filtros têm como alvo objetos que correspondem aos valores exatos que você especifica.

Se quiser replicar subgrupos de objetos diferentes, adicione várias regras em uma configuração de replicação. Em cada regra, você especifica um filtro que seleciona um subgrupo diferente. Por exemplo, talvez você queira replicar objetos com os prefixos de chaves `tax/` ou `document/`. Para fazer isso, você adiciona duas regras, uma que especifica o filtro de prefixo das chaves `tax/` e outro que especifica o prefixo das chaves `document/`. Consulte mais informações sobre prefixos de chave de objeto em Organizar objetos usando prefixos.

As seções a seguir fornecem informações adicionais.

Tópicos

- Configuração da regra básica
- Opcional: Especificação de um filtro
- Configurações adicionais de destino
- Exemplo de configurações de replicação
- Considerações sobre a compatibilidade com versões anteriores

Configuração da regra básica

Cada regra deve incluir o status e a prioridade da regra. A regra também precisa indicar se os marcadores de exclusão devem ser replicados.

- O elemento `<Status>` indica se a regra está habilitada ou desabilitada usando os valores `Enabled` ou `Disabled`. Se uma regra estiver desabilitada, o Amazon S3 não executará as ações especificadas nela.
- O elemento `<Priority>` indica qual regra tem precedência sempre que duas ou mais regras de replicação entram em conflito. O Simple Storage Service (Amazon S3) tenta replicar objetos de acordo com todas as regras de replicação. Porém, se houver duas ou mais regras com o mesmo bucket de destino, os objetos serão replicados de acordo com a regra com a prioridade mais alta. Quanto maior o número, maior a prioridade.
- O elemento `<DeleteMarkerReplication>` indica se os marcadores de exclusão devem ser replicados usando os valores `Enabled` ou `Disabled`.

Na configuração o elemento `<Destination>`, é necessário fornecer o nome do bucket ou buckets de destino onde você deseja que o Amazon S3 replique objetos.

O exemplo a seguir mostra os requisitos mínimos para uma regra da V2. Para compatibilidade com versões anteriores, o Amazon S3 continua a oferecer compatibilidade com o formato XML V1. Para obter mais informações, consulte Considerações sobre a compatibilidade com versões anteriores.

```
...
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled-or-Disabled</Status>
        <Filter>
            <Prefix></Prefix>
        </Filter>
        <Priority>integer</Priority>
        <DeleteMarkerReplication>
           <Status>Enabled-or-Disabled</Status>
        </DeleteMarkerReplication>
        <Destination>
           <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
        </Destination>
    </Rule>
    <Rule>
         ...
```

```
    </Rule>
     ...
...
```

Você também pode especificar outras opções de configuração. Por exemplo: você pode optar pelo uso de uma classe de armazenamento para réplicas de objetos diferentes da classe do objeto de origem.

Opcional: Especificação de um filtro

Para escolher um subgrupo de objetos aos quais a regra se aplique, adicione um filtro opcional. Você pode filtrar pelo prefixo das chaves do objeto, as etiquetas do objeto ou uma combinação de ambos. Se você filtrar tanto pelo prefixo das chaves quanto pelas etiquetas do objeto, o Amazon S3 combinará os filtros usando o operador lógico `AND`. Em outras palavras, a regra se aplica ao subgrupo de objetos com as etiquetas e o prefixo de chave específicos.

Filtro baseado no prefixo da chave de objeto

Para especificar uma regra com um filtro baseado no prefixo de chaves de um objeto, use o XML a seguir. É possível especificar apenas um prefixo por regra.

```
<Rule>
    ...
    <Filter>
        <Prefix>key-prefix</Prefix>
    </Filter>
    ...
</Rule>
...
```

Filtrar com base em tags de objeto

Para especificar uma regra com um filtro baseado nas tags do objeto, use o XML a seguir. Você pode especificar uma ou mais tags de objeto.

```
<Rule>
    ...
    <Filter>
        <And>
            <Tag>
```

```
                <Key>key1</Key>
                <Value>value1</Value>
            </Tag>
            <Tag>
                <Key>key2</Key>
                <Value>value2</Value>
            </Tag>
             ...
        </And>
    </Filter>
    ...
</Rule>
...
```

Filtrar com um prefixo de chave e tags de objeto

Para especificar um filtro de regra com uma combinação de um prefixo de chaves e tags de objeto, use o XML a seguir. Você envolve esses filtros em um elemento pai <And>. O Amazon S3 executa uma operação lógica AND para combinar esses filtros. Em outras palavras, a regra se aplica ao subgrupo de objetos com as etiquetas e o prefixo de chave específicos.

```
<Rule>
    ...
    <Filter>
        <And>
            <Prefix>key-prefix</Prefix>
            <Tag>
                <Key>key1</Key>
                <Value>value1</Value>
            </Tag>
            <Tag>
                <Key>key2</Key>
                <Value>value2</Value>
            </Tag>
             ...
    </Filter>
    ...
</Rule>
...
```

Note

- Se você especificar uma regra com um elemento `<Filter>` vazio, a regra será aplicada a todos os objetos do bucket.
- Ao usar regras de replicação baseadas em etiquetas com replicação em tempo real, novos objetos precisam ser marcados com a etiqueta da regra de replicação correspondente na operação `PutObject`. Caso contrário, os objetos não serão replicados. Se os objetos forem marcados após a operação `PutObject`, esses objetos também não serão replicados.

  Para replicar objetos que foram marcados após a operação `PutObject`, use a funcionalidade Replicação em Lote do S3. Para obter mais informações sobre replicação em lote, consulte Replicar objetos existentes.

Configurações adicionais de destino

Na configuração de destino, especifique o bucket onde você quer que o Amazon S3 replique objetos. Você pode definir configurações para replicar objetos de um bucket de origem para um bucket de destino.

```
...
<Destination>
    <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
</Destination>
...
```

Você pode adicionar as seguintes opções no elemento `<Destination>`.

Tópicos

- Especificar classe de armazenamento
- Adicionar vários buckets de destino
- Especificar parâmetros diferentes para cada regra de replicação com vários buckets de destino
- Alterar a propriedade da réplica
- Ativar o controle do tempo de replicação do S3
- Replicar objetos criados com criptografia do lado do servidor com o uso do AWS KMS.

Especificar classe de armazenamento

Você pode especificar a classe de armazenamento para as réplicas do objeto. Por padrão, o Amazon S3 usa a classe de armazenamento do objeto de origem para criar as réplicas do objeto.

```
...
<Destination>
       <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
       <StorageClass>storage-class</StorageClass>
</Destination>
...
```

Adicionar vários buckets de destino

Você pode adicionar vários buckets de destino em uma única configuração de replicação, como segue.

```
...
<Rule>
    <ID>Rule-1</ID>
    <Status>Enabled-or-Disabled</Status>
    <Priority>integer</Priority>
    <DeleteMarkerReplication>
       <Status>Enabled-or-Disabled</Status>
    </DeleteMarkerReplication>
    <Destination>
       <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket1</Bucket>
    </Destination>
</Rule>
<Rule>
    <ID>Rule-2</ID>
    <Status>Enabled-or-Disabled</Status>
    <Priority>integer</Priority>
    <DeleteMarkerReplication>
       <Status>Enabled-or-Disabled</Status>
    </DeleteMarkerReplication>
    <Destination>
       <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket2</Bucket>
    </Destination>
</Rule>
...
```

Especificar parâmetros diferentes para cada regra de replicação com vários buckets de destino

Ao adicionar vários buckets de destino em uma única configuração de replicação, você pode especificar parâmetros diferentes para cada regra de replicação, da seguinte forma.

```
...
<Rule>
    <ID>Rule-1</ID>
    <Status>Enabled-or-Disabled</Status>
    <Priority>integer</Priority>
    <DeleteMarkerReplication>
       <Status>Disabled</Status>
    </DeleteMarkerReplication>
      <Metrics>
    <Status>Enabled</Status>
    <EventThreshold>
      <Minutes>15</Minutes>
    </EventThreshold>
  </Metrics>
    <Destination>
       <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket1</Bucket>
    </Destination>
</Rule>
<Rule>
    <ID>Rule-2</ID>
    <Status>Enabled-or-Disabled</Status>
    <Priority>integer</Priority>
    <DeleteMarkerReplication>
       <Status>Enabled</Status>
    </DeleteMarkerReplication>
      <Metrics>
    <Status>Enabled</Status>
    <EventThreshold>
      <Minutes>15</Minutes>
    </EventThreshold>
  </Metrics>
  <ReplicationTime>
    <Status>Enabled</Status>
    <Time>
      <Minutes>15</Minutes>
    </Time>
  </ReplicationTime>
    <Destination>
       <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket2</Bucket>
```

```
    </Destination>
</Rule>
...
```

Alterar a propriedade da réplica

Quando os buckets de origem e de destino não pertencem às mesmas contas, você pode alterar a propriedade da réplica para a Conta da AWS que for a proprietária do bucket de destino. Para fazer isso, adicione o elemento `<AccessControlTranslation>`. Esse elemento assume o valor de `Destination`.

```
...
<Destination>
   <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
   <Account>destination-bucket-owner-account-id</Account>
   <AccessControlTranslation>
       <Owner>Destination</Owner>
   </AccessControlTranslation>
</Destination>
...
```

Se você não adicionar o elemento `<AccessControlTranslation>` à configuração de replicação, as réplicas pertencerão à mesma Conta da AWS que for a proprietária do objeto de origem. Para obter mais informações, consulte Alterar o proprietário da réplica.

Ativar o controle do tempo de replicação do S3

Você pode habilitar o Controle do tempo de replicação do S3 (S3 RTC) na configuração de replicação. O S3 RTC replica a maioria dos objetos em segundos e 99,99 por cento dos objetos em 15 minutos (baseado em um acordo de nível de serviço).

> **Note**
>
> Somente um valor de `<Minutes>15</Minutes>` é aceito para os elementos `<EventThreshold>` e `<Time>`.

```
...
<Destination>
  <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
  <Metrics>
```

```
    <Status>Enabled</Status>
    <EventThreshold>
      <Minutes>15</Minutes>
    </EventThreshold>
  </Metrics>
  <ReplicationTime>
    <Status>Enabled</Status>
    <Time>
      <Minutes>15</Minutes>
    </Time>
  </ReplicationTime>
</Destination>
...
```

Para obter mais informações, consulte Atender aos requisitos de conformidade com o Controle do Tempo de Replicação do S3. Consulte exemplos de API em PutBucketReplication na Referência de API do Amazon Simple Storage Service.

Replicar objetos criados com criptografia do lado do servidor com o uso do AWS KMS.

Seu bucket de origem pode conter objetos que foram criados com criptografia no servidor usando as chaves do AWS Key Management Service (AWS KMS) (SSE-KMS). Por padrão, o Amazon S3 não replica esses objetos. Opcionalmente, você pode direcionar o Amazon S3 para replicar esses objetos. Para fazer isso, primeiro opte explicitamente por esse recurso adicionando o elemento `<SourceSelectionCriteria>`. Depois, forneça a AWS KMS key (para a Região da AWS do bucket de destino) a ser usada para criptografar réplicas de objetos. Os exemplo a seguir mostra como especificar esses elementos.

```
...
<SourceSelectionCriteria>
  <SseKmsEncryptedObjects>
    <Status>Enabled</Status>
  </SseKmsEncryptedObjects>
</SourceSelectionCriteria>
<Destination>
  <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
  <EncryptionConfiguration>
    <ReplicaKmsKeyID>AWS KMS key ID to use for encrypting object replicas</
ReplicaKmsKeyID>
  </EncryptionConfiguration>
</Destination>
...
```

Para obter mais informações, consulte Replicar objetos criptografados (SSE-S3, SSE-KMS, DSSE-KMS, SSE-C).

Exemplo de configurações de replicação

Para começar, você pode adicionar os seguintes exemplos de configuração de replicação ao bucket, conforme adequado.

> **Important**
>
> Para adicionar uma configuração de replicação a um bucket, é preciso ter a permissão `iam:PassRole`. Com essa permissão, você pode aprovar a função do IAM que concede as permissões de replicação do Amazon S3. Você especifica a função do IAM ao fornecer o nome de recurso da Amazon (ARN) usado no elemento `<Role>` na configuração de replicação XML. Para obter mais informações, consulte Conceder permissões ao usuário para transmitir uma função a um AWS service (Serviço da AWS) no Guia do usuário do IAM.

Example 1: Configuração de replicação com uma regra

A configuração de replicação básica a seguir especifica uma regra. A regra especifica uma função do IAM que o Amazon S3 pode assumir e um bucket de destino para único para réplicas de objetos. O valor do elemento `<Status>` de `Enabled` indica que a regra está em vigor.

```
<?xml version="1.0" encoding="UTF-8"?>
<ReplicationConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Role>arn:aws:iam::account-id:role/role-name</Role>
  <Rule>
    <Status>Enabled</Status>

    <Destination>
      <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
    </Destination>
  </Rule>
</ReplicationConfiguration>
```

Para escolher um subgrupo de objetos a serem replicados, adicione um filtro. Na configuração a seguir, o filtro especifica um prefixo de chaves do objeto. Essa regra se aplica aos objetos que têm o prefixo *Tax/* no nome da chave.

```
<?xml version="1.0" encoding="UTF-8"?>
```

```
<ReplicationConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Role>arn:aws:iam::account-id:role/role-name</Role>
  <Rule>
    <Status>Enabled</Status>
    <Priority>1</Priority>
    <DeleteMarkerReplication>
       <Status>string</Status>
    </DeleteMarkerReplication>

    <Filter>
       <Prefix>Tax/</Prefix>
    </Filter>

    <Destination>
       <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
    </Destination>

  </Rule>
</ReplicationConfiguration>
```

Se você especificar o elemento <Filter>, inclua também os elementos <Priority> e <DeleteMarkerReplication>. Neste exemplo, o valor que você define para o elemento <Priority> é irrelevante, pois há somente uma regra.

Na configuração a seguir, o filtro especifica um prefixo e duas tags. A regra se aplica ao subgrupo de objetos com o prefixo de chaves e as tags especificados. Mais especificamente, ela se aplica aos objetos com o prefixo *Tax/* nos nomes de chave e às duas tags de objeto especificadas. Neste exemplo, o valor que você define para o elemento <Priority> é irrelevante, pois há somente uma regra.

```
<?xml version="1.0" encoding="UTF-8"?>
<ReplicationConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Role>arn:aws:iam::account-id:role/role-name</Role>
  <Rule>
    <Status>Enabled</Status>
    <Priority>1</Priority>
    <DeleteMarkerReplication>
       <Status>string</Status>
    </DeleteMarkerReplication>

    <Filter>
        <And>
```

```
          <Prefix>Tax/</Prefix>
          <Tag>
             <Tag>
                <Key>tagA</Key>
                <Value>valueA</Value>
             </Tag>
          </Tag>
          <Tag>
             <Tag>
                <Key>tagB</Key>
                <Value>valueB</Value>
             </Tag>
          </Tag>
       </And>

    </Filter>

    <Destination>
        <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
    </Destination>

  </Rule>
</ReplicationConfiguration>
```

Você pode especificar uma classe de armazenamento para as réplicas, da seguinte forma:

```
<?xml version="1.0" encoding="UTF-8"?>

<ReplicationConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Role>arn:aws:iam::account-id:role/role-name</Role>
  <Rule>
    <Status>Enabled</Status>
    <Destination>
       <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
       <StorageClass>storage-class</StorageClass>
    </Destination>
  </Rule>
</ReplicationConfiguration>
```

Você pode especificar uma classe de armazenamento à qual o Amazon S3 ofereça suporte.

Example 2: Configuração de replicação com duas regras

Example

Na configuração de replicação a seguir, as regras especificam o seguinte:

- Cada regra filtra em um prefixo de chave diferente para que cada regra se aplique a um subconjunto distinto de objetos. Nesse exemplo, o Simple Storage Service (Amazon S3) replica objetos com os nomes de chave *Tax/doc1.pdf* e *Project/project1.txt*, mas não replica objetos com o nome da chave *PersonalDoc/documentA*.
- Embora ambas as regras especifiquem um valor para o elemento `<Priority>`, a prioridade da regra é irrelevante, pois as regras se aplicam a dois grupos distintos de objetos. O exemplo a seguir mostra o que acontece quando aplicamos uma prioridade de regras.
- A segunda regra especifica uma classe de armazenamento S3 Standard – IA para réplicas de objetos. O Amazon S3 usa a classe de armazenamento especificada para essas réplicas de objetos.

```
<?xml version="1.0" encoding="UTF-8"?>

<ReplicationConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Role>arn:aws:iam::account-id:role/role-name</Role>
  <Rule>
    <Status>Enabled</Status>
    <Priority>1</Priority>
    <DeleteMarkerReplication>
       <Status>string</Status>
    </DeleteMarkerReplication>
    <Filter>
        <Prefix>Tax</Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Destination>
      <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
    </Destination>
     ...
  </Rule>
 <Rule>
    <Status>Enabled</Status>
    <Priority>2</Priority>
    <DeleteMarkerReplication>
```

```
        <Status>string</Status>
    </DeleteMarkerReplication>
    <Filter>
        <Prefix>Project</Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Destination>
      <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
     <StorageClass>STANDARD_IA</StorageClass>
    </Destination>
     ...
  </Rule>


</ReplicationConfiguration>
```

Example 3: Configuração da replicação com duas regras e prefixos sobrepostos

Nessa configuração, as duas regras especificam filtros com os prefixos das chaves sobrepostos, *star/* e *starship/*. As duas regras se aplicam aos objetos com o nome de chave *starship-x*. Nesse caso, o Amazon S3 usa a prioridade da regra para determinar qual regra deve ser aplicada. Quanto maior o número, maior a prioridade.

```
<ReplicationConfiguration>

  <Role>arn:aws:iam::account-id:role/role-name</Role>

  <Rule>
    <Status>Enabled</Status>
    <Priority>1</Priority>
    <DeleteMarkerReplication>
       <Status>string</Status>
    </DeleteMarkerReplication>
    <Filter>
        <Prefix>star</Prefix>
    </Filter>
    <Destination>
      <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
    </Destination>
  </Rule>
  <Rule>
    <Status>Enabled</Status>
    <Priority>2</Priority>
```

```
    <DeleteMarkerReplication>
       <Status>string</Status>
    </DeleteMarkerReplication>
    <Filter>
        <Prefix>starship</Prefix>
    </Filter>
    <Destination>
      <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
    </Destination>
  </Rule>
</ReplicationConfiguration>
```

Example 4: Demonstrações de exemplo

Para obter exemplos de demonstrações, consulte Exemplos para configurar a replicação em tempo real.

Para obter mais informações sobre a estrutura XML da configuração de replicação, consulte PutBucketReplication na Referência da API do Amazon Simple Storage Service.

Considerações sobre a compatibilidade com versões anteriores

A versão mais recente do formato XML de configuração da replicação é V2. As configurações de replicação XML V2 são aquelas que contêm o elemento `<Filter>` para regras e regras que especificam o Controle do tempo de replicação do S3 (S3 RTC).

Para ver a versão da configuração de replicação, você pode usar a operação de API `GetBucketReplication`. Para obter mais informações, consulte GetBucketReplication na Referência da API do Amazon Simple Storage Service.

Para compatibilidade com versões anteriores, o Amazon S3 continua a permitir o formato de configuração de replicação XML V1. Se você usou o formato de configuração da replicação XML V1, leve em consideração as seguintes questões que afetam a compatibilidade com versões anteriores:

- O formato XML V2 da configuração de replicação inclui o elemento `<Filter>` para regras. Com o elemento `<Filter>`, você pode especificar filtros de objeto com base no prefixo de chaves do objeto, tags ou ambos para colocar dentro do escopo os objetos aos quais a regra se aplica. O formato XML V1 da configuração de replicação permite a filtragem com base apenas no prefixo da chave. Nesse caso, você adiciona o elemento `<Prefix>` diretamente como elemento-filho do elemento `<Rule>`, conforme o seguinte exemplo:

  ```
  <?xml version="1.0" encoding="UTF-8"?>
  ```

```
<ReplicationConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Role>arn:aws:iam::account-id:role/role-name</Role>
  <Rule>
    <Status>Enabled</Status>
    <Prefix>key-prefix</Prefix>
    <Destination>
       <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
    </Destination>

  </Rule>
</ReplicationConfiguration>
```

- Ao excluir um objeto do bucket de origem sem especificar um ID da versão do objeto, o Amazon S3 adicionar um marcador de exclusão. Se você usar o formato XML V1 da configuração de replicação, o Amazon S3 replicará somente os marcadores de exclusão resultantes das ações do usuário. Em outras palavras: o Amazon S3 só replica o marcador de exclusão se um usuário excluir um objeto. Se um objeto expirado for removido pelo Amazon S3 (como parte de uma ação de ciclo de vida), ele não replicará o marcador de exclusão.

  No formato XML V2 da configuração de replicação, é possível habilitar a replicação do marcador de exclusão para regras que não se baseiam em tags. Para obter mais informações, consulte Replicação de marcadores de exclusão entre intervalos.

Configurar permissões para replicação em tempo real

Ao configurar a replicação em tempo real no Amazon S3, você deve adquirir as permissões necessárias do seguinte modo:

- O Simple Storage Service (Amazon S3) precisa de permissões para replicar objetos em seu nome. Você concede essas permissões criando um perfil do AWS Identity and Access Management (IAM) e especificando esse perfil na configuração de replicação.
- Quando os buckets de origem e de destino não pertencem à mesma conta, o proprietário do bucket de destino também deve conceder ao proprietário do bucket de origem permissões para armazenar réplicas.

Tópicos

- Configurar permissões para criar regras de replicação
- Criar um perfil do IAM

- Conceder permissões quando os buckets de origem e de destino pertencerem a Contas da AWS diferentes
- Alterar a propriedade da réplica
- Conceder permissões para operações em lote do S3

Configurar permissões para criar regras de replicação

O usuário ou o perfil do IAM que você usará para criar regras de replicação precisa de permissões para isso, seja para replicações unidirecionais ou bidirecionais. Se o usuário ou o perfil não tiver essas permissões, não será possível criar regras de replicação. Consulte mais informações em Identidades do IAM no Guia do usuário do IAM.

O usuário ou o perfil precisa das seguintes ações:

- `iam:AttachRolePolicy`
- `iam:CreatePolicy`
- `iam:CreateServiceLinkedRole`
- `iam:PassRole`
- `iam:PutRolePolicy`
- `s3:GetBucketVersioning`
- `s3:GetObjectVersionAcl`
- `s3:GetObjectVersionForReplication`
- `s3:GetReplicationConfiguration`
- `s3:PutReplicationConfiguration`

Veja a seguir uma amostra de política do IAM que inclui essas ações.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetAccessPoint",
                "s3:GetAccountPublicAccessBlock",
                "s3:GetBucketAcl",
```

```
                "s3:GetBucketLocation",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:ListAccessPoints",
                "s3:ListAllMyBuckets",
                "s3:PutReplicationConfiguration",
                "s3:GetReplicationConfiguration",
                "s3:GetBucketVersioning",
                "s3:GetObjectVersionForReplication",
                "s3:GetObjectVersionAcl",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:GetObjectVersion",
                "s3:GetBucketOwnershipControls",
                "s3:PutBucketOwnershipControls",
                "s3:GetObjectLegalHold",
                "s3:GetObjectRetention",
                "s3:GetBucketObjectLockConfiguration"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket1-*",
                "arn:aws:s3:::amzn-s3-demo-bucket2-*/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:List*AccessPoint*",
                "s3:GetMultiRegion*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:Get*",
                "iam:CreateServiceLinkedRole",
                "iam:CreateRole",
                "iam:PassRole"
            ],
            "Resource": "arn:aws:iam::*:role/service-role/s3*"
        },
        {
            "Effect": "Allow",
```

```
            "Action": [
                "iam:List*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:AttachRolePolicy",
                "iam:PutRolePolicy",
                "iam:CreatePolicy"
              ],
            "Resource": [
                "arn:aws:iam::*:policy/service-role/s3*",
                "arn:aws:iam::*:role/service-role/s3*"
            ]
        }
    ]
}
```

Criar um perfil do IAM

Por padrão, todos os recursos do Simple Storage Service (Amazon S3): buckets, objetos e sub-recursos relacionados, são privados, e somente o proprietário do recurso pode acessá-lo. O Amazon S3 precisa de permissões de leitura e replicação de objetos a partir do bucket de origem. Você concede essas permissões criando um perfil do IAM e especificando esse perfil na configuração da replicação.

Esta seção explica a política de confiança e a política de permissões mínimas necessárias anexadas a esse perfil do IAM. As demonstrações de exemplo fornecem instruções passo a passo para criar uma função do IAM. Para obter mais informações, consulte Exemplos para configurar a replicação em tempo real.

A política de confiança identifica quais identidades de entidade principal podem assumir o perfil do IAM. A política de permissões especifica quais ações o perfil do IAM pode realizar, em quais recursos e sob quais condições.

- O exemplo a seguir mostra uma política de confiança na qual você identifica o Amazon S3 como a entidade principal do AWS service (Serviço da AWS) que pode assumir o perfil:

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service":"s3.amazonaws.com"
         },
         "Action":"sts:AssumeRole"
      }
   ]
}
```

- O exemplo a seguir mostra uma política de confiança na qual você identifica o Amazon S3 e o Operações em Lote do S3 como entidades principais que podem assumir o perfil. Use essa abordagem se estiver criando um trabalho do recurso Replicação em Lote. Para obter mais informações, consulte Criar um trabalho de replicação em lote para novas regras ou destinos de replicação.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service": [
              "s3.amazonaws.com",
              "batchoperations.s3.amazonaws.com"
            ]
         },
         "Action":"sts:AssumeRole"
      }
   ]
}
```

  Para obter mais informações sobre funções do IAM, consulte Funções do IAM no Manual do usuário do IAM.

- O exemplo a seguir mostra a política de permissões, na qual você concede ao perfil do IAM permissões para realizar as tarefas de replicação em seu nome. Quando o Amazon S3 assumir a função, ele terá as permissões que você especificar nessa política. Nesta política, *amzn-s3-*

demo-source-bucket é o bucket de origem e *amzn-s3-demo-destination-bucket* é o bucket de destino.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "s3:GetReplicationConfiguration",
            "s3:ListBucket"
         ],
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-source-bucket"
         ]
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3:GetObjectVersionForReplication",
            "s3:GetObjectVersionAcl",
            "s3:GetObjectVersionTagging"
         ],
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
         ]
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3:ReplicateObject",
            "s3:ReplicateDelete",
            "s3:ReplicateTags"
         ],
         "Resource":"arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
      }
   ]
}
```

Essa política concede permissões para as seguintes ações:

- `s3:GetReplicationConfiguration` e `s3:ListBucket`: as permissões para essas ações no bucket *amzn-s3-demo-source-bucket* permitem que o Amazon S3 recupere a

configuração de replicação e liste o conteúdo do bucket. (O modelo de permissões atual exige a permissão `s3:ListBucket` para acessar marcadores de exclusão.)

- `s3:GetObjectVersionForReplication` e `s3:GetObjectVersionAcl`: as permissões para essas ações são concedidas em todos os objetos para permitir que o Simple Storage Service (Amazon S3) obtenha uma versão específica dos objetos e as listas de controle de acesso (ACL) associadas aos objetos.

- `s3:ReplicateObject` e `s3:ReplicateDelete`: as permissões para essas ações em todos os objetos no bucket *`amzn-s3-demo-destination-bucket`* permitem que o Simple Storage Service (Amazon S3) replique objetos ou marcadores de exclusão no bucket de destino. Para obter mais informações sobre marcadores de exclusão, consulte Como a exclusão de operações afeta a replicação.

  > **Note**
  >
  > As permissões para a ação `s3:ReplicateObject` no bucket *`amzn-s3-demo-destination-bucket`* também permitem a replicação de metadados, como tags de objeto e ACLs. Portanto, você não precisa conceder permissão explícita para a ação `s3:ReplicateTags`.

- `s3:GetObjectVersionTagging`: as permissões para essa ação nos objetos do bucket *`amzn-s3-demo-source-bucket`* permitem que o Amazon S3 leia as tags dos objetos para replicação. Para obter mais informações sobre etiquetas de objeto, consulte Categorizar seu armazenamento usando tags. Se o Amazon S3 não tiver a permissão `s3:GetObjectVersionTagging`, ele replicará os objetos, mas não as tags dos objetos.

Consulte uma lista de ações do Amazon S3 em Actions, resources, and condition keys for Amazon S3 na Referência de autorização do serviço.

Para ter mais informações sobre as permissões referentes a operações de API do S3 de acordo com os tipos de recurso do S3, consulte Permissões obrigatórias para operações de API do Amazon S3.

> **Important**
>
> Mais especificamente, a Conta da AWS proprietária da função do IAM precisa ter permissões para as ações que ela concede à função do IAM.

Por exemplo, suponha que o bucket de origem contenha objetos pertencentes a uma outra Conta da AWS. O proprietário dos objetos deverá conceder explicitamente as permissões exigidas à Conta da AWS proprietária do perfil do IAM por meio de listas de controle de acesso (ACLs) dos objetos. Caso contrário, o Amazon S3 não conseguirá acessar os objetos e haverá falha na replicação dos objetos. Para obter informações sobre as permissões da ACL, consulte Visão geral da lista de controle de acesso (ACL).
As permissões descritas aqui são relativas à configuração mínima da replicação. Se optar por adicionar configurações de replicação opcionais, será necessário conceder permissões adicionais ao Amazon S3:

- Para replicar objetos criptografados, você também precisará conceder as permissões de chave do AWS Key Management Service (AWS KMS) necessárias. Para obter mais informações, consulte the section called “Replicar objetos criptografados”.
- Para usar a funcionalidade Bloqueio de Objetos com replicação, é necessário conceder duas permissões adicionais no bucket de origem do S3 no perfil do AWS Identity and Access Management (IAM) usado para configurar a replicação. As duas permissões adicionais são `s3:GetObjectRetention` e `s3:GetObjectLegalHold`. Se o perfil tiver uma instrução de permissão `s3:Get*`, essa instrução satisfará o requisito. Para obter mais informações, consulte the section called “Usar a funcionalidade Bloqueio de Objetos com a funcionalidade Replicação do S3”.

Conceder permissões quando os buckets de origem e de destino pertencerem a Contas da AWS diferentes

Quando os buckets de origem e de destino não pertencem à mesma conta, o proprietário do bucket de destino também deve adicionar uma política de bucket para conceder ao proprietário do bucket de origem permissões para realizar as ações de replicação, como mostrado no exemplo a seguir. Neste exemplo de política, *amzn-s3-demo-destination-bucket* é o bucket de destino.

Também é possível usar o console do Amazon S3 para que essa política de bucket seja gerada automaticamente para você. Consulte mais informações em Habilitar o recebimento de objetos replicados de um bucket de origem.

> **Note**
>
> O formato do ARN do perfil pode parecer diferente. Se o perfil tiver sido criado usando o console, o formato do ARN será `arn:aws:iam::account-ID:role/service-`

`role/role-name`. Se o perfil tiver sido criado usando a AWS CLI, o formato do ARN será `arn:aws:iam::account-ID:role/role-name`. Para obter mais informações, consulte Funções do IAM no Guia do usuário do IAM.

```
{
   "Version":"2012-10-17",
   "Id":"PolicyForDestinationBucket",
   "Statement":[
      {
         "Sid":"Permissions on objects",
         "Effect":"Allow",
         "Principal":{
            "AWS":"arn:aws:iam::source-bucket-account-ID:role/service-role/source-
account-IAM-role"
         },
         "Action":[
            "s3:ReplicateDelete",
            "s3:ReplicateObject"
         ],
         "Resource":"arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
      },
      {
         "Sid":"Permissions on bucket",
         "Effect":"Allow",
         "Principal":{
            "AWS":"arn:aws:iam::source-bucket-account-ID:role/service-role/source-
account-IAM-role"
         },
         "Action": [
            "s3:List*",
            "s3:GetBucketVersioning",
            "s3:PutBucketVersioning"
         ],
         "Resource":"arn:aws:s3::amzn-s3-demo-destination-bucket"
      }
   ]
}
```

Para obter um exemplo, consulte Configuração da replicação de buckets em contas diferentes.

Se os objetos no bucket de origem estiverem marcados, observe o seguinte:

- Se o proprietário do bucket de origem conceder ao Amazon S3 permissão para as ações `s3:GetObjectVersionTagging` e `s3:ReplicateTags` para replicação de tags de objeto (pela função do IAM), o Amazon S3 replicará as tags com os objetos. Para obter informações sobre a função do IAM, consulte Criar um perfil do IAM.
- Se o proprietário do bucket de destino não quiser replicar as tags, ele poderá adicionar a seguinte instrução à política do bucket de destino para negar explicitamente a permissão para a ação `s3:ReplicateTags`. Nesta política, *amzn-s3-demo-destination-bucket* é o bucket de destino.

```
...
   "Statement":[
      {
         "Effect":"Deny",
         "Principal":{
            "AWS":"arn:aws:iam::source-bucket-account-id:role/service-role/source-account-IAM-role"
         },
         "Action":"s3:ReplicateTags",
         "Resource":"arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
      }
   ]
...
```

> **Note**
>
> - Se você quiser replicar objetos criptografados, também precisará conceder as permissões de chave do AWS Key Management Service (AWS KMS) necessárias. Para obter mais informações, consulte the section called “Replicar objetos criptografados”.
> - Para usar a funcionalidade Bloqueio de Objetos com replicação, é necessário conceder duas permissões adicionais no bucket de origem do S3 no perfil do AWS Identity and Access Management (IAM) usado para configurar a replicação. As duas permissões adicionais são `s3:GetObjectRetention` e `s3:GetObjectLegalHold`. Se o perfil tiver uma instrução de permissão `s3:Get*`, essa instrução satisfará o requisito. Para obter mais informações, consulte the section called “Usar a funcionalidade Bloqueio de Objetos com a funcionalidade Replicação do S3”.

Habilitar o recebimento de objetos replicados de um bucket de origem

Em vez de adicionar manualmente a política anterior ao bucket de destino, é possível gerar rapidamente as políticas necessárias para permitir o recebimento de objetos replicados de um bucket de origem no console do Amazon S3.

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets.
3. Na lista Buckets, escolha o bucket que você deseja usar como bucket de destino.
4. Escolha Management (Gerenciamento) e role para baixo até Replication rules (Regras de replicação).
5. Em Actions (Ações), escolha Receive replicated objects (Receber objetos replicados).

   Siga as instruções e insira o ID da Conta da AWS do bucket de origem e escolha Gerar políticas. O console gera uma política de bucket do Amazon S3 e uma política de chave do KMS.
6. Para adicionar essa política à política de bucket existente, escolha Apply settings (Aplicar configurações) ou Copy (Copiar) para copiar manualmente as alterações.
7. (Opcional) Copie a política AWS KMS na política de chave do KMS desejada no console do AWS Key Management Service.

Alterar a propriedade da réplica

Quando diferentes Contas da AWS são proprietárias dos buckets de origem e de destino, é possível instruir o Amazon S3 para alterar a propriedade da réplica para a Conta da AWS proprietária do bucket de destino. Para obter mais informações sobre a substituição do proprietário, consulte Alterar o proprietário da réplica.

Conceder permissões para operações em lote do S3

O recurso de Replicação em Lote do S3 oferece uma maneira de replicar os seguintes objetos:

- Objetos que já existiam antes da implantação de uma configuração de replicação
- Objetos que já foram replicados anteriormente
- Objetos que já falharam em uma replicação

É possível criar um trabalho único de replicação em lote ao criar a primeira regra em uma configuração de replicação nova ou ao adicionar um novo destino a uma configuração existente por meio do console do Amazon S3. Você também pode iniciar o Replicação em Lote para uma configuração de replicação existente criando um trabalho do Operações em Lote.

Consulte exemplos de política e perfil do IAM do Replicação em Lote em Configurar um perfil do IAM para o Replicação em Lote do S3.

Exemplos para configurar a replicação em tempo real

Os exemplos a seguir fornecem demonstrações passo a passo que mostram como configurar a replicação em tempo real para casos de uso comuns.

> **Note**
>
> Replicação em tempo real refere-se à Same-Region Replication (SRR – Replicação na Mesma Região) e à Cross-Region Replication (CRR – Replicação entre Regiões). A replicação em tempo real não replica nenhum objeto que já existia no bucket antes de você configurar a replicação. Para replicar objetos que já existiam antes de você configurar a replicação, use a replicação sob demanda. Para sincronizar buckets e replicar os objetos existentes sob demanda, consulte Replicar objetos existentes.

Esses exemplos demonstram como criar uma configuração de replicação usando o console do Amazon S3, a AWS Command Line Interface (AWS CLI) e AWS SDKs (exemplos de AWS SDK para Java e AWS SDK para .NET são mostrados).

Consulte informações sobre como instalar e configurar a AWS CLI nos seguintes tópicos do Guia do usuário da AWS Command Line Interface:

- Get started with the AWS CLI
- Configurar a AWS CLI: é necessário configurar pelo menos um perfil. Se você estiver explorando cenários entre contas, configure dois perfis.

Consulte informações sobre os SDKs da AWS em AWS SDK para Java e AWS SDK para .NET.

> **Tip**
>
> Consulte um tutorial detalhado que demonstra como usar a replicação em tempo real para replicar dados em Tutorial: Replicar dados dentro das Regiões da AWS e entre elas usando a replicação do Amazon S3.

Tópicos

- Configurar a replicação para buckets na mesma conta
- Configuração da replicação de buckets em contas diferentes
- Atender aos requisitos de conformidade com o Controle do Tempo de Replicação do S3
- Replicar objetos criptografados (SSE-S3, SSE-KMS, DSSE-KMS, SSE-C)
- Replicação de alterações de metadados com sincronização de modificação de réplica
- Replicação de marcadores de exclusão entre intervalos

Configurar a replicação para buckets na mesma conta

A replicação em tempo real é a cópia assíncrona automática de objetos em buckets de uso geral em Regiões da AWS diferentes ou na mesma região. A replicação em tempo real copia os objetos recém-criados e as atualizações de objeto de um bucket de origem para buckets de destino. Para obter mais informações, consulte Replicar objetos dentro de uma região e entre regiões.

Ao configurar a replicação, você adiciona regras de replicação ao bucket de origem. As regras de replicação definem quais objetos do bucket de origem devem ser replicados e o bucket de destino ou buckets nos quais os objetos replicados são armazenados. Você pode criar uma regra para replicar todos os objetos dentro de um bucket ou um subgrupo de objetos com um prefixo específico de nome de chaves, uma ou mais tags de objetos ou ambos. Um bucket de destino pode estar na mesma Conta da AWS que o bucket de origem ou pode estar em uma conta diferente.

Se você especificar um ID da versão do objeto a ser excluído, o Amazon S3 excluirá essa versão do objeto no bucket de origem. No entanto, ele não replica a exclusão no bucket de destino. Em outras palavras: ele não exclui a mesma versão do objeto do bucket de destino. Isso protege os dados contra exclusões mal-intencionadas.

Quando você adiciona uma regra de replicação a um bucket, ela fica ativada por padrão, portanto, começa a funcionar assim que é salva.

Neste exemplo, você configura a replicação em tempo real para os buckets de origem e de destino que pertencem à mesma Conta da AWS. São apresentados exemplos de uso do console do Amazon S3, da AWS Command Line Interface (AWS CLI), do AWS SDK para Java e do AWS SDK para .NET.

Pré-requisitos

Antes de usar os procedimentos a seguir, configure as permissões necessárias para replicação, dependendo se os buckets de origem e de destino pertencem à mesma conta ou a contas diferentes. Para obter mais informações, consulte the section called “Configurar permissões”.

> **Note**
>
> - Se você quiser replicar objetos criptografados, também precisará conceder as permissões de chave do AWS Key Management Service (AWS KMS) necessárias. Para obter mais informações, consulte the section called “Replicar objetos criptografados”.
> - Para usar a funcionalidade Bloqueio de Objetos com replicação, é necessário conceder duas permissões adicionais no bucket de origem do S3 no perfil do AWS Identity and Access Management (IAM) usado para configurar a replicação. As duas permissões adicionais são `s3:GetObjectRetention` e `s3:GetObjectLegalHold`. Se o perfil tiver uma instrução de permissão `s3:Get*`, essa instrução satisfará o requisito. Para obter mais informações, consulte the section called “Usar a funcionalidade Bloqueio de Objetos com a funcionalidade Replicação do S3”.

Uso do console do S3

Para configurar uma regra de replicação quando o bucket de destino estiver na mesma Conta da AWS que o bucket de origem, siga estas etapas.

Se o bucket de destino estiver um uma conta diferente do bucket de origem, você deverá adicionar uma política ao bucket de destino. Assim, será possível conceder ao proprietário da conta do bucket de origem permissão para replicar objetos no bucket de destino. Para obter mais informações, consulte Conceder permissões quando os buckets de origem e de destino pertencerem a Contas da AWS diferentes.

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.

2. No painel de navegação à esquerda, escolha Buckets de uso geral.
3. Na lista de buckets, escolha o nome do bucket desejado.
4. Selecione a guia Gerenciamento, role para baixo até Regras de replicação e selecione Criar regra de replicação.
5. Na seção Configuração da regra de replicação, em Nome da regra de replicação, insira um nome para sua regra para ajudar a identificá-la posteriormente. O nome é obrigatório e precisa ser exclusivo dentro do bucket.
6. Em Status, Enabled (Habilitado) é selecionado por padrão. Uma regra ativada começa a funcionar assim que você a salva. Se você quiser ativar a regra posteriormente, selecione Desabilitado.
7. Se o bucket tiver regras de replicação existentes, você será instruído a definir uma prioridade para a regra. Defina uma prioridade para a regra, de maneira a evitar conflitos causados pelos objetos incluídos no escopo de mais de uma regra. No caso de sobreposição de regras, o Amazon S3 usa a prioridade da regra para determinar qual regra aplicar. Quanto maior o número, maior a prioridade. Para obter mais informações sobre prioridade de regra, consulte Elementos do arquivo de configuração de replicação.
8. Em Bucket de origem, você tem as seguintes opções para definir a origem da replicação:

   - Para replicar todo o bucket, escolha Apply to all objects in the bucket (Aplicar a todos os objetos no bucket).
   - Para replicar todos os objetos que tenham o mesmo prefixo, escolha Limit the scope of this rule using one or more filters (Limitar o escopo desta regra usando um ou mais filtros). Isso limita a replicação a todos os objetos que tenham nomes que começam com o prefixo especificado (por exemplo, `pictures`). Insira um prefixo na caixa Prefixo.

     > **Note**
     >
     > Se você inserir um prefixo que seja o nome de uma pasta, é preciso usar / (barra) como o último caractere (por exemplo, `pictures/`).

   - Para replicar todos os objetos com uma ou mais tags de objeto, selecione Adicionar tag e insira o par de chave-valor nas caixas. Repita o procedimento para adicionar outra tag. Você pode combinar um prefixo e tags. Para obter mais informações sobre etiquetas de objeto, consulte Categorizar seu armazenamento usando tags.

O novo esquema XML de configuração de replicação é compatível com os filtros de prefixo e tags e com a priorização das regras. Para obter mais informações sobre o novo esquema, consulte Considerações sobre a compatibilidade com versões anteriores. Para obter mais informações sobre o XML usado com a API do Amazon S3 que funciona atrás da interface do usuário, consulte Elementos do arquivo de configuração de replicação. O novo esquema é descrito como configuração de replicação XML V2.

9. Em Destino, selecione o bucket no qual você deseja que o Amazon S3 replique objetos.

> **Note**
>
> O número de buckets de destino é limitado ao número de Regiões da AWS em determinada partição. Uma partição é um agrupamento de regiões. Atualmente, a AWS tem três partições: `aws` (regiões padrão), `aws-cn` (regiões da China) e `aws-us-gov` (regiões AWS GovCloud (US)). Para solicitar um aumento da cota do bucket de destino, você pode usar cotas de serviço.

- Para replicar para um bucket ou buckets em sua conta, selecione Escolher um bucket nesta conta e digite ou procure nomes de buckets de destino.
- Para replicar em um ou mais buckets em uma Conta da AWS diferente, selecione Selecionar um bucket em outra conta e insira o ID e o nome da conta do bucket de destino.

  Se o destino estiver um uma conta diferente do bucket de origem, você deverá adicionar uma política de bucket aos buckets de destino para conceder ao proprietário da conta do bucket de origem permissão para replicar objetos. Para obter mais informações, consulte Conceder permissões quando os buckets de origem e de destino pertencerem a Contas da AWS diferentes.

  Opcionalmente, se você quiser padronizar a propriedade de novos objetos no bucket de destino, escolha Alterar propriedade do objeto para o proprietário do bucket de destino. Para obter mais informações sobre essa opção, consulte Controlar a propriedade de objetos e desabilitar ACLs para seu bucket.

> **Note**
>
> Se o versionamento não estiver ativado no bucket de destino, você receberá uma advertência que contém um botão Enable versioning (Habilitar versionamento). Escolha esse botão para habilitar o versionamento no bucket.

10. Configure uma função do AWS Identity and Access Management (IAM) que o Amazon S3 possa assumir para replicar objetos em seu nome.

    Para configurar um perfil do IAM, na seção Perfil do IAM, selecione uma das seguintes opções na lista suspensa de perfis do IAM:

    - Recomendamos que você escolha Create new role (Criar nova função) para que o Amazon S3 crie uma nova função do IAM para você. Quando você salva a regra, uma nova política é gerada para a função do IAM que coincide com os buckets de origem e de destino que você escolher.
    - Você pode usar uma função do IAM existente. Se fizer isso, escolha uma função que conceda ao Amazon S3 as permissões necessárias para a replicação. A replicação falhará se essa função não conceder ao Amazon S3 permissões suficientes para seguir sua regra de replicação.

    > **Important**
    >
    > Quando você adiciona uma regra de replicação a um bucket, você deve ter a permissão `iam:PassRole` para poder transmitir a função do IAM que concede permissões de replicação do Amazon S3. Para ter mais informações, consulte Conceder permissões ao usuário para transmitir um perfil a um AWS service (Serviço da AWS) no Guia do usuário do IAM.

11. Para replicar objetos no bucket de origem que estão criptografados com a criptografia do lado do servidor com chaves do AWS Key Management Service (AWS KMS) (SSE-KMS), em Criptografia, selecione Replicar objetos criptografados com o AWS KMS. Em chaves do AWS KMS para criptografar objetos de destino estão as chaves de origem que você permite que a replicação use. Todas as chaves de origem do KMS são incluídas por padrão. Para limitar a seleção de chaves do KMS, você pode selecionar um alias ou um ID de chave.

Os objetos criptografados pelas AWS KMS keys que você não seleciona não são replicados. A chave do KMS ou um grupo de chaves do KMS é escolhido para você, mas você pode escolher as chaves do KMS, se desejar. Para obter informações sobre como usar o AWS KMS com replicação, consulte Replicar objetos criptografados (SSE-S3, SSE-KMS, DSSE-KMS, SSE-C).

> **Important**
>
> Ao replicar objetos que estão criptografados com AWS KMS, a taxa de solicitações do AWS KMS dobra na Região de origem e aumenta na Região de destino pelo mesmo valor. Essas taxas de chamada aprimoradas para AWS KMS se devem à forma com que os dados são recriptografados usando a chave do KMS que você define na região de destino de replicação. O AWS KMS tem uma cota de taxas de solicitação por conta de chamada por região. Para ter informações sobre os padrões de limite, consulte Cotas do AWS KMS: solicitações por segundo: varia no Guia do desenvolvedor do AWS Key Management Service.
>
> Se a taxa de solicitações do objeto PUT do Amazon S3 durante a replicação for maior do que a metade do limite da taxa padrão do AWS KMS para sua conta, recomendamos que você solicite um aumento da cota de taxa de solicitação do AWS KMS. Para solicitar um aumento, crie um caso no Suporte Center em Entre em contato conosco. Por exemplo, suponha que a sua taxa de solicitação do objeto PUT seja 1.000 solicitações por segundo e você use o AWS KMS para criptografar seus objetos. Nesse caso, recomendamos solicitar que o Suporte aumente o limite da taxa do AWS KMS para 2,5 mil solicitações por segundo nas regiões de origem e de destino (se forem diferentes) para garantir que não haja nenhum controle de utilização por parte do AWS KMS.
>
> Para ver a taxa de solicitação de objeto PUT no bucket de origem, visualize `PutRequests` nas métricas de solicitação do Amazon CloudWatch para o Amazon S3. Consulte informações sobre como visualizar métricas do CloudWatch em Uso do console do S3.

Se você escolheu replicar objetos criptografados com o AWS KMS, faça o seguinte:

- Em AWS KMS key para criptografar objetos de destino, especifique sua chave do KMS de uma das seguintes formas:
  - Para escolher em uma lista de chaves do KMS disponíveis, selecione Escolher entre suas AWS KMS keys e escolha sua chave do KMS na lista de chaves disponíveis.

As chaves Chave gerenciada pela AWS (`aws/s3`) e as chaves gerenciadas pelo cliente são exibidas nessa lista. Para ter mais informações sobre chaves gerenciadas pelo cliente, consulte Chaves de clientes e chaves da AWS no Guia do desenvolvedor do AWS Key Management Service.

- Para inserir o nome do recurso da Amazon (ARN) da chave do KMS, selecione Inserir ARN da AWS KMS key e insira o ARN da chave do KMS no campo exibido. Isso criptografa as réplicas no bucket de destino. Você pode encontrar o ARN da chave do KMS no console do IAM em Chaves de criptografia.
- Para criar uma chave gerenciada pelo cliente no console do AWS KMS, selecione Criar uma chave do KMS.

  Para ter mais informações sobre como criar uma AWS KMS key, consulte Criação de chaves no Guia do desenvolvedor do AWS Key Management Service.

> **Important**
>
> Você só pode usar chaves do KMS habilitadas na mesma Região da AWS que o bucket. Quando você seleciona Escolher de suas chaves do KMS, o console do S3 lista somente 100 chaves do KMS por região. Se você tiver mais de 100 chaves do KMS na mesma região, será possível ver somente as primeiras 100 chaves do KMS no console do S3. Para usar uma chave do KMS que não esteja listada no console, escolha Inserir o ARN da AWS KMS key e insira o ARN de sua chave do KMS. Ao usar uma AWS KMS key para criptografia no lado do servidor no Amazon S3, você deve escolher uma chave de criptografia do KMS simétrica. O Amazon S3 só é compatível com chaves do KMS de criptografia simétrica, e não com chaves assimétricas do KMS. Para ter mais informações, consulte Identificar chaves do KMS simétricas e assimétricas no Guia do desenvolvedor do AWS Key Management Service.

Para obter mais informações sobre como criar uma AWS KMS key, consulte Criação de chaves no Guia do desenvolvedor do AWS Key Management Service. Para obter mais informações sobre como usar o AWS KMS com o Amazon S3, consulte Usar criptografia do lado do servidor com o AWS KMS (SSE-KMS).

12. Em Classe de armazenamento de destino, se você quiser replicar seus dados em uma classe de armazenamento específica no destino, escolha Alterar a classe de armazenamento dos objetos replicados. Em seguida, escolha a classe de armazenamento que você deseja usar para os objetos replicados no destino. Se você não selecionar essa opção, a classe de armazenamento para objetos replicados será a mesma classe dos objetos originais.
13. Você tem as seguintes opções adicionais ao definir as Opções de replicação adicionais:

    - Se você quiser ativar o Controle do Tempo de Replicação do S3 (S3 RTC) na configuração de replicação, selecione Controle do Tempo de Replicação (RTC). Para obter mais informações sobre essa opção, consulte Atender aos requisitos de conformidade com o Controle do Tempo de Replicação do S3.
    - Se você quiser habilitar métricas de replicação do S3 na configuração de replicação, selecione Replication metrics and events (Métricas e eventos de replicação). Para obter mais informações, consulte Monitorar a replicação com métricas, notificações de eventos e status.
    - Se quiser habilitar a replicação de marcadores de exclusão na configuração de replicação, selecione Delete marker replication (Excluir replicação de marcador). Para obter mais informações, consulte Replicação de marcadores de exclusão entre intervalos.
    - Se você quiser habilitar a sincronização de modificação de réplica do Amazon S3 em sua configuração de replicação, selecione Replica modification sync (Sincronização de modificação de réplica). Para obter mais informações, consulte Replicação de alterações de metadados com sincronização de modificação de réplica.

    > **Note**
    >
    > Quando você usa métricas de replicação do S3 RTC ou S3, aplicam-se taxas adicionais.

14. Para terminar, escolha Save (Salvar).
15. Depois de salvar sua regra, você pode editar, ativar, desativar ou excluir sua regra selecionando sua regra e escolhendo Edit rule (Editar regra).

Como usar o AWS CLI

Para configurar a AWS CLI para configurar a replicação quando os buckets de origem e de destino pertencem à mesma Conta da AWS, faça o seguinte:

- Crie os buckets de origem e de destino.

- Habilite o versionamento nos buckets.
- Crie um perfil do AWS Identity and Access Management (IAM) que dê ao Amazon S3 permissão para replicar objetos.
- Adicione uma configuração de replicação ao bucket de origem.

Para verificar sua configuração, teste-a.

Como configurar a replicação quando os buckets de origem e de destino pertencem à mesma Conta da AWS

1. Defina um perfil de credenciais para a AWS CLI. Este exemplo usa o nome de perfil `acctA`. Consulte mais informações sobre como configurar perfis de credenciais e como usar perfis nomeados em Configuration and credential file settings no Guia do usuário da AWS Command Line Interface.

   > **Important**
   >
   > O perfil que você usar para este exemplo deve ter as permissões necessárias. Por exemplo, na configuração da replicação, especifique a função do IAM que o Amazon S3 pode assumir. Você só poderá fazer isso se o perfil usado tiver a permissão `iam:PassRole`. Consulte mais informações em Conceda permissões a um usuário para passar um perfil para um AWS service (Serviço da AWS) no Guia do usuário do IAM. Se você usar credenciais de administrador para criar um perfil nomeado, poderá executar todas as tarefas.

2. Crie um bucket de origem e habilite o versionamento nele usando os comandos da AWS CLI a seguir. Para usar esses comandos, substitua *`user input placeholders`* por suas próprias informações.

   O comando `create-bucket` a seguir cria um bucket de origem chamado *`amzn-s3-demo-source-bucket`* na região Leste dos EUA (N. da Virgínia) (`us-east-1`):

   ```
   aws s3api create-bucket \
   --bucket amzn-s3-demo-source-bucket \
   --region us-east-1 \
   --profile acctA
   ```

O comando `put-bucket-versioning` a seguir habilita o Versionamento do S3 no bucket do *amzn-s3-demo-source-bucket*:

```
aws s3api put-bucket-versioning \
--bucket amzn-s3-demo-source-bucket \
--versioning-configuration Status=Enabled \
--profile acctA
```

3. Crie um bucket de destino e habilite o versionamento nele usando os comandos da AWS CLI a seguir. Para usar esses comandos, substitua *user input placeholders* por suas próprias informações.

> **Note**
>
> Para fazer a configuração de uma replicação quando os buckets de origem e de destino estiverem na mesma Conta da AWS, use o mesmo perfil para os buckets de origem e destino. Este exemplo usa `acctA`.
> Para testar a configuração da replicação quando os buckets pertencerem a diferentes contas da Contas da AWS, especifique diferentes perfis para cada conta. Por exemplo, use um perfil `acctB` para o bucket de destino.

O comando `create-bucket` a seguir cria um bucket de destino chamado *amzn-s3-demo-destination-bucket* na região Oeste dos EUA (Oregon) (`us-west-2`):

```
aws s3api create-bucket \
--bucket amzn-s3-demo-destination-bucket \
--region us-west-2 \
--create-bucket-configuration LocationConstraint=us-west-2 \
--profile acctA
```

O comando `put-bucket-versioning` a seguir habilita o Versionamento do S3 no bucket do *amzn-s3-demo-destination-bucket*:

```
aws s3api put-bucket-versioning \
--bucket amzn-s3-demo-destination-bucket \
--versioning-configuration Status=Enabled \
```

```
--profile acctA
```

4. Crie uma função do IAM. Você especifica essa função na configuração da replicação que adiciona ao bucket de *origem* posteriormente. O Amazon S3 assume essa função para replicar objetos em seu nome. A função do IAM é criada em duas etapas:

   - Crie uma função.
   - Anexar uma política de permissões à função.

   a. Crie a função do IAM.

      i. Copie a política de confiança a seguir e salve-a em um arquivo chamado `s3-role-trust-policy.json` no diretório atual do computador local. Essa política concede à entidade principal do serviço Amazon S3 permissões para assumir o perfil.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service":"s3.amazonaws.com"
         },
         "Action":"sts:AssumeRole"
      }
   ]
}
```

      ii. Execute o comando a seguir para criar uma função.

```
$ aws iam create-role \
--role-name replicationRole \
--assume-role-policy-document file://s3-role-trust-policy.json  \
--profile acctA
```

   b. Anexar uma política de permissões à função.

      i. Copie a política de permissões a seguir e salve-a em um arquivo com o nome `s3-role-permissions-policy.json` no diretório atual do computador local. Essa política concede permissões para várias ações de bucket e objetos do Amazon S3.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "s3:GetObjectVersionForReplication",
            "s3:GetObjectVersionAcl",
            "s3:GetObjectVersionTagging"
         ],
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
         ]
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3:ListBucket",
            "s3:GetReplicationConfiguration"
         ],
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-source-bucket"
         ]
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3:ReplicateObject",
            "s3:ReplicateDelete",
            "s3:ReplicateTags"
         ],
         "Resource":"arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
      }
   ]
}
```

Note

- Se você quiser replicar objetos criptografados, também precisará conceder as permissões de chave do AWS Key Management Service (AWS KMS)

necessárias. Para obter mais informações, consulte the section called "Replicar objetos criptografados".

- Para usar a funcionalidade Bloqueio de Objetos com replicação, é necessário conceder duas permissões adicionais no bucket de origem do S3 no perfil do AWS Identity and Access Management (IAM) usado para configurar a replicação. As duas permissões adicionais são `s3:GetObjectRetention` e `s3:GetObjectLegalHold`. Se o perfil tiver uma instrução de permissão `s3:Get*`, essa instrução satisfará o requisito. Para obter mais informações, consulte the section called "Usar a funcionalidade Bloqueio de Objetos com a funcionalidade Replicação do S3".

ii. Execute o comando a seguir para criar uma política e ligá-la à função. Substitua os *`user input placeholders`* por suas próprias informações.

```
$ aws iam put-role-policy \
--role-name replicationRole \
--policy-document file://s3-role-permissions-policy.json \
--policy-name replicationRolePolicy \
--profile acctA
```

5. Adicione uma configuração de replicação ao bucket de origem.

a. Embora a API do Amazon S3 exija que você especifique a configuração da replicação como XML, a AWS CLI requer que você especifique a configuração de replicação como JSON. Salve o JSON a seguir em um arquivo chamado `replication.json` no diretório local do seu computador.

```
{
  "Role": "IAM-role-ARN",
  "Rules": [
    {
      "Status": "Enabled",
      "Priority": 1,
      "DeleteMarkerReplication": { "Status": "Disabled" },
      "Filter" : { "Prefix": "Tax"},
      "Destination": {
        "Bucket": "arn:aws:s3:::amzn-s3-demo-destination-bucket"
      }
    }
  ]
```

```
}
```

b. Atualize o JSON substituindo os valores de *amzn-s3-demo-destination-bucket* e *IAM-role-ARN* por suas próprias informações. Salve as alterações.

c. Execute o comando `put-bucket-replication` a seguir para adicionar a configuração de replicação ao bucket de origem. Dê um nome ao bucket de origem:

```
$ aws s3api put-bucket-replication \
--replication-configuration file://replication.json \
--bucket amzn-s3-demo-source-bucket \
--profile acctA
```

Para recuperar a configuração de replicação, use o comando `get-bucket-replication`:

```
$ aws s3api get-bucket-replication \
--bucket amzn-s3-demo-source-bucket \
--profile acctA
```

6. Teste a configuração no console do Amazon S3, seguindo estas etapas:

a. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.

b. No painel de navegação à esquerda, escolha Buckets. Na lista Buckets de uso geral, selecione o bucket de origem.

c. No bucket de origem, crie uma pasta chamada *Tax*.

d. Adicione objetos de amostra à pasta *Tax* no bucket de origem.

> **Note**
>
> O tempo necessário para o Amazon S3 replicar um objeto depende do tamanho do objeto. Para obter informações sobre como ver o status da replicação, consulte Obtenção de informações sobre o status da replicação.

No bucket de *destino*, verifique o seguinte:

- Se o Amazon S3 replicou os objetos.

- Se os objetos são réplicas. Na guia Propriedades dos objetos, role para baixo até a seção Visão geral do gerenciamento de objetos. Em Configurações de gerenciamento, veja o valor em Status da replicação. Esse valor deve ser definido como `REPLICA`.
- Se as réplicas pertencem à conta do bucket de origem. É possível verificar a propriedade do objeto na guia Permissões dos objetos.

  Se os buckets de origem e de destino pertencerem a contas diferentes, você poderá adicionar uma configuração opcional para instruir o Amazon S3 a alterar a propriedade da réplica à conta de destino. Para obter um exemplo, consulte Como alterar o proprietário da réplica.

Uso dos SDKs da AWS

Use os exemplos de código a seguir para adicionar uma configuração de replicação ao bucket com AWS SDK para Java e AWS SDK para .NET, respectivamente.

> **Note**
>
> - Se você quiser replicar objetos criptografados, também precisará conceder as permissões de chave do AWS Key Management Service (AWS KMS) necessárias. Para obter mais informações, consulte the section called “Replicar objetos criptografados”.
> - Para usar a funcionalidade Bloqueio de Objetos com replicação, é necessário conceder duas permissões adicionais no bucket de origem do S3 no perfil do AWS Identity and Access Management (IAM) usado para configurar a replicação. As duas permissões adicionais são `s3:GetObjectRetention` e `s3:GetObjectLegalHold`. Se o perfil tiver uma instrução de permissão `s3:Get*`, essa instrução satisfará o requisito. Para obter mais informações, consulte the section called “Usar a funcionalidade Bloqueio de Objetos com a funcionalidade Replicação do S3”.

Java

O exemplo a seguir adiciona uma configuração de replicação a um bucket e, depois, a recupera e verifica a configuração. Consulte instruções sobre como criar e testar uma amostra funcional em Getting Started no Guia do desenvolvedor do AWS SDK para Java.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.identitymanagement.AmazonIdentityManagement;
import
 com.amazonaws.services.identitymanagement.AmazonIdentityManagementClientBuilder;
import com.amazonaws.services.identitymanagement.model.CreateRoleRequest;
import com.amazonaws.services.identitymanagement.model.PutRolePolicyRequest;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3Client;
import com.amazonaws.services.s3.model.BucketReplicationConfiguration;
import com.amazonaws.services.s3.model.BucketVersioningConfiguration;
import com.amazonaws.services.s3.model.CreateBucketRequest;
import com.amazonaws.services.s3.model.DeleteMarkerReplication;
import com.amazonaws.services.s3.model.DeleteMarkerReplicationStatus;
import com.amazonaws.services.s3.model.ReplicationDestinationConfig;
import com.amazonaws.services.s3.model.ReplicationRule;
import com.amazonaws.services.s3.model.ReplicationRuleStatus;
import com.amazonaws.services.s3.model.SetBucketVersioningConfigurationRequest;
import com.amazonaws.services.s3.model.StorageClass;
import com.amazonaws.services.s3.model.replication.ReplicationFilter;
import com.amazonaws.services.s3.model.replication.ReplicationFilterPredicate;
import com.amazonaws.services.s3.model.replication.ReplicationPrefixPredicate;

import java.io.IOException;
import java.util.ArrayList;
import java.util.HashMap;
import java.util.List;
import java.util.Map;

public class CrossRegionReplication {

        public static void main(String[] args) throws IOException {
                Regions clientRegion = Regions.DEFAULT_REGION;
                String accountId = "*** Account ID ***";
                String roleName = "*** Role name ***";
                String sourceBucketName = "*** Source bucket name ***";
                String destBucketName = "*** Destination bucket name ***";
                String prefix = "Tax/";

                String roleARN = String.format("arn:aws:iam::%s:%s", accountId,
 roleName);
                String destinationBucketARN = "arn:aws:s3:::" + destBucketName;
```

```
                AmazonS3 s3Client = AmazonS3Client.builder()
                                .withCredentials(new ProfileCredentialsProvider())
                                .withRegion(clientRegion)
                                .build();

                createBucket(s3Client, clientRegion, sourceBucketName);
                createBucket(s3Client, clientRegion, destBucketName);
                assignRole(roleName, clientRegion, sourceBucketName,
destBucketName);

                try {

                        // Create the replication rule.
                        List<ReplicationFilterPredicate> andOperands = new
ArrayList<ReplicationFilterPredicate>();
                        andOperands.add(new ReplicationPrefixPredicate(prefix));

                        Map<String, ReplicationRule> replicationRules = new
HashMap<String, ReplicationRule>();
                        replicationRules.put("ReplicationRule1",
                                        new ReplicationRule()
                                                        .withPriority(0)

.withStatus(ReplicationRuleStatus.Enabled)

.withDeleteMarkerReplication(
                                                                        new
DeleteMarkerReplication().withStatus(

   DeleteMarkerReplicationStatus.DISABLED))
                                                        .withFilter(new
ReplicationFilter().withPredicate(
                                                                        new
ReplicationPrefixPredicate(prefix)))
                                                        .withDestinationConfig(new
ReplicationDestinationConfig()

.withBucketARN(destinationBucketARN)

.withStorageClass(StorageClass.Standard)));

                        // Save the replication rule to the source bucket.
                        s3Client.setBucketReplicationConfiguration(sourceBucketName,
```

```
                                        new BucketReplicationConfiguration()
                                                .withRoleARN(roleARN)

.withRules(replicationRules));

                        // Retrieve the replication configuration and verify that
the configuration
                        // matches the rule we just set.
                        BucketReplicationConfiguration replicationConfig = s3Client

.getBucketReplicationConfiguration(sourceBucketName);
                        ReplicationRule rule =
replicationConfig.getRule("ReplicationRule1");
                        System.out.println("Retrieved destination bucket ARN: "
                                        +
rule.getDestinationConfig().getBucketARN());
                        System.out.println("Retrieved priority: " +
rule.getPriority());
                        System.out.println("Retrieved source-bucket replication rule
status: " + rule.getStatus());
                } catch (AmazonServiceException e) {
                        // The call was transmitted successfully, but Amazon S3
couldn't process
                        // it, so it returned an error response.
                        e.printStackTrace();
                } catch (SdkClientException e) {
                        // Amazon S3 couldn't be contacted for a response, or the
client
                        // couldn't parse the response from Amazon S3.
                        e.printStackTrace();
                }
        }

        private static void createBucket(AmazonS3 s3Client, Regions region, String
bucketName) {
                CreateBucketRequest request = new CreateBucketRequest(bucketName,
region.getName());
                s3Client.createBucket(request);
                BucketVersioningConfiguration configuration = new
BucketVersioningConfiguration()
                                .withStatus(BucketVersioningConfiguration.ENABLED);

                SetBucketVersioningConfigurationRequest enableVersioningRequest =
new SetBucketVersioningConfigurationRequest(
```

```
                                bucketName, configuration);
                s3Client.setBucketVersioningConfiguration(enableVersioningRequest);

        }

        private static void assignRole(String roleName, Regions region, String
 sourceBucket, String destinationBucket) {
                AmazonIdentityManagement iamClient =
 AmazonIdentityManagementClientBuilder.standard()
                                .withRegion(region)
                                .withCredentials(new ProfileCredentialsProvider())
                                .build();
                StringBuilder trustPolicy = new StringBuilder();
                trustPolicy.append("{\\r\\n   ");
                trustPolicy.append("\\\"Version\\\":\\\"2012-10-17\\\",\\r\\n   ");
                trustPolicy.append("\\\"Statement\\\":[\\r\\n      {\\r\\n
 ");
                trustPolicy.append("\\\"Effect\\\":\\\"Allow\\\",\\r\\n         \\
\"Principal\\\":{\\r\\n            ");
                trustPolicy.append("\\\"Service\\\":\\\"s3.amazonaws.com\\\"\\r\\n
       },\\r\\n         ");
                trustPolicy.append("\\\"Action\\\":\\\"sts:AssumeRole\\\"\\r\\n
  }\\r\\n   ]\\r\\n}");

                CreateRoleRequest createRoleRequest = new CreateRoleRequest()
                                .withRoleName(roleName)

 .withAssumeRolePolicyDocument(trustPolicy.toString());

                iamClient.createRole(createRoleRequest);

                StringBuilder permissionPolicy = new StringBuilder();
                permissionPolicy.append(
                                "{\\r\\n   \\\"Version\\\":\\\"2012-10-17\\\",\\r\\n
   \\\"Statement\\\":[\\r\\n      {\\r\\n         ");
                permissionPolicy.append(
                                "\\\"Effect\\\":\\\"Allow\\\",\\r\\n         \\
\"Action\\\":[\\r\\n             ");
                permissionPolicy.append("\\\"s3:GetObjectVersionForReplication\\\",\
\r\\n            ");
                permissionPolicy.append(
                                "\\\"s3:GetObjectVersionAcl\\\"\\r\\n         ],\\r\
\n         \\\"Resource\\\":[\\r\\n            ");
                permissionPolicy.append("\\\"arn:aws:s3:::");
```

```
                permissionPolicy.append(sourceBucket);
                permissionPolicy.append("/*\\\"\\r\\n         ]\\r\\n      },\\r\\n
     {\\r\\n         ");
                permissionPolicy.append(
                                "\\\"Effect\\\":\\\"Allow\\\",\\r\\n         \\
\"Action\\\":[\\r\\n            ");
                permissionPolicy.append(
                                "\\\"s3:ListBucket\\\",\\r\\n            \\
\"s3:GetReplicationConfiguration\\\"\\r\\n         ");
                permissionPolicy.append("],\\r\\n         \\\"Resource\\\":[\\r\\n
          \\\"arn:aws:s3:::");
                permissionPolicy.append(sourceBucket);
                permissionPolicy.append("\\r\\n         ");
                permissionPolicy
                                .append("]\\r\\n      },\\r\\n      {\\r\\n
 \\\"Effect\\\":\\\"Allow\\\",\\r\\n         ");
                permissionPolicy.append(
                                "\\\"Action\\\":[\\r\\n            \\
\"s3:ReplicateObject\\\",\\r\\n            ");
                permissionPolicy
                                .append("\\\"s3:ReplicateDelete\\\",\\r\\n
  \\\"s3:ReplicateTags\\\",\\r\\n            ");
                permissionPolicy.append("\\\"s3:GetObjectVersionTagging\\\"\\r\\n\\r
\\n         ],\\r\\n         ");
                permissionPolicy.append("\\\"Resource\\\":\\\"arn:aws:s3:::");
                permissionPolicy.append(destinationBucket);
                permissionPolicy.append("/*\\\"\\r\\n      }\\r\\n   ]\\r\\n}");

                PutRolePolicyRequest putRolePolicyRequest = new
 PutRolePolicyRequest()
                                .withRoleName(roleName)
                                .withPolicyDocument(permissionPolicy.toString())
                                .withPolicyName("crrRolePolicy");

                iamClient.putRolePolicy(putRolePolicyRequest);

        }
}
```

C#

O exemplo de código de AWS SDK para .NET a seguir adiciona uma configuração de replicação a um bucket e, depois, a recupera. Para usar esse código, dê nomes aos buckets e o nome

de recurso da Amazon (ARN) à função do IAM. Consulte informações sobre como configurar e executar exemplos de código, em Getting Started with the AWS SDK para .NET no Guia do desenvolvedor do AWS SDK para .NET.

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class CrossRegionReplicationTest
    {
        private const string sourceBucket = "*** source bucket ***";
        // Bucket ARN example - arn:aws:s3:::destinationbucket
        private const string destinationBucketArn = "*** destination bucket ARN
 ***";
        private const string roleArn = "*** IAM Role ARN ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint sourceBucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 s3Client;
        public static void Main()
        {
            s3Client = new AmazonS3Client(sourceBucketRegion);
            EnableReplicationAsync().Wait();
        }
        static async Task EnableReplicationAsync()
        {
            try
            {
                ReplicationConfiguration replConfig = new ReplicationConfiguration
                {
                    Role = roleArn,
                    Rules =
                        {
                            new ReplicationRule
                            {
                                Prefix = "Tax",
                                Status = ReplicationRuleStatus.Enabled,
                                Destination = new ReplicationDestination
                                {
```

```
                                    BucketArn = destinationBucketArn
                                }
                            }
                        }
                };

                PutBucketReplicationRequest putRequest = new
PutBucketReplicationRequest
                {
                    BucketName = sourceBucket,
                    Configuration = replConfig
                };

                PutBucketReplicationResponse putResponse = await
s3Client.PutBucketReplicationAsync(putRequest);

                // Verify configuration by retrieving it.
                await RetrieveReplicationConfigurationAsync(s3Client);
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered on server. Message:'{0}' when
writing an object", e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
writing an object", e.Message);
            }
        }
        private static async Task RetrieveReplicationConfigurationAsync(IAmazonS3
client)
        {
            // Retrieve the configuration.
            GetBucketReplicationRequest getRequest = new GetBucketReplicationRequest
            {
                BucketName = sourceBucket
            };
            GetBucketReplicationResponse getResponse = await
client.GetBucketReplicationAsync(getRequest);
            // Print.
            Console.WriteLine("Printing replication configuration information...");
            Console.WriteLine("Role ARN: {0}", getResponse.Configuration.Role);
            foreach (var rule in getResponse.Configuration.Rules)
```

```
            {
                Console.WriteLine("ID: {0}", rule.Id);
                Console.WriteLine("Prefix: {0}", rule.Prefix);
                Console.WriteLine("Status: {0}", rule.Status);
            }
        }
    }
}
```

Configuração da replicação de buckets em contas diferentes

A replicação em tempo real é a cópia assíncrona automática de objetos em buckets na mesma região da AWS ou em Regiões da AWS diferentes. A replicação em tempo real copia os objetos recém-criados e as atualizações de objeto de um bucket de origem para buckets de destino. Para obter mais informações, consulte Replicar objetos dentro de uma região e entre regiões.

Ao configurar a replicação, você adiciona regras de replicação ao bucket de origem. As regras de replicação definem quais objetos do bucket de origem devem ser replicados e o bucket de destino ou buckets nos quais os objetos replicados são armazenados. Você pode criar uma regra para replicar todos os objetos dentro de um bucket ou um subgrupo de objetos com um prefixo específico de nome de chaves, uma ou mais tags de objetos ou ambos. Um bucket de destino pode estar na mesma Conta da AWS que o bucket de origem ou pode estar em uma conta diferente.

Se você especificar um ID da versão do objeto a ser excluído, o Amazon S3 excluirá essa versão do objeto no bucket de origem. No entanto, ele não replica a exclusão no bucket de destino. Em outras palavras: ele não exclui a mesma versão do objeto do bucket de destino. Isso protege os dados contra exclusões mal-intencionadas.

Quando você adiciona uma regra de replicação a um bucket, ela fica ativada por padrão, portanto, começa a funcionar assim que é salva.

A configuração da replicação em tempo real quando os buckets de origem e de destino pertencem a Contas da AWS diferentes é semelhante à configuração da replicação quando os dois buckets pertencem à mesma conta. No entanto, há várias diferenças quando você configura a replicação em um cenário entre contas diferentes:

- O proprietário do bucket de destino deve conceder ao proprietário do bucket de destino permissão para replicar objetos na política do bucket de destino.

- Se você estiver replicando objetos criptografados com a criptografia do lado do servidor com chaves do AWS Key Management Service (AWS KMS) (SSE-KMS) em um cenário entre contas diferentes, o proprietário da chave do KMS deverá conceder ao proprietário do bucket de origem permissão para usar a chave do KMS. Para obter mais informações, consulte Conceder permissões adicionais para cenários entre contas.
- Por padrão, os objetos replicados pertencem ao proprietário do bucket de origem. Em um cenário entre contas diferentes, você pode querer configurar a replicação para alterar a propriedade dos objetos replicados ao proprietário do bucket de destino. Para obter mais informações, consulte Alterar o proprietário da réplica.

Para configurar a replicação quando os buckets de origem e destino pertencem a Contas da AWS diferentes

1. Neste exemplo, você cria buckets de origem e de destino em duas Contas da AWS diferentes. Você deve ter dois perfis de credencial definidos para a AWS CLI. Este exemplo usa `acctA` e `acctB` para esses nomes de perfil. Consulte mais informações sobre como configurar perfis de credenciais e como usar perfis nomeados em Configuration and credential file settings no Guia do usuário da AWS Command Line Interface.
2. Siga as instruções passo a passo em Configurar a replicação para buckets na mesma conta com as seguintes alterações:
   - Para todos os comandos da AWS CLI relacionados a atividades do bucket de origem (como criar o bucket de origem, habilitar o versionamento e criar o perfil do IAM), use o perfil `acctA`. Use o perfil `acctB` para criar o bucket de destino.
   - Verifique se a política e permissões para o perfil do IAM especifica os buckets de origem e de destino que você criou para este exemplo.
3. No console, adicione a seguinte política do bucket ao bucket de *`destino`* para permitir que o proprietário do bucket de *`origem`* replique objetos. Para instruções, consulte Adicionar uma política de bucket usando o console do Amazon S3. Edite a política fornecendo o ID da Conta da AWS do proprietário do bucket de origem, o nome do perfil do IAM e o nome do bucket de destino.

   > **Note**
   >
   > Para usar o exemplo a seguir, substitua os *`user input placeholders`* por suas próprias informações. Substitua *`amzn-s3-demo-destination-bucket`* pelo nome

do bucket de destino. Substitua *source-bucket-account-ID*:role/service-role/*source-account-IAM-role* no nome do recurso da Amazon (ARN) pelo perfil do IAM que você está usando para essa configuração de replicação.
Se você criou o perfil de serviço do IAM manualmente, defina o caminho do perfil no ARN do IAM como `role/service-role/`, conforme mostrado no exemplo de política a seguir. Para obter mais informações, consulte ARNs do IAM no Guia do usuário do IAM.

```
{
   "Version":"2012-10-17",
   "Id":"",
   "Statement":[
      {
         "Sid":"Set-permissions-for-objects",
         "Effect":"Allow",
         "Principal":{
            "AWS":"arn:aws:iam::source-bucket-account-ID:role/service-role/source-account-IAM-role"
         },
         "Action":["s3:ReplicateObject", "s3:ReplicateDelete"],
         "Resource":"arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
      },
      {
         "Sid":"Set permissions on bucket",
         "Effect":"Allow",
         "Principal":{
            "AWS":"arn:aws:iam::source-bucket-account-ID:role/service-role/source-account-IAM-role"
         },
         "Action":["s3:GetBucketVersioning", "s3:PutBucketVersioning"],
         "Resource":"arn:aws:s3:::amzn-s3-demo-destination-bucket"
      }
   ]
}
```

4. (Opcional) Se você estiver replicando objetos criptografados com a SSE-KMS, o proprietário da chave do KMS deverá conceder ao proprietário do bucket de origem permissão para usar a chave do KMS. Para obter mais informações, consulte Conceder permissões adicionais para cenários entre contas.

5. (Opcional) Na replicação, o proprietário do objeto de origem possui a réplica por padrão. Quando os buckets de origem e de destino pertencerem a Contas da AWS diferentes, é possível adicionar configurações opcionais para alterar a propriedade da réplica para a Conta da AWS que possui os buckets de destino. Isso inclui conceder a permissão `ObjectOwnerOverrideToBucketOwner`. Para obter mais informações, consulte Alterar o proprietário da réplica.

Alterar o proprietário da réplica

Na replicação, por padrão o proprietário do objeto de origem também é proprietário da réplica. No entanto, quando os buckets de origem e de destino pertencem a Contas da AWS diferentes, você pode querer alterar a propriedade da réplica. Por exemplo, você pode querer alterar a propriedade para restringir o acesso a replicas de objetos. Na configuração de replicação, é possível adicionar configurações opcionais para alterar a propriedade da réplica para a Conta da AWS que possui os buckets de destino.

Para alterar o proprietário da réplica, faça o seguinte:

- Adicione a opção de substituição do proprietário à configuração da replicação para instruir o Amazon S3 a alterar a propriedade da réplica.
- Conceda ao Amazon S3 a permissão `s3:ObjectOwnerOverrideToBucketOwner` para alterar a propriedade da réplica.
- Adicione a permissão `s3:ObjectOwnerOverrideToBucketOwner` na política do bucket de destino para permitir a alteração da propriedade da réplica. A permissão `s3:ObjectOwnerOverrideToBucketOwner` autoriza que o proprietário do bucket de destino aceite a propriedade das réplicas de objetos.

Para obter mais informações, consulte the section called “Considerações sobre a opção de substituição da propriedade” e Adicionar a opção de substituição do proprietário à configuração da replicação. Para ver um exemplo funcional com instruções detalhadas, consulte Como alterar o proprietário da réplica.

> **Important**
>
> Em vez de usar a opção de substituição do proprietário do bucket, é possível usar a configuração aplicada pelo proprietário do bucket em Propriedade de objeto. Quando você usa a replicação e os buckets de origem e de destino pertencem a Contas da AWS

diferentes, o proprietário do bucket de destino pode usar a configuração aplicada pelo proprietário do bucket em Propriedade de objetos para alterar a propriedade da réplica para a Conta da AWS que possui o bucket de destino. Essa configuração desabilita listas de controle de acesso (ACLs) de objetos.
A configuração aplicada pelo proprietário do bucket imita o comportamento de substituição do proprietário existente sem a necessidade da permissão `s3:ObjectOwnerOverrideToBucketOwner`. Todos os objetos que são replicados para o bucket de destino com a configuração aplicada pelo proprietário do bucket pertencem ao proprietário do bucket de destino. Para obter informações sobre o Object Ownership, consulte Controlar a propriedade de objetos e desabilitar ACLs para seu bucket.

Considerações sobre a opção de substituição da propriedade

Ao configurar a opção de substituição da propriedade, aplicam-se as seguintes considerações:

- Por padrão, o proprietário do objeto de origem também possui a réplica. O Amazon S3 replica a versão do objeto e a ACL associada a ela.

  Se você adicionar a opção de substituição do proprietário à configuração de replicação, o Amazon S3 replicará somente a versão do objeto, não a ACL. Além disso, o Amazon S3 não replica as alterações subsequentes na ACL do objeto de origem. O Amazon S3 define a ACL na réplica que concede controle total ao proprietário do bucket de destino.
- Ao atualizar uma configuração de replicação para habilitar ou desabilitar a substituição do proprietário, ocorrerá o seguinte comportamento:
  - Se você adicionar a opção de substituição do proprietário à configuração da replicação:

    Quando o Amazon S3 replica uma versão do objeto, ele descarta a ACL associada ao objeto de origem. Em vez disso, o Amazon S3 define a ACL na réplica, dando o controle total ao proprietário do bucket de destino. O Amazon S3 não replica as alterações subsequentes na ACL do objeto de origem. No entanto, essa alteração na ACL não se aplica às versões de objeto replicadas antes de você definir a opção de substituição do proprietário. As atualizações da ACL nos objetos de origem replicados antes da substituição do proprietário foram definidas para continuarem a ser replicadas (porque o objeto e suas réplicas continuam a ter o mesmo proprietário).
  - Se você remover a opção de substituição do proprietário da configuração da replicação:

O Amazon S3 replica novos objetos que aparecem no bucket de origem e as ACLs associadas aos buckets de destino. Para objetos replicados antes de você ter removido a substituição do proprietário, o Amazon S3 não replicará as ACLs, pois a propriedade do objeto muda, de maneira que o Amazon S3 feito permanece em vigor. Em outras palavras: as ACLs colocaram a versão do objeto que foi replicada quando a substituição do proprietário tinha sido substituída para não continuarem a ser replicadas.

Adicionar a opção de substituição do proprietário à configuração da replicação

> **Warning**
>
> Adicione a opção de substituição do proprietário somente quando os buckets de origem e de destino pertencerem a Contas da AWS diferentes. O Amazon S3 não verifica se os buckets pertencem à mesma conta ou a contas diferentes. Se você adicionar a substituição do proprietário quando os dois buckets pertencerem à mesma Conta da AWS, o Amazon S3 aplicará a substituição do proprietário. Essa opção concede permissões completas ao proprietário do bucket de destino e não replica as atualizações subsequentes às listas de controle de acesso (ACLs) dos objetos de origem. O proprietário da réplica pode alterar diretamente na ACL associada a uma réplica com uma solicitação `PutObjectAcl`, mas não por replicação.

Para especificar a opção de substituição do proprietário, adicione o seguinte ao elemento `Destination`:

- O elemento `AccessControlTranslation`, que diz ao Amazon S3 para alterar a propriedade da réplica
- O elemento `Account`, que especifica a Conta da AWS do proprietário do bucket de destino

```
<ReplicationConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
    ...
    <Destination>
      ...
      <AccessControlTranslation>
           <Owner>Destination</Owner>
       </AccessControlTranslation>
      <Account>destination-bucket-owner-account-id</Account>
```

```
    </Destination>
  </Rule>
</ReplicationConfiguration>
```

A configuração da replicação do exemplo a seguir instrui o Amazon S3 a replicar os objetos que têm o prefixo de chaves *Tax* ao bucket de destino *amzn-s3-demo-destination-bucket* e alterar a propriedade das réplicas. Para usar esse exemplo, substitua os *user input placeholders* por suas próprias informações.

```
<?xml version="1.0" encoding="UTF-8"?>
<ReplicationConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
   <Role>arn:aws:iam::account-id:role/role-name</Role>
   <Rule>
      <ID>Rule-1</ID>
      <Priority>1</Priority>
      <Status>Enabled</Status>
      <DeleteMarkerReplication>
         <Status>Disabled</Status>
      </DeleteMarkerReplication>
      <Filter>
         <Prefix>Tax</Prefix>
      </Filter>
      <Destination>
         <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
         <Account>destination-bucket-owner-account-id</Account>
         <AccessControlTranslation>
            <Owner>Destination</Owner>
         </AccessControlTranslation>
      </Destination>
   </Rule>
</ReplicationConfiguration>
```

Conceder permissão do Amazon S3 para alterar a propriedade da réplica

Conceda permissões do Amazon S3 para alterar a propriedade da réplica adicionando permissão para a ação `s3:ObjectOwnerOverrideToBucketOwner` na política de permissões associada ao perfil do AWS Identity and Access Management (IAM). Esse é o perfil do IAM especificado na configuração de replicação que permite que o Amazon S3 assuma e replique objetos em seu nome. Para usar o exemplo a seguir, substitua *amzn-s3-demo-destination-bucket* pelo nome do bucket de destino.

```
...
{
    "Effect":"Allow",
         "Action":[
       "s3:ObjectOwnerOverrideToBucketOwner"
    ],
    "Resource":"arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
}
...
```

Adicionar a permissão na política do bucket de destino para permitir a alteração da propriedade da réplica

O proprietário do bucket de destino deve conceder ao proprietário da permissão do bucket de origem para alterar a propriedade da réplica. A propriedade do bucket de destino concede ao proprietário do bucket de origem permissão para a ação `s3:ObjectOwnerOverrideToBucketOwner`. Essa permissão autoriza que o proprietário do bucket de destino aceite a propriedade das réplicas de objetos. O exemplo de declaração de política do bucket a seguir mostra como fazer isso. Para usar esse exemplo, substitua os *`user input placeholders`* por suas próprias informações.

```
...
{
    "Sid":"1",
    "Effect":"Allow",
    "Principal":{"AWS":"source-bucket-account-id"},
    "Action":["s3:ObjectOwnerOverrideToBucketOwner"],
    "Resource":"arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
}
...
```

Como alterar o proprietário da réplica

Quando os buckets de origem e de destino em uma configuração de replicação pertencem a Contas da AWS diferentes, você pode instruir o Amazon S3 a alterar a propriedade da réplica para a Conta da AWS que possui o bucket de destino. Os exemplos a seguir mostram como usar o console do Amazon S3, a AWS Command Line Interface (AWS CLI) e os SDKs da AWS para alterar a propriedade da réplica.

Uso do console do S3

Para obter instruções detalhadas, consulte Configurar a replicação para buckets na mesma conta. Este tópico fornece instruções para definir a configuração da replicação quando os buckets de origem e de destino pertencerem às mesmas Contas da AWS ou a contas diferentes.

Como usar o AWS CLI

O procedimento a seguir mostra como alterar a propriedade da réplica usando a AWS CLI. Neste procedimento, você faz o seguinte:

- Crie os buckets de origem e de destino.
- Habilite o versionamento nos buckets.
- Crie um perfil do AWS Identity and Access Management (IAM) que dê ao Amazon S3 permissão para replicar objetos.
- Adicione uma configuração de replicação ao bucket de origem.
- Na configuração da replicação, você instrui o Amazon S3 a alterar a propriedade da réplica.
- Você testa a configuração de replicação.

Como alterar o proprietário da réplica quando os buckets de origem e de destino pertencem a Contas da AWS diferentes (AWS CLI)

Para usar os comandos AWS CLI de exemplo neste procedimento, substitua *`user input placeholders`* por suas informações.

1. Neste exemplo, você cria os buckets de origem e de destino em duas Contas da AWS diferentes. Para trabalhar com essas duas contas, configure a AWS CLI com dois perfis nomeados. Este exemplo usa os perfis nomeados *`acctA`* e *`acctB`*, respectivamente. Consulte mais informações sobre como configurar perfis de credenciais e como usar perfis nomeados em Configuration and credential file settings no Guia do usuário da AWS Command Line Interface.

   > **Important**
   >
   > Os perfis que você usar para este procedimento devem ter as permissões necessárias. Por exemplo, na configuração da replicação, especifique a função do IAM que o Amazon S3 pode assumir. Você só poderá fazer isso se o perfil usado tiver a permissão `iam:PassRole`. Se usar as credenciais do usuário administrador para criar um perfil nomeado, você poderá realizar todas as tarefas nesse procedimento. Para ter mais

informações, consulte Conceder permissões ao usuário para transmitir um perfil a um AWS service (Serviço da AWS) no Guia do usuário do IAM.

2. Crie o bucket de *origem* e habilite o versionamento. Esse exemplo cria um bucket de origem chamado *amzn-s3-demo-source-bucket* na região Leste dos EUA (N. da Virgínia) (us-east-1).

```
aws s3api create-bucket \
--bucket amzn-s3-demo-source-bucket \
--region us-east-1 \
--profile acctA
```

```
aws s3api put-bucket-versioning \
--bucket amzn-s3-demo-source-bucket \
--versioning-configuration Status=Enabled \
--profile acctA
```

3. Crie um bucket de *destino* e habilite o versionamento. Esse exemplo cria um bucket de destino chamado *amzn-s3-demo-destination-bucket* na região Oeste dos EUA (Oregon) (us-west-2). Use um perfil de Conta da AWS diferente do usado para o bucket de origem.

```
aws s3api create-bucket \
--bucket amzn-s3-demo-destination-bucket \
--region us-west-2 \
--create-bucket-configuration LocationConstraint=us-west-2 \
--profile acctB
```

```
aws s3api put-bucket-versioning \
--bucket amzn-s3-demo-destination-bucket \
--versioning-configuration Status=Enabled \
--profile acctB
```

4. É necessário adicionar permissões à política de bucket de *destino* para permitir a alteração da propriedade da réplica.

   a. Salve a política a seguir em um arquivo chamado *destination-bucket-policy*.json. Substitua *user input placeholders* por suas próprias informações.

```
{
  "Version": "2012-10-17",
```

```
  "Statement": [
    {
      "Sid": "destination_bucket_policy_sid",
      "Principal": {
        "AWS": "source-bucket-owner-account-id"
      },
      "Action": [
        "s3:ReplicateObject",
        "s3:ReplicateDelete",
        "s3:ObjectOwnerOverrideToBucketOwner",
        "s3:ReplicateTags",
        "s3:GetObjectVersionTagging"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
      ]
    }
  ]
}
```

b. Adicione a política anterior ao bucket de destino usando o seguinte comando `put-bucket-policy`:

```
aws s3api put-bucket-policy --region $ {destination-region} --bucket $ {amzn-s3-demo-destination-bucket} --policy file://destination_bucket_policy.json
```

5. Crie uma função do IAM. Você especifica essa função na configuração da replicação que adiciona ao bucket de *origem* posteriormente. O Amazon S3 assume essa função para replicar objetos em seu nome. A função do IAM é criada em duas etapas:

   - Crie a função.
   - Anexar uma política de permissões à função.

   a. Crie a função do IAM.

      i. Copie a política de confiança a seguir e salve-a em um arquivo chamado *s3-role-trust-policy*`.json` no diretório atual do computador local. Essa política concede ao Amazon S3 permissões para assumir a função.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service":"s3.amazonaws.com"
         },
         "Action":"sts:AssumeRole"
      }
   ]
}
```

ii. Execute o seguinte comando `create-role` da AWS CLI para criar o perfil do IAM:

```
$ aws iam create-role \
--role-name replicationRole \
--assume-role-policy-document file://s3-role-trust-policy.json  \
--profile acctA
```

Anote o nome do recurso da Amazon (ARN) do perfil do IAM que você criou. Você precisará desse AR em uma etapa posterior.

b. Anexar uma política de permissões à função.

i. Copie a política de permissões a seguir e salve-a em um arquivo com o nome *s3-role-perm-pol-changeowner*`.json` no diretório atual do computador local. Essa política concede permissões para várias ações de bucket e objetos do Amazon S3. Nas etapas a seguir, anexe essa política ao perfil do IAM criado anteriormente.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "s3:GetObjectVersionForReplication",
            "s3:GetObjectVersionAcl"
         ],
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
```

```
            ]
        },
        {
            "Effect":"Allow",
            "Action":[
                "s3:ListBucket",
                "s3:GetReplicationConfiguration"
            ],
            "Resource":[
                "arn:aws:s3:::amzn-s3-demo-source-bucket"
            ]
        },
        {
            "Effect":"Allow",
            "Action":[
                "s3:ReplicateObject",
                "s3:ReplicateDelete",
                "s3:ObjectOwnerOverrideToBucketOwner",
                "s3:ReplicateTags",
                "s3:GetObjectVersionTagging"
            ],
            "Resource":"arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
        }
    ]
}
```

ii. Para anexar a política de permissões anterior ao perfil, execute o seguinte comando `put-role-policy`:

```
$ aws iam put-role-policy \
--role-name replicationRole \
--policy-document file://s3-role-perm-pol-changeowner.json \
--policy-name replicationRolechangeownerPolicy \
--profile acctA
```

6. Adicione uma configuração de replicação ao bucket de origem.

   a. A AWS CLI requer que você especifique a configuração de replicação como JSON. Salve o JSON a seguir em um arquivo chamado *replication*`.json` no diretório atual local do computador local. Na configuração, `AccessControlTranslation` especifica a mudança na propriedade da réplica do proprietário do bucket de origem para o proprietário do bucket de destino.

```
{
   "Role":"IAM-role-ARN",
   "Rules":[
      {
         "Status":"Enabled",
         "Priority":1,
         "DeleteMarkerReplication":{
            "Status":"Disabled"
         },
         "Filter":{
         },
         "Status":"Enabled",
         "Destination":{
            "Bucket":"arn:aws:s3:::amzn-s3-demo-destination-bucket",
            "Account":"destination-bucket-owner-account-id",
            "AccessControlTranslation":{
               "Owner":"Destination"
            }
         }
      }
   ]
}
```

b. Edite o JSON fornecendo os valores do nome do bucket de destino, o ID da conta do proprietário do bucket de destino e o *IAM-role-ARN*. Substitua *IAM-role-ARN* pelo ARN do perfil do IAM que você criou anteriormente. Salve as alterações.

c. Para adicionar a configuração de replicação ao bucket de origem, execute o seguinte comando:

```
$ aws s3api put-bucket-replication \
--replication-configuration file://replication.json \
--bucket amzn-s3-demo-source-bucket \
--profile acctA
```

7. Teste a configuração de replicação verificando a propriedade da réplica no console do Amazon S3.

a. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.

b. Adicione objetos ao bucket de *origem*. Verifique se o bucket de destino contém as réplicas de objetos e se a propriedade das réplicas mudou para a Conta da AWS que possui o bucket de destino.

Uso dos SDKs da AWS

Consulte um exemplo de código para adicionar uma configuração de replicação em Uso dos SDKs da AWS. Você precisa modificar a configuração de replicação adequadamente. Para obter informações conceituais, consulte Alterar o proprietário da réplica.

Atender aos requisitos de conformidade com o Controle do Tempo de Replicação do S3

O Controle do tempo de replicação do S3 (S3 RTC) ajuda a atender aos requisitos empresariais ou de conformidade relacionados à replicação de dados, além de fornecer visibilidade dos tempos de replicação do Amazon S3. O S3 RTC replica a maioria dos objetos carregados no Amazon S3 em questão de segundos e 99,99% desses objetos em 15 minutos.

Por padrão, o S3 RTC inclui duas maneiras de monitorar o progresso da replicação:

- Métricas de Replicação do S3: é possível usar as métricas de Replicação do S3 para monitorar o número total de operações de API do S3 com replicação pendente, o tamanho total dos objetos com replicação pendente, o tempo máximo de replicação para a região de destino e o número total de operações cuja replicação apresentou falha. Você pode monitorar cada conjunto de dados replicado separadamente. Também é possível habilitar as métricas de Replicação do S3 independentemente do S3 RTC. Para obter mais informações, consulte the section called “Usar métricas de replicação do S3”.

  As regras de replicação com o Controle de Tempo de Replicação do S3 (S3 RTC) habilitado publicam as métricas de Replicação do S3. As métricas de replicação ficam disponíveis 15 minutos após a ativação do S3 RTC. As métricas de replicação estão disponíveis por meio do console do Amazon S3, da API do Amazon S3, dos SDKs da AWS, da AWS Command Line Interface (AWS CLI) e do Amazon CloudWatch. Para ter mais informações sobre métricas do CloudWatch, consulte Monitoramento de métricas com o Amazon CloudWatch. Consulte mais informações sobre como visualizar métricas de replicação por meio do console do Amazon S3 em Visualizar métricas de replicação.

  As métricas de replicação de S3 são cobradas usando a mesma taxa das métricas personalizadas do Amazon CloudWatch. Para obter mais informações, consulte Definição de preço do Amazon CloudWatch.

- Notificações de Eventos do Amazon S3: o S3 RTC fornece eventos `OperationMissedThreshold` e `OperationReplicatedAfterThreshold` que notificam o proprietário do bucket se a replicação do objeto exceder ou ocorrer após o limite de 15 minutos. Com o S3 RTC, as Notificações de Eventos do Amazon S3 podem notificar você nas raras vezes em que objetos não são replicados em até 15 minutos e quando esses objetos são replicados depois do limite de 15 minutos.

  Os eventos de replicação estão disponíveis dentro de 15 minutos após a ativação do S3 RTC. As Notificações de Eventos do Amazon S3 estão disponíveis por meio do Amazon SQS, Amazon SNS ou AWS Lambda. Para obter mais informações, consulte the section called “Recebimento de eventos de falha de replicação”.

Melhores práticas e diretrizes do S3 RTC

Ao replicar dados no Amazon S3 com o Controle de Tempo de Replicação do S3 (S3 RTC) habilitado, siga estas diretrizes de práticas recomendadas para otimizar o desempenho da replicação para workloads.

Tópicos

- Diretrizes de performance da taxa de replicação e de solicitação do Amazon S3
- Estimar as taxas de solicitação de replicação
- Exceder as cotas da taxa de transferência de dados do S3 RTC
- Taxas de solicitação de replicação de objetos criptografados do AWS KMS

Diretrizes de performance da taxa de replicação e de solicitação do Amazon S3

Ao fazer upload e recuperar armazenamento do Amazon S3, as aplicações podem realizar milhares de transações por segundo em performance de solicitação. Por exemplo, uma aplicação pode atingir pelo menos 3.500 solicitações `PUT/COPY/POST/DELETE` ou 5.500 solicitações `GET/HEAD` por segundo por prefixo em um bucket do S3, incluindo as solicitações que a Replicação do S3 faz em seu nome. Não há limite para o número de prefixos em um bucket. Você pode aumentar sua performance de leitura ou gravação paralelizando as leituras. Por exemplo, se criar 10 prefixos em um bucket do S3 para paralelizar leituras, você poderá escalar o desempenho de leitura para 55.000 solicitações de leitura por segundo.

O Amazon S3 escala automaticamente em resposta a taxas de solicitação sustentadas acima dessas diretrizes ou taxas de solicitação sustentadas simultâneas às solicitações `LIST`. Enquanto

o Amazon S3 estiver sendo otimizado internamente para a nova taxa de solicitação, você pode receber respostas de solicitação HTTP 503 temporariamente até que a otimização seja concluída. Esse comportamento pode ocorrer com aumentos nas taxas de solicitação por segundo ou quando você habilita o S3 RTC pela primeira vez. Durante esses períodos, sua latência de replicação pode aumentar. O acordo de nível de serviço (SLA) do S3 RTC não se aplica a períodos em que as diretrizes de performance do Amazon S3 em solicitações por segundo são excedidas.

O SLA do S3 RTC também não se aplica durante períodos em que a taxa de transferência de dados de replicação excede a cota padrão de 1 gigabit por segundo (Gbps). Se você espera que a taxa de transferência de replicação exceda 1 Gbps, entre em contato com o AWS Support Center ou use o Service Quotas para solicitar um aumento na cota da taxa de transferência de replicação.

Estimar as taxas de solicitação de replicação

A taxa total de solicitações, incluindo as solicitações que a replicação do Amazon S3 faz em seu nome, deve estar dentro das diretrizes de taxa de solicitação do Amazon S3 para os buckets de origem e destino da replicação. Para cada objeto replicado, a replicação do Amazon S3 faz até cinco solicitações `GET/HEAD` e uma solicitação `PUT` para o bucket de origem e uma solicitação `PUT` para cada bucket de destino.

Por exemplo, se você espera replicar 100 objetos por segundo, a replicação do Amazon S3 pode executar mais 100 solicitações `PUT` em seu nome para um total de 200 solicitações `PUT` por segundo para o bucket do S3 de origem. A replicação do Amazon S3 também pode executar até 500 solicitações `GET/HEAD` (5 solicitações `GET/HEAD` para cada objeto replicado).

> **Note**
>
> Você receberá a cobrança por apenas uma solicitação `PUT` por objeto replicado. Consulte mais informações sobre o preço nas Perguntas frequentes sobre replicação do Amazon S3.

Exceder as cotas da taxa de transferência de dados do S3 RTC

Se você espera que a taxa de transferência de dados do S3 RTC exceda a cota padrão de 1 Gbps, entre em contato com o AWS Support Center ou use o Service Quotas para solicitar um aumento na cota da taxa de transferência de replicação.

Taxas de solicitação de replicação de objetos criptografados do AWS KMS

Quando você replica objetos criptografados com a criptografia do lado do servidor com chaves do AWS Key Management Service (AWS KMS) (SSE-KMS), cotas de solicitação por segundo do AWS KMS são aplicadas. O AWS KMS pode rejeitar uma solicitação válida, pois a taxa de solicitação excede a cota do número de solicitações por segundo. Quando uma solicitação é rejeitada, o AWS KMS retorna um erro `ThrottlingException`. A cota da taxa de solicitação do AWS KMS se aplica a solicitações feitas diretamente e a solicitações feitas pela replicação do Amazon S3 em seu nome.

Por exemplo, se espera replicar 1.000 objetos por segundo, você poderá subtrair 2.000 solicitações da cota de taxa de solicitações do AWS KMS. A taxa de solicitação resultante por segundo está disponível para as workloads do AWS KMS excluindo a replicação. Você pode usar métricas de solicitação do AWS KMS no Amazon CloudWatch para monitorar a taxa total de solicitações do AWS KMS em sua Conta da AWS.

Para solicitar um aumento em sua cota de solicitações por segundo do AWS KMS, entre em contato com o AWS Support Center ou use o Service Quotas.

Habilitar o Controle do tempo de replicação do S3

Você pode começar a usar o Controle do tempo de replicação do S3 (S3 RTC) com uma regra de replicação nova ou existente. Você pode optar por aplicar a regra de replicação a um bucket inteiro ou a objetos com um prefixo ou uma tag específica. Quando você habilita o S3 RTC, as métricas de Replicação do S3 também são habilitadas na regra de replicação.

É possível configurar o S3 RTC usando o console do Amazon S3, a API do Amazon S3, os SDKs da AWS e a AWS Command Line Interface (AWS CLI).

Uso do console do S3

Para obter instruções detalhadas, consulte Configurar a replicação para buckets na mesma conta. Este tópico traz instruções para ativar as métricas de replicação do S3 em sua configuração da replicação quando os buckets de origem e destino pertencerem às mesmas Contas da AWS ou a outras.

Como usar o AWS CLI

Para usar a AWS CLI para replicar objetos com o S3 RTC habilitado, crie buckets, habilite o versionamento nos buckets, crie uma função do IAM que conceda permissão ao Amazon S3 para

replicar objetos e adicione a configuração da replicação ao bucket de origem. A configuração de replicação deve ter o S3 RTC habilitado, conforme mostrado no exemplo a seguir.

Consulte instruções passo a passo para definir a configuração da replicação usando a AWS CLI em Configurar a replicação para buckets na mesma conta.

O exemplo de configuração de replicação a seguir habilita e define os valores de `ReplicationTime` e `EventThreshold` para uma regra de replicação. Habilitar e definir esses valores habilita o S3 RTC na regra.

```
{
    "Rules": [
        {
            "Status": "Enabled",
            "Filter": {
                "Prefix": "Tax"
            },
            "DeleteMarkerReplication": {
                "Status": "Disabled"
            },
            "Destination": {
                "Bucket": "arn:aws:s3:::amzn-s3-demo-destination-bucket",
                "Metrics": {
                    "Status": "Enabled",
                    "EventThreshold": {
                        "Minutes": 15
                    }
                },
                "ReplicationTime": {
                    "Status": "Enabled",
                    "Time": {
                        "Minutes": 15
                    }
                }
            },
            "Priority": 1
        }
    ],
    "Role": "IAM-Role-ARN"
}
```

> **Important**
>
> `Metrics:EventThreshold:Minutes` e `ReplicationTime:Time:Minutes` só podem ter `15` como um valor válido.

Usar o AWS SDK para Java

O exemplo de Java a seguir adiciona a configuração da replicação com o Controle de Tempo de Replicação do S3 (S3 RTC) habilitado.

```
import software.amazon.awssdk.auth.credentials.AwsBasicCredentials;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3.model.DeleteMarkerReplication;
import software.amazon.awssdk.services.s3.model.Destination;
import software.amazon.awssdk.services.s3.model.Metrics;
import software.amazon.awssdk.services.s3.model.MetricsStatus;
import software.amazon.awssdk.services.s3.model.PutBucketReplicationRequest;
import software.amazon.awssdk.services.s3.model.ReplicationConfiguration;
import software.amazon.awssdk.services.s3.model.ReplicationRule;
import software.amazon.awssdk.services.s3.model.ReplicationRuleFilter;
import software.amazon.awssdk.services.s3.model.ReplicationTime;
import software.amazon.awssdk.services.s3.model.ReplicationTimeStatus;
import software.amazon.awssdk.services.s3.model.ReplicationTimeValue;

public class Main {

  public static void main(String[] args) {
    S3Client s3 = S3Client.builder()
      .region(Region.US_EAST_1)
      .credentialsProvider(() -> AwsBasicCredentials.create(
          "AWS_ACCESS_KEY_ID",
          "AWS_SECRET_ACCESS_KEY")
      )
      .build();

    ReplicationConfiguration replicationConfig = ReplicationConfiguration
      .builder()
      .rules(
          ReplicationRule
            .builder()
            .status("Enabled")
```

```
            .priority(1)
            .deleteMarkerReplication(
                DeleteMarkerReplication
                    .builder()
                    .status("Disabled")
                    .build()
            )
            .destination(
                Destination
                    .builder()
                    .bucket("destination_bucket_arn")
                    .replicationTime(
                        ReplicationTime.builder().time(
                            ReplicationTimeValue.builder().minutes(15).build()
                        ).status(
                            ReplicationTimeStatus.ENABLED
                        ).build()
                    )
                    .metrics(
                        Metrics.builder().eventThreshold(
                            ReplicationTimeValue.builder().minutes(15).build()
                        ).status(
                            MetricsStatus.ENABLED
                        ).build()
                    )
                    .build()
            )
            .filter(
                ReplicationRuleFilter
                    .builder()
                    .prefix("testtest")
                    .build()
            )
        .build())
        .role("role_arn")
        .build();

    // Put replication configuration
    PutBucketReplicationRequest putBucketReplicationRequest =
PutBucketReplicationRequest
      .builder()
      .bucket("source_bucket")
      .replicationConfiguration(replicationConfig)
      .build();
```

```
    s3.putBucketReplication(putBucketReplicationRequest);
  }
}
```

Replicar objetos criptografados (SSE-S3, SSE-KMS, DSSE-KMS, SSE-C)

> **Important**
>
> O Amazon S3 agora aplica criptografia do lado do servidor com chaves gerenciadas do Amazon S3 (SSE-S3) como nível básico de criptografia para cada bucket no Amazon S3. Desde 5 de janeiro de 2023, todos os novos uploads de objetos para o Amazon S3 são automaticamente criptografados sem custo adicional e sem impacto na performance. O status de criptografia automática para a configuração de criptografia padrão do bucket do S3 e para novos uploads de objetos está disponível em logs do AWS CloudTrail, no Inventário do S3, na Lente de Armazenamento do S3, no console do Amazon S3 e como cabeçalho adicional de resposta da API do Amazon S3 na AWS Command Line Interface e em AWS SDKs. Para obter mais informações, consulte Perguntas frequentes sobre criptografia padrão.

Há algumas considerações especiais quando você está replicando objetos que foram criptografados usando criptografia do lado do servidor. O Amazon S3 agora é compatível com seguintes tipos de criptografia do lado do servidor:

- Criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3)
- Criptografia no lado do servidor com chaves do AWS Key Management Service (AWS KMS) (SSE-KMS)
- Criptografia de camada dupla do lado do servidor com chaves do AWS KMS (DSSE-KMS)
- Criptografia do lado do servidor com chaves fornecidas pelo cliente (SSE-C)

Para obter mais informações sobre criptografia no lado do servidor, consulte the section called “Criptografia do lado do servidor”.

Este tópico explica as permissões necessárias para direcionar o Amazon S3 a replicar objetos que foram criptografados usando a criptografia do lado do servidor. Este tópico também fornece elementos de configuração adicionais aos quais você pode adicionar e dar exemplos de políticas

do AWS Identity and Access Management (IAM) que concedem as permissões necessárias para replicar objetos criptografados.

Para obter um exemplo com instruções passo a passo, consulte Habilitar a replicação para objetos criptografados. Para obter informações sobre como criar uma configuração da replicação, consulte Replicar objetos dentro de uma região e entre regiões.

> **Note**
>
> Você pode usar uma AWS KMS keys de várias regiões no Amazon S3. No entanto, o Amazon S3 trata no momento as chaves de várias regiões como se fossem chaves de região única e não usa os recursos de várias regiões da chave. Consulte mais informações em Using multi-Region keys no Guia do desenvolvedor do AWS Key Management Service.

Tópicos

- Como a criptografia de bucket padrão afeta a replicação
- Replicar objetos criptografados com SSE-C
- Replicar objetos criptografados com SSE-S3, SSE-KMS ou DSSE-KMS
- Habilitar a replicação para objetos criptografados

Como a criptografia de bucket padrão afeta a replicação

Ao habilitar a criptografia padrão para um bucket de destino de replicação, o seguinte comportamento de criptografia será aplicado:

- Se os objetos no bucket de origem não estiverem criptografados, os objetos de réplica no bucket de destino serão criptografados usando as configurações de criptografia padrão do bucket de destino. Como resultado, as tags de entidade (ETags) dos objetos de origem diferem dos ETags dos objetos de réplica. Se você tiver aplicações que usam ETags, será necessário atualizar essas aplicações para considerar essa diferença.
- Se os objetos no bucket de origem forem criptografados usando a criptografia do lado do servidor com chaves gerenciadas do Amazon S3 (SSE-S3), a criptografia do lado do servidor com chaves do AWS Key Management Service (AWS KMS) (SSE-KMS) ou a criptografia de camada dupla do lado do servidor com chaves do AWS KMS (DSSE-KMS), os objetos de réplica no bucket de destino usarão o mesmo tipo de criptografia que os objetos de origem. As configurações de criptografia padrão do bucket de destino não são usadas.

Replicar objetos criptografados com SSE-C

Ao usar a criptografia do lado do servidor com chaves fornecidas pelo cliente (SSE-C), é possível gerenciar suas próprias chaves de criptografia proprietárias. Com o SSE-C, você gerencia as chaves enquanto o Amazon S3 gerencia o processo de criptografia e descriptografia. Você deve fornecer uma chave de criptografia como parte de sua solicitação, mas não precisa escrever nenhum código para realizar a criptografia ou descriptografia de objetos. Quando você faz upload de um objeto, o Amazon S3 criptografa o objeto usando a chave que você forneceu. Depois, o Amazon S3 remove essa chave da memória. Quando você recupera um objeto, deve fornecer a mesma chave de criptografia como parte de sua solicitação. Para obter mais informações, consulte the section called “Chaves de criptografia fornecidas pelo cliente (SSE-C)”.

A Replicação do S3 é compatível com objetos criptografados com SSE-C. É possível configurar a replicação de objetos com SSE-C no console do Amazon S3 ou com os SDKs da AWS, da mesma forma que você configura a replicação para objetos não criptografados. Não há permissões de SSE-C adicionais além das atualmente necessárias para replicação.

A Replicação do S3 replica automaticamente objetos criptografados com SSE-C recém-carregados, se eles forem elegíveis, de acordo com sua configuração de Replicação do S3. Para replicar objetos existentes nos buckets, use a replicação em lote do S3. Para obter mais informações sobre replicação de objetos, consulte the section called “Configurar a replicação em tempo real” e the section called “Replicar objetos existentes”.

Não há cobranças adicionais pela replicação de objetos SSE-C. Consulte detalhes sobre os preços de replicação em Preço do Amazon S3.

Replicar objetos criptografados com SSE-S3, SSE-KMS ou DSSE-KMS

Por padrão, o Amazon S3 não replica objetos criptografados com SSE-KMS ou DSSE-KMS. Esta seção explica outros elementos de configuração que você pode adicionar para orientar o Amazon S3 a replicar esses objetos.

Para obter um exemplo com instruções passo a passo, consulte Habilitar a replicação para objetos criptografados. Para obter informações sobre como criar uma configuração da replicação, consulte Replicar objetos dentro de uma região e entre regiões.

Especificar informações adicionais na configuração de replicação

Na configuração de replicação, você faz o seguinte:

- No elemento `Destination` na configuração de replicação, adicione o ID da chave do AWS KMS simétrica gerenciada pelo cliente que você deseja que o Amazon S3 use para criptografar réplicas de objetos, conforme mostrado no exemplo de configuração de replicação a seguir.
- Aceite explicitamente ao habilitar a replicação de objetos criptografados por meio das chaves do KMS (SSE-KMS ou DSSE-KMS). Para ativar, adicione o elemento `SourceSelectionCriteria`, conforme mostrado no exemplo de configuração de replicação a seguir.

```
<ReplicationConfiguration>
   <Rule>
      ...
      <SourceSelectionCriteria>
         <SseKmsEncryptedObjects>
           <Status>Enabled</Status>
         </SseKmsEncryptedObjects>
      </SourceSelectionCriteria>

      <Destination>
          ...
          <EncryptionConfiguration>
             <ReplicaKmsKeyID>AWS KMS key ARN or Key Alias ARN that's in the same
 Região da AWS as the destination bucket.</ReplicaKmsKeyID>
          </EncryptionConfiguration>
       </Destination>
      ...
   </Rule>
</ReplicationConfiguration>
```

> **Important**
>
> - A chave do KMS deve ter sido criada na mesma Região da AWS que o bucket de destino.
> - A chave do KMS deve ser válida. A operação de API `PutBucketReplication` não verifica a validade de chaves do KMS. Se você usar uma chave do KMS inválida, receberá o código de status HTTP `200 OK` como resposta, mas a replicação falhará.

O exemplo a seguir mostra uma configuração de replicação, que inclui elementos de configuração opcionais. Essa configuração de replicação tem uma regra. Esta regra aplica-se aos objetos com

o prefixo de chaves *Tax*. O Amazon S3 usa o ID da AWS KMS key especificado para criptografar essas réplicas de objeto.

```
<?xml version="1.0" encoding="UTF-8"?>
<ReplicationConfiguration>
   <Role>arn:aws:iam::account-id:role/role-name</Role>
   <Rule>
      <ID>Rule-1</ID>
      <Priority>1</Priority>
      <Status>Enabled</Status>
      <DeleteMarkerReplication>
         <Status>Disabled</Status>
      </DeleteMarkerReplication>
      <Filter>
         <Prefix>Tax</Prefix>
      </Filter>
      <Destination>
         <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
         <EncryptionConfiguration>
            <ReplicaKmsKeyID>AWS KMS key ARN or Key Alias ARN that's in the same Região
 da AWS as the destination bucket.</ReplicaKmsKeyID>
         </EncryptionConfiguration>
      </Destination>
      <SourceSelectionCriteria>
         <SseKmsEncryptedObjects>
            <Status>Enabled</Status>
         </SseKmsEncryptedObjects>
      </SourceSelectionCriteria>
   </Rule>
</ReplicationConfiguration>
```

Conceder permissões adicionais para a função do IAM

Para replicar objetos criptografados em repouso usando SSE-S3, SSE-KMS ou DSSE-KMS, conceda as permissões adicionais a seguir ao perfil do AWS Identity and Access Management (IAM) especificado na configuração da replicação. Você concede essas permissões ao atualizar a política de permissões associada ao perfil do IAM.

- Ação **`s3:GetObjectVersionForReplication`** para objetos de origem: essa ação permite que o Amazon S3 replique objetos não criptografados e objetos criados com criptografia do lado do servidor usando SSE-S3, SSE-KMS ou DSSE-KMS.

> **Note**
>
> Recomendamos que você use a ação `s3:GetObjectVersionForReplication` em vez da ação `s3:GetObjectVersion`, porque `s3:GetObjectVersionForReplication` fornece ao Amazon S3 somente as permissões mínimas necessárias para a replicação. Além disso, a ação `s3:GetObjectVersion` permite a replicação de objetos não criptografados e objetos criptografados com SSE-S3, mas não objetos criptografados usando chaves do KMS (SSE-KMS ou DSSE-KMS).

- Ações **`kms:Decrypt`** e **`kms:Encrypt`** AWS KMS para as chaves do KMS
  - Você deve conceder permissões `kms:Decrypt` para a AWS KMS key que é usada para descriptografar o objeto de origem.
  - Você deve conceder permissões `kms:Encrypt` para a AWS KMS key que é usada para criptografar a réplica do objeto.
- A ação **`kms:GenerateDataKey`** para replicar objetos de texto sem formatação: se você estiver replicando objetos de texto sem formatação em um bucket com a criptografia SSE-KMS ou DSSE-KMS habilitada por padrão, é necessário incluir a permissão `kms:GenerateDataKey` para o contexto de criptografia de destino e a chave do KMS na política do IAM.

Recomendamos que você restrinja essas permissões apenas aos buckets e objetos de destino usando chaves de condição do AWS KMS. A Conta da AWS proprietária do perfil do IAM precisa ter permissões para as ações `kms:Encrypt` e `kms:Decrypt` para as chaves do KMS listadas na política. Se as chaves do KMS pertencerem a outra Conta da AWS, o proprietário da chave do KMS precisará conceder essas permissões à Conta da AWS proprietária do perfil do IAM. Consulte mais informações sobre como gerenciar o acesso a essas chaves do KMS em Using IAM policies with AWS KMS no Guia do desenvolvedor do AWS Key Management Service.

Chaves de bucket do S3 e replicação

Para usar a replicação com uma chave de bucket do S3, a política AWS KMS key para a chave do KMS usada para criptografar a réplica do objeto deve incluir a permissão `kms:Decrypt` para a entidade principal da chamada. A chamada para `kms:Decrypt` verifica a integridade da chave do bucket do S3 antes de usá-la. Para obter mais informações, consulte Uso de uma chave de bucket do S3 com replicação.

Quando uma chave de bucket do S3 estiver habilitada para o bucket de origem ou de destino, o contexto de criptografia será o nome do recurso da Amazon (ARN) do bucket e não o ARN do objeto (por exemplo, `arn:aws:s3:::bucket_ARN`). Você precisa atualizar suas políticas do IAM para usar o ARN do bucket para o contexto de criptografia:

```
"kms:EncryptionContext:aws:s3:arn": [
"arn:aws:s3:::bucket_ARN"
]
```

Para obter mais informações, consulte Contexto de criptografia (`x-amz-server-side-encryption-context`) (na seção “Usar a API REST”) e Alterações na observação antes de habilitar uma chave de bucket do S3.

Exemplo de políticas: usar SSE-S3 e SSE-KMS com replicação

Os exemplos de políticas do IAM a seguir mostram instruções para o uso de SSE-S3 e SSE-KMS com replicação.

Example – Usar SSE-KMS com buckets de destino separados

A política de exemplo a seguir mostra instruções para usar SSE-KMS com buckets de destino separados.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Action": ["kms:Decrypt"],
         "Effect": "Allow",
         "Condition": {
             "StringLike": {
                  "kms:ViaService": "s3.source-bucket-region.amazonaws.com",
                  "kms:EncryptionContext:aws:s3:arn": [
                      "arn:aws:s3:::amzn-s3-demo-source-bucket/key-prefix1*"
                  ]
             }
          },
          "Resource": [
             "List of AWS KMS key ARNs that are used to encrypt source objects."
          ]
      },
      {
```

```
         "Action": ["kms:Encrypt"],
         "Effect": "Allow",
         "Condition": {
            "StringLike": {
               "kms:ViaService": "s3.destination-bucket-1-region.amazonaws.com",
               "kms:EncryptionContext:aws:s3:arn": [
                  "arn:aws:s3:::amzn-s3-demo-destination-bucket1/key-prefix1*"
               ]
         }
         },
         "Resource": [
            "AWS KMS key ARNs (in the same Região da AWS as destination bucket 1). Used
 to encrypt object replicas created in destination bucket 1."
         ]
      },
      {
         "Action": ["kms:Encrypt"],
         "Effect": "Allow",
         "Condition": {
            "StringLike": {
               "kms:ViaService": "s3.destination-bucket-2-region.amazonaws.com",
               "kms:EncryptionContext:aws:s3:arn": [
                  "arn:aws:s3:::amzn-s3-demo-destination-bucket2/key-prefix1*"
               ]
         }
         },
         "Resource": [
            "AWS KMS key ARNs (in the same Região da AWS as destination bucket 2). Used
 to encrypt object replicas created in destination bucket 2."
         ]
      }
   ]
}
```

Example – Replicar objetos criados com SSE-S3 e SSE-KMS

Veja a seguir uma política completa do IAM que concede as permissões necessárias para replicar objetos não criptografados, objetos criados com SSE-3 e objetos criados com SSE-KMS.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
```

```
        "Effect":"Allow",
        "Action":[
           "s3:GetReplicationConfiguration",
           "s3:ListBucket"
        ],
        "Resource":[
           "arn:aws:s3:::amzn-s3-demo-source-bucket"
        ]
     },
     {
        "Effect":"Allow",
        "Action":[
           "s3:GetObjectVersionForReplication",
           "s3:GetObjectVersionAcl"
        ],
        "Resource":[
           "arn:aws:s3:::amzn-s3-demo-source-bucket/key-prefix1*"
        ]
     },
     {
        "Effect":"Allow",
        "Action":[
           "s3:ReplicateObject",
           "s3:ReplicateDelete"
        ],
        "Resource":"arn:aws:s3:::amzn-s3-demo-destination-bucket/key-prefix1*"
     },
     {
        "Action":[
           "kms:Decrypt"
        ],
        "Effect":"Allow",
        "Condition":{
           "StringLike":{
              "kms:ViaService":"s3.source-bucket-region.amazonaws.com",
              "kms:EncryptionContext:aws:s3:arn":[
                 "arn:aws:s3:::amzn-s3-demo-source-bucket/key-prefix1*"
              ]
           }
        },
        "Resource":[
          "List of the AWS KMS key ARNs that are used to encrypt source objects."
        ]
     },
```

```
      {
         "Action":[
            "kms:Encrypt"
         ],
         "Effect":"Allow",
         "Condition":{
            "StringLike":{
               "kms:ViaService":"s3.destination-bucket-region.amazonaws.com",
               "kms:EncryptionContext:aws:s3:arn":[
                  "arn:aws:s3:::amzn-s3-demo-destination-bucket/prefix1*"
               ]
            }
         },
         "Resource":[
            "AWS KMS key ARNs (in the same Região da AWS as the destination bucket) to
 use for encrypting object replicas"
         ]
      }
   ]
}
```

Example – Replicar objetos com chaves de bucket do S3

Veja a seguir uma política completa do IAM que concede as permissões necessárias para replicar objetos com chaves de bucket do S3.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "s3:GetReplicationConfiguration",
            "s3:ListBucket"
         ],
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-source-bucket"
         ]
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3:GetObjectVersionForReplication",
```

```
            "s3:GetObjectVersionAcl"
         ],
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-source-bucket/key-prefix1*"
         ]
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3:ReplicateObject",
            "s3:ReplicateDelete"
         ],
         "Resource":"arn:aws:s3:::amzn-s3-demo-destination-bucket/key-prefix1*"
      },
      {
         "Action":[
            "kms:Decrypt"
         ],
         "Effect":"Allow",
         "Condition":{
            "StringLike":{
               "kms:ViaService":"s3.source-bucket-region.amazonaws.com",
               "kms:EncryptionContext:aws:s3:arn":[
                  "arn:aws:s3:::amzn-s3-demo-source-bucket"
               ]
            }
         },
         "Resource":[
           "List of the AWS KMS key ARNs that are used to encrypt source objects."
         ]
      },
      {
         "Action":[
            "kms:Encrypt"
         ],
         "Effect":"Allow",
         "Condition":{
            "StringLike":{
               "kms:ViaService":"s3.destination-bucket-region.amazonaws.com",
               "kms:EncryptionContext:aws:s3:arn":[
                  "arn:aws:s3:::amzn-s3-demo-destination-bucket"
               ]
            }
         },
```

```
        "Resource":[
           "AWS KMS key ARNs (in the same Região da AWS as the destination bucket) to
 use for encrypting object replicas"
        ]
      }
   ]
}
```

Conceder permissões adicionais para cenários entre contas

Em um cenário entre contas, no qual os buckets de origem e destino pertencem a diferentes Contas da AWS, é possível usar uma chave do KMS para criptografar réplicas de objetos. No entanto, o proprietário da chave do KMS deve conceder ao proprietário do bucket de origem permissão para usar a chave do KMS.

> **Note**
>
> Se você precisar replicar dados da SSE-KMS entre contas, a regra de replicação deverá especificar uma chave gerenciada pelo cliente do AWS KMS para a conta de destino. As Chaves gerenciadas pela AWS não permitem o uso entre contas e, portanto, não podem ser usadas para realizar a replicação entre contas.

Como conceder ao proprietário do bucket de origem permissão para usar a chave do KMS (console do AWS KMS)

1. Faça login no AWS Management Console e abra o console do AWS KMS em https://console.aws.amazon.com/kms.
2. Para alterar a Região da AWS, use o Region selector (Seletor de regiões) no canto superior direito da página.
3. Para exibir as chaves em sua conta que você cria e gerencia, no painel de navegação, escolha Customer managed keys (Chaves gerenciadas de cliente).
4. Selecione a chave do KMS.
5. Na seção Configuração geral, selecione a guia Política de chaves.
6. Role para baixo até Outras Contas da AWS.
7. Selecione Adicionar outras Contas da AWS.

   A caixa de diálogo Outras Contas da AWS é exibida.

8. Na caixa de diálogo, escolha Adicionar outra Conta da AWS. Para arn:aws:iam::, insira o ID da conta do bucket de origem.
9. Escolha Salvar alterações.

Para conceder ao proprietário do bucket de origem permissão para usar a chave do KMS (AWS CLI).

- Para obter informações sobre o comando `put-key-policy` da AWS Command Line Interface (AWS CLI), consulte put-key-policy na Referência de comandos da AWS CLI. Para obter informações sobre a operação de API subjacente `PutKeyPolicy`, consulte PutKeyPolicy na Referência de API do AWS Key Management Service.

Considerações sobre cotas de transação do AWS KMS

Ao adicionar muitos novos objetos com a criptografia do AWS KMS depois de habilitar replicação entre regiões (CRR), pode ocorrer controle de utilização (erros de respostas HTTP `503 Service Unavailable`). O controle de utilização acontece quando o número de transações do AWS KMS por segundo excede a cota atual. Para obter mais informações, consulte Cotas do no Guia do desenvolvedor do AWS Key Management Service.

Para solicitar um aumento de cota, use Service Quotas. Consulte Requesting a quota increase (Como solicitar um aumento de cota) para obter mais informações. Se não houver compatibilidade de Service Quotas com sua região, abra um caso do AWS Support.

Habilitar a replicação para objetos criptografados

Por padrão, o Amazon S3 não replica objetos criptografados por meio da criptografia do lado do servidor com chaves do AWS Key Management Service (AWS KMS) (SSE-KMS) ou da criptografia de camada dupla do lado do servidor com chaves do AWS KMS (DSSE-KMS). Para replicar objetos criptografados com SSE-KMS ou DSS-KMS, você deve modificar a configuração da replicação do bucket para instruir o Amazon S3 a replicar esses objetos. Este exemplo explica como usar o console do Amazon S3 e a AWS Command Line Interface (AWS CLI) para alterar a configuração de replicação do bucket de maneira que a replicação de objetos criptografados seja habilitada.

> **Note**
>
> Quando uma chave de bucket do S3 estiver habilitada para o bucket de origem ou de destino, o contexto de criptografia será o nome do recurso da Amazon (ARN) do bucket e não o ARN do objeto. Você precisa atualizar suas políticas do IAM a fim de usar o ARN do

bucket para o contexto de criptografia. Para obter mais informações, consulte Chaves de bucket do S3 e replicação.

> **Note**
>
> Você pode usar uma AWS KMS keys de várias regiões no Amazon S3. No entanto, o Amazon S3 trata no momento as chaves de várias regiões como se fossem chaves de região única e não usa os recursos de várias regiões da chave. Consulte mais informações em Using multi-Region keys no Guia do desenvolvedor do AWS Key Management Service.

Uso do console do S3

Para obter instruções detalhadas, consulte Configurar a replicação para buckets na mesma conta. Este tópico fornece instruções para definir a configuração da replicação quando os buckets de origem e de destino pertencem às mesmas Contas da AWS ou a contas diferentes.

Como usar o AWS CLI

Para replicar objetos criptografados com a AWS CLI, faça o seguinte:

- Crie os buckets de origem e destino e habilite o versionamento neles.
- Crie um perfil de serviço do AWS Identity and Access Management (IAM) que dê ao Amazon S3 permissão para replicar objetos. As permissões do perfil do IAM incluem aquelas necessárias para replicar objetos criptografados.
- Adicione uma configuração de replicação ao bucket de origem. A configuração de replicação fornece informações relacionadas à replicação de objetos que são criptografados por meio das chaves do KMS.
- Adicione objetos criptografados ao bucket de origem.
- Teste a configuração para confirmar se os objetos criptografados estão sendo replicados no bucket de destino.

Os procedimentos a seguir demonstram esse processo.

Para replicar objetos criptografados no lado do servidor (AWS CLI)

Para usar os exemplos neste procedimento, substitua *user input placeholders* por suas informações.

1. Neste exemplo, você cria tanto o bucket de origem (*amzn-s3-demo-source-bucket*) como o de destino (*amzn-s3-demo-destination-bucket*) na mesma Conta da AWS. Defina também um perfil de credenciais para a AWS CLI. Este exemplo usa o nome de perfil *acctA*.

   Consulte mais informações sobre como configurar perfis de credenciais e como usar perfis nomeados em Configuration and credential file settings no Guia do usuário da AWS Command Line Interface.

2. Use os comandos a seguir para criar o bucket *amzn-s3-demo-source-bucket* e habilitar o versionamento nele. O comando *amzn-s3-demo-source-bucket* a seguir cria um bucket na região Leste dos EUA (Norte da Virgínia) (`us-east-1`).

   ```
   aws s3api create-bucket \
   --bucket amzn-s3-demo-source-bucket \
   --region us-east-1 \
   --profile acctA
   ```

   ```
   aws s3api put-bucket-versioning \
   --bucket amzn-s3-demo-source-bucket \
   --versioning-configuration Status=Enabled \
   --profile acctA
   ```

3. Use os comandos a seguir para criar o bucket *amzn-s3-demo-destination-bucket* e habilitar o versionamento nele. Os comandos de exemplo a seguir criam o bucket *amzn-s3-demo-destination-bucket* na região Oeste dos EUA (Oregon) (`us-west-2`).

   > **Note**
   >
   > Para configurar a replicação quando os buckets *amzn-s3-demo-source-bucket* e *amzn-s3-demo-destination-bucket* estiverem na mesma Conta da AWS, use o mesmo perfil. Este exemplo usa *acctA*. Para configurar a replicação quando os buckets pertencerem a Contas da AWS distintas, especifique diferentes perfis para cada um.

```
aws s3api create-bucket \
--bucket amzn-s3-demo-destination-bucket \
--region us-west-2 \
--create-bucket-configuration LocationConstraint=us-west-2 \
--profile acctA
```

```
aws s3api put-bucket-versioning \
--bucket amzn-s3-demo-destination-bucket \
--versioning-configuration Status=Enabled \
--profile acctA
```

4. Em seguida, crie um perfil de serviço do IAM. Você especifica esse perfil na configuração da replicação que adiciona ao bucket *amzn-s3-demo-source-bucket* posteriormente. O Amazon S3 assume essa função para replicar objetos em seu nome. A função do IAM é criada em duas etapas:

   - Crie uma função de serviço.
   - Anexar uma política de permissões à função.

   a. Para criar um perfil de serviço do IAM, faça o seguinte:

      i. Copie a política de confiança a seguir e salve-a em um arquivo com o nome *s3-role-trust-policy-kmsobj*`.json` no diretório atual do seu computador local. Essa política concede à entidade principal do serviço Amazon S3 as permissões para assumir o perfil a fim de que o Amazon S3 possa executar tarefas em seu nome.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service":"s3.amazonaws.com"
         },
         "Action":"sts:AssumeRole"
      }
   ]
}
```

ii. Use o comando a seguir para criar o perfil.

```
$ aws iam create-role \
--role-name replicationRolekmsobj \
--assume-role-policy-document file://s3-role-trust-policy-kmsobj.json  \
--profile acctA
```

b. Em seguida, anexe uma política de permissões ao perfil. Essa política concede permissões para várias ações de bucket e objetos do Amazon S3.

i. Copie a política de permissões a seguir e salve-a em um arquivo com o nome *s3-role-permissions-policykmsobj*`.json` no diretório atual do computador local. Crie um perfil do IAM e, posteriormente, anexe a política a ele.

> **Important**
>
> Na política de permissões, especifique os IDs de chave do AWS KMS que serão usados para criptografar os buckets *amzn-s3-demo-source-bucket* e *amzn-s3-demo-destination-bucket*. É necessário criar duas chaves separadas do KMS para os buckets *amzn-s3-demo-source-bucket* e *amzn-s3-demo-destination-bucket*. As AWS KMS keys nunca são compartilhadas fora da Região da AWS em que foram criadas.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Action":[
            "s3:ListBucket",
            "s3:GetReplicationConfiguration",
            "s3:GetObjectVersionForReplication",
            "s3:GetObjectVersionAcl",
            "s3:GetObjectVersionTagging"
         ],
         "Effect":"Allow",
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-source-bucket",
            "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
         ]
```

```
      },
      {
         "Action":[
            "s3:ReplicateObject",
            "s3:ReplicateDelete",
            "s3:ReplicateTags"
         ],
         "Effect":"Allow",
         "Condition":{
            "StringLikeIfExists":{
               "s3:x-amz-server-side-encryption":[
                  "aws:kms",
                  "AES256",
                  "aws:kms:dsse"
               ],
               "s3:x-amz-server-side-encryption-aws-kms-key-id":[
                  "AWS KMS key IDs(in ARN format) to use for encrypting
object replicas"
               ]
            }
         },
         "Resource":"arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
      },
      {
         "Action":[
            "kms:Decrypt"
         ],
         "Effect":"Allow",
         "Condition":{
            "StringLike":{
               "kms:ViaService":"s3.us-east-1.amazonaws.com",
               "kms:EncryptionContext:aws:s3:arn":[
                  "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
               ]
            }
         },
         "Resource":[
            "AWS KMS key IDs(in ARN format) used to encrypt source
objects."
         ]
      },
      {
         "Action":[
            "kms:Encrypt"
```

```
         ],
         "Effect":"Allow",
         "Condition":{
            "StringLike":{
               "kms:ViaService":"s3.us-west-2.amazonaws.com",
               "kms:EncryptionContext:aws:s3:arn":[
                  "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
               ]
            }
         },
         "Resource":[
            "AWS KMS key IDs (in ARN format) to use for encrypting object
 replicas"
         ]
      }
   ]
}
```

ii. Crie uma política e anexe-a à função.

```
$ aws iam put-role-policy \
--role-name replicationRolekmsobj \
--policy-document file://s3-role-permissions-policykmsobj.json \
--policy-name replicationRolechangeownerPolicy \
--profile acctA
```

5. Depois, adicione a configuração de replicação a seguir ao bucket *amzn-s3-demo-source-bucket*. Isso instrui o Amazon S3 a replicar objetos com o prefixo *Tax/* no bucket *amzn-s3-demo-destination-bucket*.

> **Important**
>
> Na configuração da replicação, especifique o perfil do IAM que o Amazon S3 pode assumir. Você só poderá fazer isso se tiver a permissão `iam:PassRole`. O perfil especificado no comando da CLI deve ter essa permissão. Para ter mais informações, consulte Conceder permissões ao usuário para transmitir um perfil a um AWS service (Serviço da AWS) no Guia do usuário do IAM.

```
<ReplicationConfiguration>
 <Role>IAM-Role-ARN</Role>
```

```
  <Rule>
    <Priority>1</Priority>
    <DeleteMarkerReplication>
       <Status>Disabled</Status>
    </DeleteMarkerReplication>
    <Filter>
       <Prefix>Tax</Prefix>
    </Filter>
    <Status>Enabled</Status>
    <SourceSelectionCriteria>
      <SseKmsEncryptedObjects>
        <Status>Enabled</Status>
      </SseKmsEncryptedObjects>
    </SourceSelectionCriteria>
    <Destination>
      <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
      <EncryptionConfiguration>
        <ReplicaKmsKeyID>AWS KMS key IDs to use for encrypting object replicas</
ReplicaKmsKeyID>
      </EncryptionConfiguration>
    </Destination>
  </Rule>
</ReplicationConfiguration>
```

Para adicionar a configuração de replicação ao bucket *amzn-s3-demo-source-bucket*, faça o seguinte:

a. A AWS CLI requer que você especifique a configuração de replicação como JSON. Salve o JSON a seguir em um arquivo (*replication*.json) no diretório atual local do seu computador local.

```
{
   "Role":"IAM-Role-ARN",
   "Rules":[
      {
         "Status":"Enabled",
         "Priority":1,
         "DeleteMarkerReplication":{
            "Status":"Disabled"
         },
         "Filter":{
            "Prefix":"Tax"
```

```
         },
         "Destination":{
            "Bucket":"arn:aws:s3:::amzn-s3-demo-destination-bucket",
            "EncryptionConfiguration":{
               "ReplicaKmsKeyID":"AWS KMS key IDs (in ARN format) to use for
 encrypting object replicas"
            }
         },
         "SourceSelectionCriteria":{
            "SseKmsEncryptedObjects":{
               "Status":"Enabled"
            }
         }
      }
   ]
}
```

b. Edite o JSON para fornecer valores para o bucket *amzn-s3-demo-destination-bucket*, os *AWS KMS key IDs (in ARN format)* e o *IAM-role-ARN*. Salve as alterações.

c. Use o comando a seguir para adicionar a configuração de replicação ao bucket *amzn-s3-demo-source-bucket*. Não deixe fornece o nome do bucket de *amzn-s3-demo-source-bucket*.

```
$ aws s3api put-bucket-replication \
--replication-configuration file://replication.json \
--bucket amzn-s3-demo-source-bucket \
--profile acctA
```

6. Teste a configuração para verificar se os objetos criptografados estão replicados. No console do Amazon S3, faça o seguinte:

a. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.

b. No bucket de *amzn-s3-demo-source-bucket*, crie uma pasta denominada *Tax*.

c. Adicione objetos de amostra à pasta. Não se esqueça de escolher a opção de criptografia e especificar a chave do KMS para criptografar os objetos.

d. Verifique se o bucket *amzn-s3-demo-destination-bucket* contém as réplicas dos objetos e se elas são criptografadas usando a chave do KMS especificada na

configuração. Para obter mais informações, consulte the section called “Obtenção de status da replicação”.

Uso da SDKs AWS

Para obter um exemplo de código que mostra como adicionar uma configuração da replicação, consulte Uso dos SDKs da AWS. Você precisa modificar a configuração de replicação adequadamente.

Replicação de alterações de metadados com sincronização de modificação de réplica

A sincronização da modificação de réplica do Amazon S3 pode ajudar a manter metadados de objetos, como tags, listas de controle de acesso (ACLs) e configurações do Bloqueio de Objetos replicadas entre réplicas e objetos de origem. Por padrão, o Amazon S3 replica metadados dos objetos de origem somente para as réplicas. Quando a sincronização de modificação de réplica está habilitada, o Amazon S3 replica as alterações de metadados feitas nas cópias da réplica de volta ao objeto de origem, tornando a replicação bidirecional.

Ativação da sincronização de modificação da réplica

Você pode usar a sincronização de modificação de réplica do Amazon S3 com regras de replicação novas ou existentes. É possível aplicá-la a um bucket inteiro ou a objetos que tenham um prefixo específico.

Para habilitar a sincronização de modificação de réplica usando o console do Amazon S3, consulte Exemplos para configurar a replicação em tempo real. Este tópico fornece instruções para habilitar a sincronização da modificação de réplicas na configuração de replicação quando os buckets de origem e de destino pertencem às mesmas Contas da AWS ou a contas diferentes.

Para habilitar a sincronização da modificação de réplicas usando a AWS Command Line Interface (AWS CLI), você deve adicionar uma configuração de replicação ao bucket que contém as réplicas com `ReplicaModifications` habilitado. Para configurar a replicação bidirecional, crie uma regra de replicação do bucket de origem (*`amzn-s3-demo-source-bucket`*) para o bucket que contém as réplicas (*`amzn-s3-demo-destination-bucket`*). Depois, crie uma segunda regra de replicação do bucket que contém as réplicas (*`amzn-s3-demo-destination-bucket`*) para o bucket de origem (*`amzn-s3-demo-source-bucket`*). Os buckets de origem e de destino podem estar em Regiões da AWS diferentes ou na mesma região.

> **Note**
>
> Você deve habilitar a sincronização de modificação de réplica em ambos os buckets, de origem e de destino, para replicar alterações de metadados de réplica, como listas de controle de acesso (ACLs) de objetos, tags de objeto ou configurações de Bloqueio de Objetos nos objetos replicados. Como todas as regras de replicação, é possível aplicá-las a todo o bucket ou a um subconjunto de objetos filtrados por prefixo ou tags de objeto.

No exemplo de configuração a seguir, o Amazon S3 replica alterações de metadados sob o prefixo *Tax* para o bucket *amzn-s3-demo-source-bucket*, que conteria os objetos de origem.

```
{
    "Rules": [
        {
            "Status": "Enabled",
            "Filter": {
                "Prefix": "Tax"
            },
            "SourceSelectionCriteria": {
                "ReplicaModifications":{
                    "Status": "Enabled"
                }
            },
            "Destination": {
                "Bucket": "arn:aws:s3:::amzn-s3-demo-source-bucket"
            },
            "Priority": 1
        }
    ],
    "Role": "IAM-Role-ARN"
}
```

Consulte instruções completas sobre como criar regras de replicação usando a AWS CLI em Configurar a replicação para buckets na mesma conta.

Replicação de marcadores de exclusão entre intervalos

Por padrão, quando a replicação do S3 está habilitada e um objeto é excluído no bucket de origem, o Amazon S3 adiciona um marcador de exclusão somente no bucket de origem. Essa ação ajuda a proteger os dados nos buckets de destino contra exclusões acidentais ou mal-intencionadas. Se

você tiver a replicação de marcadores de exclusão habilitada, esses marcadores serão copiados para os buckets de destino e o Amazon S3 se comportará como se o objeto tivesse sido excluído nos buckets de origem e de destino. Para obter mais informações sobre como funcionam os marcadores de exclusão, consulte Trabalhar com marcadores de exclusão.

> **Note**
>
> - A replicação de marcadores de exclusão não é permitida para regras de replicação baseadas em tags. A replicação de marcadores de exclusão também não adere ao acordo de serviço (SLA) de 15 minutos concedido ao usar o Controle de Tempo de Replicação do S3 (S3 RTC).
> - Se você não estiver usando a versão XML da configuração de replicação mais recente, as operações de exclusão afetarão a replicação de forma diferente. Para obter mais informações, consulte Como a exclusão de operações afeta a replicação.
> - Se você habilitar a replicação do marcador de exclusão e o bucket de origem tiver uma regra de expiração do Ciclo de Vida do S3, os marcadores de exclusão adicionados por essa regra não serão replicados no bucket de destino.

Habilitando a replicação de marcadores de exclusão

Você pode começar a usar a replicação de marcadores de exclusão com uma regra de replicação nova ou existente. É possível aplicar a replicação do marcador de exclusão a um bucket inteiro ou a objetos que tenham um prefixo específico.

Para habilitar a replicação de marcadores de exclusão usando o console do Amazon S3, consulte Uso do console do S3. Este tópico fornece instruções para habilitar a replicação de marcadores de exclusão na configuração de replicação quando os buckets de origem e destino pertencem às mesmas Contas da AWS ou a contas diferentes.

Para habilitar a replicação de marcadores de exclusão usando a AWS Command Line Interface (AWS CLI), você deve adicionar uma configuração de replicação ao bucket de origem com `DeleteMarkerReplication` habilitado, conforme mostrado no exemplo de configuração a seguir.

No exemplo de configuração de replicação a seguir, os marcadores de exclusão são replicados para o bucket de destino *`amzn-s3-demo-destination-bucket`* para objetos sob o prefixo *`Tax`*.

```
{
```

```
    "Rules": [
        {
            "Status": "Enabled",
            "Filter": {
                "Prefix": "Tax"
            },
            "DeleteMarkerReplication": {
                "Status": "Enabled"
            },
            "Destination": {
                "Bucket": "arn:aws:s3:::amzn-s3-demo-destination-bucket"
            },
            "Priority": 1
        }
    ],
    "Role": "IAM-Role-ARN"
}
```

Consulte instruções completas sobre como criar regras de replicação por meio da AWS CLI em Configurar a replicação para buckets na mesma conta.

Gerenciar ou pausar a replicação em tempo real

A replicação em tempo real é a cópia assíncrona automática de objetos em buckets na mesma região da AWS ou em Regiões da AWS diferentes. Depois de definir a configuração da replicação, o Amazon S3 replica os objetos recém-criados e as atualizações de objeto de um bucket de origem para um ou mais buckets de destino.

Você usa o console do Amazon S3 para adicionar regras de replicação ao bucket de origem. As regras de replicação definem os objetos do bucket de origem que devem ser replicados e o bucket de destino ou buckets nos quais os objetos replicados estão armazenados. Para obter mais informações sobre a replicação, consulte Replicar objetos dentro de uma região e entre regiões.

É possível gerenciar as regras de replicação na página Replicação do console do Amazon S3. É possível adicionar, visualizar, editar, habilitar, desabilitar ou excluir as regras de replicação. Você também pode alterar a prioridade das regras de replicação. Para obter informações sobre como adicionar regras de replicação a um bucket, consulte Uso do console do S3.

Como gerenciar as regras de replicação para um bucket usando o console do Amazon S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.

2. No painel de navegação à esquerda, escolha Buckets.
3. Na guia Buckets de uso geral, selecione o nome do bucket que você deseja.
4. Escolha Gerenciamento e role para baixo até Regras de replicação.
5. É possível alterar as regras de replicação das seguintes formas:
   - Para habilitar ou desabilitar uma regra de replicação, selecione o botão de opção à esquerda da regra. No menu Ações, selecione Habilitar regra ou Desabilitar regra. Você também pode desabilitar, habilitar ou excluir todas as regras do bucket no menu Ações.

     > **Note**
     >
     > Se você desabilitar uma regra de replicação e, depois, reabilitá-la, qualquer objeto novo ou alterado que não tenha sido replicado enquanto a regra estava desabilitada não será replicado automaticamente quando a regra for reabilitada. Para replicar esses objetos, é necessário usar a Replicação em Lote do S3. Para obter mais informações, consulte the section called “Replicar objetos existentes”.

   - Para alterar a prioridade de uma regra, selecione o botão de opção à esquerda da regra e escolha Editar regra.

     Defina prioridades para a regra, de maneira a evitar conflitos causados pelos objetos incluídos no escopo de mais de uma regra. No caso de sobreposição de regras, o Amazon S3 usa a prioridade da regra para determinar qual regra aplicar. Quanto maior o número, maior a prioridade. Para obter mais informações sobre prioridade de regra, consulte Elementos do arquivo de configuração de replicação.

Pausar ou interromper a replicação

Para pausar temporariamente a replicação e fazer com que ela seja retomada automaticamente mais tarde, você pode usar a ação `aws:s3:bucket-pause-replication` no AWS Fault Injection Service. Consulte mais informações em aws:s3:bucket-pause-replication e em Pause S3 Replication no Guia do usuário do AWS Fault Injection Service.

Para interromper a replicação no Amazon S3, recomendamos desabilitar as regras de replicação. Se você desabilitar uma regra de replicação e, depois, reabilitá-la, qualquer objeto novo ou alterado que não tenha sido replicado enquanto a regra estava desabilitada não será replicado automaticamente quando a regra for reabilitada. Para replicar esses objetos, é necessário usar a Replicação em Lote do S3. Para obter mais informações, consulte the section called “Replicar objetos existentes”.

A replicação também será interrompida se você remover o perfil do AWS Identity and Access Management (IAM), as permissões do AWS Key Management Service (AWS KMS) ou as permissões da política de bucket que concedem ao Amazon S3 as permissões necessárias. No entanto, não recomendamos essas abordagens porque elas causam falhas na replicação. O Amazon S3 relata o status da replicação para objetos afetados como `FAILED`. Se as permissões forem restauradas posteriormente, os objetos marcados como `FAILED` não serão replicados automaticamente. Para replicar esses objetos, é necessário usar a Replicação em Lote do S3.

Replicar objetos existentes com o Replicação em Lote

A funcionalidade Replicação em Lote do S3 é diferente da replicação em tempo real, que replica contínua e automaticamente novos objetos nos buckets do Amazon S3. Em vez disso, o Replicação em Lote do S3 ocorre sob demanda em objetos existentes. É possível usar o Replicação em Lote do S3 para replicar os seguintes tipos de objeto:

- Objetos que já existiam antes da implantação de uma configuração de replicação
- Objetos que já foram replicados anteriormente
- Objetos que já falharam em uma replicação

Você pode replicar esses objetos sob demanda usando um trabalho da funcionalidade Operações em Lote.

Para começar a usar a funcionalidade Replicação em Lote, você pode:

- Iniciar o Replicação em Lote para uma nova regra ou destino de replicação: é possível criar um trabalho único do Replicação em Lote ao criar a primeira regra em uma nova configuração de replicação ou ao adicionar um novo bucket de destino a uma configuração existente por meio do console do Amazon S3.
- Iniciar o Replicação em Lote para uma configuração de replicação existente: é possível criar um trabalho de replicação em lote usando o Operações em Lote do S3 por meio do console do Amazon S3, da AWS Command Line Interface (AWS CLI), dos SDKs da AWS ou da API REST do Amazon S3.

Quando o trabalho de replicação em lote termina, você recebe um relatório de conclusão. Consulte mais informações sobre como usar esse relatório para examinar o trabalho em Monitoramento de relatórios de status e conclusão.

Considerações sobre o recurso S3 Batch Replication

Antes de usar o Replicação em Lote do S3, examine a seguinte lista de considerações:

- O bucket de origem deve ter uma configuração de replicação existente. Para habilitar a replicação, consulte Visão geral da configuração da replicação em tempo real e Exemplos para configurar a replicação em tempo real.
- Se a funcionalidade Ciclo de Vida do S3 estiver configurada para o bucket, recomendamos desabilitar as regras de ciclo de vida enquanto o trabalho da funcionalidade Replicação em Lote estiver ativo. Isso ajudará a garantir a paridade entre os buckets de origem e de destino. Caso contrário, esses buckets poderão divergir e o bucket de destino não será uma réplica exata do bucket de origem. Por exemplo, considere os seguintes cenários:
  - Seu bucket de origem tem várias versões de um objeto e um marcador de exclusão nesse objeto.
  - Seus buckets de origem e destino têm uma configuração de ciclo de vida para remover marcadores de exclusão expirados.

  Nesse cenário, a funcionalidade Replicação em Lote pode acabar replicando o marcador de exclusão para o bucket de destino antes de replicar as versões do objeto. Esse comportamento pode fazer com que a configuração de ciclo de vida marque o marcador de exclusão como expirado e com que o marcador de exclusão seja removido do bucket de destino antes que as versões do objeto sejam replicadas.
- O perfil do AWS Identity and Access Management (IAM) que você especifica para executar o trabalho da funcionalidade Operações em Lote precisa ter as permissões necessárias para executar a operação da funcionalidade Replicação em Lote subjacente. Para obter mais informações sobre como criar funções do IAM, consulte Configurar um perfil do IAM para o Replicação em Lote do S3.
- A funcionalidade Replicação em Lote requer um manifesto que pode ser gerado pelo Amazon S3. O manifesto gerado deve ser armazenado na mesma Região da AWS que o bucket de origem. Se escolher não gerar o manifesto, você poderá fornecer um relatório da funcionalidade Inventário Amazon S3 ou um arquivo CSV que contenha os objetos que deseja replicar. Para obter mais informações, consulte the section called “Especificando um manifesto para um trabalho de replicação em lote”.
- O Replicação em Lote não é compatível com a nova replicação de objetos que foram excluídos especificando o ID de versão do objeto do bucket de destino. Para replicar esses objetos novamente, copie os objetos de origem no local com um trabalho de cópia em lote. Copiar

esses objetos no local criará versões dos objetos no bucket de origem e iniciará a replicação automaticamente para o bucket de destino. A exclusão e a recriação do bucket de destino não iniciam a replicação.

Para obter mais informações sobre a cópia em lote, consulte Exemplos que usam o Batch Operations para copiar objetos.

- Se você estiver usando uma regra de replicação no bucket de origem, atualize a configuração de replicação, concedendo ao perfil do IAM anexado à regra de replicação as permissões adequadas para replicar objetos. O perfil do IAM precisa ter permissões necessárias para executar a replicação nos buckets de origem e de destino.
- Se você enviar vários trabalhos do Replicação em Lote para o mesmo bucket em um curto espaço de tempo, o Amazon S3 executará esses trabalhos simultaneamente.
- Se você enviar vários trabalhos da funcionalidade Replicação em Lote para dois buckets diferentes, esteja ciente de que o Amazon S3 poderá não executar todos os trabalhos simultaneamente. Se você exceder o número de trabalhos do Replicação em Lote que podem ser executados ao mesmo tempo em sua conta, o Amazon S3 pausará os trabalhos de menor prioridade para trabalhar nos de maior prioridade. Depois que os trabalhos de maior prioridade forem concluídos, todos os trabalhos pausados se tornarão ativos novamente.
- A funcionalidade Replicação em Lote não é compatível com objetos armazenados nas classes de armazenamento S3 Glacier Flexible Retrieval e S3 Glacier Deep Archive.
- Para replicar em lote objetos da classe S3 Intelligent-Tiering armazenados nos níveis de armazenamento Archive Access ou Deep Archive Access, primeiro é necessário iniciar uma solicitação de restauração e aguardar até que os objetos sejam movidos para o nível Frequent Access.
- Um único trabalho de cópia de replicação em lote pode comportar um manifesto com até 20 bilhões de objetos.

Especificando um manifesto para um trabalho de replicação em lote

Um manifesto é um objeto do Amazon S3 que contém as chaves de objeto em que você deseja que o Amazon S3 atue. Se quiser criar um trabalho da funcionalidade Replicação em Lote, você deverá fornecer um manifesto gerado pelo usuário ou fazer com que o Amazon S3 gere um manifesto com base na configuração de replicação.

Se você fornecer um manifesto gerado pelo usuário, ele deverá estar na forma de um relatório da funcionalidade Inventário Amazon S3 ou um arquivo CSV. Se os objetos no manifesto estiverem em

um bucket versionado, você deverá especificar os IDs de versão dos objetos. Somente o objeto com o ID de versão especificado no manifesto será replicado. Para saber mais sobre como especificar um manifesto, consulte Especificar um manifesto.

Se você preferir que o Amazon S3 gere um arquivo de manifesto em seu nome, os objetos listados usarão o mesmo bucket de origem, prefixo e tags das configurações de replicação no bucket de origem. Com um manifesto gerado, o Amazon S3 replicará todas as versões elegíveis dos objetos.

> **Note**
>
> Se você decidir que o Amazon S3 deve gerar o manifesto, ele deverá ser armazenado na mesma Região da AWS que o bucket de origem.

Filtros para um trabalho de replicação em lote

Ao criar o trabalho da funcionalidade Replicação em Lote, você pode especificar filtros adicionais, como data de criação e status de replicação do objeto, para reduzir o escopo do trabalho.

É possível filtrar os objetos a serem replicados com base no valor de `ObjectReplicationStatuses`, fornecendo um ou mais dos seguintes valores:

- `"NONE"`: indica que o Simple Storage Service (Amazon S3) nunca tentou replicar o objeto antes.
- `"FAILED"`: indica que o Amazon S3 tentou replicar o objeto, mas não conseguiu.
- `"COMPLETED"`: indica que o Simple Storage Service (Amazon S3) já replicou com êxito o objeto anteriormente.
- `"REPLICA"`: indica que esse objeto é uma réplica que o Amazon S3 replicou de outro bucket de origem.

Para obter mais informações sobre a replicação, consulte Obtenção de informações sobre o status da replicação.

Se você não filtrar o trabalho de replicação em lote, o recurso Operações em Lote tentará replicar todos os objetos (independentemente do `ObjectReplicationStatus` deles) no manifesto que correspondam às regras na configuração de replicação, exceto alguns objetos que não são replicados por padrão. Para obter mais informações, consulte the section called “O que não é replicado com as configurações de replicação?”.

Dependendo do objetivo, você pode definir `ObjectReplicationStatuses` com um ou mais dos seguintes valores:

- Para replicar somente objetos existentes que nunca foram replicados, inclua apenas `"NONE"`.
- Para repetir a replicação somente dos objetos cuja replicação falhou anteriormente, inclua apenas `"FAILED"`.
- Para replicar os objetos existentes e tentar replicar novamente os objetos cuja replicação falhou anteriormente, inclua `"NONE"` e `"FAILED"`.
- Para preencher um bucket de destino com objetos que foram replicados para outro destino, inclua `"COMPLETED"`.
- Para replicar objetos que já foram replicados anteriormente, inclua `"REPLICA"`.

Relatório de conclusão da replicação em lote

Ao criar um trabalho de replicação em lote, solicite um relatório de conclusão CSV. Esse relatório mostra objetos, códigos de sucesso ou falha na replicação, saídas e descrições. Para obter mais informações sobre o monitoramento de trabalhos e relatórios de conclusão, consulte Relatórios de conclusão.

Para obter uma lista de códigos e descrições de falhas de replicação, consulte Motivos de falha da replicação do Amazon S3.

Consulte mais informações sobre como solucionar problemas de Replicação em Lote em Erros de replicação em lote.

Introdução à replicação em lote

Para saber mais sobre como usar a replicação em lote, consulte o Tutorial: replicar objetos existentes nos buckets do Amazon S3 com o S3 Batch Replication.

Configurar um perfil do IAM para o Replicação em Lote do S3

Como o Replicação em Lote do Amazon S3 é um tipo de trabalho do operações em lote, você deve criar um perfil do AWS Identity and Access Management (IAM) para conceder permissões ao recurso Operações em Lote para realizar ações em seu nome. Você também deve anexar uma política do IAM de replicação em lote à função do IAM de operações em lote.

Use os procedimentos a seguir para criar uma política e um perfil do IAM que conceda ao recurso Operações em Lote permissão para iniciar um trabalho de replicação em lote.

Para criar uma política para replicação em lote

1. Faça login no AWS Management Console e abra o console do IAM, em https://console.aws.amazon.com/iam/.
2. Em Access management (Gerenciamento de acesso), escolha Policies (Políticas).
3. Escolha Criar política.
4. Na página Especificar permissões, escolha JSON.
5. Insira uma das políticas a seguir, dependendo se o manifesto é gerado pelo Amazon S3 ou se você está fornecendo seu próprio manifesto. Para mais informações sobre manifestos, consulte Especificando um manifesto para um trabalho de replicação em lote.

   Antes de usar essas políticas, substitua *user input placeholders* nas políticas a seguir pelos nomes do bucket de origem de replicação, do bucket de manifesto e do bucket de relatório de conclusão.

   > **Note**
   >
   > O perfil do IAM para Replicação em Lote precisa de permissões diferentes, dependendo se você gerar um manifesto ou fornecer um; portanto, escolha a política apropriada nos exemplos a seguir.

   Política se usar e armazenar um manifesto gerado pelo Amazon S3

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Action":[
            "s3:InitiateReplication"
         ],
         "Effect":"Allow",
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
         ]
      },
      {
         "Action":[
            "s3:GetReplicationConfiguration",
```

```
            "s3:PutInventoryConfiguration"
         ],
         "Effect":"Allow",
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-source-bucket"
         ]
      },
      {
         "Action":[
            "s3:GetObject",
            "s3:GetObjectVersion"
         ],
         "Effect":"Allow",
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
         ]
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3:PutObject"
         ],
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*",
            "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
         ]
      }
   ]
}
```

Política se usar um manifesto fornecido pelo usuário

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Action":[
            "s3:InitiateReplication"
         ],
         "Effect":"Allow",
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
         ]
```

```
      },
            {
         "Action":[
            "s3:GetObject",
            "s3:GetObjectVersion"
         ],
         "Effect":"Allow",
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
         ]
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3:PutObject"
         ],
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*"
         ]
      }
   ]
}
```

6. Escolha Próximo.
7. Especifique um nome para a política e escolha Criar política.

Como criar um perfil do IAM para Replicação em Lote

1. Faça login no AWS Management Console e abra o console do IAM, em https://console.aws.amazon.com/iam/.
2. Em Access management (Gerenciamento de acesso), escolha Roles (Funções).
3. Selecione Criar perfil.
4. Escolha AWS service (Serviço da AWS) como o tipo de entidade confiável. Na seção Caso de uso, escolha S3 como serviço e Operações em Lote do S3 como caso de uso.
5. Escolha Próximo. A página Adicionar permissões é exibida. Na caixa de pesquisa, pesquise a política que você criou no procedimento anterior. Marque a caixa de seleção ao lado do nome da política e escolha Próximo.
6. Na página Nomear, revisar e criar, especifique um nome para o perfil do IAM.

7. Na seção Etapa 1: identidades confiáveis, verifique se o perfil do IAM está usando a seguinte política de confiança:

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service":"batchoperations.s3.amazonaws.com"
         },
         "Action":"sts:AssumeRole"
      }
   ]
}
```

8. Na seção Etapa 2: adicionar permissões, verifique se o perfil do IAM está usando a política que você criou anteriormente.
9. Selecione Criar perfil.

Criar um trabalho de replicação em lote para novas regras ou destinos de replicação

No Amazon S3, a replicação em tempo real não replica nenhum objeto que já existia no bucket de origem antes de você criar uma configuração de replicação. A replicação em tempo real replica automaticamente somente objetos novos e atualizados que são gravados no bucket após a criação da configuração de replicação. Para replicar objetos existentes, é possível usar o Replicação em Lote do S3 para replicá-los sob demanda.

Ao criar a primeira regra em uma nova configuração de replicação em tempo real ou ao adicionar um novo bucket de destino a uma configuração de replicação existente por meio do console do Amazon S3, você tem a opção de criar um trabalho de replicação em lote. É possível usar esse trabalho de replicação em lote para replicar objetos existentes no bucket de origem para o bucket de destino.

Para usar o Replicação em Lote em uma configuração existente sem adicionar um novo bucket de destino, consulte Criar um trabalho de replicação em lote para regras de replicação existentes.

Pré-requisitos

Antes de criar o trabalho de replicação em lote, você deve criar um perfil do AWS Identity and Access Management (IAM) de operações em lote para conceder permissões ao Amazon S3 para realizar

ações em seu nome. Para obter mais informações, consulte Configurar um perfil do IAM para o Replicação em Lote do S3.

Usar o Replicação em Lote para uma nova regra ou destino de replicação pelo console do Amazon S3

Ao criar a primeira regra em uma nova configuração de replicação ou ao adicionar um novo bucket de destino a uma configuração existente por meio do console do Amazon S3, você tem a opção de criar um trabalho de replicação em lote para replicar objetos existentes no bucket de origem.

Como criar um trabalho de replicação em lote ao criar ou atualizar uma configuração de replicação

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets.
3. Na lista Buckets de uso geral, escolha o nome do bucket que contém os objetos que você deseja replicar.
4. Para criar uma regra de replicação ou editar uma existente, selecione a guia Gerenciamento e role para baixo até Regras de replicação:
   - Para criar uma regra de replicação, selecione Create replication rule (Criar regra de replicação). Consulte exemplos sobre como configurar uma regra de replicação básica em Exemplos para configurar a replicação em tempo real.
   - Para editar uma regra de replicação existente, selecione o botão de opção ao lado do nome da regra e escolha Editar regra.
5. Crie sua regra de replicação ou edite o destino da regra de replicação existente e selecione Save (Salvar).

   Depois de criar a primeira regra em uma nova configuração de replicação ou editar uma configuração existente para adicionar um novo destino, a caixa de diálogo Replicate existing objects? (Replicar objetos existentes?) é exibida, oferecendo a você a opção de criar um trabalho de replicação em lote.
6. Se você quiser criar e executar esse trabalho agora, escolha Sim, replicar objetos existentes.

   Se você quiser criar um trabalho de replicação em lote posteriormente, selecione Não, não replicar objetos existentes.

7. Se você escolher Sim, replicar objetos existentes, a página Criar trabalho de operações em lote será exibida. No recurso Replicação em Lote do S3, um trabalho tem as seguintes configurações:

   Opções de execução do trabalho

   Se você quiser que o trabalho do Replicação em Lote do S3 seja executado imediatamente, selecione Executar automaticamente o trabalho quando estiver pronto. Se quiser executar o trabalho mais tarde, selecione Aguardar para executar o trabalho quando ele estiver pronto.

   > **Note**
   >
   > Se escolher Executar automaticamente o trabalho quando estiver pronto, você não poderá criar e salvar um manifesto de operações em lote. Para salvar o manifesto de operações em lote, escolha Aguardar para executar o trabalho quando ele estiver pronto.

   Manifesto de operações em lote

   Se escolher Aguardar para executar o trabalho quando ele estiver pronto, a seção Manifesto do Batch Operations será exibida. O manifesto é uma lista de todos os objetos em que você deseja que a ação especificada seja executada. Você pode escolher salvar o manifesto. Como acontece com os arquivos do S3 Inventory, o manifesto será salvo como um arquivo CSV e armazenado em um bucket. Para saber mais sobre os manifestos de operações em lote, consulte Especificar um manifesto.

   Relatórios de conclusão

   O recurso Operações em Lote do S3 executa uma tarefa para cada objeto especificado no manifesto. Os relatórios de conclusão oferecem uma maneira fácil de visualizar os resultados das tarefas em um formato consolidado, sem a necessidade de configurações adicionais. Você pode solicitar um relatório de conclusão para todas as tarefas ou somente para as que apresentarem falha. Para saber mais sobre relatórios de conclusão, consulte Relatórios de conclusão.

   Permissões

   Uma das causas mais comuns de falhas de replicação são permissões insuficientes no perfil do AWS Identity and Access Management (IAM) fornecido. Para obter informações sobre

como criar essa função, consulte Configurar um perfil do IAM para o Replicação em Lote do S3. Crie ou escolha um perfil do IAM que tenha as permissões necessárias para a replicação em lote.

8. Escolha Salvar.

Criar um trabalho de replicação em lote para regras de replicação existentes

No Amazon S3, a replicação em tempo real não replica nenhum objeto que já existia no bucket de origem antes de você criar uma configuração de replicação. A replicação em tempo real replica automaticamente somente objetos novos e atualizados que são gravados no bucket após a criação da configuração de replicação. Para replicar objetos existentes, é possível usar o Replicação em Lote do S3 para replicá-los sob demanda.

Você pode configurar o S3 Batch Replication para uma configuração de replicação existente usando os AWS SDKs, a AWS Command Line Interface (AWS CLI) ou o console do Simple Storage Service (Amazon S3). Consulte uma visão geral sobre a replicação em lote em Replicar objetos existentes com o Replicação em Lote.

Quando o trabalho de replicação em lote termina, você recebe um relatório de conclusão. Para obter mais informações sobre como usar o relatório para examinar o trabalho, consulte Monitoramento de relatórios de status e conclusão.

Pré-requisitos

Antes de criar o trabalho de replicação em lote, você deve criar um perfil do AWS Identity and Access Management (IAM) de operações em lote para conceder permissões ao Amazon S3 para realizar ações em seu nome. Para obter mais informações, consulte Configurar um perfil do IAM para o Replicação em Lote do S3.

Uso do console do S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação esquerdo, escolha Batch Operations (Operações em lote).
3. Escolha Criar trabalho.
4. Verifique se a seção Região da AWS mostra a região onde você deseja criar o trabalho.

5. Na seção Manifesto, especifique o formato de manifesto que você deseja usar. O manifesto é uma lista de todos os objetos em que você deseja que a ação especificada seja executada. Para saber mais sobre os manifestos de operações em lote, consulte Especificar um manifesto.

   - Se você tiver um manifesto preparado, escolha S3 inventory report (manifest.json) [Relatório de inventário do S3 (manifest.json)] ou CSV. Se o manifesto estiver em um bucket com versionamento, você poderá especificar o ID de versão do manifesto. Se você não especificar um ID de versão, o Operações em Lote usará a versão atual do manifesto. Consulte mais informações sobre como criar um manifesto em Especificar um manifesto.

     > **Note**
     >
     > Se os objetos no manifesto estiverem em um bucket versionado, você deverá especificar os IDs de versão dos objetos. Para obter mais informações, consulte Especificar um manifesto.

   - Para criar um manifesto com base na configuração de replicação, escolha Create manifest using S3 Replication configuration (Criar manifesto usando a configuração do S3 Replication). Depois, escolha o bucket de origem da configuração de replicação.

6. (Opcional) Se escolher Criar manifesto usando a configuração de replicação do S3, você poderá incluir filtros adicionais, como data de criação e status de replicação do objeto. Consulte exemplos de como filtrar por status de replicação em Especificando um manifesto para um trabalho de replicação em lote.

7. (Opcional) Se escolher Criar manifesto usando a configuração de replicação do S3, você poderá salvar o manifesto gerado. Para salvar esse manifesto, selecione Salvar manifesto do Batch Operations. Depois, especifique o bucket de destino para o manifesto e escolha se deseja criptografar o manifesto.

   > **Note**
   >
   > O manifesto gerado deve ser armazenado na mesma Região da AWS que o bucket de origem.

8. Escolha Próximo.

9. Na página Operações, escolha Replicar e Próximo.

10. (Opcional) Forneça uma Description (Descrição).

11. Ajuste a Priority (Prioridade) do trabalho, se necessário. Números mais altos indicam maior prioridade. O Simple Storage Service (Amazon S3) tenta executar trabalhos de prioridade mais alta antes dos trabalhos de prioridade mais baixa. Para obter mais informações sobre prioridade de trabalhos, consulte Atribuir prioridade aos trabalhos.
12. (Opcional) Gere um relatório de conclusão. Para gerar esse relatório, selecione Gerar relatório de conclusão.

    Se escolher gerar um relatório de conclusão, você deverá escolher se o relatório informará Failed tasks only (Apenas as tarefas que falharam) ou All tasks (Todas as tarefas) e fornecer um bucket de destino para o relatório.
13. Na seção Permissões, escolha um perfil do IAM que tenha as permissões necessárias para a replicação em lote. Uma das causas mais comuns de falhas de replicação são permissões insuficientes no perfil do IAM fornecido. Para obter informações sobre como criar essa função, consulte Configurar um perfil do IAM para o Replicação em Lote do S3.
14. (Opcional) Adicione etiquetas de trabalho à tarefa de replicação em lote.
15. Escolha Próximo.
16. Analise a configuração do trabalho e selecione Criar trabalho.

Usar o AWS CLI com um manifesto do S3

O exemplo do comando `create-job` a seguir cria um trabalho do Replicação em Lote do S3 usando um manifesto gerado pelo S3 para a Conta da AWS *111122223333*. Esse exemplo replica os objetos existentes e os objetos cuja replicação falhou anteriormente. Consulte informações sobre como filtrar por status de replicação em Especificando um manifesto para um trabalho de replicação em lote.

Para usar esse comando, substitua *user input placeholders* por suas informações. Substitua o perfil do IAM `role/`*batch-Replication-IAM-policy* pelo perfil do IAM que você criou anteriormente. Para obter mais informações, consulte Configurar um perfil do IAM para o Replicação em Lote do S3.

```
aws s3control create-job --account-id 111122223333 \
--operation '{"S3ReplicateObject":{}}' \
--report '{"Bucket":"arn:aws:s3:::amzn-s3-demo-completion-report-bucket",\
"Prefix":"batch-replication-report", \
"Format":"Report_CSV_20180820","Enabled":true,"ReportScope":"AllTasks"}' \
--manifest-generator '{"S3JobManifestGenerator": {"ExpectedBucketOwner":
 "111122223333", \
```

```
"SourceBucket": "arn:aws:s3:::amzn-s3-demo-source-bucket", \
"EnableManifestOutput": false, "Filter": {"EligibleForReplication": true, \
"ObjectReplicationStatuses": ["NONE","FAILED"]}}}' \
--priority 1 \
--role-arn arn:aws:iam::111122223333:role/batch-Replication-IAM-policy \
--no-confirmation-required \
--region source-bucket-region
```

> **Note**
>
> É necessário iniciar o trabalho na mesma Região da AWS do bucket de origem da replicação.

Após iniciar com êxito um trabalho de replicação em lote, você receberá o ID do trabalho como resposta. Você pode monitorar o trabalho usando o comando `describe-job` a seguir. Para usar esse comando, substitua *`user input placeholders`* por suas informações.

```
aws s3control describe-job --account-id 111122223333 --job-id job-id --region source-bucket-region
```

Usar o AWS CLI com um manifesto fornecido pelo usuário

O exemplo a seguir cria um trabalho de Replicação em Lote do S3 usando um manifesto definido pelo usuário para a Conta da AWS *`111122223333`*. Se os objetos no manifesto estiverem em um bucket versionado, você deverá especificar os IDs de versão dos objetos. Somente o objeto com o ID de versão especificado no manifesto será replicado. Consulte mais informações sobre como criar um manifesto em Especificar um manifesto.

Para usar esse comando, substitua *`user input placeholders`* por suas informações. Substitua o perfil do IAM `role/`*`batch-Replication-IAM-policy`* pelo perfil do IAM que você criou anteriormente. Para obter mais informações, consulte Configurar um perfil do IAM para o Replicação em Lote do S3.

```
aws s3control create-job --account-id 111122223333 \
--operation '{"S3ReplicateObject":{}}' \
--report '{"Bucket":"arn:aws:s3:::amzn-s3-demo-completion-report-bucket",\
"Prefix":"batch-replication-report", \
"Format":"Report_CSV_20180820","Enabled":true,"ReportScope":"AllTasks"}' \
--manifest '{"Spec":{"Format":"S3BatchOperations_CSV_20180820",\
```

```
"Fields":["Bucket","Key","VersionId"]},\
"Location":{"ObjectArn":"arn:aws:s3:::amzn-s3-demo-manifest-bucket/manifest.csv",\
"ETag":"Manifest Etag"}}' \
--priority 1 \
--role-arn arn:aws:iam::111122223333:role/batch-Replication-IAM-policy \
--no-confirmation-required \
--region source-bucket-region
```

> **Note**
>
> É necessário iniciar o trabalho na mesma Região da AWS do bucket de origem da replicação.

Após iniciar com êxito um trabalho de replicação em lote, você receberá o ID do trabalho como resposta. Você pode monitorar o trabalho usando o comando `describe-job` a seguir.

```
aws s3control describe-job --account-id 111122223333 --job-id job-id --region source-bucket-region
```

Solução de problemas de replicação

Esta seção lista dicas de solução de problemas para a replicação do Amazon S3 e apresenta informações sobre erros de replicação em lote do S3.

Tópicos

- Dicas de solução de problemas para a replicação do S3
- Erros de replicação em lote

Dicas de solução de problemas para a replicação do S3

Se as réplicas dos objetos não aparecerem no bucket de destino depois de configurar a replicação, use as dicas a seguir para identificar e corrigir os problemas.

- Para a maioria dos objetos, a replicação ocorre em até 15 minutos. O tempo que o Amazon S3 leva para replicar um objeto depende de vários fatores, incluindo o par de regiões de origem e destino e o tamanho do objeto. Para objetos grandes, a replicação pode levar várias horas. Para ter visibilidade dos tempos de replicação, você pode usar o Controle de Tempo de Replicação do S3 (S3 RTC).

Se o objeto que estiver sendo replicado for grande, aguarde um pouco antes de conferir se ele está sendo exibido no destino. Você também pode conferir o status de replicação do objeto de origem. Se o status de replicação do objeto for `PENDING`, isso indicará que o Amazon S3 não concluiu a replicação. Se o status de replicação do objeto for `FAILED`, confira a configuração de replicação definida no bucket de origem.

Além disso, para receber informações sobre falhas durante a replicação, você pode configurar a replicação de notificações de eventos do Amazon S3 para receber eventos de falha. Para obter mais informações, consulte Receber eventos de falha de replicação com Notificações de Eventos do Amazon S3.

- Para conferir o status de replicação de um objeto, chame a operação de API `HeadObject`. A operação de API `HeadObject` retorna o status de replicação `PENDING`, `COMPLETED` ou `FAILED` de um objeto. Em resposta a uma chamada de API `HeadObject`, o status da replicação é retornado no cabeçalho `x-amz-replication-status`.

  > **Note**
  >
  > Para executar `HeadObject`, você deve ter acesso de leitura ao objeto que está solicitando. Uma solicitação `HEAD` tem as mesmas opções de uma solicitação `GET`, sem realizar uma operação `GET`. Por exemplo, para executar uma solicitação `HeadObject` usando a AWS Command Line Interface (AWS CLI), você pode executar o comando a seguir. Substitua os *`user input placeholders`* por suas próprias informações.
  >
  > ```
  > aws s3api head-object --bucket amzn-s3-demo-source-bucket --key index.html
  > ```

- Se `HeadObject` retornar os objetos com um status de replicação `FAILED`, você poderá usar o Replicação em Lote do S3 para replicar esses objetos com falha. Para obter mais informações, consulte the section called “Replicar objetos existentes”. Como alternativa, você pode recarregar os objetos com falha no bucket de origem, o que iniciará a replicação dos novos objetos.
- Na configuração de replicação do bucket de origem, verifique o seguinte:
  - O nome de recurso da Amazon (ARN) do bucket de destino está correto.
  - O prefixo do nome de chave está correto. Por exemplo, se você definiu a configuração para replicar objetos com o prefixo `Tax`, apenas objetos com nomes de chaves como `Tax/document1` ou `Tax/document2` serão replicados. Um objeto com o nome de chave `document3` não será replicado.

  - O status da regra de replicação é `Enabled`.
- Verifique se o versionamento não foi suspenso em nenhum bucket na configuração da replicação. Tanto o bucket de origem quanto o de destino devem ter o versionamento ativado.
- Se uma regra de replicação for definida como Alterar a propriedade do objeto para o proprietário do bucket de destino, a o perfil do AWS Identity and Access Management (IAM) usado para replicação deverá ter a permissão `s3:ObjectOwnerOverrideToBucketOwner`. Essa permissão é concedida ao recurso (nesse caso, o bucket de destino). Por exemplo, a declaração `Resource` a seguir mostra como conceder essa permissão no bucket de destino:

```
{
  "Effect":"Allow",
  "Action":[
    "s3:ObjectOwnerOverrideToBucketOwner"
  ],
  "Resource":"arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
}
```

- Se o bucket de destino for de propriedade de outra conta, o proprietário do bucket de destino também deve conceder a permissão `s3:ObjectOwnerOverrideToBucketOwner` ao bucket de destino por meio da política de bucket de destino. Para usar o exemplo de política de bucket a seguir, substitua *`user input placeholders`* por suas próprias informações:

```
{
  "Version": "2012-10-17",
  "Id": "Policy1644945280205",
  "Statement": [
    {
      "Sid": "Stmt1644945277847",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789101:role/s3-replication-role"
      },
      "Action": [
        "s3:ReplicateObject",
        "s3:ReplicateTags",
        "s3:ObjectOwnerOverrideToBucketOwner"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
    }
  ]
```

```
}
```

> **Note**
>
> Se as configurações de propriedade do objeto de Imposto pelo proprietário do bucket, você não precisará atualizar a configuração para Alterar a propriedade do objeto para o proprietário do bucket de destino na regra de replicação. A alteração de propriedade do objeto ocorrerá por padrão. Para obter mais informações sobre alterações da propriedade da réplica, consulte Alterar o proprietário da réplica.

- Se você estiver definindo a configuração de replicação em um cenário entre contas, no qual os buckets de origem e de destino pertencem a Contas da AWS diferentes, os buckets de destino não poderão ser configurados como um bucket de Pagamento pelo solicitante. Para obter mais informações, consulte Utilizar buckets de uso geral com pagamento pelo solicitante para transferência e uso de armazenamento.
- Se os objetos de origem de um bucket forem criptografados usando a criptografia do lado do servidor com chaves do AWS Key Management Service (AWS KMS) (SSE-KMS), a regra de replicação deverá ser configurada para incluir objetos criptografados pelo AWS KMS. Certifique-se de selecionar Replicar objetos criptografados com o AWS KMS nas configurações de Criptografia no console do Amazon S3. Depois, selecione uma chave do AWS KMS para criptografar os objetos de destino.

> **Note**
>
> Se o bucket de destino estiver em uma conta diferente, especifique uma chave gerenciada pelo cliente do AWS KMS que seja de propriedade da conta de destino. Não use a chave gerenciada padrão do Amazon S3 (`aws/s3`). O uso da chave padrão criptografa os objetos com a chave gerenciada do Amazon S3 que pertence à conta de origem, impedindo que o objeto seja compartilhado com outra conta. Como resultado, a conta de destino não conseguirá acessar os objetos no bucket de destino.

Para usar uma chave do AWS KMS que pertence à conta de destino para criptografar os objetos de destino, a conta de destino deve conceder as permissões `kms:GenerateDataKey` e `kms:Encrypt` ao perfil de replicação na política de chave do KMS. Para usar o exemplo de declaração a seguir na sua política de chave do KMS, substitua *`user input placeholders`* por suas próprias informações:

```
{
    "Sid": "AllowS3ReplicationSourceRoleToUseTheKey",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::123456789101:role/s3-replication-role"
    },
    "Action": ["kms:GenerateDataKey", "kms:Encrypt"],
    "Resource": "*"
}
```

Se você usar um asterisco (*) para a declaração `Resource` na política de chave do AWS KMS, a política concederá permissão para usar a chave do KMS somente para o perfil de replicação. A política não permite que o perfil de replicação eleve suas permissões.

Por padrão, a política de chave do KMS concede ao usuário raiz permissões totais para a chave. Essas permissões podem ser delegadas a outros usuários na mesma conta. A menos que haja declarações `Deny` na política de chave do KMS de origem, usar uma política do IAM para conceder permissões ao perfil de replicação para a chave do KMS de origem é suficiente.

> **Note**
>
> As políticas de chave do KMS que restringem o acesso a intervalos CIDR específicos, endpoints da nuvem privada virtual (VPC) ou pontos de acesso do S3 podem causar falhas na replicação.

Se as chaves do KMS de origem ou de destino concederem permissões com base no contexto de criptografia, confirme se as chaves de bucket do Amazon S3 estão ativadas para os buckets. Se os buckets tiverem as chaves de bucket do S3 ativadas, o contexto de criptografia deverá ser o recurso no nível de bucket, assim:

```
"kms:EncryptionContext:arn:aws:arn": [
     "arn:aws:s3:::amzn-s3-demo-source-bucket"
     ]
"kms:EncryptionContext:arn:aws:arn": [
     "arn:aws:s3:::amzn-s3-demo-destination-bucket"
     ]
```

Além das permissões concedidas pela política de chave do KMS, a conta de origem deve adicionar as seguintes permissões mínimas à política do IAM do perfil de replicação:

```
{
    "Effect": "Allow",
    "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
    ],
    "Resource": [
        "Source-KMS-Key-ARN"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "kms:GenerateDataKey",
        "kms:Encrypt"
    ],
    "Resource": [
        "Destination-KMS-Key-ARN"
    ]
}
```

Para obter mais informações sobre como replicar objetos criptografados com o AWS KMS, consulte Replicar objetos criptografados.

- Se o bucket de destino pertencer a outra Conta da AWS, verifique se o proprietário do bucket tem uma política de bucket no bucket de destino que permita ao proprietário do bucket de origem replicar objetos. Para obter um exemplo, consulte Configuração da replicação de buckets em contas diferentes.
- Para usar a funcionalidade Bloqueio de Objetos com replicação, é necessário conceder duas permissões adicionais no bucket de origem do S3 no perfil do AWS Identity and Access Management (IAM) usado para configurar a replicação. As duas permissões adicionais são `s3:GetObjectRetention` e `s3:GetObjectLegalHold`. Se o perfil tiver uma instrução de permissão `s3:Get*`, essa instrução satisfará o requisito. Para obter mais informações, consulte the section called “Usar a funcionalidade Bloqueio de Objetos com a funcionalidade Replicação do S3”.

- Se os objetos ainda não estiverem se replicando depois de você validar as permissões, verifique se há declarações `Deny` explícitas nos seguintes locais:
  - Declarações `Deny` nas políticas do bucket de origem ou destino. A replicação falhará se a política de bucket negar o acesso à função de replicação para qualquer uma das seguintes ações:

    Bucket de origem:

    ```
            "s3:GetReplicationConfiguration",
            "s3:ListBucket",
            "s3:GetObjectVersionForReplication",
            "s3:GetObjectVersionAcl",
            "s3:GetObjectVersionTagging"
    ```

    Buckets de destino:

    ```
            "s3:ReplicateObject",
            "s3:ReplicateDelete",
            "s3:ReplicateTags"
    ```

  - Instruções `Deny` ou limites de permissões associados ao perfil do IAM podem fazer com que a replicação falhe.
  - Instruções `Deny` nas políticas de controle de serviços (SCPs) do AWS Organizations anexadas às contas de origem ou de destino podem causar falha na replicação.
  - Instruções `Deny` nas políticas de controle de recursos (RCPs) do AWS Organizations anexadas aos buckets de origem ou de destino podem causar falha na replicação.
- Se a réplica do objeto não aparecer no bucket de destino, os seguintes problemas podem ter impedido a replicação:
  - O Amazon S3 não replica um objeto em um bucket de origem que seja uma réplica criada por outra configuração de replicação. Por exemplo, se você definir uma configuração de replicação do bucket A para o bucket B e para o bucket C, o Amazon S3 não replicará réplicas de objetos no bucket B para o bucket C.
  - O proprietário do bucket de origem pode conceder a outras Contas da AWS permissão para carregar objetos. Por padrão, o proprietário do bucket de origem não tem nenhuma permissão para os objetos criados por outras contas. A configuração de replicação vai replicar somente os objetos para os quais o proprietário do bucket de origem tem permissões de acesso. Para evitar esse problema, o proprietário do bucket de origem pode conceder a outras Contas da

AWS permissões para criar objetos condicionalmente, exigindo permissões explícitas de acesso nesses objetos. Para visualizar um exemplo de política, consulte Conceder permissões entre contas para fazer upload de objetos garantindo que o proprietário do bucket tenha controle total.

- Vamos supor que, na configuração da replicação, você adicione uma regra para replicar um subconjunto de objetos com uma tag específica. Nesse caso, atribua a chave da tag específica e o valor no momento de criar o objeto para o Amazon S3 replicar o objeto. Se você primeiro criar um objeto e depois adicionar a tag ao objeto existente, o Amazon S3 não replicará o objeto.
- Use Notificações de Eventos do Amazon S3 para notificar você sobre instâncias quando os objetos não são replicados para a Região da AWS de destino. As Notificações de Eventos do Amazon S3 estão disponíveis no Amazon Simple Queue Service (Amazon SQS), no Amazon Simple Notification Service (Amazon SNS) ou no AWS Lambda. Para obter mais informações, consulte Receber eventos de falha de replicação com Notificações de Eventos do Amazon S3.

  Você também pode ver motivos da falha de replicação usando as notificações de eventos do Amazon S3. Para ver a lista de motivos da falha, consulte Motivos de falha de replicação do Amazon S3.

Erros de replicação em lote

Para solucionar problemas de objetos que não são replicados no bucket de destino, verifique os diferentes tipos de permissões para os buckets, o perfil de replicação e o perfil do IAM que são usados para criar o trabalho de Replicação em Lote. Além disso, verifique as configurações de Bloqueio de Acesso Público e as configurações de Propriedade de Objetos do S3 dos buckets.

Consulte mais dicas de solução de problemas para trabalhar com operações em lote em the section called “Solução de problemas do Operações em Lote”.

Se você configurou a replicação e os objetos não estão se replicando, consulte Por que meus objetos do Amazon S3 não estão se replicando quando eu configuro a replicação entre meus buckets? no Centro de Conhecimento do AWS re:Post.

Ao usar a replicação em lote, você pode encontrar um destes erros:

- A geração do manifesto não encontrou chaves que correspondam aos critérios do filtro.

  Esse erro ocorre por um dos seguintes motivos:

  - Quando objetos no bucket de destino são armazenados nas classes de armazenamento S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive.

Para usar o Replicação em Lote nesses objetos, primeiro restaure-os na classe de armazenamento S3 Standard usando uma operação de Restaurar (`S3InitiateRestoreObjectOperation`) em um trabalho do Operações em Lote. Para obter mais informações, consulte Restaurar um objeto arquivado e Restaurar objetos (operações em lote). Depois de restaurar os objetos, você pode replicá-los usando um trabalho de replicação em lote.

- Quando os critérios de filtro fornecidos não corresponderem a nenhum objeto válido no bucket de origem.

  Verifique e corrija os critérios do filtro. Por exemplo, na regra do Replicação em Lote, o critério do filtro procura todos os objetos no bucket de origem com o prefixo `Tax/`. Se o nome do prefixo foi inserido de forma incorreta, com uma barra no início e no final `/Tax/` em vez de apenas no final, nenhum objeto do S3 foi encontrado. Para resolver o erro, corrija o prefixo, nesse caso, de `/Tax/` para `Tax/` na regra de replicação.

- O status da operação Batch falhou devido ao motivo: não foi possível gravar o relatório do trabalho em seu bucket de relatórios.

  Esse erro ocorrerá se o perfil do IAM usado para o trabalho de operações em lote não conseguir colocar o relatório de conclusão no local especificado quando você criou o trabalho. Para resolver esse erro, verifique se o perfil do IAM tem a permissão `s3:PutObject` para o bucket em que você deseja salvar o relatório de conclusão do Operações em Lote. Recomendamos entregar o relatório em um bucket diferente do bucket de origem.

  Consulte mais dicas sobre como resolver esse erro em the section called “O relatório do trabalho não é entregue quando há um problema com as permissões ou quando o modo de retenção está habilitado”.

- A operação em lote é concluída com falhas e o total de falhas não é 0.

  Esse erro ocorre se houver problemas de permissões insuficientes de objetos com o trabalho de replicação em lote que está sendo executado. Se você estiver usando uma regra de replicação para o trabalho de Replicação em Lote, verifique se o perfil do IAM usado para replicação tem as permissões adequadas para acessar objetos do bucket de origem ou de destino. Você também pode verificar o Relatório de conclusão da replicação em lote para analisar o Motivo de falha da replicação do Amazon S3 específico.

- O trabalho em lote foi executado com êxito, mas o número de objetos esperados no bucket de destino não é o mesmo.

Esse erro ocorre quando há uma incompatibilidade entre os objetos listados no manifesto fornecido no trabalho de replicação em lote e os filtros que você selecionou ao criar o trabalho. Você também pode receber essa mensagem quando os objetos no bucket de origem não corresponderem a nenhuma regra de replicação e não estiverem incluídos no manifesto gerado.

As falhas de operações em lote ocorrem após a adição de uma nova regra de replicação a uma configuração de replicação existente

As operações em lote tentam realizar a replicação de objetos existente para cada regra na configuração de replicação do bucket de origem. Se houver problemas com qualquer uma das regras de replicação existentes, poderão ocorrer falhas.

O relatório de conclusão do trabalho de operações em lote explica os motivos da falha do trabalho. Para obter uma lista de erros comuns, consulte Motivos de falha da replicação do Amazon S3.

Monitorar a replicação com métricas, notificações de eventos e status

É possível monitorar suas configurações de replicação em tempo real e os trabalhos de Replicação em Lote do S3 por meio dos seguintes mecanismos:

- Métricas de replicação do S3: quando você habilita as métricas de replicação do S3, o Amazon CloudWatch emite métricas que você pode usar para monitorar bytes pendentes, operações pendentes e latência de replicação em nível de regra de replicação. É possível visualizar métricas de replicação do S3 no console do Amazon S3 ou do Amazon CloudWatch. No console do Amazon S3, é possível visualizar essas métricas na guia Métricas do bucket de origem. Para ter mais informações sobre as métricas de replicação do S3, consulte the section called “Usar métricas de replicação do S3”.
- Métricas da Lente de Armazenamento do S3: além das métricas de replicação do S3, é possível usar as métricas de proteção de dados relacionadas à replicação fornecidas pelos painéis da Lente de Armazenamento do S3. Por exemplo, se você usar as métricas gratuitas na Lente de Armazenamento do S3, poderá ver determinadas métricas, como o número total de bytes replicados ou a contagem de objetos replicados do bucket de origem.

  Para realizar a auditoria do procedimento geral de replicação, habilite as métricas avançadas na Lente de Armazenamento do S3. Com as métricas avançadas na Lente de Armazenamento do S3, é possível ver quantas regras de replicação você tem de diferentes tipos, incluindo a contagem de regras com um destino inválido.

Para ter mais informações sobre como trabalhar com métricas de replicação na Lente de Armazenamento do S3, consulte the section called “Visualizar métricas de replicação nos painéis da Lente de Armazenamento do S3”.

- Notificações de eventos do S3: as notificações de eventos do S3 em instâncias podem notificar você em nível de objeto quando os objetos não são replicados para a Região da AWS de destino ou quando não são replicados dentro de determinados limites. As notificações de eventos do S3 fornecem os seguintes tipos de evento de replicação: `s3:Replication:OperationFailedReplication`, `s3:Replication:OperationMissedThreshold`, `s3:Replication:OperationReplicatedAfterThreshold` e `s3:Replication:OperationNotTracked`.

  Os eventos do Amazon S3 estão disponíveis no Amazon Simple Queue Service (Amazon SQS), no Amazon Simple Notification Service (Amazon SNS) ou no AWS Lambda. Para obter mais informações, consulte the section called “Recebimento de eventos de falha de replicação”.

- Valores de status de replicação: também é possível recuperar o status de replicação dos objetos. O status da replicação pode ajudar você a determinar o estado atual de um objeto que está sendo replicado. O status de replicação de um objeto de origem retornará `PENDING`, `COMPLETED`, ou `FAILED`. O status de replicação de uma réplica retornará `REPLICA`.

  Também é possível usar valores de status de replicação ao criar trabalhos de replicação em lote do S3. Por exemplo, é possível usar esses valores de status para replicar objetos que nunca foram replicados ou que apresentaram falha na replicação.

  Para ter mais informações sobre a recuperação do status de replicação dos objetos, consulte the section called “Obtenção de status da replicação”. Para ter mais informações sobre como usar esses valores com a replicação em lote, consulte the section called “Filtros para um trabalho de replicação em lote”.

Tópicos

- Usar métricas de replicação do S3
- Visualizar métricas de replicação nos painéis da Lente de Armazenamento do S3
- Receber eventos de falha de replicação com Notificações de Eventos do Amazon S3
- Obtenção de informações sobre o status da replicação

Usar métricas de replicação do S3

As métricas da funcionalidade Replicação do S3 são métricas detalhadas para as regras de replicação na configuração de replicação. Com as métricas de replicação, você pode monitorar o andamento minuto a minuto rastreando bytes pendentes, operações pendentes, operações com falha na replicação e latência de replicação.

> **Note**
>
> - As métricas de replicação de S3 são cobradas usando a mesma taxa das métricas personalizadas do Amazon CloudWatch. Para obter mais informações, consulte Preço do Amazon CloudWatch.
> - Se você estiver usando o controle de tempo de replicação do S3, o Amazon CloudWatch começará a relatar métricas de replicação 15 minutos após você ativar o S3 RTC na respectiva regra de replicação.

As métricas de replicação do S3 são ativadas automaticamente quando você habilita o Controle de Tempo de Replicação do S3 (S3 RTC). Também é possível habilitar as métricas de replicação do S3 independentemente do S3 RTC ao criar ou editar uma regra. O S3 RTC inclui outros recursos, como um Acordo de Serviço (SLA) e notificações para limites perdidos. Para obter mais informações, consulte Atender aos requisitos de conformidade com o Controle do Tempo de Replicação do S3.

Quando as métricas de replicação do S3 são habilitadas, o Amazon S3 publica as métricas a seguir no Amazon CloudWatch. As métricas do CloudWatch são entregues com base em melhor esforço.

Nome da métrica	Descrição da métrica	A quais objetos essa métrica se aplica?	Em qual região essa métrica é publicada?	Essa métrica ainda será publicada se o bucket de destino for excluído?	Essa métrica ainda será publicada se a replicação não ocorrer?
Bytes com replicação pendente	O número total de bytes de objetos com replicaçã	Essa métrica se aplica somente a novos objetos	Essa métrica é publicada na região do	Não	Sim

Nome da métrica	Descrição da métrica	A quais objetos essa métrica se aplica?	Em qual região essa métrica é publicada?	Essa métrica ainda será publicada se o bucket de destino for excluído?	Essa métrica ainda será publicada se a replicação não ocorrer?
	o pendente para determina da regra de replicação.	que são replicado s com Replicação do S3 Entre Regiões Diferentes (S3 CRR) ou Replicaçã o do S3 na Mesma Região (S3 SRR).	bucket de destino.		
Latência da replicação	O número máximo de segundos em que o bucket de destino da replicaçã o fica atrás do bucket de origem de uma regra de replicação específica.	Essa métrica aplica-se somente a novos objetos replicados com S3 CRR ou S3 SRR.	Essa métrica é publicada na região do bucket de destino.	Não	Sim

Nome da métrica	Descrição da métrica	A quais objetos essa métrica se aplica?	Em qual região essa métrica é publicada?	Essa métrica ainda será publicada se o bucket de destino for excluído?	Essa métrica ainda será publicada se a replicação não ocorrer?
Operações com replicação pendente	O número de operações com replicação pendente para uma regra de replicação específica. Essa métrica rastreia operações relacionadas a objetos, marcadores de exclusão, tags, listas de controle de acesso (ACLs) e bloqueio de objetos do S3.	Essa métrica aplica-se somente a novos objetos replicados com S3 CRR ou S3 SRR.	Essa métrica é publicada na região do bucket de destino.	Não	Sim

Nome da métrica	Descrição da métrica	A quais objetos essa métrica se aplica?	Em qual região essa métrica é publicada?	Essa métrica ainda será publicada se o bucket de destino for excluído?	Essa métrica ainda será publicada se a replicação não ocorrer?
Operações com falha de replicação	O número de operações com falha na replicação para determinada regra de replicação. Essa métrica monitora operações relacionadas a objetos, marcadores de exclusão, tags, listas de controle de acesso (ACLs) e Bloqueio de Objetos. Operações de replicação com falha rastreia as falhas de replicação do S3 agregadas	Essa métrica aplica-se a novos objetos que são replicados com S3 CRR ou S3 SRR e também aos objetos existentes que são replicados com a Replicação em Lote do S3. **Note** Se um trabalho de Replicação em Lote do S3 não for executado	Essa métrica é publicada na região do bucket de origem.	Sim	Não

Nome da métrica	Descrição da métrica	A quais objetos essa métrica se aplica?	Em qual região essa métrica é publicada?	Essa métrica ainda será publicada se o bucket de destino for excluído?	Essa métrica ainda será publicada se a replicação não ocorrer?
	em um intervalo por minuto. Para identificar os objetos específicos que falharam na replicação e seus motivos, assine o evento `OperationFailedReplication` nas Notificações de eventos do Amazon S3. Para obter mais informações, consulte Receber eventos de falha de replicação com Notificações de	, as métricas não serão enviadas ao Amazon CloudWatch. Por exemplo, seu trabalho não será executado se você não tiver as permissões necessárias para executar um trabalho de replicaçã			

Nome da métrica	Descrição da métrica	A quais objetos essa métrica se aplica?	Em qual região essa métrica é publicada?	Essa métrica ainda será publicada se o bucket de destino for excluído?	Essa métrica ainda será publicada se a replicação não ocorrer?
	Eventos do Amazon S3.	o em lote do S3 ou se as tags ou o prefixo em sua configuração de replicação não coincidirem.			

Para ter mais informações sobre como trabalhar com essas métricas no CloudWatch, consulte the section called “Métricas de replicação do S3 no CloudWatch”.

Habilitar métricas de replicação do S3

Você pode começar a usar métricas de replicação do S3 com uma regra de replicação nova ou existente. Para obter instruções completas sobre como criar regras de replicação, consulte Configurar a replicação para buckets na mesma conta. Você pode optar por aplicar a regra de replicação a um bucket do S3 inteiro ou a objetos do Amazon S3 com um prefixo ou tag específica.

Este tópico traz instruções para ativar as métricas de replicação do S3 em sua configuração da replicação quando os buckets de origem e destino pertencerem às mesmas Contas da AWS ou a outras.

Para ativar métricas de replicação usando a AWS Command Line Interface (AWS CLI), você deve adicionar uma configuração de replicação ao bucket de origem com `Metrics` ativado. Neste exemplo de configuração, os objetos sob o prefixo *`Tax`* são replicados para o bucket de destino *`amzn-s3-demo-bucket`*, e são geradas métricas para esses objetos.

```
{
    "Rules": [
        {
            "Status": "Enabled",
            "Filter": {
                "Prefix": "Tax"
            },
            "Destination": {
                "Bucket": "arn:aws:s3:::amzn-s3-demo-bucket",
                "Metrics": {
                    "Status": "Enabled"
                }
            },
            "Priority": 1
        }
    ],
    "Role": "IAM-Role-ARN"
}
```

Visualizar métricas de replicação

É possível visualizar as métricas da funcionalidade Replicação do S3 na guia Métricas do bucket de uso geral de origem no console do Amazon S3. Essas métricas do Amazon CloudWatch também estão disponíveis no console do Amazon CloudWatch. Quando você habilita as métricas de replicação do S3, o Amazon CloudWatch emite métricas que você pode usar para monitorar bytes pendentes, operações pendentes e latência de replicação em nível de regra de replicação.

As métricas de replicação do S3 são ativadas automaticamente quando você habilita a replicação com Controle de Tempo de Replicação do S3 (S3 RTC) usando o console do Amazon S3 ou a API REST do Amazon S3. Também é possível habilitar as métricas de replicação do S3 independentemente do S3 RTC ao criar ou editar uma regra.

Se você estiver usando o controle de tempo de replicação do S3, o Amazon CloudWatch começará a relatar métricas de replicação 15 minutos após você ativar o S3 RTC na respectiva regra de replicação. Para obter mais informações, consulte Usar métricas de replicação do S3.

As métricas de replicação controlam os IDs de regra da configuração de replicação. Um ID de regra de replicação pode ser específico para um prefixo, uma tag ou uma combinação de ambos.

Para obter mais informações sobre métricas do CloudWatch para o Amazon S3, consulte Monitoramento de métricas com o Amazon CloudWatch.

Pré-requisitos

Crie uma regra de replicação que tenha métricas de replicação do S3 habilitadas. Para obter mais informações, consulte the section called “Ativação de métricas de replicação”.

Como visualizar as métricas de replicação do S3 por meio da guia Métricas do bucket de origem

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets de uso geral.
3. Na lista de buckets, selecione o nome do bucket que contém os objetos para os quais você deseja métricas de replicação.
4. Escolha a guia Métricas.
5. Em Métricas de replicação, selecione as regras de replicação para as quais você deseja ver as métricas.
6. Escolha Display charts (Exibir gráficos).

   O Amazon S3 exibe os gráficos Latência da replicação, Bytes com replicação pendente, Operações com replicação pendente e Operações com falha de replicação correspondentes às regras selecionadas.

Visualizar métricas de replicação nos painéis da Lente de Armazenamento do S3

Além das métricas de replicação do S3, é possível usar as métricas de proteção de dados relacionadas à replicação fornecidas pela Lente de Armazenamento do S3. A Lente de Armazenamento do S3 é um recurso de análise de armazenamento em nuvem que você pode usar para obter visibilidade em toda a organização sobre o uso e a atividade do armazenamento de

objetos. Para obter mais informações, consulte Como usar a Lente de Armazenamento do S3 para proteger seus dados.

A Lente de Armazenamento do S3 tem dois níveis de métricas: métricas gratuitas e métricas e recomendações avançadas, que podem ser adquiridas por um custo adicional. Com métricas e recomendações avançadas, você pode acessar métricas e recursos adicionais para obter informações sobre seu armazenamento. Para obter mais informações sobre a definição de preço do S3 Storage Lens, consulte Definição de preço do Amazon S3.

Se você usar as métricas gratuitas na Lente de Armazenamento do S3, poderá ver determinadas métricas, como o número total de bytes replicados ou a contagem de objetos replicados do bucket de origem.

Para realizar a auditoria do procedimento geral de replicação, habilite as métricas avançadas na Lente de Armazenamento do S3. Com as métricas avançadas na Lente de Armazenamento do S3, é possível ver quantas regras de replicação você tem de diferentes tipos, incluindo a contagem de regras com um destino inválido.

Para ter uma lista completa das métricas da Lente de Armazenamento do S3, incluindo quais métricas de replicação estão em cada camada, consulte o Glossário de métricas de lente de armazenamento do S3.

Pré-requisitos

Crie uma configuração de replicação em tempo real ou um trabalho de Replicação em Lote do S3.

Como visualizar métricas de replicação na Lente de Armazenamento do S3

1. Crie um painel da Lente de Armazenamento do S3. Para obter instruções detalhadas, consulte the section called “Usar o console do S3”.
2. (Opcional) Durante a configuração do painel, se você quiser ver todas as métricas de replicação da Lente de Armazenamento do S3, selecione Métricas e recomendações avançadas e escolha Métricas avançadas de proteção de dados. Consulte uma lista completa de métricas em Glossário de métricas de lente de armazenamento do Amazon S3.

   Se você habilitar métricas e recomendações avançadas, poderá ganhar mais insights sobre as configurações de replicação. Por exemplo, é possível usar as métricas de contagem de regras de replicação da Lente de Armazenamento do S3 para ter informações detalhadas sobre os buckets configurados para replicação. Essas informações incluem regras de replicação dentro

e entre buckets e regiões. Para obter mais informações, consulte the section called “Contar o número total de regras de replicação para cada bucket”.

3. Depois de criar o painel, abra-o e selecione a guia Buckets.
4. Role para baixo até a seção Buckets. Em Metrics categories (Categorias de métricas), escolha Data protection (Proteção de dados). Depois, desmarque Summary (Resumo).
5. Para filtrar a lista Buckets de modo que somente as métricas de replicação sejam exibidas, escolha o ícone de preferências ().
6. Desmarque o botão alternador referente a todas as métricas de proteção de dados, mantendo somente as métricas de replicação selecionadas.
7. (Opcional) Em Page size (Tamanho da página), escolha o número de buckets a serem exibidos na lista.
8. Escolha Continuar.

Receber eventos de falha de replicação com Notificações de Eventos do Amazon S3

Se você habilitou as métricas de replicação do S3 na configuração de replicação, poderá configurar as notificações de eventos do Amazon S3 para notificar você quando os objetos não forem replicados para a Região da AWS de destino. Se você habilitou o Controle de Tempo de Replicação do S3 (S3 RTC) na configuração de replicação, também poderá receber notificação quando os objetos não forem replicados no limite de 15 minutos do S3 RTC para replicação.

Ao usar os tipos de evento `Replication` a seguir, é possível acompanhar o andamento minuto a minuto dos eventos de replicação monitorando os bytes pendentes, as operações pendentes e a latência da replicação. Para ter mais informações sobre as métricas de replicação do S3, consulte Usar métricas de replicação do S3.

- O tipo de evento `s3:Replication:OperationFailedReplication` notifica você quando um objeto qualificado para replicação falhou ao replicar.
- O tipo de evento `s3:Replication:OperationMissedThreshold` notifica você quando um objeto qualificado para replicação e que usa o S3 RTC excede o limite de 15 minutos para replicação.
- O tipo de evento `s3:Replication:OperationReplicatedAfterThreshold` notifica você quando um objeto qualificado para replicação e que usa o S3 RTC replica após o limite de 15 minutos.

- O tipo de evento `s3:Replication:OperationNotTracked` notifica você quando um objeto que era elegível para a replicação em tempo real [Replicação na Mesma Região (SRR) ou Replicação Entre Regiões Diferentes (CRR)] não está mais sendo monitorado por métricas de replicação.

Para ter descrições completas de todos os tipos de evento de replicação compatíveis, consulte the section called “Tipos de evento compatíveis com SQS, SNS e Lambda”.

Para ter uma lista dos códigos de falha capturados pelas notificações de eventos do S3, consulte Motivos de falha da replicação do Amazon S3.

Você pode receber Notificações de eventos do S3 por meio do Amazon Simple Queue Service (Amazon SQS), do Amazon Simple Notification Service (Amazon SNS) ou do AWS Lambda. Para obter mais informações, consulte the section called “Notificações de eventos do Amazon S3”.

Para obter instruções sobre como configurar as notificações de evento do Amazon S3, consulte Habilitar notificações de eventos.

> **Note**
>
> Além das notificações de eventos, habilite também as métricas de replicação do S3. Para obter mais informações, consulte the section called “Ativação de métricas de replicação”.

Veja a seguir um exemplo de mensagem que o Amazon S3 envia para publicar um evento `s3:Replication:OperationFailedReplication`. Para obter mais informações, consulte the section called “Estrutura de mensagens de evento”.

```
{
  "Records": [
    {
      "eventVersion": "2.2",
      "eventSource": "aws:s3",
      "awsRegion": "us-east-1",
      "eventTime": "2024-09-05T21:04:32.527Z",
      "eventName": "Replication:OperationFailedReplication",
      "userIdentity": {
        "principalId": "s3.amazonaws.com"
      },
```

```
      "requestParameters": {
        "sourceIPAddress": "s3.amazonaws.com"
      },
      "responseElements": {
        "x-amz-request-id": "123bf045-2b4b-4ca8-a211-c34a63c59426",
        "x-amz-id-2":
 "12VAWNDIHnwJsRhTccqQTeAPoXQmRt22KkewMV8G3XZihAuf9CLDdmkApgZzudaIe2KlLfDqGS0="
      },
      "s3": {
        "s3SchemaVersion": "1.0",
        "configurationId": "ReplicationEventName",
        "bucket": {
          "name": "amzn-s3-demo-bucket1",
          "ownerIdentity": {
            "principalId": "111122223333"
          },
          "arn": "arn:aws:s3:::amzn-s3-demo-bucket1"
        },
        "object": {
          "key": "replication-object-put-test.png",
          "size": 520080,
          "eTag": "e12345ca7e88a38428305d3ff7fcb99f",
          "versionId": "abcdeH0Xp66ep__QDjR76LK7Gc9X4wKO",
          "sequencer": "0066DA1CBF104C0D51"
        }
      },
      "replicationEventData": {
        "replicationRuleId": "notification-test-replication-rule",
        "destinationBucket": "arn:aws:s3:::amzn-s3-demo-bucket2",
        "s3Operation": "OBJECT_PUT",
        "requestTime": "2024-09-05T21:03:59.168Z",
        "failureReason": "AssumeRoleNotPermitted"
      }
    }
  ]
}
```

Motivos de falha da replicação do Amazon S3

A tabela a seguir relaciona os motivos de falha da replicação do Amazon S3. É possível visualizar esses motivos ao receber o evento `s3:Replication:OperationFailedReplication` com as notificações de eventos do Amazon S3 e, depois, examinar o valor `failureReason`.

Você também pode visualizar esses motivos de falha em um relatório de conclusão da replicação em lote do S3. Para obter mais informações, consulte Relatório de conclusão da replicação em lote.

Motivos de falha da replicação	Descrição
`AssumeRoleNotPermitted`	O Amazon S3 não pode assumir o perfil do AWS Identity and Access Management (IAM) especificado na configuração de replicação ou no trabalho de operações em lote.
`DstBucketInvalidRegion`	O bucket de destino não está na mesma Região da AWS especificada pelo trabalho de operações em lote. Esse erro é específico da replicação em lote.
`DstBucketNotFound`	O Amazon S3 não consegue encontrar o bucket de destino especificado na configura ção de replicação.
`DstBucketObjectLockConfigMissing`	Para replicar objetos de um bucket de origem com o bloqueio de objetos habilitad o, o destino também deve ter o bloqueio de objetos habilitado. O erro indica que o bloqueio de objetos pode não estar ativado no bucket de destino. Para obter mais informações, consulte Considerações sobre a funcionalidade Bloqueio de Objetos.
`DstBucketUnversioned`	O versionamento não está ativado no bucket de destino do S3. Para ativar objetos com replicação do S3, ative o versionamento no bucket de destino.
`DstDelObjNotPermitted`	O Amazon S3 não consegue replicar marcadores de exclusão no bucket de destino. A permissão `s3:Replic ateDelete` pode estar faltando para o bucket de destino.

Motivos de falha da replicação	Descrição
`DstKmsKeyInvalidState`	A chave do AWS Key Management Service (AWS KMS) para o bucket de destino está em estado inválido. Revise e ative a chave do AWS KMS necessária. Para ter mais informações sobre o gerenciamento de chaves do AWS KMS, consulte Estados das chaves do AWS KMS no Guia do desenvolvedor do AWS Key Management Service.
`DstKmsKeyNotFound`	A chave AWS KMS configurada para o bucket de destino na configuração de replicação não existe.
`DstMultipartCompleteNotPermitted`	O Amazon S3 não consegue concluir o multipart uploads de objetos para o bucket de destino. A permissão `s3:ReplicateObject` pode estar faltando para o bucket de destino.
`DstMultipartInitNotPermitted`	O Amazon S3 não consegue iniciar multipart uploads de objetos para o bucket de destino. A permissão `s3:ReplicateObject` pode estar faltando para o bucket de destino.
`DstMultipartUploadNotPermitted`	O Amazon S3 não consegue fazer o carregamento fracionado de objetos no bucket de destino. A permissão `s3:ReplicateObject` pode estar faltando para o bucket de destino.
`DstObjectHardDeleted`	A replicação em lote não é compatível com a nova replicação de objetos excluídos com o ID de versão do objeto do bucket de destino. Esse erro é específico da replicação em lote.

Motivos de falha da replicação	Descrição
`DstPutAclNotPermitted`	O Amazon S3 não consegue replicar listas de controle de acesso (ACLs) de objetos no bucket de destino. A permissão `s3:ReplicateObject` pode estar faltando para o bucket de destino.
`DstPutLegalHoldNotPermitted`	O Amazon S3 não consegue colocar uma retenção jurídica da funcionalidade Bloqueio de Objetos nos objetos de destino ao replicar objetos imutáveis. A permissão `s3:PutObjectLegalHold` pode estar faltando para o bucket de destino. Para obter mais informações, consulte Retenções legais.
`DstPutObjectNotPermitted`	O Amazon S3 não consegue replicar objetos no bucket de destino. Isso pode ocorrer quando faltam as permissões (`s3:ReplicateObject` ou `s3:ObjectOwnerOverrideToBucketOwner`) necessárias para o bucket de destino ou quando a política de chaves do AWS KMS não permite que o perfil de replicação do bucket de origem use a chave do AWS KMS (ações `kms:Decrypt` e `kms:GenerateDataKey*`) no bucket de destino.
`DstPutRetentionNotPermitted`	O Amazon S3 não consegue colocar um período de retenção nos objetos de destino ao replicar objetos imutáveis. A permissão `s3:PutObjectRetention` pode estar faltando para o bucket de destino.

Motivos de falha da replicação	Descrição
`DstPutTaggingNotPermitted`	O Amazon S3 não consegue replicar etiquetas de objetos no bucket de destino. A permissão `s3:ReplicateObject` pode estar faltando para o bucket de destino.
`DstVersionNotFound`	O Amazon S3 não consegue encontrar a versão necessária do objeto no bucket de destino para o qual os metadados precisam ser replicados.
`InitiateReplicationNotPermitted`	O Amazon S3 não consegue iniciar a replicação em objetos. A permissão `s3:InitiateReplication` pode estar ausente para o trabalho de operações em lote. Esse erro é específico da replicação em lote.
`SrcBucketInvalidRegion`	O bucket de origem não está na mesma Região da AWS especificada pelo trabalho da funcionalidade Operações em Lote. Esse erro é específico da replicação em lote.
`SrcBucketNotFound`	O Amazon S3 não consegue encontrar o bucket de origem.
`SrcBucketReplicationConfigMissing`	O Amazon S3 não conseguiu encontrar uma configuração de replicação para o bucket de origem.

Motivos de falha da replicação	Descrição
`SrcGetAclNotPermitted`	O Amazon S3 não consegue acessar o objeto no bucket de origem para replicação. A permissão `s3:GetObjectVersionAcl` pode estar faltando para o objeto do bucket de origem. Os objetos no bucket de origem devem ser de do proprietário do bucket. Se as ACLs estiverem habilitadas, verifique se a “Propriedade do objeto” está definida como “Proprietário do bucket preferido” ou “Autor do objeto”. Se a “Propriedade do objeto” estiver definida como “Proprietário do bucket preferido”, os objetos do bucket de origem deverão ter a ACL `bucket-owner-full-control` para que o proprietário do bucket se torne o proprietário do objeto. A conta de origem pode se tornar proprietária de todos os objetos no bucket definindo a “Propriedade do objeto” como “Imposto pelo proprietário do bucket” e desabilitando as ACLs.
`SrcGetLegalHoldNotPermitted`	O Amazon S3 não consegue acessar as informações de retenção legal do Bloqueio de objetos do S3.
`SrcGetObjectNotPermitted`	O Amazon S3 não consegue acessar o objeto no bucket de origem para replicação. A permissão `s3:GetObjectVersionForReplication` pode estar faltando para o bucket de origem.
`SrcGetRetentionNotPermitted`	O Amazon S3 não consegue acessar as informações do período de retenção do Bloqueio de objetos do S3.

Motivos de falha da replicação	Descrição
`SrcGetTaggingNotPermitted`	O Amazon S3 não consegue acessar as informações da tag do objeto pelo bucket de origem. A permissão `s3:GetObjectVersionTagging` pode estar faltando para o bucket de origem.
`SrcHeadObjectNotPermitted`	O Amazon S3 não consegue recuperar os metadados do objeto pelo bucket de origem. A permissão `s3:GetObjectVersionForReplication` pode estar faltando para o bucket de origem.
`SrcKeyNotFound`	O Amazon S3 não consegue encontrar a chave do objeto de origem para replicar. O objeto de origem pode ter sido excluído antes da conclusão da replicação.
`SrcKmsKeyInvalidState`	A chave do AWS KMS para o para o bucket de origem não está em estado válido. Revise e ative a chave do AWS KMS necessária. Para ter mais informações sobre o gerenciamento de chaves do AWS KMS, consulte Estados das chaves do AWS KMS no Guia do desenvolvedor do AWS Key Management Service.
`SrcObjectNotEligible`	Alguns objetos não são elegíveis para replicação. O motivo disso pode ser a falta de correspondência entre a classe de armazenamento do objeto ou as tags do objeto com a configuração da replicação.
`SrcObjectNotFound`	O objeto de origem não existe.
`SrcReplicationNotPending`	O Amazon S3 já replicou esse objeto. Esse objeto não está mais pendente de replicação.

Motivos de falha da replicação	Descrição
`SrcVersionNotFound`	O Amazon S3 não consegue encontrar a versão do objeto de origem para replicar. A versão do objeto de origem pode ter sido excluída antes da conclusão da replicação.

Tópicos relacionados

Configurar permissões para replicação em tempo real

Solução de problemas de replicação

Obtenção de informações sobre o status da replicação

O status da replicação pode ajudá-lo a determinar o estado atual de um objeto que está sendo replicado. O status de replicação de um objeto de origem retornará `PENDING`, `COMPLETED`, ou `FAILED`. O status de replicação de uma réplica retornará `REPLICA`.

Também é possível usar valores de status de replicação ao criar trabalhos de replicação em lote do S3. Por exemplo, é possível usar esses valores de status para replicar objetos que nunca foram replicados ou que apresentaram falha na replicação. Para ter mais informações sobre como usar esses valores com a replicação em lote, consulte the section called “Usar informações de status de replicação com trabalhos de replicação em lote”.

Tópicos

- Visão geral do status da replicação
- Status da replicação, se replicar para vários intervalos de destino
- Status da replicação se a sincronização de modificação de réplica do Amazon S3 estiver ativada
- Usar informações de status de replicação com trabalhos de replicação em lote
- Localização do status de replicação

Visão geral do status da replicação

Na replicação, você tem um bucket de origem em que configura a replicação e um ou mais buckets de destino nos quais o Amazon S3 replica objetos. Ao solicitar um objeto (usando `GetObject`) ou

metadados de objeto (usando `HeadObject`) nesses buckets, o Amazon S3 exibirá o cabeçalho `x-amz-replication-status` na resposta:

- Ao solicitar um objeto no bucket de origem, o Amazon S3 retornará o cabeçalho `x-amz-replication-status` se o objeto em sua solicitação for qualificado para replicação.

  Por exemplo, suponha que, em sua configuração de replicação, você especifique o prefixo de objeto `TaxDocs` para dizer ao Amazon S3 para replicar somente objetos com o prefixo de nome de chave `TaxDocs`. Todos os objetos dos quais você fizer upload e tiverem esse prefixo de nome de chave, por exemplo, `TaxDocs/document1.pdf`, serão replicados. Para qualquer solicitação de objeto com esse prefixo de nome de chave, o Amazon S3 retorna o cabeçalho `x-amz-replication-status` com um dos seguintes valores para o status de replicação de objeto: `PENDING`, `COMPLETED` ou `FAILED`.

  > **Note**
  >
  > Se a replicação do objeto falhar depois de você fazer upload de um objeto, não será possível tentar novamente a replicação. É necessário fazer upload do objeto novamente ou usar a Replicação em Lote do S3 para replicar qualquer objeto com falha. Para ter mais informações sobre o uso da replicação em lote, consulte the section called “Replicar objetos existentes”.
  >
  > Os objetos mudam para um estado `FAILED` em caso de problemas, como a ausência das permissões do perfil de replicação, do AWS Key Management Service (AWS KMS) ou do bucket. Em caso de falhas temporárias, por exemplo, se um bucket ou uma região não estiver disponível, o status da replicação não fará a transição para `FAILED`, mas permanecerá `PENDING`. Depois que o recurso estiver on-line novamente, o Amazon S3 retomará a replicação desses objetos.

- Ao solicitar um objeto no bucket de destino, se o objeto da sua solicitação for uma réplica criada pelo Amazon S3, o Amazon S3 retornará o cabeçalho `x-amz-replication-status` com valor `REPLICA`.

> **Note**
>
> Antes de excluir um objeto de um bucket de origem com a replicação habilitada, confira o status de replicação para confirmar se o objeto foi replicado.

Se a configuração de ciclo de vida do S3 estiver habilitada no bucket de origem, o Amazon S3 suspenderá as ações de ciclo de vida até que o status dos objetos seja `COMPLETED` ou `FAILED`.

Status da replicação, se replicar para vários intervalos de destino

Quando você replica objetos para vários intervalos de destino, o cabeçalho`x-amz-replication-status` age de forma diferente. O cabeçalho do objeto de origem exibe um valor de `COMPLETED` somente quando a replicação é bem-sucedida para todos os destinos. O cabeçalho permanece no valor `PENDING` até que a replicação tenha sido concluída para todos os destinos. Se um ou mais destinos falharem na replicação, o cabeçalho retornará `FAILED`.

Status da replicação se a sincronização de modificação de réplica do Amazon S3 estiver ativada

Quando suas regras de replicação habilitam a sincronização de modificação de réplica do Simple Storage Service (Amazon S3), as réplicas podem informar um status diferente de `REPLICA`.
Se alterações de metadados estiverem no processo de replicação, o cabeçalho do `x-amz-replication-status` retorna `PENDING`. Se a sincronização de modificação de réplica falhar ao replicar metadados, o cabeçalho retornará `FAILED`. Se os metadados forem replicados corretamente, as réplicas retornarão o cabeçalho `REPLICA`.

Usar informações de status de replicação com trabalhos de replicação em lote

Ao criar um trabalho de replicação em lote, é possível especificar filtros adicionais, como data de criação e status de replicação do objeto, para reduzir o escopo do trabalho.

É possível filtrar os objetos a serem replicados com base no valor de `ObjectReplicationStatuses`, fornecendo um ou mais dos seguintes valores:

- `"NONE"`: indica que o Simple Storage Service (Amazon S3) nunca tentou replicar o objeto antes.
- `"FAILED"`: indica que o Amazon S3 tentou replicar o objeto, mas não conseguiu.
- `"COMPLETED"`: indica que o Simple Storage Service (Amazon S3) já replicou com êxito o objeto anteriormente.
- `"REPLICA"`: indica que essa é uma réplica de um objeto que foi replicado pelo Amazon S3 de outra origem.

Para ter mais informações sobre como usar esses valores de status de replicação com replicação em lote, consulte the section called “Filtros para um trabalho de replicação em lote”.

Localização do status de replicação

Para obter o status de replicação dos objetos em um bucket, você pode usar a ferramenta Amazon S3 Inventory. O Amazon S3 envia um arquivo CSV para o bucket de destino especificado na configuração de inventário. Você também pode usar o Amazon Athena para consultar o status da replicação no relatório de inventário. Para obter mais informações sobre o Amazon S3 Inventory, consulte Catalogar e analisar seus dados com o Inventário S3.

Também é possível encontrar o status de replicação do objeto usando o console do Amazon S3, a AWS Command Line Interface (AWS CLI) ou o SDK da AWS.

Uso do console do S3

No console do S3, é possível visualizar o status da replicação de um objeto na página de detalhes do objeto.

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets.
3. Na lista Buckets de uso geral, selecione o nome do bucket de origem da replicação.
4. Na lista Objects (Objetos), escolha o nome do objeto. A página de detalhes do objeto é exibida.
5. Na guia Propriedades, role para baixo até a seção Visão geral do gerenciamento de objetos. Em Configurações de gerenciamento, veja o valor em Status da replicação.

Como usar o AWS CLI

Use o comando AWS CLI (`head-object`) da AWS Command Line Interface para recuperar metadados, como mostrado no exemplo a seguir. Substitua *`amzn-s3-demo-source-bucket1`* pelo nome do bucket de origem da replicação e substitua os outros *`user input placeholders`* por suas próprias informações.

```
aws s3api head-object --bucket amzn-s3-demo-source-bucket1 --key object-key --version-id object-version-id
```

O comando retorna os metadados do objeto, inclusive `ReplicationStatus`, conforme exibido no exemplo de resposta a seguir.

```
{
```

```
   "AcceptRanges":"bytes",
   "ContentType":"image/jpeg",
   "LastModified":"Mon, 23 Mar 2015 21:02:29 GMT",
   "ContentLength":3191,
   "ReplicationStatus":"COMPLETED",
   "VersionId":"jfnW.HIMOfYiD_9rGbSkmroXsFj3fqZ.",
   "ETag":"\"6805f2cfc46c0f04559748bb039d69ae\"",
   "Metadata":{

   }
}
```

Uso dos SDKs da AWS

Os fragmentos de código a seguir recebem o status de replicação utilizando o AWS SDK para Java e o AWS SDK para .NET, respectivamente.

Java

```
GetObjectMetadataRequest metadataRequest = new GetObjectMetadataRequest(bucketName,
 key);
ObjectMetadata metadata = s3Client.getObjectMetadata(metadataRequest);

System.out.println("Replication Status : " +
 metadata.getRawMetadataValue(Headers.OBJECT_REPLICATION_STATUS));
```

.NET

```
GetObjectMetadataRequest getmetadataRequest = new GetObjectMetadataRequest
    {
         BucketName = sourceBucket,
         Key        = objectKey
    };

GetObjectMetadataResponse getmetadataResponse =
 client.GetObjectMetadata(getmetadataRequest);
Console.WriteLine("Object replication status: {0}",
 getmetadataResponse.ReplicationStatus);
```

Gerenciar o tráfego multirregional com Pontos de Acesso Multirregionais

O recurso Pontos de Acesso Multirregionais do Amazon S3 fornece um endpoint global que as aplicações podem usar para atender a solicitações de buckets do S3 localizados em várias Regiões da AWS. Você pode usar pontos de acesso multirregionais para criar aplicações de várias regiões com a mesma arquitetura usada em uma única região, depois executar essas aplicações em qualquer lugar do mundo. Em vez de enviar solicitações pela internet pública congestionada, o recurso Pontos de Acesso Multirregionais fornece resiliência de rede integrada com aceleração de solicitações baseadas na internet para o Amazon S3. As solicitações de aplicações feitas para um endpoint global do recurso Pontos de Acesso Multirregional usam o AWS Global Accelerator para rotear automaticamente pela rede global da AWS para o bucket do S3 mais próximo com status de roteamento ativo.

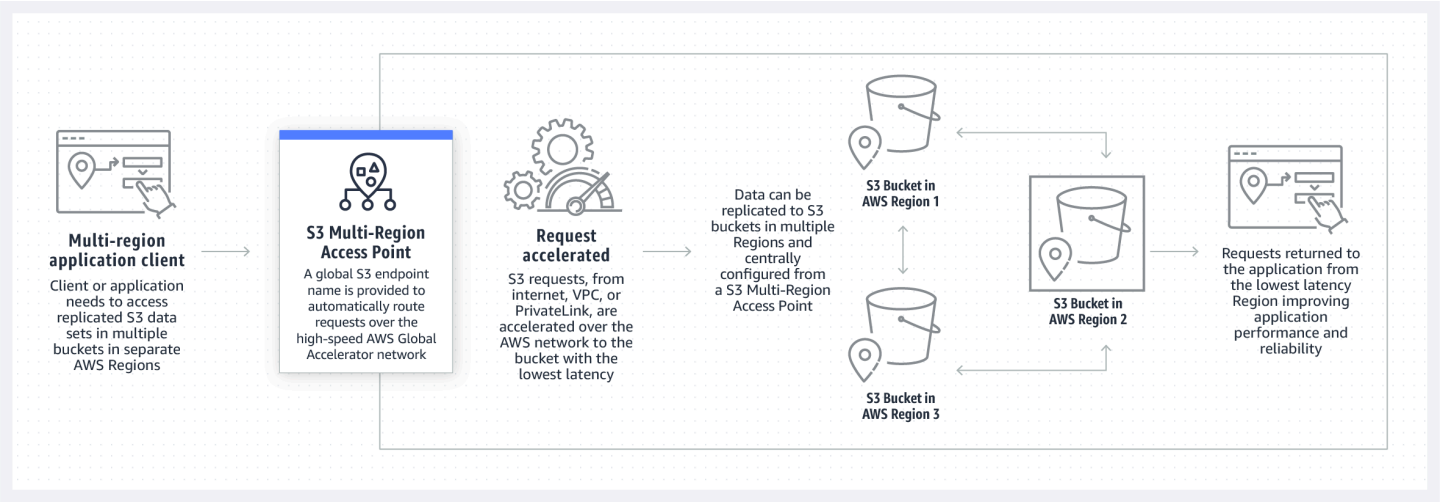
Se ocorrer uma interrupção no tráfego regional, você poderá usar os controles de failover do recurso Pontos de Acesso Multirregionais para deslocar o tráfego da solicitação de dados do S3 entre Regiões da AWS e redirecionar o tráfego do S3 para longe das interrupções em questão de minutos. Também é possível testar a resiliência da aplicação contra uma interrupção para fazer failover da aplicação e realizar simulações de recuperação de desastres. Se precisar conectar e acelerar as solicitações para o S3 de fora de uma VPC, você poderá simplificar as aplicações e a arquitetura de rede com o recurso Pontos de Acesso Multirregionais do Amazon S3. As solicitações de pontos de acesso multirregionais serão roteadas pela rede global da AWS e, depois, retornam ao S3 dentro da Região da AWS, sem precisar atravessar a internet pública. Como resultado, é possível criar aplicações mais altamente disponíveis.

Durante a criação e configuração de pontos de acesso multirregionais, você especifica um conjunto de Regiões da AWS onde deseja armazenar dados que serão fornecidos por meio desse ponto de acesso multirregional. É possível usar o nome do endpoint de pontos de acesso multirregionais para conectar os clientes. Depois de estabelecer conexões de clientes, você poderá selecionar os buckets novos ou existentes entre os quais gostaria de rotear as solicitações de pontos de acesso multirregionais. É possível usar regras da Replicação do S3 Entre Regiões Diferentes (CRR) para sincronizar dados entre buckets nessas regiões.

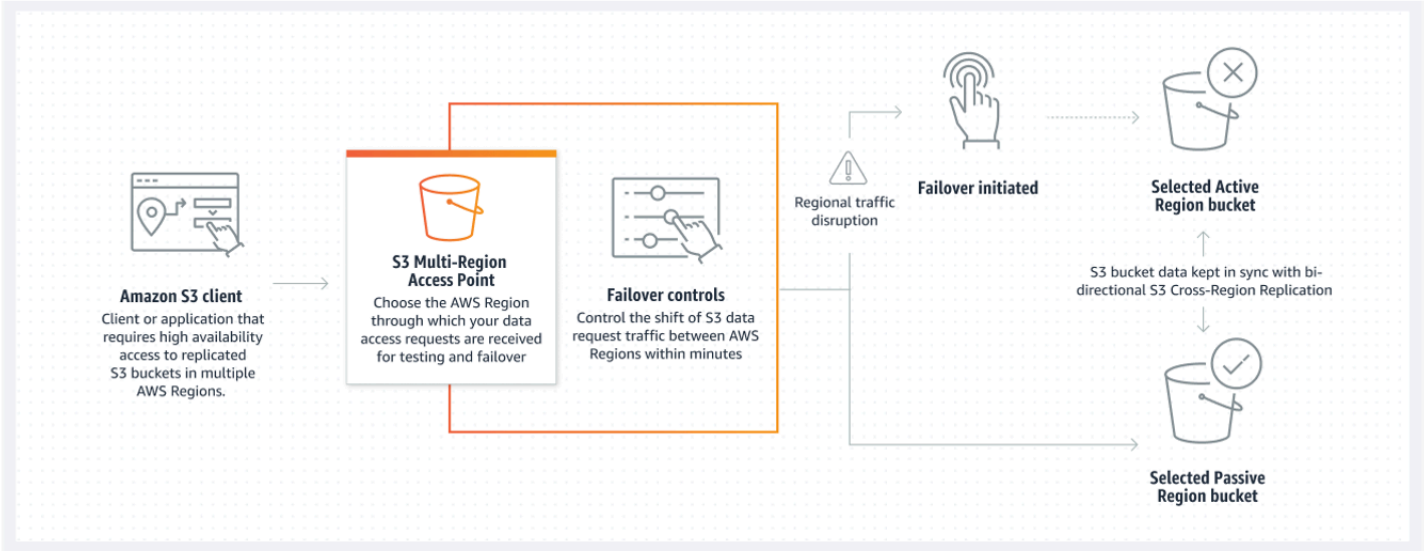
Depois de configurar o ponto de acesso multirregional, você poderá solicitar ou gravar dados por meio do endpoint global de pontos de acesso multirregionais. O Amazon S3 atende automaticamente às solicitações para o conjunto de dados replicado da região mais próxima disponível. No AWS Management Console, também é possível visualizar a topologia de replicação subjacente e as

métricas de replicação relacionadas às solicitações de pontos de acesso multirregionais. Isso oferece uma maneira ainda mais fácil de criar, gerenciar e monitorar o armazenamento para aplicações multirregionais. Se preferir, você poderá usar o Amazon CloudFront para automatizar a criação e a configuração do recurso Pontos de Acesso Multirregionais do S3.

A imagem a seguir é uma representação gráfica de um ponto de acesso multirregional do Amazon S3 em uma representação ativa-ativa. O gráfico mostra como as solicitações do Amazon S3 são roteadas automaticamente para buckets no Região da AWS ativo mais próximo.



A imagem a seguir é uma representação gráfica de um ponto de acesso multirregional do Amazon S3 em uma representação ativa-passiva. O gráfico mostra como você pode controlar o tráfego de acesso a dados do Amazon S3 para realizar failover entre Regiões da AWS ativas e passivas.



Para saber mais sobre como usar pontos de acesso multirregiões, consulte o Tutorial: Introdução aos pontos de acesso multirregionais do Amazon S3.

Tópicos

- Criação de pontos de acesso multirregionais
- Configurar um ponto de acesso multirregional para uso com AWS PrivateLink
- Como fazer solicitações por meio de um ponto de acesso multirregional

Criação de pontos de acesso multirregionais

Para criar um ponto de acesso multirregional no Amazon S3, faça o seguinte:

- Especifique nome do ponto de acesso multirregional.
- Selecione um bucket em cada Região da AWS na qual deseja atender às solicitações para o ponto de acesso multirregional.
- Defina as configurações de bloqueio de acesso público do Amazon S3 para o ponto de acesso multirregional.

Você fornece todas essas informações em uma solicitação de criação, que o Amazon S3 processa de forma assíncrona. O Amazon S3 fornece um token que você pode usar para monitorar o status da solicitação de criação assíncrona.

Solucione avisos de segurança, erros, avisos gerais e sugestões de AWS Identity and Access Management Access Analyzer antes de salvar a política. O IAM Access Analyzer executa verificações de política para validar sua política em relação à gramática das políticas e às práticas recomendadas do IAM. Essas verificações geram descobertas e fornecem recomendações práticas que ajudam a criar políticas que sejam funcionais e estejam em conformidade com as práticas recomendadas de segurança. Para saber mais sobre a validação de políticas usando o IAM Access Analyzer, consulte Validação de políticas do IAM Access Analyzer no Guia do usuário IAM. Para visualizar uma lista de avisos, erros e sugestões retornados pelo IAM Access Analyzer, consulte Referência de verificação de políticas do IAM Access Analyzer.

Quando você usa a API, a solicitação para criar um ponto de acesso multirregional é assíncrona. Quando você envia uma solicitação para criar um ponto de acesso multirregional, o Amazon S3 autoriza a solicitação de forma síncrona. Em seguida, retorna imediatamente um token que você pode usar para rastrear o progresso da solicitação de criação. Para obter mais informações sobre o

rastreamento de solicitações assíncronas para criar e gerenciar pontos de acesso multirregionais, consulte Usar pontos de acesso multirregionais com operações de API compatíveis.

Depois de criar o ponto de acesso multirregional, você pode criar uma política de controle de acesso para ele. Cada ponto de acesso multirregional pode ter uma política associada. Uma política de pontos de acesso multirregionais é uma política baseada em recursos que você pode usar para limitar o uso do ponto de acesso multirregional por recurso, usuário ou outras condições.

> **Note**
>
> Para que uma aplicação ou um usuário possa acessar um objeto por meio de um ponto de acesso multirregional, as duas políticas a seguir devem permitir a solicitação:
>
> - A política de acesso para o ponto de acesso multirregional
> - A política de acesso para o bucket subjacente que contém o objeto
>
> Quando as duas políticas são diferentes, a política mais restritiva tem precedência.
> Para simplificar o gerenciamento de permissões para pontos de acesso multirregionais, você pode delegar o controle de acesso do bucket para o ponto de acesso multirregional. Para ter mais informações, consulte the section called “Exemplos de políticas de pontos de acesso multirregionais”.

Usar um bucket com um ponto de acesso multirregional não altera o comportamento do bucket quando o bucket é acessado por meio do nome do bucket existente ou de um nome do recurso da Amazon (ARN). Todas as operações existentes no bucket continuarão a funcionar como antes. As restrições que você incluir em uma política de ponto de acesso multirregional se aplicam somente a solicitações feitas por meio desse ponto de acesso multirregional.

Você pode atualizar a política de um ponto de acesso multirregional depois de criá-lo, mas não pode excluir a política. No entanto, você pode atualizar a política de pontos de acesso multirregionais para negar todas as permissões.

Tópicos

- Regras para nomear pontos de acesso multirregionais do Amazon S3
- Regras para escolher buckets para pontos de acesso multirregionais do Amazon S3
- Criar um ponto de acesso multirregional do Amazon S3

- Bloqueio de acesso público de pontos de acesso multirregionais do Amazon S3
- Visualizar detalhes de configuração de pontos de acesso multirregionais do Amazon S3
- Excluir um ponto de acesso multirregional

Regras para nomear pontos de acesso multirregionais do Amazon S3

Ao criar um ponto de acesso multirregional, atribua a ele um nome, que é uma string escolhida. Não é possível alterar o nome do ponto de acesso multirregional depois que ele for criado. O nome deve ser exclusivo na Conta da AWS, e deve estar em conformidade com os requisitos de nomenclatura listados em Restrições e limitações de pontos de acesso multirregionais. Para ajudá-lo a identificar o ponto de acesso multirregional, use um nome que seja significativo para você, para sua organização ou que reflita o cenário.

Use esse nome ao chamar operações de gerenciamento de pontos de acesso multirregionais, como `GetMultiRegionAccessPoint` e `PutMultiRegionAccessPointPolicy`. O nome não é usado para enviar solicitações ao ponto de acesso multirregional e não precisa ser exposto a clientes que fazem solicitações utilizando o ponto de acesso multirregional.

Quando o Amazon S3 cria um ponto de acesso multirregional, ele atribui automaticamente um alias a ele. Este alias é uma string alfanumérica exclusiva que termina em `.mrap`. O alias é usado para construir o nome do host e o nome do recurso da Amazon (ARN) para um ponto de acesso multirregional. O nome totalmente qualificado também se baseia no alias do ponto de acesso multirregional.

Não é possível determinar o nome de um ponto de acesso multirregional de seu alias, portanto, você pode divulgar um alias sem o risco de expor o nome, a finalidade ou o proprietário do ponto de acesso multirregional. O Amazon S3 seleciona o alias para cada novo ponto de acesso multirregional, e o alias não pode ser alterado. Para obter mais informações sobre como lidar com um ponto de acesso multirregional, consulte Como fazer solicitações por meio de um ponto de acesso multirregional.

Os aliases de pontos de acesso multirregionais são exclusivos ao longo do tempo e não se baseiam no nome ou na configuração de um ponto de acesso multirregional. Se você criar um ponto de acesso multirregional, excluí-lo e criar outro com o mesmo nome e configuração, o segundo ponto de acesso multirregional terá um alias diferente do primeiro. Novos pontos de acesso multirregionais nunca podem ter o mesmo alias de um ponto de acesso multirregional anterior.

Regras para escolher buckets para pontos de acesso multirregionais do Amazon S3

Cada ponto de acesso multirregional está associado às regiões nas quais você deseja atender a solicitações. O ponto de acesso multirregional deve estar associado a exatamente um bucket em cada uma dessas regiões. Especifique o nome de cada bucket na solicitação para criar o ponto de acesso multirregional. Os buckets que são compatíveis com o ponto de acesso multirregional podem estar na mesma Conta da AWS que tem o ponto de acesso multirregional, ou em outras Contas da AWS.

Um único bucket pode ser usado por vários pontos de acesso multirregionais.

Important

- Você pode especificar os buckets associados a um ponto de acesso multirregional somente no momento em que o criou. Depois que ele é criado, você não pode adicionar, modificar ou remover buckets da configuração do ponto de acesso multirregional. Para alterar os buckets, você deve excluir todo o ponto de acesso multirregional e criar um novo.
- Não é possível excluir um bucket que faça parte de um ponto de acesso multirregional. Se quiser excluir um bucket anexado a um ponto de acesso multirregional, exclua primeiro o ponto de acesso multirregional.
- Se você adicionar um bucket de outra conta ao seu ponto de acesso multirregional, o proprietário do bucket também deverá atualizar a política do bucket para conceder permissões de acesso ao ponto de acesso multirregional. Caso contrário, o ponto de acesso multirregional não conseguirá recuperar dados desse bucket. Por ver exemplos de política que mostram como conceder esse acesso, consulte Exemplos de políticas de pontos de acesso multirregionais.
- Nem todas as regiões suportam pontos de acesso multirregionais. Para visualizar a lista de regiões compatíveis, consulte Restrições e limitações de pontos de acesso multirregionais.

Você pode criar regras de replicação para sincronizar dados entre buckets. Essas regras permitem que você copie automaticamente dados de buckets de origem para buckets de destino. Ter buckets conectados a um ponto de acesso multirregional não afeta o funcionamento da replicação. A configuração da replicação com pontos de acesso multirregionais é descrita em uma seção posterior.

> **Important**
>
> Quando você faz uma solicitação para um ponto de acesso multirregional, o ponto de acesso multirregional não está ciente dos conteúdos dos dados dos buckets no ponto de acesso multirregional. Portanto, o bucket que recebe a solicitação pode não conter os dados solicitados. Para criar conjuntos de dados consistentes nos buckets do Amazon S3 associados a um ponto de acesso multirregional, recomendamos que você configure a Replicação do S3 Entre Regiões Diferentes (CRR). Para ter mais informações, consulte Configurar a replicação para uso com pontos de acesso multirregionais.

Criar um ponto de acesso multirregional do Amazon S3

Os exemplos a seguir demonstram como criar um ponto de acesso multirregional usando o console do Amazon S3.

Uso do console do S3

Para criar um ponto de acesso multirregional

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação esquerdo, escolha Multi-Region Access Points (Pontos de acesso multirregionais).
3. Selecione Criar pontos de acesso multirregionais para começar a criar seu ponto de acesso multirregional.
4. Na página Ponto de acesso multirregional, forneça um nome para o ponto de acesso multirregional no campo Nome do ponto de acesso multirregional.
5. Selecione os buckets que serão associados a esse ponto de acesso multirregional. Você pode selecionar buckets que estão em sua conta ou buckets de outras contas.

> **Note**
>
> Você deve adicionar pelo menos um bucket de sua conta ou de outras. Além disso, esteja ciente de que os pontos de acesso multirregionais são compatíveis apenas com um bucket por Região da AWS. Portanto, você não pode adicionar dois buckets

da mesma região. Regiões da AWS que estão desativados por padrão não são compatíveis.

- Para adicionar um bucket que esteja em sua conta, selecione Adicionar buckets. Uma lista de todos os buckets em sua conta é exibida. Você pode pesquisar seu bucket pelo nome ou classificar os nomes dos buckets em ordem alfabética.
- Para adicionar um bucket de outra conta, selecione Adicionar bucket de outras contas. É necessário saber o nome exato do bucket e o ID da Conta da AWS, pois não é possível pesquisar nem procurar buckets em outras contas.

> **Note**
>
> Você deve inserir um ID da Conta da AWS e um nome de bucket válidos. O bucket também deve estar em uma região compatível, ou você encontrará um erro ao tentar criar seu ponto de acesso multirregional. Para ver a lista de regiões que são compatíveis com pontos de acesso multirregionais, consulte Restrições e limitações de pontos de acesso multirregionais.

6. (Opcional) Se você precisar remover um bucket adicionado, selecione Remover.

> **Note**
>
> Você não pode adicionar nem remover buckets desse ponto de acesso multirregional depois de terminar de criá-lo.

7. Em Block Public Access settings for this Multi-Region Access Point (Configurações do bloqueio de acesso público para este ponto de acesso multirregional), selecione as configurações de bloqueio de acesso público que você deseja aplicar ao ponto de acesso multirregional. Por padrão, todas as configurações de bloqueio de acesso público são habilitadas para novos pontos de acesso multirregionais. Recomendamos que você deixe todas as configurações ativadas, a menos que saiba que tem uma necessidade específica de desabilitar qualquer uma delas.

> **Note**
>
> Você não pode alterar as configurações de bloqueio de acesso público de um ponto de acesso multirregional após a criação dele. Portanto, se você quiser bloquear o acesso

público, certifique-se de que suas aplicações funcionem corretamente sem acesso público antes de criar um ponto de acesso multirregional.

8. Selecione Create Multi-Region Access Point (Criar ponto de acesso multirregional).

> **Important**
>
> Quando você adicionar um bucket de outra conta ao seu ponto de acesso multirregional, o proprietário do bucket também deverá atualizar a política do bucket para conceder permissões de acesso ao ponto de acesso multirregional. Caso contrário, o ponto de acesso multirregional não conseguirá recuperar dados desse bucket. Por ver exemplos de política que mostram como conceder esse acesso, consulte Exemplos de políticas de pontos de acesso multirregionais.

Uso do AWS CLI

Você pode usar a AWS CLI para criar um ponto de acesso multirregional. Ao criar o ponto de acesso multirregional, você deve fornecer todos os buckets aos quais ele oferecerá suporte. Você não pode adicionar buckets ao ponto de acesso multirregional depois de ele ter sido criado.

O exemplo a seguir cria um ponto de acesso multirregional com dois buckets usando a AWS CLI. Para usar esse exemplo de comando, substitua os *`user input placeholders`* por suas próprias informações.

```
aws s3control create-multi-region-access-point --account-id 111122223333 --details '{
        "Name": "simple-multiregionaccesspoint-with-two-regions",
        "PublicAccessBlock": {
            "BlockPublicAcls": true,
            "IgnorePublicAcls": true,
            "BlockPublicPolicy": true,
            "RestrictPublicBuckets": true
        },
        "Regions": [
            { "Bucket": "amzn-s3-demo-bucket1" },
            { "Bucket": "amzn-s3-demo-bucket2" }
        ]
    }' --region us-west-2
```

Bloqueio de acesso público de pontos de acesso multirregionais do Amazon S3

Cada ponto de acesso multirregional tem configurações distintas para o bloqueio de acesso público do Amazon S3. Essas configurações operam em conjunto com as configurações de bloqueio de acesso público para a Conta da AWS que possui o ponto de acesso multirregional e os buckets subjacentes.

Quando o Amazon S3 autoriza uma solicitação, ele aplica a combinação mais restritiva dessas configurações. Se as configurações de bloqueio de acesso público para qualquer um desses recursos (o ponto de acesso multirregional, o bucket subjacente ou a conta de proprietário) bloquearem o acesso para a ação ou o recurso solicitado, o Amazon S3 rejeitará a solicitação.

Recomendamos que você ative todas as configurações de bloqueio de acesso público, a menos que você tenha uma necessidade específica de desabilitar qualquer uma delas. Por padrão, todas as configurações de bloqueio de acesso público são habilitadas para um ponto de acesso multirregional. Se o bloqueio de acesso público estiver ativado, o ponto de acesso multirregional não poderá aceitar solicitações baseadas na Internet.

> **Important**
>
> Você não pode alterar as configurações de bloqueio de acesso público para um ponto de acesso multirregional após a criação do ponto de acesso.

Para obter mais informações sobre o bloqueio de acesso público do Amazon S3, consulte Bloquear o acesso público ao armazenamento do Amazon S3.

Visualizar detalhes de configuração de pontos de acesso multirregionais do Amazon S3

O exemplo a seguir demonstra como visualizar detalhes de configuração de pontos de acesso multirregionais usando o console do Amazon S3.

Uso do console do S3

Para criar um ponto de acesso multirregional

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.

2. No painel de navegação esquerdo, escolha Multi-Region Access Points (Pontos de acesso multirregionais).
3. Selecione o nome do ponto de acesso multirregional cujos detalhes de configuração você deseja visualizar.

   - A guia Propriedades lista todos os buckets associados ao seu ponto de acesso multirregional, a data de criação, o nome do recurso da Amazon (ARN) e o alias. A coluna ID da Conta da AWS também lista todos os buckets pertencentes a contas externas associadas ao seu ponto de acesso multirregional.
   - A guia Permissões lista as configurações de Bloqueio de Acesso Público que são aplicadas aos buckets associados a esse ponto de acesso multirregional. Você também pode visualizar a política de pontos de acesso multirregionais para o seu ponto de acesso multirregional, se tiver criado uma. O alerta de informações na página Permissões também lista todos os buckets (em sua conta e em outras) desse ponto de acesso multirregional que tem a configuração Acesso público está bloqueado ativada.
   - A guia Replicação e failover fornece uma visualização do mapa dos buckets associados ao seu ponto de acesso multirregional e das regiões nas quais eles residem. Se houver buckets de outra conta dos quais você não tenha permissão para extrair dados, a região será marcada em vermelho no mapa Resumo da replicação, indicando que está em uma Região da AWS com erros ao obter o status de replicação.

     > **Note**
     >
     > Para recuperar informações de status de replicação de um bucket em uma conta externa, o proprietário do bucket deve conceder a você a permissão `s3:GetBucketReplication` em sua política de bucket.

     Essa guia também fornece as métricas de replicação, as regras de replicação e os status de failover para as regiões que são usadas com seu ponto de acesso multirregional.

Uso do AWS CLI

Você pode usar a AWS CLI para visualizar os detalhes de configuração de um ponto de acesso multirregional.

O exemplo de AWS CLI a seguir obtém sua configuração de ponto de acesso multirregional atual. Para usar esse exemplo de comando, substitua os *user input placeholders* por suas próprias informações.

```
aws s3control get-multi-region-access-point --account-id 111122223333 --name amzn-s3-demo-bucket
```

Excluir um ponto de acesso multirregional

O procedimento a seguir explica como excluir um ponto de acesso multirregional usando o console do Amazon S3.

A exclusão de um ponto de acesso multirregional não exclui os buckets associados ao ponto de acesso multirregional, apenas o próprio ponto de acesso multirregional.

Uso do console do S3

Como excluir um ponto de acesso multirregional

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação esquerdo, escolha Multi-Region Access Points (Pontos de acesso multirregionais).
3. Selecione o botão de opção ao lado do nome do seu ponto de acesso multirregional.
4. Escolha Excluir.
5. Na caixa de diálogo Excluir ponto de acesso multirregional, insira o nome do bucket da AWS que você deseja excluir.

   > **Note**
   >
   > Insira um nome de bucket válido. Caso contrário, o botão Excluir será desativado.

6. Selecione Excluir para confirmar a exclusão de seu ponto de acesso multirregional.

Uso do AWS CLI

Você pode usar a AWS CLI para criar um ponto de acesso multirregional. A ação não exclui os buckets associados ao ponto de acesso multirregional, apenas o próprio ponto de acesso

multirregional. Para usar esse exemplo de comando, substitua os *user input placeholders* por suas próprias informações.

```
aws s3control delete-multi-region-access-point --account-id 123456789012 --details
 Name=example-multi-region-access-point-name
```

Configurar um ponto de acesso multirregional para uso com AWS PrivateLink

Você pode usar pontos de acesso multirregionais para direcionar o tráfego de solicitação do Amazon S3 entre Regiões da AWS. Cada endpoint global de ponto de acesso multirregional roteia o tráfego de solicitação de dados do Amazon S3 de várias fontes sem que você precise criar configurações de rede complexas com endoints separados. Essas fontes de tráfego de solicitação de dados incluem:

- Tráfego originado de uma nuvem privada virtual (VPC)
- Tráfego de datacenters on-premises que percorre o AWS PrivateLink
- Tráfego da Internet pública

Se você estabelecer uma conexão do AWS PrivateLink com um ponto de acesso multirregional do S3, poderá rotear solicitações do S3 para a AWS, ou entre várias Regiões da AWS, por meio de uma conexão privada usando uma arquitetura e configuração de rede simples. Ao usar o AWS PrivateLink, você não precisa configurar uma conexão de emparelhamento da VPC.

Tópicos

- Configurar um ponto de acesso multirregional para uso com AWS PrivateLink
- Remoção do acesso a um ponto de acesso multirregional de um endpoint da VPC

Configurar um ponto de acesso multirregional para uso com AWS PrivateLink

AWS PrivateLink fornece conectividade privada com o Amazon S3 usando endereços IP privados na nuvem privada virtual (VPC). Você pode provisionar um ou mais endpoints de interface dentro da VPC para se conectar aos pontos de acesso multirregionais do Amazon S3.

Você pode criar endpoints com.amazonaws.s3-global.accesspoint para pontos de acesso multirregionais por meio do AWS Management Console, da AWS CLI ou de AWS SDKs. Para saber mais sobre como configurar um endpoint de interface para o ponto de acesso multirregional, consulte Endpoints de VPC da interface no Guia do usuário da VPC.

Para fazer solicitações a um ponto de acesso multirregional por meio de endpoints de interface, siga estas etapas para configurar a VPC e o ponto de acesso multirregional.

Para configurar um ponto de acesso multirregional para usar com AWS PrivateLink

1. Crie ou tenha um endpoint de VPC apropriado que possa se conectar a pontos de acesso multirregionais. Para obter mais informações sobre a criação de endpoints de VPC, consulte Endpoints da VPC da interface no Guia do usuário da VPC.

   > **Important**
   >
   > Certifique-se de criar um endpoint com.amazonaws.s3-global.accesspoint. Outros tipos de endpoint não podem acessar pontos de acesso multirregionais.

   Depois que esse endpoint da VPC é criado, todas as solicitações de pontos de acesso multirregionais na VPC são roteadas por esse endpoint, se você tiver o DNS privado habilitado para o endpoint. Esta opção está ativada por padrão.
2. Se a política de ponto de acesso multirregional não oferecer suporte a conexões de endpoints da VPC, você precisará atualizá-la.
3. Verifique se as políticas de bucket individuais permitirão acesso aos usuários do ponto de acesso multirregional.

Lembre-se de que os pontos de acesso multirregionais funcionam roteando solicitações para buckets, não atendendo às próprias solicitações. É importante se lembrar disso porque o originador da solicitação deve ter permissões para o ponto de acesso multirregional e ter permissão para acessar os buckets individuais no ponto de acesso multirregional. Caso contrário, a solicitação pode ser encaminhada para um bucket onde o originador não tem permissões para atender à solicitação. Um ponto de acesso multirregional e os buckets associados podem pertencer à mesma conta ou a outra conta da AWS. No entanto, as VPCs de contas diferentes poderão usar um ponto de acesso multirregional se as permissões estiverem configuradas corretamente.

Por isso, a política de endpoint da VPC deve permitir o acesso ao ponto de acesso multirregional e a cada bucket subjacente que você deseja que possa atender às solicitações. Por exemplo, digamos que você tenha um ponto de acesso multirregional com o alias `mfzwi23gnjvgw.mrap`. É suportado por buckets `amzn-s3-demo-bucket1` e `amzn-s3-demo-bucket2`, todos pertencentes à conta `123456789012` da AWS. Nesse caso, a política de endpoint da VPC a seguir permitiria que

solicitações `GetObject` da VPC feitas para `mfzwi23gnjvgw.mrap` fossem atendidas por qualquer um dos buckets de suporte.

```
{
    "Version": "2012-10-17",
    "Statement": [
    {
        "Sid": "Read-buckets-and-MRAP-VPCE-policy",
        "Principal": "*",
        "Action": [
            "s3:GetObject"
        ],
        "Effect": "Allow",
        "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket1/*",
            "arn:aws:s3:::amzn-s3-demo-bucket2/*",
            "arn:aws:s3::123456789012:accesspoint/mfzwi23gnjvgw.mrap/object/*"
        ]
    }]
}
```

Conforme mencionado anteriormente, você também deve se certificar de que a política de pontos de acesso multirregionais esteja configurada para oferecer suporte ao acesso, por meio de um endpoint da VPC. Você não precisa especificar o endpoint da VPC que está solicitando acesso. O exemplo de política a seguir concederia acesso a qualquer solicitante que tentasse usar o ponto de acesso multirregional para as solicitações `GetObject`.

```
{
    "Version": "2012-10-17",
    "Statement": [
    {
        "Sid": "Open-read-MRAP-policy",
        "Effect": "Allow",
        "Principal": "*",
        "Action": [
            "s3:GetObject"
          ],
        "Resource": "arn:aws:s3::123456789012:accesspoint/mfzwi23gnjvgw.mrap/object/*"
    }]
}
```

E, claro, cada um dos buckets individuais precisaria de uma política para dar suporte ao acesso de solicitações enviadas por meio do endpoint da VPC. A política de exemplo a seguir concede acesso de leitura a usuários anônimos, o que incluiria solicitações feitas por meio do endpoint da VPC.

```
{
    "Version":"2012-10-17",
   "Statement": [
   {
       "Sid": "Public-read",
       "Effect":"Allow",
       "Principal": "*",
       "Action": "s3:GetObject",
       "Resource": [
           "arn:aws:s3:::amzn-s3-demo-bucket1",
           "arn:aws:s3:::amzn-s3-demo-bucket2/*"]
    }]
}
```

Para obter mais informações sobre como editar uma política de endpoint da VPC, consulte Controlar o acesso aos serviços com endpoints da VPC no Guia do usuário da VPC.

Remoção do acesso a um ponto de acesso multirregional de um endpoint da VPC

Se você tiver um ponto de acesso multirregional e quiser remover o acesso dele de um endpoint de interface, você deverá fornecer uma nova política de acesso para o ponto de acesso multirregional que impede o acesso para solicitações que chegam por meio de endpoints da VPC. No entanto, se os buckets em seu ponto de acesso multirregional forem compatíveis com solicitações por meio de endpoints da VPC, eles continuarão a oferecer compatibilidade com essas solicitações. Se quiser impedir esse suporte, você deverá atualizar também as políticas para os buckets. O fornecimento de uma nova política de acesso ao ponto de acesso multirregional só impede o acesso ao ponto de acesso multirregional, não a buckets subjacentes.

> **Note**
>
> Não é possível excluir uma política de acesso para um ponto de acesso multirregional. Para remover o acesso a um ponto de acesso multirregional, você deve fornecer uma nova política de acesso com o acesso modificado desejado.

Em vez de atualizar a política de acesso para o ponto de acesso multirregional, você pode atualizar as políticas de bucket para evitar solicitações por meio de endpoints da VPC. Nesse caso, os usuários ainda podem acessar o ponto de acesso multirregional por meio do endpoint da VPC. Porém, se a solicitação de ponto de acesso multirregional for encaminhada para um bucket no qual a política de bucket impeça o acesso, ela gerará uma mensagem de erro.

Como fazer solicitações por meio de um ponto de acesso multirregional

Assim como outros recursos, os pontos de acesso multirregionais do Amazon S3 têm nomes de recurso da Amazon (ARNs). Você pode usar esses ARNs para direcionar solicitações para pontos de acesso multirregionais usando a AWS Command Line Interface (AWS CLI), os AWS SDKs ou a API do Amazon S3. Você também pode usar esses ARNs para identificar pontos de acesso multirregionais nas políticas de controle de acesso. Um ARN de ponto de acesso multirregional não inclui nem divulga o nome do ponto de acesso multirregional. Para obter mais informações sobre ARNs, consulte Nomes de recurso da Amazon (ARNs) no Referência geral da AWS.

> **Note**
>
> O alias do ponto de acesso multirregional e o ARN não podem ser usados de forma intercambiável.

Os ARNs de ponto de acesso multirregional usam o seguinte formato:

`arn:aws:s3::`*`account-id`*`:accesspoint/`*`MultiRegionAccessPoint_alias`*

Veja a seguir alguns exemplos de ARNs de pontos de acesso multirregionais:

- `arn:aws:s3::123456789012:accesspoint/mfzwi23gnjvgw.mrap` representa o ponto de acesso multirregional com o alias `mfzwi23gnjvgw.mrap`, de propriedade da Conta da AWS `123456789012`.
- `arn:aws:s3::123456789012:accesspoint/*` representa todos os pontos de acesso multirregionais na conta `123456789012`. Este ARN corresponde a todos os pontos de acesso multirregionais para a conta `123456789012`, mas não corresponde a nenhum Ponto de Acesso Regional Amazon S3 porque o ARN não inclui uma Região da AWS. Por outro lado, o ARN `arn:aws:s3:us-west-2:123456789012:accesspoint/*` corresponde a todos os Pontos de Acesso Regionais Amazon S3 na região `us-west-2` para a conta `123456789012`, mas não corresponde a nenhum ponto de acesso multirregional.

Os ARNs para objetos que são acessados por meio de um ponto de acesso multirregional usam o seguinte formato:

`arn:aws:s3::account_id:accesspoint/MultiRegionAccessPoint_alias//key`

Assim como no caso de ARNs de pontos de acesso multirregionais, os ARNs para objetos acessados por meio de pontos de acesso multirregionais não incluem uma Região da AWS. Aqui estão alguns exemplos.

- `arn:aws:s3::123456789012:accesspoint/mfzwi23gnjvgw.mrap//-01` representa o `-01`, acessado por meio do ponto de acesso multirregional com o alias `mfzwi23gnjvgw.mrap`, de propriedade da conta `123456789012`.
- `arn:aws:s3::123456789012:accesspoint/mfzwi23gnjvgw.mrap//*` representa todos os objetos que podem ser acessados por meio do ponto de acesso multirregional com alias `mfzwi23gnjvgw.mrap`, na conta `123456789012`.
- `arn:aws:s3::123456789012:accesspoint/mfzwi23gnjvgw.mrap//-01/finance/*` representa todos os objetos que podem ser acessados sob o `-01/finance/` para o ponto de acesso multirregional com o alias `mfzwi23gnjvgw.mrap`, na conta `123456789012`.

Nomes de host do ponto de acesso multirregional

Você pode acessar dados no Amazon S3 por meio de um ponto de acesso multirregional usando o nome de host do ponto de acesso multirregional. As solicitações podem ser direcionadas para esse nome de host pela Internet pública. Se você tiver configurado um ou mais gateways da Internet para o ponto de acesso multirregional, as solicitações também poderão ser direcionadas de uma nuvem privada virtual (VPC) para esse nome de host. Para obter mais informações sobre a criação de endpoints de interface da VPC para usar com pontos de acesso multirregionais, consulte Configurar um ponto de acesso multirregional para uso com AWS PrivateLink.

Para fazer solicitações por meio de um ponto de acesso multirregional de uma VPC usando um endpoint da VPC, use AWS PrivateLink. Ao fazer solicitações para um ponto de acesso multirregional usando o AWS PrivateLink, você não pode usar diretamente um nome de SISTEMA DE NOMES DE DOMÍNIO (DNS) regional específico do endpoint que termine com *`region`*`.vpce.amazonaws.com`. Este nome de host não terá um certificado associado a ele, portanto ele não poderá ser usado diretamente. Você ainda pode usar o nome de SISTEMA DE NOMES DE DOMÍNIO (DNS) público do endpoint da VPC como um destino de `CNAME` ou `ALIAS`. Como alternativa, você pode ativar o SISTEMA DE NOMES DE DOMÍNIO

(DNS) privado no endpoint e usar o nome de SISTEMA DE NOMES DE DOMÍNIO (DNS) *MultiRegionAccessPoint_alias*.accesspoint.s3-global.amazonaws.com do ponto de acesso multirregional padrão, conforme descrito nesta seção.

Quando você faz solicitações à API para operações de dados do Amazon S3 (por exemplo, GetObject) por meio de um ponto de acesso multirregional, o nome de host para a solicitação é o seguinte:

MultiRegionAccessPoint_alias.accesspoint.s3-global.amazonaws.com

Por exemplo, para fazer uma solicitação GetObject por meio do ponto de acesso multirregional com alias mfzwi23gnjvgw.mrap, faça uma solicitação para o nome de host mfzwi23gnjvgw.mrap.accesspoint.s3-global.amazonaws.com. A parte s3-global do nome de host indica que esse nome de host não é para uma região específica.

Fazer solicitações por meio de um ponto de acesso multirregional é semelhante a fazer solicitações por meio de um ponto de acesso de região única. No entanto, é importante estar ciente das seguintes diferenças:

- Os ARNs de pontos de acesso multirregionais não incluem uma Região da AWS. Eles seguem o formato arn:aws:s3::*account-id*:accesspoint/*MultiRegionAccessPoint_alias*.
- Para solicitações feitas por meio de APIs (essas solicitações não exigem o uso de um ARN), os pontos de acesso multirregionais usam um esquema de endpoint diferente. O esquema é *MultiRegionAccessPoint_alias*.accesspoint.s3-global.amazonaws.com, por exemplo, mfzwi23gnjvgw.mrap.accesspoint.s3-global.amazonaws.com. Observe as diferenças em comparação com um ponto de acesso de região única:
  - Os nomes de host de pontos de acesso multirregionais usam seu alias, não o nome do ponto de acesso multirregional.
  - Os nomes de host de pontos de acesso multirregionais não incluem o ID da Conta da AWS do proprietário.
  - Os nomes de host de pontos de acesso multirregionais não incluem uma Região da AWS.
  - Os nomes de host do ponto de acesso multirregional incluem s3-global.amazonaws.com, em vez de s3.amazonaws.com.
- As solicitações devem de pontos de acesso multirregionais precisam ser assinadas usando o Signature Version 4A (SigV4A). Quando você usa os AWS SDKs, o SDK converte automaticamente uma assinatura SigV4 em SigV4A. Portanto, verifique se seu AWS SDK oferece compatibilidade com o SigV4A como a implementação de assinatura usada para assinar as

solicitações globais da Região da AWS. Para obter mais informações sobre o SigV4A, consulte Assinar solicitações de API da AWS na Referência geral da AWS.

Pontos de acesso multirregionais e Amazon S3 Transfer Acceleration

O Amazon S3 Transfer Acceleration é um recurso que permite transferências de dados rápidas para os buckets. A Aceleração de Transferência é configurada em cada bucket. Para obter mais informações sobre o Transfer Acceleration, consulte Configurar transferências de arquivos rápidas e seguras usando o Amazon S3 Transfer Acceleration.

Os pontos de acesso multirregionais usam um mecanismo de transferência acelerada semelhante ao da Aceleração de Transferência para enviar objetos grandes pela rede da AWS. Por isso, você não precisa usar a Aceleração de Transferência ao enviar solicitações por meio de um ponto de acesso multirregional. Essa performance de transferência aprimorada é incorporada automaticamente ao ponto de acesso multirregional.

Tópicos

- Permissões
- Restrições e limitações de pontos de acesso multirregionais
- Roteamento de solicitação de pontos de acesso multirregionais
- Controles de failover para pontos de acesso multirregionais do Amazon S3.
- Configurar a replicação para uso com pontos de acesso multirregionais
- Usar pontos de acesso multirregionais com operações de API compatíveis
- Monitoramento e registro de solicitações feitas por meio de um ponto de acesso multirregional para recursos subjacentes

Permissões

Os pontos de acesso multirregionais do Amazon S3 podem simplificar o acesso a dados para buckets do Amazon S3 em várias Regiões da AWS. Os pontos de acesso multirregionais são endpoints globais que você pode usar para realizar operações de objeto de acesso a dados no Amazon S3, como `GetObject` e `PutObject`. Cada ponto de acesso multirregional pode ter permissões e controles de rede distintos para todas as solicitações feitas por meio do endpoint global.

Cada ponto de acesso multirregional também pode impor uma política de acesso personalizada que funciona em conjunto com a política de bucket anexada ao bucket subjacente. Para que uma solicitação entre contas seja bem-sucedida, as seguintes políticas devem permitir a operação:

- A política de ponto de acesso multirregional
- A política subjacente do AWS Identity and Access Management (IAM)
- A política de bucket subjacente (para onde a solicitação é encaminhada)

> **Note**
>
> Para solicitações na mesma conta, somente a política do IAM subjacente, que concede o acesso apropriado, é necessária.

Você pode configurar qualquer política de ponto de acesso multirregional para aceitar solicitações somente de usuários ou grupos específicos do IAM. Para obter um exemplo de como fazer isso, consulte o Exemplo 2 em the section called “Exemplos de políticas de pontos de acesso multirregionais”. Você pode configurar a política de ponto de acesso multirregional para aceitar solicitações somente de uma nuvem privada virtual (VPC) para restringir o acesso a dados do Amazon S3 a uma rede privada.

Por exemplo, suponha que você faça uma solicitação de `GetObject` por meio de um ponto de acesso multirregional usando um usuário chamado `AppDataReader` em sua conta da AWS. Para ajudar a garantir que a solicitação não será negada, o usuário `AppDataReader` deve receber a permissão `s3:GetObject` do ponto de acesso multirregional e de cada bucket subjacente ao ponto de acesso multirregional. O `AppDataReader` não será capaz de recuperar dados de todo bucket que não conceder essa permissão.

> **Important**
>
> Delegar o controle de acesso de um bucket a uma política de ponto de acesso multirregional não altera o comportamento do bucket quando o bucket é acessado diretamente por meio de seu nome ou do nome do recurso da Amazon (ARN). Todas as operações feitas diretamente no bucket continuarão a funcionar como antes. As restrições que você incluir em uma política de ponto de acesso multirregional se aplicam somente às solicitações feitas por meio desse ponto de acesso multirregional.

Como gerenciar o acesso público a um ponto de acesso multirregional

Os pontos de acesso multirregionais oferecem suporte a configurações de bloqueio de acesso público para cada ponto de acesso multirregional. Ao criar um ponto de acesso multirregional, você pode especificar configurações do bloqueio de acesso público que se aplicam a esse ponto de acesso multirregional.

> **Note**
>
> Todas as configurações de bloqueio de acesso público ativadas em Bloquear acesso público para esta conta (em sua própria conta) ou Bloquear configurações públicas para buckets externos ainda se aplicam, mesmo que as configurações independentes de bloqueio de acesso público para seu ponto de acesso multirregional estejam desativadas.

Para qualquer solicitação feita por meio de um ponto de acesso multirregional, o Amazon S3 avaliará as configurações de Bloqueio de Acesso Público para:

- O ponto de acesso multirregional
- Os buckets subjacentes (incluindo buckets externos)
- A conta que detém o ponto de acesso multirregional
- A conta que detém os buckets subjacentes (incluindo contas externas)

Se qualquer uma dessas configurações indicar que a solicitação deve ser bloqueada, o Amazon S3 rejeitará a solicitação. Para obter mais informações sobre o recurso de bloqueio de acesso público do Amazon S3, consulte Bloquear o acesso público ao armazenamento do Amazon S3.

> **Important**
>
> Por padrão, todas as configurações de Bloqueio de Acesso Público são habilitadas para pontos de acesso multirregionais. Você deve desativar explicitamente todas as configurações que não deseja aplicar a um ponto de acesso multirregional.
> Você não pode alterar as configurações de bloqueio de acesso público de um ponto de acesso multirregional após a criação dele.

Visualizar configurações de Bloqueio de Acesso Público para um ponto de acesso multirregional

Como visualizar as configurações de Bloqueio de Acesso Público para um ponto de acesso multirregional

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação esquerdo, escolha Multi-Region Access Points (Pontos de acesso multirregionais).
3. Escolha o nome do ponto de acesso multirregional que você deseja revisar.
4. Escolha a aba Permissões.
5. Em Block Public Access settings for this Multi-Region Access Point (Configurações do Bloqueio de Acesso Público para este ponto de acesso multirregional), revise as configurações de Bloqueio de Acesso Público que você deseja aplicar ao ponto de acesso multirregional.

> **Note**
>
> Não é possível editar as configurações de Bloqueio de Acesso Público após a criação do ponto de acesso multirregional. Portanto, se você quiser bloquear o acesso público, certifique-se de que suas aplicações funcionem corretamente sem acesso público antes de criar um ponto de acesso multirregional.

Como usar uma política de ponto de acesso multirregional

O exemplo de política de ponto de acesso multirregional a seguir concede a um usuário do IAM acesso para listar e baixar arquivos do ponto de acesso multirregional. Para usar esse exemplo de política, substitua os *`user input placeholders`* por suas próprias informações.

```
{
  "Version":"2012-10-17",
  "Statement":[
     {
        "Effect":"Allow",
        "Principal":{
           "AWS":"arn:aws:iam::123456789012:user/JohnDoe"
        },
        "Action":[
```

```
            "s3:ListBucket",
            "s3:GetObject"
         ],
         "Resource":[
            "arn:aws:s3::111122223333:accesspoint/MultiRegionAccessPoint_alias",
            "arn:aws:s3::111122223333:accesspoint/MultiRegionAccessPoint_alias/object/
*"
         ]
      }
   ]
}
```

Para associar sua política de ponto de acesso multirregional ao ponto de acesso multirregional especificado usando a AWS Command Line Interface (AWS CLI), use o comando `put-multi-region-access-point-policy` a seguir. Para usar esse exemplo de comando, substitua os *`user input placeholders`* por suas próprias informações. Cada ponto de acesso multirregional pode ter somente uma política, portanto uma solicitação feita para a ação `put-multi-region-access-point-policy` substitui qualquer política existente associada ao ponto de acesso multirregional especificado.

AWS CLI

```
aws s3control put-multi-region-access-point-policy
--account-id 111122223333
--details { "Name": "amzn-s3-demo-bucket-MultiRegionAccessPoint",
 "Policy": "{ \"Version\": \"2012-10-17\", \"Statement\": { \"Effect\":
 \"Allow\", \"Principal\": { \"AWS\": \"arn:aws:iam::111122223333:root
\" }, \"Action\": [\"s3:ListBucket\", \"s3:GetObject\"], \"Resource\":
 [ \"arn:aws:s3::111122223333:accesspoint/MultiRegionAccessPoint_alias",
 \"arn:aws:s3::111122223333:accesspoint/MultiRegionAccessPoint_alias/object/*
\" ] } }" }
```

Para consultar os resultados da operação anterior, use o seguinte comando:

AWS CLI

```
aws s3control describe-multi-region-access-point-operation
--account-id 111122223333
--request-token-arn requestArn
```

Para recuperar sua política de ponto de acesso multirregional, use o seguinte comando:

AWS CLI

```
aws s3control get-multi-region-access-point-policy
--account-id 111122223333
--name=amzn-s3-demo-bucket-MultiRegionAccessPoint
```

Editar a política de ponto de acesso multirregional

A política de ponto de acesso multirregional (escrita em JSON) fornece acesso de armazenamento aos buckets do Amazon S3 que são usados com esse ponto de acesso multirregional. Você pode permitir ou negar que entidades principais específicas realizem várias ações em seu ponto de acesso multirregional. Quando uma solicitação é roteada para um bucket por meio do ponto de acesso multirregional, as políticas de acesso tanto do ponto de acesso multirregional como do bucket se aplicam. A política de acesso mais restritiva sempre tem precedência.

> **Note**
>
> Se um bucket contiver objetos pertencentes a outras contas, a política de ponto de acesso multirregional não se aplicará aos objetos que pertencem a outras Contas da AWS.

Depois que você aplicar uma política de ponto de acesso multirregional, esta política não poderá ser excluída. Você poderá editar a política ou criar uma política que substitua a existente.

Como editar a política de ponto de acesso multirregional

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação esquerdo, escolha Multi-Region Access Points (Pontos de acesso multirregionais).
3. Escolha o nome do ponto de acesso multirregional para o qual deseja editar a política.
4. Escolha a aba Permissões.
5. Role para baixo até a seção Multi-Region Access Point policy (Política de ponto de acesso multirregional). Escolha Edit (Editar) para atualizar a política (em JSON).

6. A página Edit Multi-Region Access Point policy (Editar política de ponto de acesso multirregional) é exibida. Você pode inserir a política diretamente no campo de texto ou escolher Add statement (Adicionar instrução) para selecionar elementos de política em uma lista suspensa.

> **Note**
>
> O console exibe automaticamente o nome do recurso da Amazon (ARN) do ponto de acesso multirregional, que você pode usar na política. Para conferir exemplos de políticas de pontos de acesso multirregionais, consulte the section called “Exemplos de políticas de pontos de acesso multirregionais”.

Exemplos de políticas de pontos de acesso multirregionais

Os pontos de acesso multirregionais do Amazon S3 são compatíveis com políticas de recursos do AWS Identity and Access Management (IAM). Você pode usar essas políticas para controlar o uso do ponto de acesso multirregional por recurso, usuário ou outras condições. Para que uma aplicação ou um usuário possa acessar objetos por meio de um ponto de acesso multirregional, tanto o ponto de acesso multirregional quanto o bucket subjacente devem permitir o mesmo acesso.

Para permitir o mesmo acesso ao ponto de acesso multirregional e ao bucket subjacente, faça o seguinte:

- (Recomendado) Para simplificar os controles de acesso ao usar um ponto de acesso multirregional do Amazon S3, delegue o controle de acesso do bucket do Amazon S3 ao ponto de acesso multirregional. Para obter um exemplo de como fazer isso, consulte o Exemplo 1 desta seção.
- Adicione as mesmas permissões contidas na política de ponto de acesso multirregional à política do bucket subjacente.

> **Important**
>
> Delegar o controle de acesso de um bucket a uma política de ponto de acesso multirregional não altera o comportamento do bucket quando o bucket é acessado diretamente por meio de seu nome ou do nome do recurso da Amazon (ARN). Todas as operações feitas diretamente no bucket continuarão a funcionar como antes. As restrições que você incluir em uma política de ponto de acesso multirregional se aplicam somente às solicitações feitas por meio desse ponto de acesso multirregional.

Example 1: Delegar acesso a pontos de acesso multirregionais específicos em sua política de bucket (para a mesma conta ou por outras contas)

O exemplo de política de bucket a seguir concede acesso total a um ponto de acesso multirregional específico. Isso significa que todo acesso a esse bucket é controlado pelas políticas anexadas ao ponto de acesso multirregional. Recomendamos configurar seus buckets dessa maneira para todos os casos de uso que não exigem acesso direto ao bucket. Você pode usar essa estrutura de política de bucket para pontos de acesso multirregionais na mesma conta ou em outra.

```
{
    "Version": "2012-10-17",
    "Statement" : [
    {
        "Effect": "Allow",
        "Principal" : { "AWS": "*" },
        "Action" : "*",
        "Resource" : [ "Bucket ARN", "Bucket ARN/*"],
        "Condition": {
            "StringEquals" : { "s3:DataAccessPointArn" : "MultiRegionAccessPoint_ARN" }
        }
    }]
}
```

> **Note**
>
> Se houver vários pontos de acesso multirregionais aos quais você está concedendo acesso, liste cada ponto de acesso multirregional.

Example 2: Conceder acesso a um ponto de acesso multirregional em sua política de ponto de acesso multirregional

A política de ponto de acesso multirregional a seguir permite que a conta *123456789012* liste e leia os objetos contidos no ponto de acesso multirregional definido pelo *MultiRegionAccessPoint_ARN*.

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
```

```
        "Effect": "Allow",
        "Principal": {
           "AWS":"arn:aws:iam::123456789012:user/JohnDoe"
        },
        "Action":[
           "s3:ListBucket",
           "s3:GetObject"
        ],
        "Resource":[
           "MultiRegionAccessPoint_ARN",
           "MultiRegionAccessPoint_ARN/object/*"
        ]
     }
  ]
}
```

Example 3: Política de ponto de acesso mutirregional que permite a listagem de buckets

A política de ponto de acesso multirregional a seguir permite que a conta *123456789012* liste os objetos contidos no ponto de acesso multirregional definido pelo *MultiRegionAccessPoint_ARN*.

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
       "Effect": "Allow",
       "Principal": {
        "AWS": "arn:aws:iam::123456789012:user/JohnDoe"
        },
        "Action": "s3:ListBucket",
        "Resource": "MultiRegionAccessPoint_ARN"
       }
    ]
}
```

Restrições e limitações de pontos de acesso multirregionais

Os pontos de acesso multirregionais do Amazon S3 têm as seguintes restrições e limitações:

- Nomes de pontos de acesso multirregionais:
  - Devem ser exclusivos em uma única conta da AWS
  - Devem começar com um número ou uma letra minúscula

  - Devem conter entre 3 e 50 caracteres
  - Não pode começar nem terminar com hífen (-)
  - Não pode conter sublinhados (_), letras maiúsculas ou pontos (.)
  - Não podem ser editados depois que são criados
- Os aliases de pontos de acesso multirregionais são gerados pelo Amazon S3 e não podem ser editados nem reutilizados.
- Não é possível acessar dados por meio de um ponto de acesso multirregional usando endpoints de gateway. No entanto, é possível acessar dados por meio de um ponto de acesso multirregional usando endpoints de interface. Para usar AWS PrivateLink, você deve criar endpoints da VPC. Para obter mais informações, consulte Configurar um ponto de acesso multirregional para uso com AWS PrivateLink.
- Para usar pontos de acesso multirregionais com o Amazon CloudFront, você deve configurar o ponto de acesso multirregional como um tipo de distribuição `Custom Origin`. Para obter mais informações sobre vários tipos de origem, consulte Usar várias origens com distribuições do CloudFront. Para obter mais informações sobre como usar pontos de acesso multirregionais com o Amazon CloudFront, consulte Criar uma aplicação ativa-ativa baseada em proximidade em várias regiões no Blog de armazenamento da AWS.
- Requisitos mínimos para pontos de acesso multirregionais:
  - Transport Layer Security (TLS) v1.2

    > **Note**
    >
    > Não há suporte para Transport Layer Security (TLS) v1.3.

  - Signature versão 4 (SigV4A)

    Os pontos de acesso multirregionais são compatíveis com o Signature versão 4A. Esta versão do SigV4 permite que as solicitações sejam assinadas para várias Regiões da AWS. Esse recurso é útil em operações de API que podem resultar em acesso a dados de uma das várias regiões. Ao usar um AWS SDK, forneça suas credenciais, e as solicitações para pontos de acesso multirregionais usarão o Signature Version 4A sem configuração adicional. Verifique a compatibilidade de AWS SDKs com o algoritmo SigV4A. Para obter mais informações sobre o SigV4A, consulte Assinar solicitações de API da AWS na Referência geral da AWS.

> **Note**
>
> Para usar o SigV4A com credenciais de segurança temporárias (por exemplo, ao usar perfis do AWS Identity and Access Management [IAM]), solicite as credenciais temporárias de um endpoint regional do AWS Security Token Service (AWS STS). Se você solicitar credenciais temporárias do endpoint global do AWS STS (`sts.amazonaws.com`), primeiro defina a compatibilidade regional dos tokens de sessão para que o endpoint global seja válido em todas as Regiões da AWS. Para ter mais informações, consulte Gerenciar o AWS STS em uma Região da AWS no Guia do usuário do IAM.

- Os pontos de acesso multirregionais não são compatíveis com solicitações anônimas.
- Limitações do ponto de acesso multirregional:
  - O IPv6 não é compatível.
  - Não há suporte para buckets do Amazon S3 on Outposts.
  - Os pontos de acesso multirregionais permitem operações de cópia que os utilizem somente como destino ao usar o ARN do ponto de acesso multirregional.
  - O recurso Operações em Lote do S3 não é compatível.
- Alguns AWS SDKs não são compatíveis. Para confirmar quais AWS SDKs são compatíveis com pontos de acesso multirregionais, consulte Compatibilidade com AWS SDKs.
- As cotas de serviço para pontos de acesso multirregionais são as seguintes:
  - Há no máximo 100 pontos de acesso multirregionais por conta.
  - Há um limite de 17 regiões para um único ponto de acesso multirregional.
- Depois de criar um ponto de acesso multirregional, você não pode adicionar, modificar nem remover buckets da configuração do ponto de acesso multirregional. Para alterar os buckets, você deve excluir todo o ponto de acesso multirregional e criar um novo. Se um bucket entre contas em seu ponto de acesso multirregional for excluído, a única maneira de reconectar esse bucket é recriar o bucket usando o mesmo nome e região nessa conta.
- Os buckets subjacentes (na mesma conta) que são usados em um ponto de acesso multirregional só podem ser excluídos após a exclusão de um ponto de acesso multirregional.
- Todas as solicitações do ambiente de gerenciamento para criar ou manter pontos de acesso multirregionais devem ser encaminhadas para a região `US West (Oregon)`. Com relação a solicitações de plano de dados de pontos de acesso multirregionais, as regiões não precisam ser

especificadas. Para obter uma lista de operações do ambiente de gerenciamento do Amazon S3, consulte a S3 API Reference na Referência de API do Amazon Simple Storage Service.

- Para o ambiente de gerenciamento de failover do ponto de acesso multirregional, as solicitações devem ser encaminhadas para uma das cinco regiões compatíveis:
  - US East (N. Virginia)
  - US West (Oregon)
  - Asia Pacific (Sydney)
  - Asia Pacific (Tokyo)
  - Europe (Ireland)
- Seu ponto de acesso multirregional só é compatível com buckets das seguintes Regiões da AWS:
  - US East (N. Virginia)
  - US East (Ohio)
  - US West (N. California)
  - US West (Oregon)
  - Asia Pacific (Mumbai)
  - Asia Pacific (Osaka)
  - Asia Pacific (Seoul)
  - Asia Pacific (Singapore)
  - Asia Pacific (Sydney)
  - Asia Pacific (Tokyo)
  - Canada (Central)
  - Europe (Frankfurt)
  - Europe (Ireland)
  - Europe (London)
  - Europe (Paris)
  - Europe (Stockholm)
  - South America (São Paulo)

Roteamento de solicitação de pontos de acesso multirregionais

Quando você faz uma solicitação por meio de um ponto de acesso multirregional, o Amazon S3 determina qual dos buckets associados ao ponto de acesso multirregional está mais próximo. Em seguida, o Amazon S3 direciona a solicitação para esse bucket, independentemente da região da AWS no qual está localizado.

Depois que o ponto de acesso multirregional rotear a solicitação para o bucket mais próximo, o Amazon S3 processará a solicitação como se você a tivesse feito diretamente para esse bucket. Pontos de acesso multirregionais não estão cientes do conteúdo de dados de um bucket do Amazon S3. Portanto, o bucket que recebe a solicitação pode não conter os dados solicitados. Para criar conjuntos de dados consistentes nos buckets do Amazon S3 associados a um ponto de acesso multirregional, você pode configurar a Replicação do S3 Entre Regiões Diferentes (CRR). Em seguida, qualquer bucket pode cumprir a solicitação com êxito.

O Amazon S3 direciona solicitações de pontos de acesso multirregionais de acordo com as seguintes regras:

- O Amazon S3 otimiza as solicitações para que sejam atendidas de acordo com a proximidade. Ele examina os buckets compatíveis com o ponto de acesso multirregional e repassa a solicitação para o bucket mais próximo.
- Se a solicitação especificar um recurso existente (por exemplo, `GetObject`), o Amazon S3 não considera o nome do objeto ao atender a solicitação. Isso significa que mesmo se houver um objeto em um bucket no ponto de acesso multirregional, sua solicitação será roteada para um bucket que não contém o objeto. Essa situação gerará uma mensagem de erro 404 retornada ao cliente.

  Para evitar erros 404, recomendamos que você configure a Replicação do S3 Entre Regiões Diferentes (CRR) para seus buckets. A replicação ajuda a resolver o problema potencial quando o objeto desejado estiver em um bucket no ponto de acesso multirregional, mas ele não está localizado no bucket específico para o qual sua solicitação foi roteada. Para obter mais informações sobre como configurar a replicação, consulte Configurar a replicação para uso com pontos de acesso multirregionais.

  Para garantir que suas solicitações sejam atendidas usando os objetos específicos que você deseja, recomendamos que você ative o versionamento do bucket e inclua IDs de versão em suas solicitações. Essa abordagem ajuda a garantir que você tenha a versão correta do objeto que você está procurando. Buckets habilitados para versionamento também podem ajudar a recuperar

objetos de uma substituição acidental. Para ter mais informações, consulte Usar o versionamento em buckets do S3.

- Se a solicitação for para criar um recurso (por exemplo, `PutObject` ou `CreateMultipartUpload`), o Amazon S3 atenderá à solicitação usando o bucket mais próximo. Por exemplo, pense em uma empresa de vídeo que queira oferecer compatibilidade com uploads de vídeo de qualquer lugar do mundo. Quando um usuário faz uma solicitação PUT para o ponto de acesso multirregional, o objeto é colocado no bucket mais próximo. Para então disponibilizar o vídeo carregado para outras pessoas ao redor do mundo para download com a menor latência, você pode usar a CRR com replicação bidirecional. O uso de CRR com replicação bidirecional mantém o conteúdo de todos os buckets associados ao ponto de acesso multirregional sincronizado. Para ter mais informações sobre o uso de replicação com pontos de acesso multirregionais, consulte Configurar a replicação para uso com pontos de acesso multirregionais.

Controles de failover para pontos de acesso multirregionais do Amazon S3.

Com os controles de failover para pontos de acesso multirregionais do Amazon S3, você pode manter a continuidade dos negócios durante interrupções no tráfego regional e, ao mesmo tempo, oferecer às aplicações uma arquitetura multirregional para atender às necessidades de conformidade e redundância. Se seu tráfego regional for interrompido, você poderá usar controles de failover para pontos de acesso multirregionais para selecionar quais Regiões da AWS por trás de um ponto de acesso multirregional do Amazon S3 vão processar as solicitações de acesso e armazenamento de dados.

Para oferecer suporte a failover, você pode configurar seu ponto de acesso multirregional em uma configuração ativa-passiva, com tráfego fluindo para a região ativa em condições normais e uma região passiva em espera para failover.

Por exemplo, para realizar o failover para uma Região da AWS de sua escolha, o tráfego é transferido da região primária (ativa) para a região secundária (passiva). Em uma configuração ativa-passiva como essa, um bucket é ativo e aceita tráfego, enquanto o outro bucket é passivo e não aceita tráfego. O bucket passivo é usado para recuperação de desastres. Ao iniciar o failover, todo o tráfego (como solicitações `GET` ou `PUT`) é direcionado para o bucket ativo (em uma região) e para longe do bucket passivo (em outra região).

Se você tiver a Replicação do S3 Entre Regiões Diferentes (CRR) habilitada com regras de replicação bidirecional, poderá manter seus buckets sincronizados durante um failover. Além disso,

se você tiver a CRR habilitada em uma configuração ativa-ativa, os pontos de acesso multirregionais do Amazon S3 também poderão buscar dados do local do bucket mais próximo, o que melhora a performance da aplicação.

Suporte do Região da AWS

Com os controles de failover para pontos de acesso multirregionais do Amazon S3, seus buckets do S3 podem estar em qualquer uma das 17 regiões em que os pontos de acesso multirregionais são compatíveis. Você pode iniciar o failover entre duas regiões quaisquer por vez.

> **Note**
>
> Embora o failover seja iniciado apenas entre duas regiões por vez, você pode atualizar separadamente os status de roteamento para várias regiões ao mesmo tempo em seu ponto de acesso multirregional.

Os tópicos a seguir demonstram como usar e gerenciar os controles de failover para pontos de acesso multirregionais do Amazon S3.

Tópicos

- Estados de roteamento de pontos de acesso multirregionais do Amazon S3
- Como usar controles de failover para pontos de acesso multirregionais do Amazon S3
- Erros de controles de failover para pontos de acesso multirregionais do Amazon S3

Estados de roteamento de pontos de acesso multirregionais do Amazon S3

Sua configuração de failover para pontos de acesso multirregionais do Amazon S3 determina o status de roteamento das Regiões da AWS que são usadas com o ponto de acesso multirregional. Você pode configurar seu ponto de acesso multirregional do Amazon S3 para que esteja em um estado ativo-ativo ou ativo-passivo.

- Ativo-ativo: em uma configuração ativa-ativa, todas as solicitações são enviadas automaticamente para a Região da AWS mais próxima em seu ponto de acesso multirregional. Depois que o ponto de acesso multirregional for configurado para ficar em um estado ativo-ativo, todas as regiões poderão receber tráfego. Se ocorrer interrupção do tráfego em uma configuração ativa-ativa, o tráfego da rede será automaticamente redirecionado para uma das regiões ativas.

- Ativo-passivo: em uma configuração ativa-passiva, as regiões ativas em seu ponto de acesso multirregional recebem tráfego e as passivas não. Se você pretende usar os controles de failover do S3 para iniciar um failover em uma situação de desastre, configure os pontos de acesso multirregionais em um estado ativo-passivo enquanto estiver testando e realizando o planejamento de recuperação de desastres.

Como usar controles de failover para pontos de acesso multirregionais do Amazon S3

Esta seção explica como gerenciar e usar os controles de failover para pontos de acesso multirregionais do Amazon S3 usando o AWS Management Console.

Há dois controles de failover na seção Failover configuration (Configuração de failover) na página de detalhes do ponto de acesso multirregional no AWS Management Console: Edit routing status (Editar status de roteamento) e Failover. Você pode usar esses controles da seguinte maneira:

- Edit routing status (Editar status de roteamento): você pode editar manualmente os status de roteamento de até 17 Regiões da AWS em uma única solicitação para seu ponto de acesso multirregional escolhendo Edit routing status (Editar status de roteamento). Você pode usar a opção Edit routing status (Editar status de roteamento) para as seguintes finalidades:
  - Para definir ou editar os status de roteamento de uma ou mais regiões em seu ponto de acesso multirregional
  - Para criar uma configuração de failover para seu ponto de acesso multirregional configurando duas regiões em um estado ativo-passivo
  - Para fazer o failover manualmente em suas regiões
  - Para alternar manualmente o tráfego entre regiões
- Failover: ao iniciar o failover escolhendo Failover, você atualiza apenas os status de roteamento de duas regiões que já estejam configuradas em um estado ativo-passivo. Durante um failover que você iniciou escolhendo Failover, os status de roteamento entre as duas regiões são automaticamente alterados.

Editar os status de roteamento das regiões em seu ponto de acesso multirregional

Você pode atualizar manualmente os status de roteamento de até 17 Regiões da AWS em uma única solicitação para seu ponto de acesso multirregional escolhendo Edit routing status (Editar status de roteamento) na seção Failover configuration (Configuração de failover) na página de detalhes do ponto de acesso multirregional. No entanto, ao iniciar o failover escolhendo Failover, você atualiza apenas os status de roteamento de duas regiões que já estejam configuradas em

um estado ativo-passivo. Durante um failover que você iniciou escolhendo Failover, os status de roteamento entre as duas regiões são automaticamente alterados.

Você pode usar Edit routing status (Editar status de roteamento) (conforme descrito no procedimento a seguir) para as seguintes finalidades:

- Para definir ou editar os status de roteamento de uma ou mais regiões em seu ponto de acesso multirregional
- Para criar uma configuração de failover para seu ponto de acesso multirregional configurando duas regiões em um estado ativo-passivo
- Para fazer o failover manualmente em suas regiões
- Para alternar manualmente o tráfego entre regiões

Uso do console do S3

Como atualizar os status de roteamento das regiões em seu ponto de acesso multirregional

1. Faça login no Console de Gerenciamento AWS.
2. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
3. No painel de navegação esquerdo, escolha Multi-Region Access Points (Pontos de acesso multirregionais).
4. Escolha o ponto de acesso multirregional que você deseja atualizar.
5. Escolha a guia Replication and failover (Replicação e failover).
6. Selecione uma ou mais regiões para as quais deseja editar o status do roteamento.

> **Note**
>
> Para iniciar um failover, pelo menos uma Região da AWS deve ser designada como Active (Ativa) e uma região deve ser designada como Passive (Passiva) em seu ponto de acesso multirregional.

7. Escolha Edit routing status (Editar status de roteamento).
8. Na caixa de diálogo exibida, selecione Active (Ativo) ou Passive (Passivo) para o Routing status (Status de roteamento) de cada região.

Um estado ativo permite que o tráfego seja roteado para a região. Um estado passivo impede que qualquer tráfego seja direcionado para a região.

Se você estiver criando uma configuração de failover para o ponto de acesso multirregional ou iniciando um failover, pelo menos uma Região da AWS deverá ser designada como Active (Ativa) e uma região deverá ser designada como Passive (Passiva) em seu ponto de acesso multirregional.

9. Escolha Save routing status (Salvar status de roteamento). O redirecionamento do tráfego leva cerca de 2 minutos.

Depois de enviar o status de roteamento das Regiões da AWS para seu ponto de acesso multirregional, você poderá verificar as alterações no status de roteamento. Para verificar essas alterações, acesse o Amazon CloudWatch em https://console.aws.amazon.com/cloudwatch/ para monitorar a mudança do tráfego de solicitações de dados do Amazon S3 (por exemplo, solicitações `GET` e `PUT`) entre regiões ativas e passivas. Nenhuma conexão existente será encerrada durante o failover. As conexões existentes continuarão até receberem um status de sucesso ou falha.

Uso do AWS CLI

> **Note**
>
> Você pode executar comandos de roteamento da AWS CLI de pontos de acesso multirregionais em qualquer uma destas cinco regiões:
>
> - `ap-southeast-2`
> - `ap-northeast-1`
> - `us-east-1`
> - `us-west-2`
> - `eu-west-1`

O exemplo de comando a seguir atualiza sua configuração de roteamento do ponto de acesso multirregional atual. Para atualizar o status ativo ou passivo de um bucket, defina o valor de `TrafficDialPercentage` como `100` para ativo e como `0` para passivo. Neste exemplo, *`amzn-s3-demo-bucket1`* é definido como ativo e *`amzn-s3-demo-bucket2`* é definido como passivo.

Para usar esse exemplo de comando, substitua os *user input placeholders* por suas próprias informações.

```
aws s3control submit-multi-region-access-point-routes
--region ap-southeast-2
--account-id 123456789012
--mrap MultiRegionAccessPoint_ARN
--route-updates Bucket=amzn-s3-demo-bucket1,TrafficDialPercentage=100
                Bucket=amzn-s3-demo-bucket2
,TrafficDialPercentage=0
```

O exemplo de comando a seguir obtém sua configuração de roteamento do ponto de acesso multirregional atualizada. Para usar esse exemplo de comando, substitua os *user input placeholders* por suas próprias informações.

```
aws s3control get-multi-region-access-point-routes
--region eu-west-1
--account-id 123456789012
--mrap MultiRegionAccessPoint_ARN
```

Iniciar failover

Quando você inicia um failover escolhendo Failover na seção Failover configuration (Configuração de failover) na página de detalhes do ponto de acesso multirregional, o tráfego de solicitações do Amazon S3 é automaticamente transferido para uma Região da AWS alternativa. O processo de failover é concluído em 2 minutos.

Você pode iniciar um failover em duas Regiões da AWS quaisquer por vez (das 17 regiões em que os pontos de acesso multirregionais são compatíveis). Depois, os eventos de failover são registrados em logs do AWS CloudTrail. Depois da conclusão do failover, você pode monitorar o tráfego do Amazon S3 e qualquer atualização de roteamento de tráfego para a nova região ativa no Amazon CloudWatch.

> **Important**
>
> Para manter todos os metadados e objetos sincronizados entre os buckets durante a replicação de dados, recomendamos que você crie regras de replicação bidirecional e habilite a sincronização de modificações da réplica antes de configurar controles de failover. As regras de replicação bidirecional ajudam a garantir que, quando os dados são gravados no bucket do Amazon S3 para o qual o tráfego faz failover, esses dados sejam replicados de

volta para o bucket de origem. A sincronização de modificações da réplica ajuda a garantir que os metadados do objeto também sejam sincronizados entre os buckets durante a replicação bidirecional.
Para obter mais informações sobre como configurar a replicação para que ofereça suporte a failover, consulte the section called “Replicação do bucket”.

Como iniciar um failover entre buckets replicados

1. Faça login no Console de Gerenciamento AWS.
2. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
3. No painel de navegação esquerdo, escolha Multi-Region Access Points (Pontos de acesso multirregionais).
4. Escolha o ponto de acesso multirregional que deseja usar para iniciar o failover.
5. Escolha a guia Replication and failover (Replicação e failover).
6. Role para baixo até a seção Failover configuration (Configuração de failover) e selecione duas Regiões da AWS.

   > **Note**
   >
   > Para iniciar um failover, pelo menos uma Região da AWS deve ser designada como Active (Ativa) e uma região deve ser designada como Passive (Passiva) em seu ponto de acesso multirregional. Um estado ativo permite que o tráfego seja direcionado para uma região. Um estado passivo impede que qualquer tráfego seja direcionado para a região.

7. Escolha Failover.
8. Na caixa de diálogo, selecione Failover novamente para iniciar o processo de failover. Durante esse processo, os status de roteamento das duas regiões são automaticamente alterados. Todo novo tráfego é direcionado para a região que se torna ativa, e o tráfego deixa de ser direcionado para a região que se torna passiva. O redirecionamento do tráfego leva cerca de 2 minutos.

   Depois de iniciar o processo de failover, você pode verificar as alterações no tráfego. Para verificar essas alterações, acesse o Amazon CloudWatch em https://console.aws.amazon.com/cloudwatch/ para monitorar a mudança do tráfego de solicitações de dados do Amazon S3 (por exemplo, solicitações `GET` e `PUT`) entre regiões ativas e passivas. Nenhuma conexão existente

será encerrada durante o failover. As conexões existentes continuarão até receberem um status de sucesso ou falha.

Visualizar controles de roteamento de pontos de acesso multirregionais do Amazon S3

Uso do console do S3

Como visualizar controles de roteamento de pontos de acesso multirregionais do Amazon S3

1. Faça login no Console de Gerenciamento AWS.
2. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
3. No painel de navegação esquerdo, escolha Multi-Region Access Points (Pontos de acesso multirregionais).
4. Escolha o ponto de acesso multirregional que você deseja revisar.
5. Escolha a guia Replication and failover (Replicação e failover). Esta página exibe os detalhes e o resumo da configuração de roteamento do seu ponto de acesso multirregional, das regras de replicação associadas e das métricas de replicação. Você pode ver o status de roteamento de suas regiões na seção Failover configuration (Configuração de failover).

Uso do AWS CLI

O exemplo de comando da AWS CLI a seguir obtém sua configuração de roteamento atual do ponto de acesso multirregional para a região especificada. Para usar esse exemplo de comando, substitua os *`user input placeholders`* por suas próprias informações.

```
aws s3control get-multi-region-access-point-routes
--region eu-west-1
--account-id 123456789012
--mrap MultiRegionAccessPoint_ARN
```

> **Note**
>
> Esse comando só pode ser executado nestas cinco regiões:
>
> - ap-southeast-2
> - ap-northeast-1
> - us-east-1

- us-west-2
- eu-west-1

Erros de controles de failover para pontos de acesso multirregionais do Amazon S3

Ao atualizar a configuração de failover do seu ponto de acesso multirregional, você pode encontrar um destes erros:

- HTTP 400 Solicitação Inválida: esse erro poderá ocorrer se você inserir um ARN de ponto de acesso multirregional inválido ao atualizar sua configuração de failover. Você pode confirmar o ARN do ponto de acesso multirregional revisando a política de pontos de acesso multirregionais. Para revisar ou atualizar a política de pontos de acesso multirregionais, consulte Editar a política de pontos de acesso multirregionais. Esse erro também pode ocorrer se você usar uma string vazia ou aleatória ao atualizar seus controles de failover para pontos de acesso multirregionais do Amazon S3. Use o seguinte formato de ARN de ponto de acesso multirregional:

  `arn:aws:s3::account-id:accesspoint/MultiRegionAccessPoint_alias`
- HTTP 503 Desacelerar: este erro ocorrerá se você enviar muitas solicitações em um curto período. Solicitações rejeitadas resultarão em um erro.
- HTTP 409 Conflito: este erro ocorre quando duas ou mais solicitações simultâneas de atualização de configuração de roteamento têm como alvo um único ponto de acesso multirregional. A primeira solicitação é bem-sucedida, mas todas as outras solicitações falham com um erro.
- HTTP 405 Método Não Permitido: este erro ocorre quando você seleciona um ponto de acesso multirregional com apenas uma Região da AWS ao iniciar o failover. Você deve selecionar duas regiões antes de iniciar o failover. Caso contrário, um erro será retornado.

Configurar a replicação para uso com pontos de acesso multirregionais

Quando você faz uma solicitação para um endpoint de ponto de acesso multirregional, o Amazon S3 roteia automaticamente a solicitação para o bucket mais próximo de você. O Amazon S3 não considera o conteúdo da solicitação ao tomar essa decisão. Se você fizer uma solicitação `GET` para um objeto, sua solicitação poderá ser roteada para um bucket que não tenha uma cópia desse objeto. Se isso acontecer, você receberá um erro do código de status HTTP 404 (Não encontrado). Para ter mais informações sobre direcionamento de solicitações de um ponto de acesso multirregional, consulte the section called “Roteamento de solicitações”.

Se você quiser que o ponto de acesso multirregional consiga recuperar o objeto independentemente de qual bucket receba a solicitação, configure a Replicação do Amazon S3 Entre Regiões Diferentes (CRR).

Por exemplo, considere um ponto de acesso multirregional com três buckets:

- Um bucket chamado *amzn-s3-demo-bucket1* na região US West (Oregon) que contém o objeto my-image.jpg
- Um bucket chamado *amzn-s3-demo-bucket2* na região Asia Pacific (Mumbai) que contém o objeto my-image.jpg
- Um bucket chamado *amzn-s3-demo-bucket* na região Europe (Frankfurt) que não contém o objeto my-image.jpg

Nessa situação, se você fizer uma solicitação GetObject para o objeto my-image.jpg, o sucesso dessa solicitação dependerá de qual bucket receberá sua solicitação. Como o Amazon S3 não considera o conteúdo da solicitação, ele pode rotear sua solicitação GetObject para o bucket *amzn-s3-demo-bucket*, se esse bucket responder com maior proximidade. Mesmo que seu objeto esteja em um bucket no ponto de acesso multirregional, você receberá um erro HTTP 404 Não Encontrado porque o bucket individual que recebeu sua solicitação não tinha o objeto.

Habilitar a Replicação Entre Regiões Diferentes (CRR) ajuda a evitar esse resultado. Com as regras de replicação apropriadas, o objeto my-image.jpg é copiado para o bucket *amzn-s3-demo-bucket*. Portanto, se o Amazon S3 rotear sua solicitação para esse bucket, agora você poderá recuperar o objeto.

A replicação funciona normalmente com buckets atribuídos a um ponto de acesso multirregional. O Amazon S3 não executa nenhum tratamento de replicação especial com buckets que estão em pontos de acesso multirregionais. Para obter mais informações sobre como configurar a replicação em seus buckets, consulte Visão geral da configuração da replicação em tempo real.

Recomendações para usar a replicação com pontos de acesso multirregionais

Para obter a melhor performance de replicação ao trabalhar com pontos de acesso multirregionais, recomendamos o seguinte:

- Configure o Controle de Tempo de Replicação do S3 (S3 RTC). Para replicar dados em diferentes regiões dentro de um período previsível, você pode usar o S3 RTC. O S3 RTC replica 99,99 por cento dos novos objetos armazenados no Simple Storage Service (Amazon S3) em 15 minutos

(baseado em um acordo de nível de serviço). Para ter mais informações, consulte the section called “Uso do Controle do tempo de replicação do S3”. Não há cobranças adicionais por usar o S3 RTC. Para ter informações, consulte Definição de preço do Amazon S3.

- Use a replicação bidirecional para ajudar a manter os buckets sincronizados quando os buckets são atualizados por meio do ponto de acesso multirregional. Para ter mais informações, consulte the section called “Criar regras de replicação bidirecional para seu ponto de acesso multirregional”.
- Crie pontos de acesso multirregionais entre contas para replicar dados em buckets em Contas da AWS separadas. Essa abordagem oferece separação em nível de conta, para que os dados possam ser acessados e replicados em contas diferentes em regiões distintas, além do bucket de origem. A configuração de pontos de acesso multirregionais entre contas não tem custo adicional. Se você é proprietário de um bucket, mas não tem o ponto de acesso multirregional, paga somente pelos custos de transferência e solicitação de dados. Os proprietários de pontos de acesso multirregionais pagam pelos custos de roteamento de dados e aceleração da Internet. Para obter mais informações, consulte Definição de preço do Amazon S3.
- Habilite a sincronização de modificações da réplica para cada regra de replicação a fim de também manter as alterações de metadados dos objetos sincronizadas. Para obter mais informações, consulte Habilitar a sincronização de modificações da réplica.
- Habilite as métricas do Amazon CloudWatch para monitorar os eventos de replicação. As taxas de métricas do CloudWatch se aplicam. Para obter mais informações, consulte Preço do Amazon CloudWatch.

Tópicos

- Criar regras de replicação unidirecional para seu ponto de acesso multirregional
- Criar regras de replicação bidirecional para seu ponto de acesso multirregional
- Visualizar as regras de replicação para seu ponto de acesso multirregional.

Criar regras de replicação unidirecional para seu ponto de acesso multirregional

As regras de replicação possibilitam a cópia assíncrona automática de objetos entre buckets. Uma regra de replicação unidirecional ajuda a garantir que os dados sejam totalmente replicados de um bucket de origem em uma Região da AWS para um bucket de destino em outra região. Quando a replicação unidirecional é configurada, uma regra de replicação do bucket de origem (*`amzn-s3-demo-bucket`*) para o bucket de destino (*`amzn-s3-demo-bucket`*) é criada. Como todas as regras de replicação, você pode aplicar a regra de replicação unidirecional a todo o bucket do Amazon S3 ou a um subconjunto de objetos filtrados com base em um prefixo ou tags de objeto.

> **Important**
>
> Recomendamos usar a replicação unidirecional se seus usuários consumirem apenas os objetos em seus buckets de destino. Se seus usuários fizerem upload ou modificarem os objetos em seus buckets de destino, use a replicação bidirecional para manter todos os seus buckets sincronizados. Também recomendamos replicação bidirecional se você planeja usar um ponto de acesso multirregional para o failover. Para configurar a replicação bidirecional, consulte the section called “Criar regras de replicação bidirecional para seu ponto de acesso multirregional”.

Como criar uma regra de replicação unidirecional para um ponto de acesso multirregional

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação esquerdo, escolha Multi-Region Access Points (Pontos de acesso multirregionais).
3. Escolha o nome de seu ponto de acesso multirregional.
4. Escolha a guia Replication and failover (Replicação e failover).
5. Role para baixo até Replication rules (Regras de replicação) e escolha Create replication rules (Criar regras de replicação). Verifique se você tem permissões suficientes para criar a regra de replicação, caso contrário, o versionamento será desativado.

   > **Note**
   >
   > Apenas é possível criar regras de replicação para buckets em sua própria conta. Para criar regras de replicação para buckets externos, os proprietários do bucket devem criar as regras de replicação para esses buckets.

6. Na página Criar regras de replicação, selecione o modelo Replicar objetos de um ou mais buckets de origem para um ou mais buckets de destino.

   > **Important**
   >
   > Quando você cria regras de replicação usando esse modelo, todas as regras de replicação existentes que já estejam atribuídas ao bucket são substituídas.

Para adicionar ou modificar regras de replicação existentes em vez de substituí-las, acesse a guia Management (Gerenciamento) de cada bucket no console e edite as regras na seção Replication rules (Regras de replicação). Você também pode adicionar ou modificar as regras de replicação existentes usando a AWS CLI, SDKs ou a API REST. Para ter mais informações, consulte Elementos do arquivo de configuração de replicação.

7. Na seção Origem e destino, em Buckets de origem, selecione um ou mais buckets dos quais você deseja replicar objetos. Todos os buckets (origem e destino) escolhidos para replicação devem ter o Versionamento do S3 ativado, e cada bucket deve estar em uma Região da AWS diferente. Para obter mais informações sobre o Versionamento do S3, consulte Usar o versionamento em buckets do Amazon S3.

   Em Buckets de destino, selecione um ou mais buckets dos quais você deseja replicar objetos.

8. Na seção Replication rule configuration (Configuração da regra de replicação), escolha se a regra de replicação ficará Enabled (Ativada) ou Disabled (Desativada) quando for criada.

   > **Note**
   >
   > Você não pode inserir um nome na caixa Replication rule name (Nome da regra de replicação). Os nomes de regras de replicação são gerados com base na sua configuração ao criar a regra de replicação.

9. Na seção Scope (Escopo), escolha o escopo apropriado para sua replicação.

   - Para replicar todo o bucket, escolha Apply to all objects in the bucket (Aplicar a todos os objetos no bucket).
   - Para replicar um subconjunto dos objetos do bucket, escolha Limit the scope of this rule using one or more filters (Limitar o escopo desta regra usando um ou mais filtros).

     Você pode filtrar os objetos usando um prefixo, etiquetas de objeto ou uma combinação de ambos.

     - Para limitar a replicação para todos os objetos que têm nomes que começam com a mesma string (por exemplo, `pictures`), insira um prefixo na caixa Prefix (Prefixo).

       Se você inserir um prefixo que seja o nome de uma pasta, será preciso usar um delimitadores, como uma / (barra), para indicar seu nível de hierarquia (por exemplo,

`pictures/`). Para ter mais informações sobre prefixos, consulte Organizar objetos usando prefixos.

- Para replicar todos os objetos que têm uma ou mais etiquetas de objeto, selecione Add tag (Adicionar etiqueta) e insira o par de chave/valor nas caixas. Para adicionar outra etiqueta, repita o procedimento. Para obter mais informações sobre etiquetas de objeto, consulte Categorizar seu armazenamento usando tags.

10. Role para baixo até a seção Additional replication options (Opções de replicação adicionais) e selecione as opções de replicação que deseja aplicar.

> **Note**
>
> Recomendamos aplicar as seguintes opções:
>
> - Replication time control (RTC) (Controle de Tempo de Replicação (RTC)): para replicar seus dados em diferentes regiões dentro de um período previsível, você pode usar o Controle de Tempo de Replicação do S3 (S3 RTC). O S3 RTC replica 99,99 por cento dos novos objetos armazenados no Simple Storage Service (Amazon S3) em 15 minutos (baseado em um acordo de nível de serviço). Para ter mais informações, consulte the section called “Uso do Controle do tempo de replicação do S3”.
> - Replication metrics and notifications (Métricas e notificações de replicação): habilite as métricas do Amazon CloudWatch para monitorar eventos de replicação.
> - Replicação de marcadores de exclusão: os marcadores de exclusão criados pelas operações de exclusão do S3 serão replicados. Os marcadores de exclusão criados pelas regras do ciclo de vida não são replicados. Para ter mais informações, consulte Replicar marcadores de exclusão entre buckets.
>
> Há cobranças adicionais pelas métricas e notificações de replicação do S3 RTC e do CloudWatch. Para obter mais informações, consulte Definição de preço do Amazon S3 e Preço do Amazon CloudWatch.

11. Se você estiver escrevendo uma nova regra de replicação que substitui uma existente, selecione I acknowledge that by choosing Create replication rules, these existing replication rules will be overwritten (Eu reconheço que, ao escolher Criar regras de replicação, essas regras de replicação existentes serão substituídas).
12. Selecione Criar regras de replicação para criar e salvar suas novas regras de replicação unidirecional.

Criar regras de replicação bidirecional para seu ponto de acesso multirregional

As regras de replicação possibilitam a cópia assíncrona automática de objetos entre buckets. Uma regra de replicação bidirecional garante que os dados sejam totalmente replicados entre dois ou mais buckets em Regiões da AWS diferentes. Quando a replicação bidirecional é configurada, uma regra de replicação do bucket de origem (DOC-EXAMPLE-BUCKET-1) para o bucket que contém as réplicas (DOC-EXAMPLE-BUCKET-2) é criada. Depois, é criada uma segunda regra de replicação do bucket que contém as réplicas (DOC-EXAMPLE-BUCKET-2) para o bucket de origem (DOC-EXAMPLE-BUCKET-1).

Como todas as regras de replicação, você pode aplicar a regra de replicação bidirecional a todo o bucket do Amazon S3 ou a um subconjunto de objetos filtrados com base em um prefixo ou tags de objeto. Também é possível manter as alterações de metadados dos objetos sincronizadas ao habilitar a sincronização de modificações da réplica para cada regra de replicação. Você pode ativar a sincronização de modificações da réplica por meio do console do Amazon S3, a AWS CLI, os AWS SDKs, a API REST do Amazon S3 ou o AWS CloudFormation.

Para monitorar o progresso da replicação de objetos e metadados de objetos no Amazon CloudWatch, habilite as métricas e notificações da Replicação do S3. Para obter mais informações, consulte Monitoramento do progresso com métricas de replicação e notificações de eventos do Amazon S3.

Como criar uma regra de replicação bidirecional para um ponto de acesso multirregional

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação esquerdo, escolha Multi-Region Access Points (Pontos de acesso multirregionais).
3. Escolha o nome do ponto de acesso multirregional que você deseja atualizar.
4. Escolha a guia Replication and failover (Replicação e failover).
5. Role para baixo até Replication rules (Regras de replicação) e escolha Create replication rules (Criar regras de replicação).
6. Na página Create replication rules (Criar regras de replicação), escolha o modelo Replicate objects among all specified buckets (Replicar objetos entre todos os buckets especificados). O modelo Replicate objects among all specified buckets (Replicar objetos entre todos os buckets especificados) configura a replicação bidirecional (com recursos de failover) para seus buckets.

> **Important**
>
> Quando você cria regras de replicação usando esse modelo, todas as regras de replicação existentes que já estejam atribuídas ao bucket são substituídas.
> Para adicionar ou modificar regras de replicação existentes em vez de substituí-las, acesse a guia Management (Gerenciamento) de cada bucket no console e edite as regras na seção Replication rules (Regras de replicação). Você também pode adicionar ou modificar as regras de replicação existentes usando a AWS CLI, os AWS SDKs ou a API REST do Amazon S3. Para ter mais informações, consulte Elementos do arquivo de configuração de replicação.

7. Na seção Buckets, selecione pelo menos dois buckets dos quais você deseja replicar objetos. Todos os buckets escolhidos para replicação devem ter o Versionamento do S3 ativado, e cada bucket deve estar em uma Região da AWS diferente. Para obter mais informações sobre o Versionamento do S3, consulte Usar o versionamento em buckets do Amazon S3.

> **Note**
>
> Tenha as permissões de leitura e replicação necessárias para estabelecer a replicação, caso contrário, você encontrará erros. Para ter mais informações, consulte Criar um perfil do IAM.

8. Na seção Replication rule configuration (Configuração da regra de replicação), escolha se a regra de replicação ficará Enabled (Ativada) ou Disabled (Desativada) quando for criada.

> **Note**
>
> Você não pode inserir um nome na caixa Replication rule name (Nome da regra de replicação). Os nomes de regras de replicação são gerados com base na sua configuração ao criar a regra de replicação.

9. Na seção Scope (Escopo), escolha o escopo apropriado para sua replicação.

   - Para replicar todo o bucket, escolha Apply to all objects in the bucket (Aplicar a todos os objetos no bucket).
   - Para replicar um subconjunto dos objetos do bucket, escolha Limit the scope of this rule using one or more filters (Limitar o escopo desta regra usando um ou mais filtros).

Você pode filtrar os objetos usando um prefixo, etiquetas de objeto ou uma combinação de ambos.

- Para limitar a replicação para todos os objetos que têm nomes que começam com a mesma string (por exemplo, `pictures`), insira um prefixo na caixa Prefix (Prefixo).

  Se você inserir um prefixo que seja o nome de uma pasta, use uma `/` (barra) como o último caractere (por exemplo, `pictures/`).

- Para replicar todos os objetos que têm uma ou mais etiquetas de objeto, selecione Add tag (Adicionar etiqueta) e insira o par de chave/valor nas caixas. Para adicionar outra etiqueta, repita o procedimento. Para obter mais informações sobre etiquetas de objeto, consulte Categorizar seu armazenamento usando tags.

10. Role para baixo até a seção Additional replication options (Opções de replicação adicionais) e selecione as opções de replicação que deseja aplicar.

> **Note**
>
> Recomendamos que você aplique as seguintes opções, especialmente se pretender configurar um ponto de acesso multirregional para oferecer suporte a failover:
>
> - Replication time control (RTC) (Controle de Tempo de Replicação (RTC)): para replicar seus dados em diferentes regiões dentro de um período previsível, você pode usar o Controle de Tempo de Replicação do S3 (S3 RTC). O S3 RTC replica 99,99 por cento dos novos objetos armazenados no Simple Storage Service (Amazon S3) em 15 minutos (baseado em um acordo de nível de serviço). Para ter mais informações, consulte the section called “Uso do Controle do tempo de replicação do S3”.
> - Replication metrics and notifications (Métricas e notificações de replicação): habilite as métricas do Amazon CloudWatch para monitorar eventos de replicação.
> - Replicação de marcadores de exclusão: os marcadores de exclusão criados pelas operações de exclusão do S3 serão replicados. Os marcadores de exclusão criados pelas regras do ciclo de vida não são replicados. Para ter mais informações, consulte Replicar marcadores de exclusão entre buckets.
> - Replica modification sync (Sincronização de modificações da réplica): Habilite a sincronização de modificações da réplica para cada regra de replicação a fim de também manter as alterações de metadados dos objetos sincronizadas. Para obter mais informações, consulte Habilitar a sincronização de modificações da réplica.

Há cobranças adicionais pelas métricas e notificações de replicação do S3 RTC e do CloudWatch. Para obter mais informações, consulte Definição de preço do Amazon S3 e Preço do Amazon CloudWatch.

11. Se você estiver escrevendo uma nova regra de replicação que substitui uma existente, selecione I acknowledge that by choosing Create replication rules, these existing replication rules will be overwritten (Eu reconheço que, ao escolher Criar regras de replicação, essas regras de replicação existentes serão substituídas).
12. Escolha Create replication rules (Criar regras de replicação) para criar e salvar suas novas regras de replicação bidirecional.

Visualizar as regras de replicação para seu ponto de acesso multirregional.

Com os pontos de acesso multirregionais, você pode configurar regras de replicação unidirecional ou regras de replicação bidirecional (bidirecional). Para ter informações sobre como gerenciar suas regras de replicação, consulte Gerenciar regras de replicação usando o console do Amazon S3.

Como visualizar as regras de replicação para seu ponto de acesso multirregional.

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação esquerdo, escolha Multi-Region Access Points (Pontos de acesso multirregionais).
3. Escolha o nome de seu ponto de acesso multirregional.
4. Escolha a guia Replication and failover (Replicação e failover).
5. Role para baixo até a seção Regras de replicação. Esta seção lista todas as regras de replicação criadas para seu ponto de acesso multirregional.

> **Note**
>
> Se você adicionou um bucket de outra conta a esse ponto de acesso multirregional, deverá ter a permissão `s3:GetBucketReplication` do proprietário do bucket para visualizar as regras de replicação desse bucket.

Usar pontos de acesso multirregionais com operações de API compatíveis

O Amazon S3 fornece um conjunto de operações para o gerenciamento de pontos de acesso multirregionais. O Amazon S3 processa algumas dessas operações de forma síncrona e algumas de forma assíncrona. Quando você invoca uma operação assíncrona, o Amazon S3 primeiro autoriza de forma síncrona a operação solicitada. Se a autorização for bem-sucedida, o Amazon S3 retornará um token que você pode usar para rastrear o progresso e os resultados da operação solicitada.

> **Note**
>
> Solicitações feitas por meio do Amazon S3 são sempre síncronas. O console aguarda até que a solicitação seja concluída antes de permitir que você envie outra solicitação.

É possível visualizar o status atual e os resultados das operações assíncronas usando o console ou usar `DescribeMultiRegionAccessPointOperation` na AWS CLI, AWS SDKs ou a API REST. O Amazon S3 fornece um token de rastreamento na resposta a uma operação assíncrona. Você inclui esse token de rastreamento como um argumento para a `DescribeMultiRegionAccessPointOperation`. Quando você inclui o token de rastreamento, o Amazon S3 retorna o status atual e os resultados da operação especificada, incluindo erros ou informações relevantes de recursos. O Amazon S3 executa operações de `DescribeMultiRegionAccessPointOperation` de forma síncrona.

Todas as solicitações do ambiente de gerenciamento para criar ou manter pontos de acesso multirregionais devem ser encaminhadas para a região `US West (Oregon)`. Com relação a solicitações de plano de dados de pontos de acesso multirregionais, as regiões não precisam ser especificadas. Para o ambiente de gerenciamento de failover do ponto de acesso multirregional, a solicitação deve ser encaminhada a uma das cinco regiões compatíveis. Consulte mais informações sobre as regiões compatíveis com o ponto de acesso multirregional em Restrições e limitações de pontos de acesso multirregionais.

Além disso, é preciso conceder a permissão `s3:ListAllMyBuckets` para o usuário, perfil ou outra entidade do AWS Identity and Access Management (IAM) que faz uma solicitação para gerenciar um ponto de acesso multirregional.

Os exemplos a seguir demonstram como usar pontos de acesso multirregionais com operações compatíveis no Amazon S3.

Tópicos

- Compatibilidade de pontos de acesso multirregionais com Serviços da AWS e AWS SDKs
- Compatibilidade de pontos de acesso multirregionais com operações do S3
- Visualizar a configuração de roteamento de pontos de acesso multirregionais
- Atualizar a política subjacente de buckets do Amazon S3
- Atualizar a configuração de roteamento de um ponto de acesso multirregional
- Adicionar um objeto a um bucket no ponto de acesso multirregional
- Recuperar objetos do ponto de acesso multirregional
- Listar objetos que estão armazenados em um bucket subjacente ao ponto de acesso multirregional
- Usar um URL pré-assinado com pontos de acesso multirregionais
- Usar um bucket que é configurado com pagamentos do solicitante com pontos de acesso multirregionais

Compatibilidade de pontos de acesso multirregionais com Serviços da AWS e AWS SDKs

Para usar um ponto de acesso multirregional com aplicações que exigem um nome de bucket do Amazon S3, use o nome do recurso da Amazon (ARN) do ponto de acesso multirregional ao fazer solicitações usando um AWS SDK. Para conferir quais AWS SDKs são compatíveis com pontos de acesso multirregionais, consulte Compatibilidade com AWS SDKs.

Compatibilidade de pontos de acesso multirregionais com operações do S3

É possível usar as operações de API a seguir do plano de dados do Amazon S3 para executar ações em objetos em buckets associados ao ponto de acesso multirregional. As seguintes operações do S3 podem aceitar ARNs de pontos de acesso multirregionais:

- AbortMultipartUpload
- CompleteMultipartUpload
- CreateMultipartUpload
- DeleteObject
- DeleteObjectTagging
- GetObject
- GetObjectAcl
- GetObjectLegalHold

- GetObjectRetention
- GetObjectTagging
- HeadObject
- ListMultipartUploads
- ListObjectsV2
- ListParts
- PutObject
- PutObjectAcl
- PutObjectLegalHold
- PutObjectRetention
- PutObjectTagging
- RestoreObject
- UploadPart

> **Note**
>
> Os pontos de acesso multirregionais permitem operações de cópia que os utilizem somente como destino ao usar o ARN do ponto de acesso multirregional.

É possível usar as seguintes operações do ambiente de gerenciamento do Amazon S3 para criar e gerenciar pontos de acesso multirregionais:

- CreateMultiRegionAccessPoint
- DescribeMultiRegionAccessPointOperation
- GetMultiRegionAccessPoint
- GetMultiRegionAccessPointPolicy
- GetMultiRegionAccessPointPolicyStatus
- GetMultiRegionAccessPointRoutes
- ListMultiRegionAccessPoints
- PutMultiRegionAccessPointPolicy
- SubmitMultiRegionAccessPointRoutes

Visualizar a configuração de roteamento de pontos de acesso multirregionais

AWS CLI

O exemplo de comando a seguir recupera a configuração de roteamento de pontos de acesso multirregionais para que você possa ver os status de roteamento atuais de seus buckets. Para usar esse exemplo de comando, substitua os *user input placeholders* por suas próprias informações.

```
aws s3control get-multi-region-access-point-routes
--region eu-west-1
--account-id 111122223333
--mrap arn:aws:s3::111122223333:accesspoint/abcdef0123456.mrap
```

SDK for Java

O código de SDK para Java a seguir recupera a configuração de roteamento de pontos de acesso multirregionais para que você possa ver os status de roteamento atuais de seus buckets. Para usar esse exemplo de sintaxe, substitua os *user input placeholders* por suas próprias informações.

```
S3ControlClient s3ControlClient = S3ControlClient.builder()
    .region(Region.US_EAST_1)
    .credentialsProvider(credentialsProvider)
    .build();

GetMultiRegionAccessPointRoutesRequest request =
 GetMultiRegionAccessPointRoutesRequest.builder()
    .accountId("111122223333")
    .mrap("arn:aws:s3::111122223333:accesspoint/abcdef0123456.mrap")
    .build();

GetMultiRegionAccessPointRoutesResponse response =
 s3ControlClient.getMultiRegionAccessPointRoutes(request);
```

SDK for JavaScript

O código de SDK para JavaScript a seguir recupera a configuração de roteamento de pontos de acesso multirregionais para que você possa ver os status de roteamento atuais de seus buckets. Para usar esse exemplo de sintaxe, substitua os *user input placeholders* por suas próprias informações.

```
const REGION = 'us-east-1'

const s3ControlClient = new S3ControlClient({
  region: REGION
})

export const run = async () => {
  try {
    const data = await s3ControlClient.send(
      new GetMultiRegionAccessPointRoutesCommand({
        AccountId: '111122223333',
        Mrap: 'arn:aws:s3::111122223333:accesspoint/abcdef0123456.mrap',
      })
    )
    console.log('Success', data)
    return data
  } catch (err) {
    console.log('Error', err)
  }
}

run()
```

SDK for Python

O código de SDK para Python a seguir recupera a configuração de roteamento de pontos de acesso multirregionais para que você possa ver os status de roteamento atuais de seus buckets. Para usar esse exemplo de sintaxe, substitua os *user input placeholders* por suas próprias informações.

```
s3.get_multi_region_access_point_routes(
        AccountId=111122223333,
        Mrap=arn:aws:s3::111122223333:accesspoint/abcdef0123456.mrap)['Routes']
```

Atualizar a política subjacente de buckets do Amazon S3

Para conceder acesso adequado, você também deve atualizar a política subjacente de buckets do Amazon S3. Os exemplos a seguir delegam o controle de acesso à política de pontos de acesso multirregionais. Depois de delegar o controle de acesso à política de ponto de acesso multirregional, a política de bucket não é mais usada para controle de acesso quando as solicitações são feitas por meio desse ponto de acesso multirregional.

Veja a seguir um exemplo de política de bucket que delega o controle de acesso à política de pontos de acesso multirregionais. Para usar esse exemplo de política de bucket, substitua os *user input placeholders* por suas próprias informações. Para aplicar essa política por meio do comando `put-bucket-policy` da AWS CLI, conforme mostrado no próximo exemplo, salve a política em um arquivo, como `policy.json`.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Principal": { "AWS": "*" },
    "Effect": "Allow",
    "Action": ["s3:*"],
    "Resource": ["arn:aws:s3:::111122223333/*", "arn:aws:s3:::amzn-s3-demo-bucket"],
    "Condition": {
      "StringEquals": {
        "s3:DataAccessPointAccount": "444455556666"
      }
    }
  }
}
```

O seguinte exemplo de comando `put-bucket-policy` associa a política atualizada ao bucket do S3:

```
aws s3api put-bucket-policy
  --bucket amzn-s3-demo-bucket
  --policy file:///tmp/policy.json
```

Atualizar a configuração de roteamento de um ponto de acesso multirregional

O exemplo de comando a seguir atualiza a configuração de roteamento do ponto de acesso multirregional. Os comandos de roteamento de pontos de acesso multirregionais podem ser executados nestas cinco regiões:

- `ap-southeast-2`
- `ap-northeast-1`
- `us-east-1`
- `us-west-2`
- `eu-west-1`

Em uma configuração de roteamento de ponto de acesso multirregional, você pode definir buckets com status de roteamento ativo ou passivo. Os buckets ativos recebem tráfego, enquanto os passivos não recebem. Você pode definir o status de roteamento de um bucket definindo o valor de `TrafficDialPercentage` do bucket como `100` para ativo ou como `0` para passivo.

AWS CLI

O exemplo de comando a seguir atualiza a configuração de roteamento do seu ponto de acesso multirregional. Neste exemplo, *amzn-s3-demo-bucket1* é definido como ativo e *amzn-s3-demo-bucket2* é definido como passivo. Para usar esse exemplo de comando, substitua os *user input placeholders* por suas próprias informações.

```
aws s3control submit-multi-region-access-point-routes
--region ap-southeast-2
--account-id 111122223333
--mrap arn:aws:s3::111122223333:accesspoint/abcdef0123456.mrap
--route-updates Bucket=amzn-s3-demo-bucket1,TrafficDialPercentage=100
                Bucket=amzn-s3-demo-bucket2,TrafficDialPercentage=0
```

SDK for Java

O código de SDK para Java a seguir atualiza a configuração de roteamento do seu ponto de acesso multirregional. Para usar esse exemplo de sintaxe, substitua os *user input placeholders* por suas próprias informações.

```
S3ControlClient s3ControlClient = S3ControlClient.builder()
    .region(Region.ap-southeast-2)
    .credentialsProvider(credentialsProvider)
    .build();

SubmitMultiRegionAccessPointRoutesRequest request =
 SubmitMultiRegionAccessPointRoutesRequest.builder()
    .accountId("111122223333")
    .mrap("arn:aws:s3::111122223333:accesspoint/abcdef0123456.mrap")
    .routeUpdates(
        MultiRegionAccessPointRoute.builder()
            .region("eu-west-1")
            .trafficDialPercentage(100)
            .build(),
        MultiRegionAccessPointRoute.builder()
            .region("ca-central-1")
```

```
            .bucket("111122223333")
            .trafficDialPercentage(0)
            .build()
    )
    .build();

SubmitMultiRegionAccessPointRoutesResponse response =
 s3ControlClient.submitMultiRegionAccessPointRoutes(request);
```

SDK for JavaScript

O código de SDK para JavaScript a seguir atualiza a configuração de roteamento do seu ponto de acesso multirregional. Para usar esse exemplo de sintaxe, substitua os *user input placeholders* por suas próprias informações.

```
const REGION = 'ap-southeast-2'

const s3ControlClient = new S3ControlClient({
  region: REGION
})

export const run = async () => {
  try {
    const data = await s3ControlClient.send(
      new SubmitMultiRegionAccessPointRoutesCommand({
        AccountId: '111122223333',
        Mrap: 'arn:aws:s3::111122223333:accesspoint/abcdef0123456.mrap',
        RouteUpdates: [
          {
            Region: 'eu-west-1',
            TrafficDialPercentage: 100,
          },
          {
            Region: 'ca-central-1',
            Bucket: 'amzn-s3-demo-bucket1',
            TrafficDialPercentage: 0,
          },
        ],
      })
    )
    console.log('Success', data)
    return data
  } catch (err) {
```

```
    console.log('Error', err)
  }
}

run()
```

SDK for Python

O código de SDK para Python a seguir atualiza a configuração de roteamento do seu ponto de acesso multirregional. Para usar esse exemplo de sintaxe, substitua os *user input placeholders* por suas próprias informações.

```
s3.submit_multi_region_access_point_routes(
        AccountId=111122223333,
        Mrap=arn:aws:s3::111122223333:accesspoint/abcdef0123456.mrap,
        RouteUpdates= [{
            'Bucket': amzn-s3-demo-bucket,
            'Region': ap-southeast-2,
            'TrafficDialPercentage': 10
        }])
```

Adicionar um objeto a um bucket no ponto de acesso multirregional

Para adicionar um objeto ao bucket associado ao ponto de acesso multirregional, é possível usar a operação PutObject. Para manter todos os buckets no ponto de acesso multirregional sincronizados, habilite a Replicação entre regiões.

> **Note**
>
> Para usar essa operação, é necessário ter a permissão `s3:PutObject` do ponto de acesso multirregional. Para obter mais informações sobre os requisitos de permissão do ponto de acesso multirregional, consulte Permissões.

AWS CLI

O exemplo de plano de dados a seguir carrega *example.txt* para o ponto de acesso multirregional especificado. Para usar esse exemplo, substitua os *user input placeholders* por suas próprias informações.

```
aws s3api put-object --bucket
 arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap --key example.txt --
body example.txt
```

SDK for Java

```
S3Client s3Client = S3Client.builder()
        .build();

PutObjectRequest objectRequest = PutObjectRequest.builder()
        .bucket("arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap")
        .key("example.txt")
        .build();

s3Client.putObject(objectRequest, RequestBody.fromString("Hello S3!"));
```

SDK for JavaScript

```
const client = new S3Client({});

async function putObjectExample() {
    const command = new PutObjectCommand({
        Bucket: "arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap",
        Key: "example.txt",
        Body: "Hello S3!",
    });

    try {
        const response = await client.send(command);
        console.log(response);
    } catch (err) {
        console.error(err);
    }
}
```

SDK for Python

```
import boto3

client = boto3.client('s3')
client.put_object(
    Bucket='arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap',
```

```
    Key='example.txt',
    Body='Hello S3!'
)
```

Recuperar objetos do ponto de acesso multirregional

Para recuperar objetos do ponto de acesso multirregional, é possível usar a operação GetObject.

> **Note**
>
> Para usar essa operação de API, é necessário ter a permissão `s3:GetObject` do ponto de acesso multirregional. Para obter mais informações sobre os requisitos de permissões do ponto de acesso multirregional, consulte Permissões.

AWS CLI

O exemplo de solicitação de plano de dados a seguir recupera *example.txt* do ponto de acesso multirregional especificado e o baixa como *downloaded_example.txt*. Para usar esse exemplo, substitua os *user input placeholders* por suas próprias informações.

```
aws s3api get-object --bucket
 arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap --
key example.txt downloaded_example.txt
```

SDK for Java

```
S3Client s3 = S3Client
   .builder()
   .build();

GetObjectRequest getObjectRequest = GetObjectRequest.builder()
    .bucket("arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap")
    .key("example.txt")
    .build();

s3Client.getObject(getObjectRequest);
```

SDK for JavaScript

```
const client = new S3Client({})

async function getObjectExample() {
    const command = new GetObjectCommand({
        Bucket: "arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap",
        Key: "example.txt"
    });

    try {
        const response = await client.send(command);
        console.log(response);
    } catch (err) {
        console.error(err);
    }
}
```

SDK for Python

```
import boto3

client = boto3.client('s3')
client.get_object(
    Bucket='arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap',
    Key='example.txt'
)
```

Listar objetos que estão armazenados em um bucket subjacente ao ponto de acesso multirregional

Para retornar uma lista de objetos que estão armazenados em um bucket subjacente ao ponto de acesso multirregional, use a operação ListObjectsV2. No exemplo de comando a seguir, todos os objetos do ponto de acesso multirregional especificado são listados usando o ARN do ponto de acesso multirregional. Nesse caso, o ARN do ponto de acesso multirregional é:

`arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap`

> **Note**
>
> Para usar essa operação de API, é necessário ter a permissão `s3:ListBucket` para o ponto de acesso multirregional e o bucket subjacente. Para obter mais informações sobre os requisitos de permissões do ponto de acesso multirregional, consulte Permissões.

AWS CLI

O exemplo de solicitação de plano de dados a seguir lista os objetos no bucket subjacente ao ponto de acesso multirregional especificado pelo ARN. Para usar esse exemplo, substitua os *`user input placeholders`* por suas próprias informações.

```
aws s3api list-objects-v2 --bucket
 arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap
```

SDK for Java

```
S3Client s3Client = S3Client.builder()
        .build();

String bucketName = "arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap";

ListObjectsV2Request listObjectsRequest = ListObjectsV2Request
    .builder()
    .bucket(bucketName)
    .build();

 s3Client.listObjectsV2(listObjectsRequest);
```

SDK for JavaScript

```
const client = new S3Client({});

async function listObjectsExample() {
    const command = new ListObjectsV2Command({
        Bucket: "arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap",
    });

    try {
```

```
        const response = await client.send(command);
        console.log(response);
    } catch (err) {
        console.error(err);
    }
}
```

SDK for Python

```
import boto3

client = boto3.client('s3')
client.list_objects_v2(
    Bucket='arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap'
)
```

Usar um URL pré-assinado com pontos de acesso multirregionais

É possível usar um URL pré-assinado para gerar um URL que permite acessar os buckets do Amazon S3 por meio de um ponto de acesso multirregional do Amazon S3. Ao criar um URL pré-assinado, você o associa a uma ação de objeto específica, como um upload no S3 (`PutObject`) ou um download do S3 (`GetObject`). É possível compartilhar o URL pré-assinado, e qualquer pessoa com acesso a ele pode executar a ação incorporada no URL como se fosse o usuário de assinatura original.

Os URLs pré-assinados têm uma data de validade. Quando o prazo de validade for atingido, o URL não funcionará mais.

Antes de usar os pontos de acesso multirregionais do S3 com URLs pré-assinados, confira a compatibilidade de AWS SDKs com o algoritmo SigV4A. Verifique se sua versão de SDK oferece suporte ao SigV4A como a implementação de assinatura usada para assinar as solicitações globais da Região da AWS. Para obter mais informações sobre como usar URLs pré-assinados com o Amazon S3, consulte Compartilhar objetos usando URLs pré-assinados.

Os exemplos a seguir mostram como você pode usar pontos de acesso multirregionais com URLs pré-assinados. Para usar esses exemplos, substitua os *`user input placeholders`* por suas próprias informações.

AWS CLI

```
aws s3 presign
 arn:aws:s3::123456789012:accesspoint/MultiRegionAccessPoint_alias/example-file.txt
```

SDK for Python

```
import logging
import boto3
from botocore.exceptions import ClientError

s3_client = boto3.client('s3',aws_access_key_id='xxx',aws_secret_access_key='xxx')
s3_client.generate_presigned_url(HttpMethod='PUT',ClientMethod="put_object",
 Params={'Bucket':'arn:aws:s3::123456789012:accesspoint/
abcdef0123456.mrap','Key':'example-file'})
```

SDK for Java

```
S3Presigner s3Presigner = S3Presigner.builder()
    .credentialsProvider(StsAssumeRoleCredentialsProvider.builder()
        .refreshRequest(assumeRole)
        .stsClient(stsClient)
        .build())
    .build();

GetObjectRequest getObjectRequest = GetObjectRequest.builder()
    .bucket("arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap")
    .key("example-file")
    .build();

GetObjectPresignRequest preSignedReq = GetObjectPresignRequest.builder()
    .getObjectRequest(getObjectRequest)
    .signatureDuration(Duration.ofMinutes(10))
    .build();

PresignedGetObjectRequest presignedGetObjectRequest =
 s3Presigner.presignGetObject(preSignedReq);
```

> **Note**
>
> Para usar o SigV4A com credenciais de segurança temporárias, por exemplo, ao usar perfis do IAM, solicite as credenciais temporárias de um endpoint regional no AWS Security Token Service (AWS STS), em vez de um endpoint global. Se você usar o endpoint global para o AWS STS (`sts.amazonaws.com`), o AWS STS vai gerar credenciais temporárias de um endpoint global, o que não é compatível com o Sig4A. Como resultado, você receberá um erro. Para resolver esse problema, use qualquer um dos Endpoints regionais para AWS STS listados.

Usar um bucket que é configurado com pagamentos do solicitante com pontos de acesso multirregionais

Se o bucket do S3 associado aos pontos de acesso multirregionais estiver configurado para usar pagamentos do solicitante, o solicitante pagará pela solicitação do bucket, pelo download e por todos os custos relacionados aos pontos de acesso multirregionais. Para obter mais informações, consulte Definição de preço do Amazon S3.

Veja um exemplo de uma solicitação de plano de dados para um ponto de acesso multirregional conectado a um bucket de pagamentos do solicitante.

AWS CLI

Para baixar objetos de um ponto de acesso multirregional que está conectado a um bucket de pagamentos do solicitante, é necessário especificar `--request-payer requester` como parte da solicitação get-object. Também é necessário especificar o nome do arquivo no bucket e o local onde o arquivo baixado deve ser armazenado.

```
aws s3api get-object --bucket MultiRegionAccessPoint_ARN --request-payer requester
 --key example-file-in-bucket.txt example-location-of-downloaded-file.txt
```

SDK for Java

Para baixar objetos de um ponto de acesso multirregional que está conectado a um bucket de pagamentos do solicitante, você deve especificar `RequestPayer.REQUESTER` como parte da solicitação `GetObject`. Você também deve especificar o nome do arquivo no bucket, bem como o local onde ele deve ser armazenado.

```
GetObjectResponse getObjectResponse = s3Client.getObject(GetObjectRequest.builder()
```

```
    .key("example-file.txt")
    .bucket("arn:aws:s3::
123456789012:accesspoint/abcdef0123456.mrap")
    .requestPayer(RequestPayer.REQUESTER)
    .build()
).response();
```

Monitoramento e registro de solicitações feitas por meio de um ponto de acesso multirregional para recursos subjacentes

O Amazon S3 registra solicitações feitas por meio de pontos de acesso multirregionais e solicitações feitas às operações de API que os gerenciam, como `CreateMultiRegionAccessPoint` e `GetMultiRegionAccessPointPolicy`. As solicitações feitas ao Amazon S3 por meio de um ponto de acesso multirregional aparecem nos logs de acesso do servidor do Amazon S3 e em logs do AWS CloudTrail com o nome de host do ponto de acesso multirregional. O nome do host de um ponto de acesso assume a forma de *`MRAP_alias`*`.accesspoint.s3-global.amazonaws.com`. Por exemplo, suponha que você tenha a seguinte configuração de bucket e de ponto de acesso multirregional:

- Um bucket denominado `my-bucket-usw2` na região `us-west-2` que contém o objeto `my-image.jpg`.
- Um bucket denominado `my-bucket-aps1` na região `ap-south-1` que contém o objeto `my-image.jpg`.
- Um bucket denominado `my-bucket-euc1` na região `eu-central-1` que não contém um objeto denominado `my-image.jpg`.
- Um ponto de acesso multirregional chamado `my-mrap` com o alias `mfzwi23gnjvgw.mrap` que está configurado para atender a solicitações de todos os três buckets.
- O ID de sua conta da AWS é `123456789012`.

Uma solicitação feita para recuperar `my-image.jpg` diretamente por meio de quaisquer buckets aparece nos logs com um nome de host de *`bucket_name`*`.s3.`*`Region`*`.amazonaws.com`.

Se, em vez disso, você fizer a solicitação por meio do ponto de acesso multirregional, primeiro o Amazon S3 determinará quais dos buckets nas diferentes regiões é o mais próximo. Depois que o Amazon S3 determina qual bucket usar para atender à solicitação, ele envia a solicitação para esse bucket e registra a operação usando o nome de host do ponto de acesso multirregional. Neste

exemplo, se o Amazon S3 retransmitir a solicitação para `my-bucket-aps1`, seus logs refletirão uma solicitação `GET` bem-sucedida para `my-image.jpg` do `my-bucket-aps1`, usando um nome de host do `mfzwi23gnjvgw.mrap.accesspoint.s3-global.amazonaws.com`.

> **Important**
>
> Pontos de acesso multirregionais não estão cientes do conteúdo de dados de buckets subjacentes. Portanto, o bucket que recebe a solicitação pode não conter os dados solicitados. Por exemplo, se o Amazon S3 determinar que o bucket `my-bucket-euc1` é o mais próximo, seus logs refletirão uma falha de solicitação `GET` de `my-image.jpg` do `my-bucket-euc1`, usando um nome de host do `mfzwi23gnjvgw.mrap.accesspoint.s3-global.amazonaws.com`. Se a solicitação tiver sido roteada para `my-bucket-usw2`, em vez disso, seus logs indicarão uma solicitação `GET` bem-sucedida.

Para obter mais informações sobre logs de acesso do servidor do Amazon S3, consulte Registrar em log as solicitações com registro em log de acesso ao servidor. Para obter mais informações sobre o AWS CloudTrail, consulte O que é AWS CloudTrail? no Guia do Usuário doAWS CloudTrail.

Monitoramento e registro em log de solicitações feitas para operações de API de gerenciamento de pontos de acesso multirregionais

O Amazon S3 fornece várias operações de API para gerenciar pontos de acesso multirregionais, como `CreateMultiRegionAccessPoint` e `GetMultiRegionAccessPointPolicy`. Quando você faz solicitações para essas operações de API usando a AWS Command Line Interface (AWS CLI), AWS SDKs ou a API REST do Amazon S3, o Amazon S3 processa essas solicitações de forma assíncrona. Desde que você tenha as permissões apropriadas para a solicitação, o Amazon S3 retornará um token para essas solicitações. Você pode usar este token com `DescribeAsyncOperation` para ajudar você a visualizar o status das operações assíncronas em andamento. O Amazon S3 processa solicitações de `DescribeAsyncOperation` de forma síncrona. Para visualizar o status de solicitações assíncronas, você pode usar o console do Amazon S3, a AWS CLI, SDKs ou a API REST.

> **Note**
>
> O console exibe somente o status de solicitações assíncronas feitas nos 14 dias anteriores. Para exibir o status das solicitações mais antigas, use a AWS CLI, SDKs ou a API REST.

As operações de gerenciamento assíncronas podem estar em um dos vários estados:

NEW

O Amazon S3 recebeu a solicitação e está se preparando para executar a operação.

IN_PROGRESS

O Amazon S3 está executando a operação no momento.

SUCCESS

A operação foi bem-sucedida. A resposta inclui informações relevantes, como o alias de ponto de acesso multirregional para uma solicitação `CreateMultiRegionAccessPoint`.

FAILED

Falha na operação. A resposta inclui uma mensagem de erro indicando o motivo da falha da solicitação.

Usar o AWS CloudTrail com pontos de acesso multirregionais

É possível usar o AWS CloudTrail para visualizar, pesquisar, fazer download, arquivar, analisar e responder às atividades da conta em toda a infraestrutura da AWS. Com os pontos de acesso multirregionais e o registro em log do CloudTrail, você pode identificar o seguinte:

- Quem ou o que realizou qual ação
- Quais recursos foram utilizados
- Quando ocorreu o evento
- Outros detalhes sobre o evento

Você pode usar essas informações de registro em log para ajudar a analisar e responder às atividades que ocorreram por meio de seus pontos de acesso multirregionais.

Como configurar o AWS CloudTrail para pontos de acesso multirregionais

Para ativar o registro em log do CloudTrail para quaisquer operações relacionadas à criação ou à manutenção de pontos de acesso multirregionais, você deve configurar o registro em log do CloudTrail para registrar os eventos na região Oeste dos EUA (Oregon). Você deve definir a configuração de registro em log dessa forma independentemente da região em que você esteja ao fazer a solicitação ou a quais regiões o ponto de acesso multirregional oferece suporte. Todas as

solicitações para criar ou manter um ponto de acesso multirregional são encaminhadas para a região Oeste dos EUA (Oregon). Recomendamos que você adicione essa região a uma trilha existente ou crie uma trilha que contenha essa região e todas as regiões associadas ao ponto de acesso multirregional.

O Amazon S3 registra todas as solicitações feitas por meio de pontos de acesso multirregionais e solicitações feitas às operações de API que os gerenciam, como `CreateMultiRegionAccessPoint` e `GetMultiRegionAccessPointPolicy`. Quando você registra essas solicitações por meio de um ponto de acesso multirregional, elas aparecem em seus logs do AWS CloudTrail com o nome do host do ponto de acesso multirregional. Por exemplo, se você fizer solicitações para um bucket por meio de um ponto de acesso multirregional com o alias `mfzwi23gnjvgw.mrap`, as entradas no log do CloudTrail terão um nome de host de `mfzwi23gnjvgw.mrap.accesspoint.s3-global.amazonaws.com`.

Os pontos de acesso multirregionais encaminham as solicitações para o bucket mais próximo. Devido a esse comportamento, quando você estiver observando os logs do CloudTrail de um ponto de acesso multirregional, você verá solicitações sendo feitas aos buckets subjacentes. Algumas dessas solicitações podem ser solicitações diretas para o bucket e não roteadas pelo ponto de acesso multirregional. Lembre-se disso ao analisar o tráfego. Quando um bucket está em um ponto de acesso multirregional, as solicitações ainda podem ser feitas a esse bucket diretamente sem passar pelo ponto de acesso multirregional.

Há eventos assíncronos envolvidos na criação e gerenciamento de pontos de acesso multirregionais. As solicitações assíncronas não têm eventos de conclusão no log do CloudTrail. Para mais informações sobre solicitações assíncronas, consulte Monitoramento e registro em log de solicitações feitas para operações de API de gerenciamento de pontos de acesso multirregionais.

Para obter mais informações sobre o AWS CloudTrail, consulte O que é AWS CloudTrail? no Guia do Usuário doAWS CloudTrail.

Reter várias versões de objetos com o Versionamento do S3

Versionamento no Amazon S3 é um meio de manter diversas variantes de um objeto no mesmo bucket. Você pode usar o recurso S3 Versioning para preservar, recuperar e restaurar todas as versões de cada objeto armazenado em seus buckets. Com o versionamento, você pode se recuperar mais facilmente de ações não intencionais do usuário e de falhas da aplicação. Depois de habilitar o versionamento para um bucket, se o Amazon S3 receber várias solicitações de gravação do mesmo objeto simultaneamente, ele armazenará todos esses objetos.

Buckets com versionamento habilitado podem ajudar a recuperar objetos de uma exclusão ou substituição acidental. Por exemplo, se você excluir um objeto, o Amazon S3 inserirá um marcador de exclusão em vez de remover o objeto permanentemente. O marcador de exclusão se torna a versão atual do objeto. Se você substituir um objeto, isso criará uma nova versão do objeto no bucket. Você sempre pode restaurar a versão anterior. Para obter mais informações, consulte Excluir versões de objetos de um bucket com versionamento habilitado.

Por padrão, o Versionamento do S3 está desativado em buckets e você deve ativá-lo explicitamente. Para obter mais informações, consulte Habilitar o versionamento em buckets.

> **Note**
>
> - A API SOAP não é compatível com o versionamento do S3. O suporte de SOAP via HTTP está obsoleto, mas continua disponível via HTTPS. Os novos recursos do Amazon S3 não são compatíveis com SOAP.
> - As taxas normais do Amazon S3 se aplicam a cada versão de um objeto armazenado e transferido. Cada versão de um objeto é um objeto inteiro; não é apenas um diff da versão anterior. Assim, se você tiver três versões de um objeto armazenado, será cobrado pelos três objetos.

Buckets não versionados, habilitados para versão e suspensos de versão

Os buckets podem estar em um dos três estados:

- Não versionado (o padrão)
- Habilitado para versão
- Com versionamento suspenso

Você habilita e suspende o versionamento no nível do bucket. Depois que um bucket é habilitado para versionamento, ele nunca pode voltar a um estado sem versionamento. Mas você pode suspender o versionamento nesse bucket.

O estado de versionamento aplica-se a todos (nunca alguns) os objetos nesse bucket. Quando você habilita o versionamento em um bucket, todos os novos objetos são versionados e recebem um ID de versão exclusivo. Os objetos que já existiam no bucket no momento em que o versionamento foi

ativado serão sempre versionados e receberão um ID de versão exclusivo quando forem modificados por solicitações futuras. Observe o seguinte:

- Os objetos que são armazenados em seu bucket antes da habilitação do versionamento têm um ID de versão `null`. Quando você habilita o versionamento, os objetos existentes em seu bucket não são alterados. O que muda é como o Amazon S3 trata os objetos em solicitações futuras. Para obter mais informações, consulte Trabalhar com objetos em um bucket com versionamento habilitado.
- O proprietário do bucket (ou qualquer usuário com as devidas permissões) pode suspender o versionamento para interromper o acúmulo de versões de objetos. Quando você suspende o versionamento, os objetos existentes em seu bucket não são alterados. O que muda é como o Amazon S3 trata os objetos em solicitações futuras. Para obter mais informações, consulte Trabalhar com objetos em um bucket com versionamento suspenso.

Usando o versionamento do S3 com o ciclo de vida do S3

Para personalizar sua abordagem de retenção de dados e controlar os custos de armazenamento, use o versionamento de objetos com o S3 Lifecycle. Para obter mais informações, consulte Gerenciar o ciclo de vida dos objetos. Para ter informações sobre como criar configurações de ciclo de vida do S3 usando o AWS Management Console, a AWS CLI, os AWS SDKs ou a API REST, consulte Definir uma configuração do Ciclo de Vida do S3 em um bucket.

> **Important**
>
> Se você tem uma configuração de ciclo de vida de expiração do objeto em seu bucket sem versionamento e quiser manter o mesmo comportamento de exclusão permanente quando ativar o versionamento, precisará adicionar uma configuração de expiração de versão não corrente. A política de validade do ciclo de vida não atual gerencia as exclusões de versões de objeto não atuais no bucket habilitado para versionamento. (Um bucket habilitado para versionamento mantém uma versão atual e zero ou mais versões desatualizadas de objetos.) Para obter mais informações, consulte Definir uma configuração do Ciclo de Vida do S3 em um bucket.

Para obter informações sobre como trabalhar com o Versionamento do S3, consulte os tópicos a seguir.

Tópicos

- Como funciona o Versionamento do S3
- Habilitar o versionamento em buckets
- Configurando a exclusão de MFA
- Trabalhar com objetos em um bucket com versionamento habilitado
- Trabalhar com objetos em um bucket com versionamento suspenso
- Solucionar problemas de versionamento

Como funciona o Versionamento do S3

Você pode usar o versionamento do S3 para manter várias versões de um objeto em um bucket com o intuito de restaurar objetos excluídos ou substituídos acidentalmente. Por exemplo, se você aplicar o versionamento do S3 a um bucket, as seguintes alterações ocorrerão:

- Se você excluir um objeto em vez de removê-lo permanentemente, o Amazon S3 inserirá um marcador de exclusão, o que se torna a versão atual do objeto. Você pode então restaurar a versão anterior. Para obter mais informações, consulte Excluir versões de objetos de um bucket com versionamento habilitado.
- Se você substituir um objeto, o Amazon S3 adicionará uma nova versão do objeto no bucket. A versão anterior permanecerá no bucket e se tornará uma versão desatualizada. Você poderá restaurar a versão anterior.

> **Note**
>
> As taxas normais do Amazon S3 se aplicam a cada versão de um objeto armazenado e transferido. Cada versão de um objeto é um objeto inteiro, e não um diff da versão anterior. Assim, se você tiver três versões de um objeto armazenado, será cobrado pelos três objetos.

Cada bucket do S3 que você cria tem um sub-recurso de versionamento associado a ele. (Para obter mais informações, consulte opções de configuração de bucket de uso geral.) Por padrão, seu bucket não está habilitado para versionamento e o sub-recurso de versionamento armazena uma configuração vazia de versionamento, como mostrado a seguir.

```
<VersioningConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
```

```
</VersioningConfiguration>
```

Para habilitar o versionamento, você pode enviar uma solicitação ao Amazon S3 com uma configuração de versionamento que inclui um status `Enabled`.

```
<VersioningConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Status>Enabled</Status>
</VersioningConfiguration>
```

Para suspender o versionamento, você define o valor do status como `Suspended`.

> **Note**
>
> Quando você habilitar o versionamento em um bucket pela primeira vez, poderá levar um curto período para que a alteração seja totalmente propagada. Enquanto essa alteração está se propagando, você pode encontrar erros `HTTP 404 NoSuchKey` intermitentes nas solicitações de objetos criados ou atualizados após a habilitação do versionamento. Recomendamos que você aguarde 15 minutos depois de habilitar o versionamento para emitir operações de gravação (`PUT` ou `DELETE`) em objetos no bucket.

O proprietário do bucket e todos os usuários autorizados do AWS Identity and Access Management (IAM) podem habilitar o versionamento. O proprietário do bucket é a Conta da AWS que criou o bucket. Para obter mais informações sobre permissões, consulte Gerenciamento de identidade e acesso para o Amazon S3.

Para obter mais informações sobre como habilitar e desabilitar o versionamento do S3 usando o AWS Management Console, a AWS Command Line Interface (AWS CLI) ou a API REST, consulte the section called “Habilitar o versionamento em buckets”.

Tópicos

- IDs de versão
- Fluxos de trabalho de versionamento

IDs de versão

Se o versionamento estiver habilitado para um bucket, o Amazon S3 gerará um ID de versão exclusivo automaticamente para o objeto que está sendo armazenado. Por exemplo, em um bucket,

você pode ter dois objetos com a mesma chave (nome do objeto), mas diferentes IDs de versão, como `photo.gif` (versão 111111) e `photo.gif` (versão 121212).
Diagrama que retrata um bucket com versionamento habilitado que tem dois objetos com a mesma chave e IDs de versão diferentes.

Cada objeto tem um ID de versão, mesmo que o versionamento do S3 não esteja habilitado. Se o versionamento do S3 não estiver habilitado, o Amazon S3 definirá o valor do ID da versão como `null`. Se o S3 Versioning for habilitado, o Amazon S3 atribuirá um valor de ID de versão para o objeto. Esse valor o distingue de outras versões da mesma chave.

Quando você habilita o S3 Versioning em um bucket existente, os objetos que já estão armazenados no bucket permanecem inalterados. Os IDs de versão (`null`), o conteúdo e as permissões continuarão os mesmos. Depois que habilitar o versionamento do S3, cada objeto adicionado ao bucket obterá um ID de versão, que o distinguirá de outras versões da mesma chave.

Somente o Amazon S3 gera IDs de versão, e eles não podem ser editados. Os IDs de versão são strings opacas Unicode, com codificação UTF-8 e prontas para URL que não têm mais de 1.024 bytes de comprimento. Veja um exemplo a seguir:

```
3sL4kqtJlcpXroDTDmJ+rmSpXd3dIbrHY+MTRCxf3vjVBH40Nr8X8gdRQBpUMLUo
```

> **Note**
>
> Por simplicidade, os outros exemplos neste tópico usam IDs muito mais curtos.

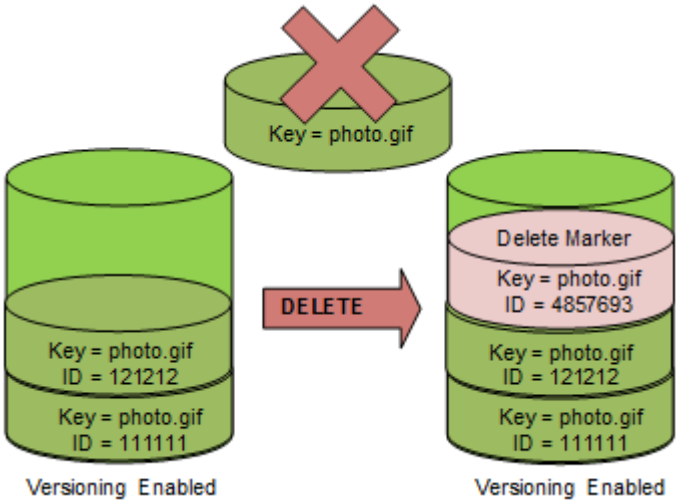
Fluxos de trabalho de versionamento

Quando você PUT um objeto em um bucket com versionamento ativado, a versão desatualizada não é substituída. Conforme mostrado na seguinte figura, quando uma nova versão de `photo.gif` é PUT em um bucket que já contém um objeto com o mesmo nome, o seguinte comportamento ocorre:

- O objeto original (ID = 111111) permanece no bucket.
- O Amazon S3 gera um novo ID de versão (121212) e adiciona essa versão mais recente do objeto ao bucket.

Com essa funcionalidade, você poderá recuperar uma versão anterior de um objeto se um objeto tiver sido sobrescrito ou excluído acidentalmente.

Quando você aplica DELETE em um objeto, todas as versões permanecem no bucket e o Amazon S3 insere um marcador de exclusão, conforme exibido na figura a seguir.



O marcador de exclusão torna-se a versão atual de objeto. Por padrão, o GET requisita a recuperação da versão armazenada mais recente. A execução de uma solicitação `GET Object` quando a versão atual é um marcador de exclusão retorna um erro `404 Not Found`, conforme exibido na figura a seguir.

Você pode, contudo, fazer uma solicitação GET de uma versão desatualizada de um objeto por especificar seu ID de versão. Na figura a seguir, você faz uma solicitação GET de uma versão específica de objeto, 111111. O Amazon S3 retorna a versão desse objeto, apesar de não ser a versão atual.

Para obter mais informações, consulte Recuperando versões de objeto de um bucket habilitado para versionamento.

Você pode excluir permanentemente um objeto, especificando a versão que deseja excluir. Somente o proprietário de um bucket do Amazon S3 ou um usuário do IAM autorizado pode excluir uma versão permanentemente. Se a operação DELETE especificar o `versionId`, essa versão do objeto será excluída permanentemente e o Amazon S3 não inserirá um marcador de exclusão.

Você pode obter segurança adicional configurando um bucket para habilitar a exclusão com autenticação multifator (MFA). Quando você habilita a exclusão com MFA para um bucket, o proprietário do bucket precisa incluir dois formulários de autenticação em qualquer solicitação para excluir uma versão ou modificar o estado de versionamento do bucket. Para obter mais informações, consulte Configurando a exclusão de MFA.

Quando novas versões são criadas para um objeto?

Novas versões de objetos são criadas somente quando você aplica PUT em um novo objeto. Esteja ciente de que certas ações como `CopyObject` funcionam implementando uma operação PUT.

Algumas ações que modificam o objeto atual não criam uma versão porque elas não aplicam PUT em um novo objeto. Isso inclui ações como alterar as tags em um objeto.

> **Important**
>
> Se você perceber um aumento significativo do número de respostas HTTP 503 (Serviço indisponível) recebidas para solicitações PUT ou DELETE de objetos do Amazon S3 a um bucket que tenha o versionamento do S3 habilitado, talvez tenha um ou mais objetos no bucket para os quais há milhões de versões. Para ter mais informações, consulte a seção Versionamento do S3 de Solucionar problemas de versionamento.

Habilitar o versionamento em buckets

Use o S3 Versioning para manter várias versões de um objeto em um bucket. Esta seção fornece exemplos de como habilitar o versionamento em um bucket usando o console, a API REST, os AWS SDKs e a AWS Command Line Interface (AWS CLI).

> **Note**
>
> Ao habilitar o versionamento em um bucket pela primeira vez, poderá levar até 15 minutos para que a alteração seja totalmente propagada no sistema do S3. Durante esse período, as solicitações `GET` de objetos criados ou atualizados após a habilitação do versionamento podem gerar erros `HTTP 404 NoSuchKey`. Recomendamos aguardar 15 minutos depois de habilitar o versionamento para executar quaisquer operações de gravação (`PUT` ou `DELETE`) em objetos no bucket. Esse período de espera ajuda a evitar possíveis problemas com a visibilidade de objetos e o rastreamento de versões.

Para obter mais informações sobre o S3 Versioning, consulte Reter várias versões de objetos com o Versionamento do S3. Para obter informações sobre como trabalhar com objetos que estão em buckets habilitados para versão, consulte Trabalhar com objetos em um bucket com versionamento habilitado.

Para saber mais sobre como usar o Versionamento do S3 para proteger dados, consulte Tutorial: Protecting data on Amazon S3 against accidental deletion or application bugs using S3 Versioning, S3 Object Lock, and S3 Replication (Tutorial: Proteção de dados no Amazon S3 contra exclusão acidental ou bugs de aplicações usando o Versionamento do S3, o Bloqueio de Objeto do S3 e a Replicação do S3.

Cada bucket do S3 que você cria tem um sub-recurso de versionamento associado a ele. (Para obter mais informações, consulte opções de configuração de bucket de uso geral.) Por padrão, seu bucket não está habilitado para versionamento e o sub-recurso de versionamento armazena uma configuração vazia de versionamento, como mostrado a seguir.

```
<VersioningConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
</VersioningConfiguration>
```

Para habilitar o versionamento, você pode enviar uma solicitação ao Amazon S3 com uma configuração de versionamento que inclui um status.

```
<VersioningConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Status>Enabled</Status>
</VersioningConfiguration>
```

Para suspender o versionamento, você define o valor do status como `Suspended`.

O proprietário do bucket e todos os usuários autorizados podem habilitar o versionamento. O proprietário do bucket é a Conta da AWS que criou o bucket (a conta root). Para obter mais informações sobre permissões, consulte Gerenciamento de identidade e acesso para o Amazon S3.

As seções a seguir fornecem mais detalhes sobre como ativar o versionamento do S3 usando o console, a AWS CLI e os AWS SDKs.

Uso do console do S3

Siga estas etapas para usar o AWS Management Console para habilitar o versionamento em um bucket do S3.

Como habilitar ou desabilitar o versionamento em um bucket de uso geral do S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.

2. No painel de navegação à esquerda, escolha Buckets de uso geral.
3. Na lista de buckets, escolha o nome do bucket para o qual você deseja habilitar o versionamento.
4. Escolha Properties (Propriedades).
5. Em Bucket Versioning (Versionamento de bucket), escolha Edit (Editar).
6. Escolha Suspend (Suspender) ou Enable (Ativar), e selecione Save changes (Salvar alterações).

> **Note**
>
> Você pode usar a autenticação multifator (MFA) da AWS com versionamento. Ao usar a MFA com versionamento, você deve fornecer as chaves de acesso da sua Conta da AWS e um código válido do dispositivo MFA da conta para excluir permanentemente uma versão de objeto ou suspender ou reativar o versionamento.
>
> Para usar a MFA com versionamento, você habilita `MFA Delete`. No entanto, não é possível habilitar o `MFA Delete` usando o AWS Management Console. É necessário usar a AWS Command Line Interface (AWS CLI) ou API. Para obter mais informações, consulte Configurando a exclusão de MFA.

Usar a AWS CLI

O exemplo a seguir habilita o versionamento em um bucket de uso geral do S3.

```
aws s3api put-bucket-versioning --bucket amzn-s3-demo-bucket1 --versioning-
configuration Status=Enabled
```

O exemplo a seguir ativa o versionamento do S3 e a exclusão de autenticação multifator (MFA) em um bucket.

```
aws s3api put-bucket-versioning --bucket amzn-s3-demo-bucket1 --versioning-
configuration Status=Enabled,MFADelete=Enabled --mfa "SERIAL 123456"
```

> **Note**
>
> O uso da exclusão de MFA requer um dispositivo de autenticação física ou virtual aprovado. Para obter mais informações sobre como usar exclusão de MFA no Amazon S3, consulte Configurando a exclusão de MFA.

Para obter mais informações sobre como ativar o versionamento usando a AWS CLI, consulte put-bucket-versioning na Referência de comandos da AWS CLI.

Uso da SDKs AWS

Os exemplos a seguir permitem o versionamento em um bucket e, em seguida, recuperam o status do versionamento usando o AWS SDK para Java e o AWS SDK para .NET. Para obter informações sobre o uso de outros AWS SDKs, consulte o Centro do Desenvolvedor da AWS.

.NET

Para obter informações sobre como configurar e executar exemplos de código, consulte Conceitos básicos do AWS SDK for .NET no Guia do desenvolvedor do AWS SDK for .NET.

```
using System;
using Amazon.S3;
using Amazon.S3.Model;

namespace s3.amazon.com.docsamples
{
    class BucketVersioningConfiguration
    {
        static string bucketName = "*** bucket name ***";

        public static void Main(string[] args)
        {
            using (var client = new AmazonS3Client(Amazon.RegionEndpoint.USEast1))
            {
                try
                {
                    EnableVersioningOnBucket(client);
                    string bucketVersioningStatus =
 RetrieveBucketVersioningConfiguration(client);
                }
                catch (AmazonS3Exception amazonS3Exception)
```

```
                {
                    if (amazonS3Exception.ErrorCode != null &&
                        (amazonS3Exception.ErrorCode.Equals("InvalidAccessKeyId")
                        ||
                        amazonS3Exception.ErrorCode.Equals("InvalidSecurity")))
                    {
                        Console.WriteLine("Check the provided AWS Credentials.");
                        Console.WriteLine(
                        "To sign up for service, go to http://aws.amazon.com/s3");
                    }
                    else
                    {
                        Console.WriteLine(
                         "Error occurred. Message:'{0}' when listing objects",
                         amazonS3Exception.Message);
                    }
                }
            }

            Console.WriteLine("Press any key to continue...");
            Console.ReadKey();
        }

        static void EnableVersioningOnBucket(IAmazonS3 client)
        {

                PutBucketVersioningRequest request = new PutBucketVersioningRequest
                {
                    BucketName = bucketName,
                    VersioningConfig = new S3BucketVersioningConfig
                    {
                        Status = VersionStatus.Enabled
                    }
                };

                PutBucketVersioningResponse response =
client.PutBucketVersioning(request);
        }


        static string RetrieveBucketVersioningConfiguration(IAmazonS3 client)
        {
                GetBucketVersioningRequest request = new GetBucketVersioningRequest
                {
```

```
                    BucketName = bucketName
                };

                GetBucketVersioningResponse response =
 client.GetBucketVersioning(request);
                return response.VersioningConfig.Status;
            }
    }
}
```

Java

Consulte instruções sobre como criar e testar uma amostra funcional em Getting Started no Guia do desenvolvedor do AWS SDK para Java.

```
import java.io.IOException;

import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Region;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3Client;
import com.amazonaws.services.s3.model.AmazonS3Exception;
import com.amazonaws.services.s3.model.BucketVersioningConfiguration;
import com.amazonaws.services.s3.model.SetBucketVersioningConfigurationRequest;

public class BucketVersioningConfigurationExample {
    public static String bucketName = "*** bucket name ***";
    public static AmazonS3Client s3Client;

    public static void main(String[] args) throws IOException {
        s3Client = new AmazonS3Client(new ProfileCredentialsProvider());
        s3Client.setRegion(Region.getRegion(Regions.US_EAST_1));
        try {

            // 1. Enable versioning on the bucket.
         BucketVersioningConfiguration configuration =
           new BucketVersioningConfiguration().withStatus("Enabled");

   SetBucketVersioningConfigurationRequest setBucketVersioningConfigurationRequest
 =
     new SetBucketVersioningConfigurationRequest(bucketName,configuration);
```

```
 s3Client.setBucketVersioningConfiguration(setBucketVersioningConfigurationRequest);

   // 2. Get bucket versioning configuration information.
   BucketVersioningConfiguration conf =
 s3Client.getBucketVersioningConfiguration(bucketName);
    System.out.println("bucket versioning configuration status:    " +
 conf.getStatus());

        } catch (AmazonS3Exception amazonS3Exception) {
            System.out.format("An Amazon S3 error occurred. Exception: %s",
 amazonS3Exception.toString());
        } catch (Exception ex) {
            System.out.format("Exception: %s", ex.toString());
        }
    }
}
```

Python

O exemplo de código Python a seguir cria um bucket do Amazon S3 bucket, habilita-o para versionamento e configura um ciclo de vida que faz com que versões não atuais de objetos expirem após 7 dias.

```
def create_versioned_bucket(bucket_name, prefix):
    """
    Creates an Amazon S3 bucket, enables it for versioning, and configures a
 lifecycle
    that expires noncurrent object versions after 7 days.

    Adding a lifecycle configuration to a versioned bucket is a best practice.
    It helps prevent objects in the bucket from accumulating a large number of
    noncurrent versions, which can slow down request performance.

    Usage is shown in the usage_demo_single_object function at the end of this
 module.

    :param bucket_name: The name of the bucket to create.
    :param prefix: Identifies which objects are automatically expired under the
                   configured lifecycle rules.
    :return: The newly created bucket.
    """
    try:
```

```
        bucket = s3.create_bucket(
            Bucket=bucket_name,
            CreateBucketConfiguration={
                "LocationConstraint": s3.meta.client.meta.region_name
            },
        )
        logger.info("Created bucket %s.", bucket.name)
    except ClientError as error:
        if error.response["Error"]["Code"] == "BucketAlreadyOwnedByYou":
            logger.warning("Bucket %s already exists! Using it.", bucket_name)
            bucket = s3.Bucket(bucket_name)
        else:
            logger.exception("Couldn't create bucket %s.", bucket_name)
            raise

    try:
        bucket.Versioning().enable()
        logger.info("Enabled versioning on bucket %s.", bucket.name)
    except ClientError:
        logger.exception("Couldn't enable versioning on bucket %s.", bucket.name)
        raise

    try:
        expiration = 7
        bucket.LifecycleConfiguration().put(
            LifecycleConfiguration={
                "Rules": [
                    {
                        "Status": "Enabled",
                        "Prefix": prefix,
                        "NoncurrentVersionExpiration": {"NoncurrentDays":
expiration},
                    }
                ]
            }
        )
        logger.info(
            "Configured lifecycle to expire noncurrent versions after %s days "
            "on bucket %s.",
            expiration,
            bucket.name,
        )
    except ClientError as error:
        logger.warning(
```

```
            "Couldn't configure lifecycle on bucket %s because %s. "
            "Continuing anyway.",
            bucket.name,
            error,
        )

    return bucket
```

Configurando a exclusão de MFA

Ao trabalhar com o Versionamento do S3 em buckets do Amazon S3, você pode, opcionalmente, adicionar outra camada de segurança configurando um bucket para habilitar a exclusão de MFA (autenticação multifator). Quando você faz isso, o proprietário do bucket precisa incluir dois formulários de autenticação em qualquer solicitação para excluir uma versão ou modificar o estado de versionamento do bucket.

A exclusão de MFA requer autenticação adicional para uma das seguintes operações:

- Alterar o estado de versionamento de seu bucket
- Excluir, permanentemente, uma versão de objeto

A exclusão de MFA exige duas formas de autenticação:

- Suas credenciais de segurança
- A concatenação de um número serial válido, um espaço e o código de seis dígitos exibidos em um dispositivo de autenticação aprovado

A exclusão de MFA oferece segurança adicional se, por exemplo, suas credenciais de segurança forem comprometidas. A exclusão de MFA pode ajudar a evitar exclusões acidentais de bucket exigindo que o usuário que inicia a ação de exclusão para provar a posse física de um dispositivo MFA com um código MFA e adicionando uma camada extra de atrito e segurança à ação de exclusão.

Para identificar buckets que têm exclusão de MFA habilitada, você pode usar as métricas da Lente de Armazenamento do Amazon S3. A Lente de Armazenamento do S3 é um recurso de análise de armazenamento em nuvem que você pode usar para obter visibilidade em toda a organização sobre

o uso e a atividade do armazenamento de objetos. Para obter mais informações, consulte Avaliar a atividade e o uso do armazenamento com o S3 Storage Lens. Para obter uma lista completa de métricas, consulte o Glossário de métricas da Lente de Armazenamento do S3.

O proprietário do bucket, a Conta da AWS que criou o bucket (conta raiz) e todos os usuários autorizados podem habilitar o versionamento. No entanto, somente o proprietário do bucket (conta raiz) pode habilitar a exclusão de MFA. Para obter mais informações, consulte a publicação Proteção do acesso à AWS usando MFA no Blog de segurança da AWS.

> **Note**
>
> Para usar a exclusão de MFA com versionamento, habilite `MFA Delete`. No entanto, não é possível habilitar o `MFA Delete` usando o AWS Management Console. É necessário usar a AWS Command Line Interface (AWS CLI) ou API.
>
> Para obter exemplos de como usar a exclusão de MFA com versionamento, consulte a seção de exemplos no tópico Habilitar o versionamento em buckets.
>
> Não é possível usar a exclusão de MFA com configurações de ciclo de vida. Para obter mais informações sobre as configurações de ciclo de vida e como elas interagem com outras configurações, consulte Como o Ciclo de Vida do S3 interage com outras configurações de bucket.

Para ativar ou desativar a exclusão de MFA, use a mesma API usada para configurar o versionamento em um bucket. O Amazon S3 armazena a configuração de exclusão de MFA no mesmo sub-recurso de versionamento que armazena o status de versionamento do bucket.

```
<VersioningConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Status>VersioningState</Status>
  <MfaDelete>MfaDeleteState</MfaDelete>
</VersioningConfiguration>
```

Para usar a exclusão de MFA, você pode usar um dispositivo de hardware ou MFA virtual para gerar um código de autenticação. O exemplo a seguir mostra um código de autenticação gerado exibido em um dispositivo de hardware.



A exclusão de MFA e o acesso à API protegido por MFA são recursos que visam fornecer proteção para diferentes cenários. Você configura a exclusão de MFA em um bucket para ajudar a garantir que os dados em seu bucket não sejam excluídos acidentalmente. O acesso à API protegido por MFA é usado para impor outro fator de autenticação (código MFA) ao acessar recursos confidenciais do Amazon S3. Você pode exigir que qualquer operação nesses recursos do Amazon S3 seja feita com credenciais temporárias criadas usando a MFA. Para ver um exemplo, consulte Exigir MFA.

Para obter mais informações sobre como comprar e ativar um dispositivo de autenticação, consulte Autenticação multifator.

Como ativar o versionamento do S3 e configurar a exclusão de MFA

Como usar o AWS CLI

O número de série é o número que identifica exclusivamente o dispositivo de MFA. Para dispositivos físicos de MFA, esse é o número de série exclusivo fornecido com o dispositivo. Para dispositivos de MFA virtuais, o número de série é o respectivo ARN.

O exemplo a seguir ativa o versionamento do S3 e a exclusão de autenticação multifator (MFA) em um bucket.

```
aws s3api put-bucket-versioning --bucket amzn-s3-demo-bucket1 --versioning-
configuration Status=Enabled,MFADelete=Enabled --mfa "SERIAL 123456"
```

Uso da API REST

Para obter mais informações sobre como especificar a exclusão de MFA usando a API REST do Amazon S3, consulte PutBucketVersioning na Referência de API do Amazon Simple Storage Service.

Trabalhar com objetos em um bucket com versionamento habilitado

Os objetos que são armazenados em um bucket do Amazon S3 antes da habilitação do versionamento têm um ID de versão `null`. Quando você habilita o versionamento, os objetos existentes em seu bucket não são alterados. O que muda é como o Amazon S3 trata os objetos em solicitações futuras.

Fazer a transição de versões de objeto

Você pode definir as regras de configuração de ciclo de vida de objetos que têm ciclo de vida bem definido para fazer a transição de versões de objeto para a classe de armazenamento S3 Glacier Flexible Retrieval em um momento específico no ciclo de vida do objeto. Para obter mais informações, consulte Gerenciar o ciclo de vida dos objetos.

Os tópicos nesta seção explicam várias operações de objeto em um bucket com versionamento ativado. Para obter mais informações sobre versionamento, consulte Reter várias versões de objetos com o Versionamento do S3.

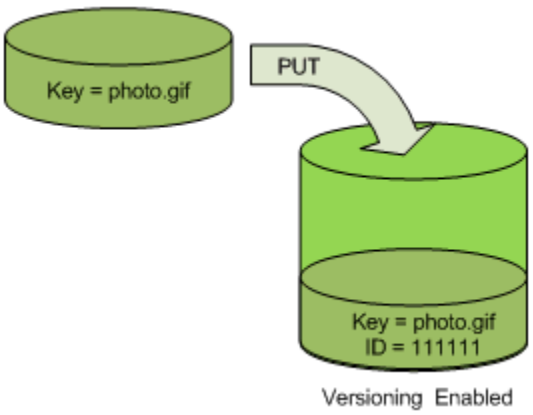
Tópicos

- Adicionar objetos a buckets com versionamento habilitado
- Listar objetos em um bucket com versionamento habilitado
- Recuperando versões de objeto de um bucket habilitado para versionamento
- Excluir versões de objetos de um bucket com versionamento habilitado
- Configurando permissões de objeto com versão

Adicionar objetos a buckets com versionamento habilitado

Depois que você habilita o versionamento em um bucket, o Amazon S3 adiciona automaticamente um ID de versão exclusivo a cada objeto armazenado (usando `PUT`, `POST` ou `CopyObject`) no bucket.

A figura a seguir mostra que o Amazon S3 adiciona um ID de versão exclusivo a um objeto quando ele é adicionado a um bucket com versionamento habilitado.



> **Note**
>
> Os valores de ID de versão que o Amazon S3 atribui são seguros para URL (podem ser incluídos como parte de um URI).

Para obter mais informações sobre versionamento, consulte Reter várias versões de objetos com o Versionamento do S3. Você pode adicionar versões de objeto a um bucket habilitado para versionamento usando o console, os AWS SDKs e a API REST.

Usar o console do

Para obter instruções, consulte Fazer upload de objetos.

Uso da SDKs AWS

Para ver exemplos de upload de objetos usando os AWS SDKs para Java, .NET e PHP, consulte Fazer upload de objetos. Os exemplos de upload de objetos em buckets com e sem versionamento habilitado são os mesmos, embora o Amazon S3 atribua um número de versão para buckets com versionamento habilitado. Caso contrário, o número de versão é nulo.

Para obter informações sobre o uso de outros AWS SDKs, consulte o Centro do Desenvolvedor da AWS.

Uso dos REST API

Para adicionar objetos a buckets com versionamento habilitado

1. Ative o versionamento de um bucket usando uma solicitação `PutBucketVersioning`.

   Para obter mais informações, consulte PutBucketVersioning na Referência da API do Amazon Simple Storage Service.
2. Envie uma solicitação `PUT`, `POST` ou `CopyObject` para armazenar um objeto no bucket.

Quando você adiciona um objeto a um bucket habilitado para versionamento, o Amazon S3 retorna o ID da versão do objeto no cabeçalho de resposta `x-amz-version-id`, como mostrado no exemplo a seguir.

```
x-amz-version-id: 3/L4kqtJlcpXroDTDmJ+rmSpXd3dIbrHY
```

Listar objetos em um bucket com versionamento habilitado

Esta seção fornece exemplos de como listar versões de objetos de um bucket com versionamento habilitado. O Amazon S3 armazena as informações de versão do objeto no sub-recurso versões associado ao bucket. Para obter mais informações, consulte opções de configuração de bucket de uso geral. Para listar os objetos em um bucket do com versionamento habilitado, a permissão `ListBucketVersions` é necessária.

Uso do console do S3

Siga estas etapas para usar o console do Amazon S3 para ver as diferentes versões de um objeto.

Para ver várias versões de um objeto

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Na lista Buckets, escolha o nome do bucket que contém o objeto.
3. Para ver uma lista das versões dos objetos no bucket, escolha a opção Show versions (Mostrar versões).

   Para cada versão do objeto, o console exibe um ID de versão exclusivo, a data e a hora em que a versão do objeto foi criada e outras propriedades. (Os objetos armazenados em seu bucket antes da habilitação do versionamento têm um ID de versão null [nulo].)

   Para listar os objetos sem as versões, escolha a opção List versions (Listar versões) .

Você também pode visualizar, fazer download e excluir versões do objeto no painel de visão geral do objeto no console. Para obter mais informações, consulte Exibir propriedades do objeto no console do Amazon S3.

> **Note**
>
> Para acessar versões de objetos anteriores a 300 versões, use a AWS CLI ou o URL do objeto.

> **Important**
>
> Você pode cancelar a exclusão de um objeto somente se ele foi excluído como a versão mais recente (atual). Não é possível cancelar a exclusão de uma versão anterior de um objeto que foi excluído. Para obter mais informações, consulte Reter várias versões de objetos com o Versionamento do S3.

Uso da SDKs AWS

Os exemplos nesta seção mostram como recuperar uma listagem de objetos de um bucket com versionamento ativado. Cada solicitação retorna até 1.000 versões, a menos que você especifique um número menor. Se o bucket contiver mais versões que esse limite, envie uma série de solicitações para recuperar a lista de todas as versões. Esse processo de retornar resultados em "páginas" é chamado paginação.

Para mostrar como a paginação funciona, os exemplos limitam cada resposta a duas versões de objeto. Depois de recuperar a primeira página de resultados, cada exemplo verifica se a lista de versões foi truncada. Em caso afirmativo, o exemplo continua a recuperar páginas até que todas as versões tenham sido recuperadas.

> **Note**
>
> Os exemplos a seguir também funcionam com bucket sem versionamento, ou para objetos sem versões individuais. Nesses casos, o Amazon S3 retorna a listagem de objetos com um ID de versão `null`.

Para obter informações sobre o uso de outros AWS SDKs, consulte o Centro do Desenvolvedor da AWS.

Java

Consulte instruções sobre como criar e testar uma amostra funcional em Getting Started no Guia do desenvolvedor do AWS SDK para Java.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
```

```
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.ListVersionsRequest;
import com.amazonaws.services.s3.model.S3VersionSummary;
import com.amazonaws.services.s3.model.VersionListing;

public class ListKeysVersioningEnabledBucket {

    public static void main(String[] args) {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "*** Bucket name ***";

        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(clientRegion)
                    .build();

            // Retrieve the list of versions. If the bucket contains more versions
            // than the specified maximum number of results, Amazon S3 returns
            // one page of results per request.
            ListVersionsRequest request = new ListVersionsRequest()
                    .withBucketName(bucketName)
                    .withMaxResults(2);
            VersionListing versionListing = s3Client.listVersions(request);
            int numVersions = 0, numPages = 0;
            while (true) {
                numPages++;
                for (S3VersionSummary objectSummary :
 versionListing.getVersionSummaries()) {
                    System.out.printf("Retrieved object %s, version %s\n",
                            objectSummary.getKey(),
                            objectSummary.getVersionId());
                    numVersions++;
                }
                // Check whether there are more pages of versions to retrieve. If
                // there are, retrieve them. Otherwise, exit the loop.
                if (versionListing.isTruncated()) {
                    versionListing =
 s3Client.listNextBatchOfVersions(versionListing);
                } else {
                    break;
                }
```

```
            }
            System.out.println(numVersions + " object versions retrieved in " +
 numPages + " pages");
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

.NET

Para obter informações sobre como configurar e executar exemplos de código, consulte Conceitos básicos do AWS SDK for .NET no Guia do desenvolvedor do AWS SDK for .NET.

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class ListObjectsVersioningEnabledBucketTest
    {
        static string bucketName = "*** bucket name ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 s3Client;

        public static void Main(string[] args)
        {
            s3Client = new AmazonS3Client(bucketRegion);
            GetObjectListWithAllVersionsAsync().Wait();
        }
```

```
        static async Task GetObjectListWithAllVersionsAsync()
        {
            try
            {
                ListVersionsRequest request = new ListVersionsRequest()
                {
                    BucketName = bucketName,
                    // You can optionally specify key name prefix in the request
                    // if you want list of object versions of a specific object.

                    // For this example we limit response to return list of 2
versions.
                    MaxKeys = 2
                };
                do
                {
                    ListVersionsResponse response = await
s3Client.ListVersionsAsync(request);
                    // Process response.
                    foreach (S3ObjectVersion entry in response.Versions)
                    {
                        Console.WriteLine("key = {0} size = {1}",
                            entry.Key, entry.Size);
                    }

                    // If response is truncated, set the marker to get the next
                    // set of keys.
                    if (response.IsTruncated)
                    {
                        request.KeyMarker = response.NextKeyMarker;
                        request.VersionIdMarker = response.NextVersionIdMarker;
                    }
                    else
                    {
                        request = null;
                    }
                } while (request != null);
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered on server. Message:'{0}' when
writing an object", e.Message);
            }
            catch (Exception e)
```

```
            {
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
 writing an object", e.Message);
            }
        }
    }
}
```

Uso da API REST

Example — Listar todas as versões de objeto em um bucket

Para listar todas as versões de todos os objetos em um bucket, você usa o sub-recurso `versions` em uma solicitação `GET Bucket`. O Amazon S3 pode recuperar no máximo 1.000 objetos, e cada versão de objeto conta como um objeto completo. Portanto, se um bucket contiver duas chaves (por exemplo, `photo.gif` e `picture.jpg`) e a primeira chave tiver 990 versões e a segunda chave tiver 400 versões, uma solicitação única recuperará as 990 versões de `photo.gif` e apenas as 10 versões mais recentes de `picture.jpg`.

O Amazon S3 retorna as versões de objetos na ordem em que foram armazenadas, com as armazenadas mais recentemente sendo retornadas primeiro.

Em uma solicitação `GET Bucket`, inclua o sub-recurso `versions`.

```
GET /?versions HTTP/1.1
Host: bucketName.s3.amazonaws.com
Date: Wed, 28 Oct 2009 22:32:00 +0000
Authorization: AWS AKIAIOSFODNN7EXAMPLE:0RQf4/cRonhpaBX5sCYVf1bNRuU=
```

Example — Recuperar todas as versões de uma chave

Para recuperar um subconjunto de versões de objeto, use os parâmetros de solicitação para `GET Bucket`. Para obter mais informações, consulte GET Bucket.

1. Defina o parâmetro `prefix` como a chave do objeto que você deseja recuperar.
2. Envie uma solicitação `GET Bucket` usando o sub-recurso `versions` e `prefix`.

   ```
   GET /?versions&prefix=objectName HTTP/1.1
   ```

Example — Recuperar objetos usando um prefixo

O exemplo a seguir recupera objetos cuja chave é ou começa com `myObject`.

```
GET /?versions&prefix=myObject HTTP/1.1
Host: bucket.s3.amazonaws.com
Date: Wed, 28 Oct 2009 22:32:00 GMT
Authorization: AWS AKIAIOSFODNN7EXAMPLE:0RQf4/cRonhpaBX5sCYVf1bNRuU=
```

Você pode usar os outros parâmetros de solicitação para recuperar um subconjunto de todas as versões do objeto. Para obter mais informações, consulte GET Bucket na Referência da API do Amazon Simple Storage Service.

Example — Recuperar uma listagem de objetos adicionais se a resposta estiver truncada

Se o número de objetos que podem ser retornados em uma solicitação `GET` exceder o valor de `max-keys`, a resposta conterá `<isTruncated>true</isTruncated>` e incluirá a primeira chave (em `NextKeyMarker`) e o primeiro ID de versão (em `NextVersionIdMarker`) que satisfazem a solicitação, mas que não foram retornados. Você usa esses valores retornados como a posição de início em uma solicitação subsequente para recuperar os objetos adicionais que satisfazem a solicitação `GET`.

Use o seguinte processo para recuperar os objetos adicionais que satisfazem a solicitação `GET Bucket versions` original de um bucket. Para obter mais informações sobre `key-marker`, `version-id-marker`, `NextKeyMarker` e `NextVersionIdMarker`, consulte GET Bucket na Referência da API do Amazon Simple Storage Service.

A seguir estão as respostas adicionais que atendem à solicitação `GET` original:

- Defina o valor de `key-marker` como a chave retornada em `NextKeyMarker` na resposta anterior.
- Defina o valor de `version-id-marker` como o ID de versão retornado em `NextVersionIdMarker` na resposta anterior.
- Envie uma solicitação `GET Bucket versions` usando `key-marker` e `version-id-marker`.

Example — Recuperar objetos que começam com a chave e o ID de versão especificados

```
GET /?versions&key-marker=myObject&version-id-marker=298459348571 HTTP/1.1
```

```
Host: bucket.s3.amazonaws.com
Date: Wed, 28 Oct 2009 22:32:00 GMT
Authorization: AWS AKIAIOSFODNN7EXAMPLE:0RQf4/cRonhpaBX5sCYVf1bNRuU=
```

Como usar o AWS CLI

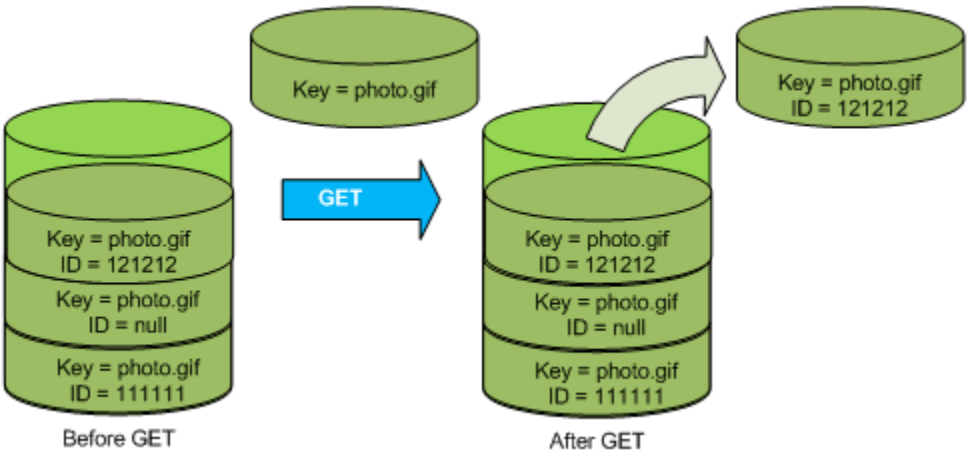
O comando a seguir retorna os metadados de todas as versões dos objetos em um bucket.

```
aws s3api list-object-versions --bucket amzn-s3-demo-bucket1
```

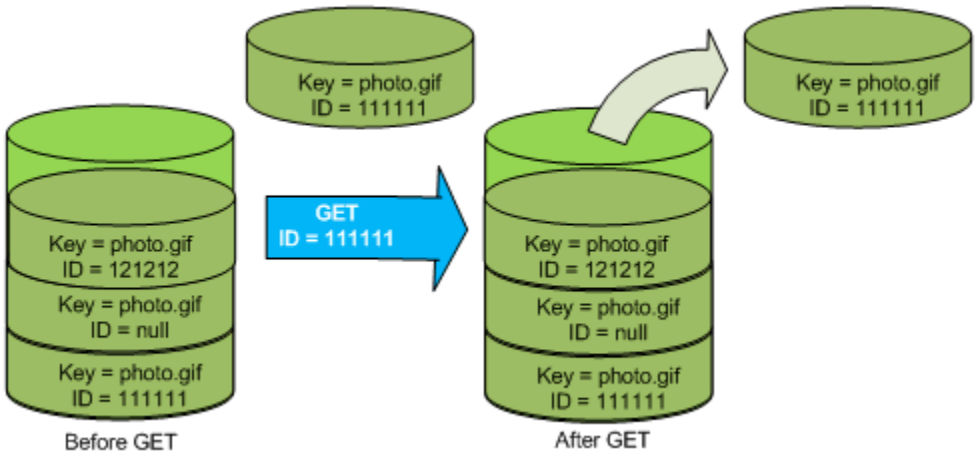
Para obter mais informações sobre `list-object-versions`, consulte list-object-versions na Referência de comandos de AWS CLI.

Recuperando versões de objeto de um bucket habilitado para versionamento

O versionamento no Amazon S3 é uma maneira de manter várias variantes de um objeto no mesmo bucket. Uma solicitação `GET` simples recupera a versão atual de um objeto. A figura a seguir mostra como o `GET` retorna a versão atual do objeto, `photo.gif`.



Para recuperar uma versão específica, você tem que especificar seu ID de versão. A figura a seguir mostra que a solicitação `GET versionId` recupera a versão especificada do objeto (não necessariamente a versão atual).



Você pode recuperar versões de objeto no Amazon S3 usando o console, os AWS SDKs ou a API REST.

> **Note**
>
> Para acessar versões de objetos anteriores a 300 versões, use a AWS CLI ou o URL do objeto.

Uso do console do S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Na lista Buckets, escolha o nome do bucket que contém o objeto.
3. Na lista Objetos , escolha o nome do objeto.
4. Escolha Versões.

   O Amazon S3 mostra todas as versões do objeto.
5. Marque a caixa de seleção ao lado do ID da versão para as versões que deseja recuperar.
6. Escolha Ações, escolha Downloade salve o objeto.

Você também pode visualizar, fazer download e excluir versões do objeto no painel de visão geral do objeto. Para obter mais informações, consulte Exibir propriedades do objeto no console do Amazon S3.

> **Important**
>
> Você pode cancelar a exclusão de um objeto somente se ele foi excluído como a versão mais recente (atual). Não é possível cancelar a exclusão de uma versão anterior de um objeto que foi excluído. Para obter mais informações, consulte Reter várias versões de objetos com o Versionamento do S3.

Uso da SDKs AWS

Os exemplos para carregar objetos em buckets não versionados e habilitados para versionamento são os mesmos. No entanto, para buckets habilitados para versionamento, o Amazon S3 atribui um número de versão. Caso contrário, o número de versão é nulo.

Para obter exemplos de download de objetos usando AWS SDKs for Java, .NET e PHP, consulte Download de objetos.

Para obter exemplos de como listar a versão de objetos usando AWS SDKs para.NET e Rust, consulte Listar a versão dos objetos em um bucket do Amazon S3.

Uso da API REST

Para recuperar uma versão específica do objeto

1. Defina `versionId` como o ID da versão do objeto que você deseja recuperar.
2. Envie uma solicitação `GET Object versionId`.

Example — Recuperar um objeto versionado

A seguinte solicitação recupera a versão `L4kqtJlcpXroDTDmpUMLUo` do `my-image.jpg`.

```
GET /my-image.jpg?versionId=L4kqtJlcpXroDTDmpUMLUo HTTP/1.1
Host: bucket.s3.amazonaws.com
Date: Wed, 28 Oct 2009 22:32:00 GMT
Authorization: AWS AKIAIOSFODNN7EXAMPLE:0RQf4/cRonhpaBX5sCYVf1bNRuU=
```

Você pode recuperar apenas os metadados de um objeto (não o conteúdo). Para obter mais informações, consulte the section called “Recuperação de metadados de versão”.

Para obter informações sobre como restaurar uma versão de objeto anterior, consulte the section called “Restaurar versões anteriores”.

Recuperar metadados de uma versão de objeto

Se você quiser recuperar apenas os metadados (e não o conteúdo) de um objeto, use a operação `HEAD`. Por padrão, você obtém os metadados da versão mais recente. Para recuperar os metadados de um objeto específico, você especifica seu ID de versão.

Para recuperar os metadados de uma versão do objeto

1. Defina `versionId` como o ID da versão do objeto cujos metadados você deseja recuperar.
2. Envie uma solicitação `HEAD Object versionId`.

Example — Recuperar metadados de um objeto versionado

A solicitação a seguir recupera os metadados da versão `3HL4kqCxf3vjVBH40Nrjfkd` de `my-image.jpg`.

```
HEAD /my-image.jpg?versionId=3HL4kqCxf3vjVBH40Nrjfkd HTTP/1.1
Host: bucket.s3.amazonaws.com
Date: Wed, 28 Oct 2009 22:32:00 GMT
Authorization: AWS AKIAIOSFODNN7EXAMPLE:0RQf4/cRonhpaBX5sCYVf1bNRuU=
```

A seguir, um exemplo de resposta.

```
HTTP/1.1 200 OK
x-amz-id-2: ef8yU9AS1ed4OpIszj7UDNEHGran
x-amz-request-id: 318BC8BC143432E5
x-amz-version-id: 3HL4kqtJlcpXroDTDmjVBH40Nrjfkd
Date: Wed, 28 Oct 2009 22:32:00 GMT
Last-Modified: Sun, 1 Jan 2006 12:00:00 GMT
ETag: "fba9dede5f27731c9771645a39863328"
Content-Length: 434234
Content-Type: text/plain
Connection: close
Server: AmazonS3
```

Restaurar versões anteriores

Você pode usar o versionamento para recuperar versões anteriores de um objeto. Existem duas abordagens para se fazer isso:

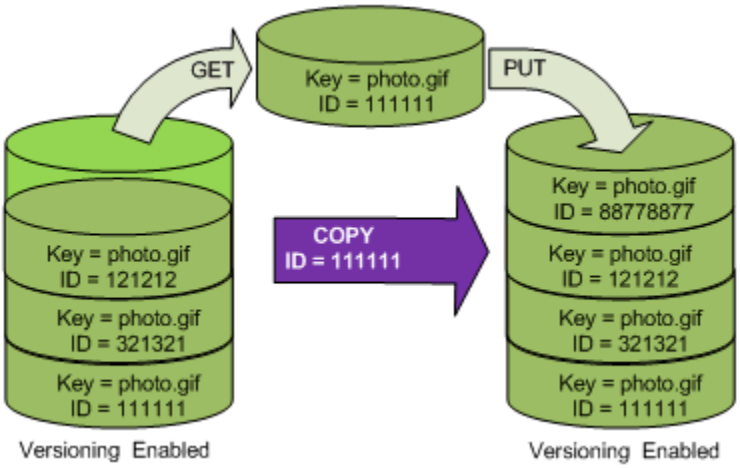
- Copie uma versão anterior do objeto para o mesmo bucket.

  O objeto copiado torna-se a versão atual desse objeto e todas as versões são preservadas.

- Exclua permanentemente a versão atual do objeto.

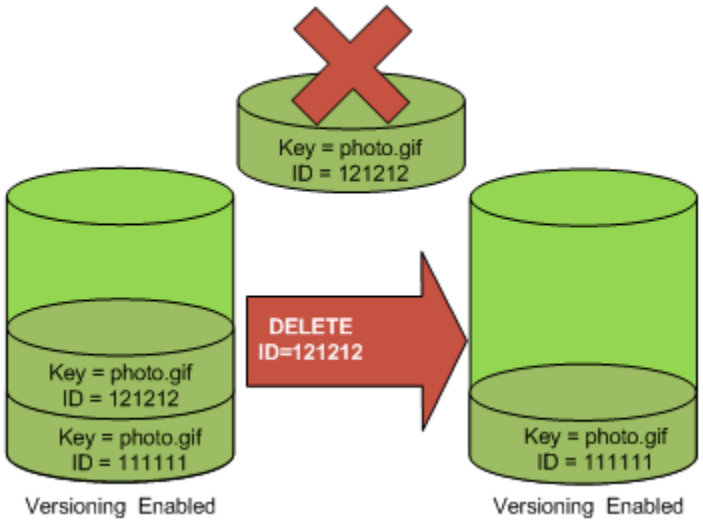
  Quando você exclui a versão atual do objeto, torna a versão anterior a versão atual desse objeto.

Como todas as versões do objeto são preservadas, você pode fazer de qualquer versão anterior a versão atual copiando uma versão específica do objeto para o mesmo bucket. Na figura a seguir, o objeto de origem (ID = 111111) é copiado para o mesmo bucket. O Amazon S3 fornece um novo ID (88778877) e ele se torna a versão atual do objeto. Assim, o bucket tem tanto a versão original (111111) quanto a cópia (88778877) do objeto. Para obter mais informações sobre como obter uma versão anterior e carregá-la para torná-la a versão atual, consulte Recuperação de versões de objeto de um bucket habilitado para versionamento e Upload de objetos.



Um subsequente GET recupera a versão 88778877.

A figura a seguir mostra como excluir a versão atual (121212) de um objeto deixa a versão anterior (111111) como a atual do objeto. Para obter mais informações sobre como excluir um objeto, consulte Excluir um único objeto.



Um subsequente GET recupera a versão 111111.

> **Note**
>
> Para restaurar versões de objetos em lotes, use a operação `CopyObject`. A operação `CopyObject` copia cada objeto especificado no manifesto. No entanto, esteja ciente de que os objetos não são necessariamente copiados na mesma ordem em que estão listados no manifesto. Para buckets versionados, se preservar a ordem de versão atual/não atual for importante, você deve copiar todas as versões não atuais primeiro. Em seguida, após a conclusão do primeiro trabalho, copie as versões atuais em um trabalho subsequente.

Para restaurar versões anteriores de objetos

Para ter mais informações sobre como restaurar objetos, consulte How can I retrieve an Amazon S3 object that was deleted in a versioning-enabled bucket? no Centro de Conhecimento do AWS re:Post.

Uso do console do S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Na lista Buckets, escolha o nome do bucket que contém o objeto.
3. Na lista Objetos , escolha o nome do objeto.
4. Escolha Versões.

O Amazon S3 mostra todas as versões do objeto.

5. Marque a caixa de seleção ao lado do ID da versão para as versões que deseja recuperar.
6. Escolha Ações, escolha Downloade salve o objeto.

Você também pode visualizar, fazer download e excluir versões do objeto no painel de visão geral do objeto. Para obter mais informações, consulte Exibir propriedades do objeto no console do Amazon S3.

> **Important**
>
> Você pode cancelar a exclusão de um objeto somente se ele foi excluído como a versão mais recente (atual). Não é possível cancelar a exclusão de uma versão anterior de um objeto que foi excluído. Para obter mais informações, consulte Reter várias versões de objetos com o Versionamento do S3.

Uso da SDKs AWS

Para obter informações sobre o uso de outros AWS SDKs, consulte o Centro do Desenvolvedor da AWS.

Python

O exemplo de código Python a seguir restaura a versão anterior de um objeto versionado excluindo todas as versões criadas após a versão de reversão especificada.

```
def rollback_object(bucket, object_key, version_id):
    """
    Rolls back an object to an earlier version by deleting all versions that
    occurred after the specified rollback version.

    Usage is shown in the usage_demo_single_object function at the end of this
 module.

    :param bucket: The bucket that holds the object to roll back.
    :param object_key: The object to roll back.
    :param version_id: The version ID to roll back to.
    """
    # Versions must be sorted by last_modified date because delete markers are
```

```
    # at the end of the list even when they are interspersed in time.
    versions = sorted(
        bucket.object_versions.filter(Prefix=object_key),
        key=attrgetter("last_modified"),
        reverse=True,
    )

    logger.debug(
        "Got versions:\n%s",
        "\n".join(
            [
                f"\t{version.version_id}, last modified {version.last_modified}"
                for version in versions
            ]
        ),
    )

    if version_id in [ver.version_id for ver in versions]:
        print(f"Rolling back to version {version_id}")
        for version in versions:
            if version.version_id != version_id:
                version.delete()
                print(f"Deleted version {version.version_id}")
            else:
                break

        print(f"Active version is now {bucket.Object(object_key).version_id}")
    else:
        raise KeyError(
            f"{version_id} was not found in the list of versions for "
f"{object_key}."
        )
```

Excluir versões de objetos de um bucket com versionamento habilitado

Você pode excluir versões de objeto de buckets do Amazon S3 sempre que desejar. Você também pode definir regras de configuração de ciclo de vida de objetos que têm um ciclo de vida bem definido para solicitar que o Amazon S3 expire as versões atuais dos objetos ou que remova permanentemente as versões anteriores dos objetos. Quando o bucket tem versionamento habilitado ou suspenso, as ações da configuração do ciclo de vida funcionam do seguinte modo:

- A `Expiration` ação se aplica à versão atual do objeto. Em vez de excluir a versão atual do objeto, o Amazon S3 a retém como uma versão desatualizada adicionando um marcador de exclusão, que se torna a versão atual.
- A ação `NoncurrentVersionExpiration` aplica-se a versões antigas do objeto, e o Amazon S3 remove permanentemente essas versões do objeto. Você não pode recuperar objetos removidos permanentemente.

Para obter mais informações sobre o Ciclo de Vida do S3, consulte Gerenciar o ciclo de vida dos objetos e Exemplos de configurações do Ciclo de Vida do S3.

Para ver quantas versões de objetos atuais e desatualizadas seus buckets têm, você pode usar as métricas da Lente de Armazenamento do Amazon S3. A Lente de Armazenamento do S3 é um recurso de análise de armazenamento em nuvem que você pode usar para obter visibilidade em toda a organização sobre o uso e a atividade do armazenamento de objetos. Para obter mais informações, consulte Usar a Lente de Armazenamento do S3 para otimizar os custos do armazenamento. Para obter uma lista completa de métricas, consulte o Glossário de métricas da Lente de Armazenamento do S3.

> **Note**
>
> As taxas normais do Amazon S3 se aplicam a cada versão de um objeto armazenado e transferido, incluindo versões desatualizadas de objetos. Para obter mais informações, consulte Preço do Amazon S3.

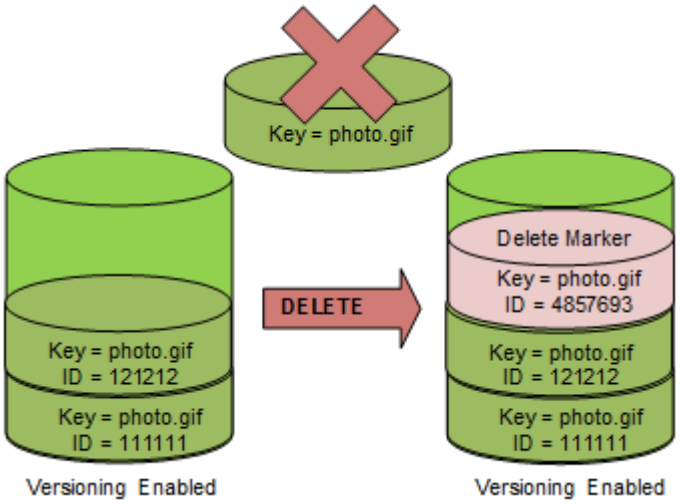
Excluir casos de uso de solicitação

Uma solicitação `DELETE` tem os seguintes casos de uso:

- Quando o versionamento está habilitado, um `DELETE` simples não pode excluir permanentemente um objeto. (Uma solicitação `DELETE` simples é uma solicitação que não especifica um ID de versão.) Em vez disso, o Amazon S3 insere um marcador de exclusão no bucket, que se torna a versão atual do objeto com um novo ID.

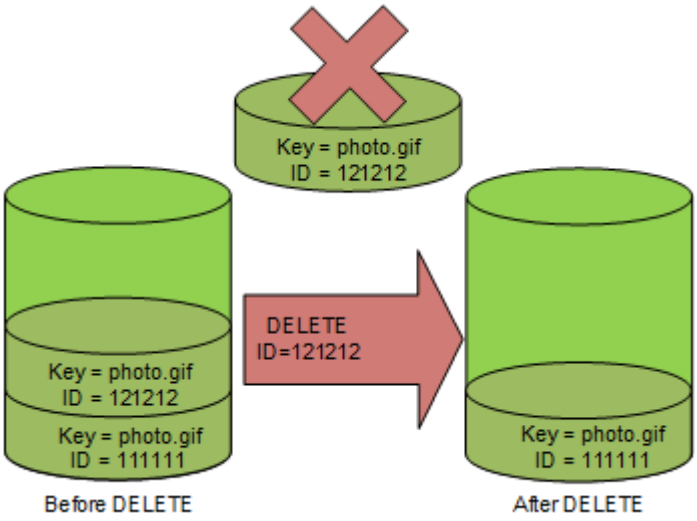
  Quando você tenta um `GET` de um objeto cuja versão atual é um marcador de exclusão, o Amazon S3 se comporta como se o objeto tivesse sido excluído (mesmo que não tenha sido apagado) e retorna um erro 404. Para obter mais informações, consulte Trabalhar com marcadores de exclusão.

A figura a seguir mostra que uma simples solicitação `DELETE` não remove de fato o objeto especificado. Em vez disso, o Amazon S3 insere um marcador de exclusão.



- Para excluir objetos com versões permanentemente, você deve usar `DELETE Object versionId`.

  A figura a seguir mostra que excluir uma versão do objeto especificada remove permanentemente esse objeto.



Para excluir versões de objeto

Você pode excluir versões de objeto no Amazon S3 usando o console, os AWS SDKs, a API REST ou a AWS Command Line Interface.

Uso do console do S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Na lista Buckets, escolha o nome do bucket que contém o objeto.
3. Na lista Objetos , escolha o nome do objeto.
4. Escolha Versões.

   O Amazon S3 mostra todas as versões do objeto.
5. Marque a caixa de seleção ao lado do ID da versão para as versões que deseja recuperar permanentemente.
6. Escolha Excluir.
7. Em Excluir objetos permanentemente? , insira **`permanently delete`**.

   > **Warning**
   >
   > Quando você exclui permanentemente uma versão de objeto, a ação não pode ser desfeita.
8. Escolha Delete objects (Excluir objetos).

   O Amazon S3 exclui a versão do objeto.

Uso dos SDKs da AWS

Para ver exemplos de exclusão de objetos usando os AWS SDKs para Java, o .NET e o PHP, consulte Excluir objetos do Amazon S3. Os exemplos para excluir objetos em buckets não versionados e habilitados para versionamento são os mesmos. No entanto, para buckets habilitados para versionamento, o Amazon S3 atribui um número de versão. Caso contrário, o número de versão é nulo.

Para obter informações sobre o uso de outros AWS SDKs, consulte o Centro do Desenvolvedor da AWS.

Python

O exemplo de código Python a seguir exclui permanente um objeto versionado ao remover todas as suas versões.

```
def permanently_delete_object(bucket, object_key):
    """
    Permanently deletes a versioned object by deleting all of its versions.

    Usage is shown in the usage_demo_single_object function at the end of this
 module.

    :param bucket: The bucket that contains the object.
    :param object_key: The object to delete.
    """
    try:
        bucket.object_versions.filter(Prefix=object_key).delete()
        logger.info("Permanently deleted all versions of object %s.", object_key)
    except ClientError:
        logger.exception("Couldn't delete all versions of %s.", object_key)
        raise
```

Uso da API REST

Como excluir uma versão específica de um objeto

- Em `DELETE`, especifique o ID da versão.

Example — Excluir uma versão específica

O exemplo a seguir exclui a versão `UIORUnfnd89493jJFJ` do `photo.gif`.

```
DELETE /photo.gif?versionId=UIORUnfnd89493jJFJ HTTP/1.1
Host: bucket.s3.amazonaws.com
Date: Wed, 12 Oct 2009 17:50:00 GMT
Authorization: AWS AKIAIOSFODNN7EXAMPLE:xQE0diMbLRepdf3YB+FIEXAMPLE=
Content-Type: text/plain
Content-Length: 0
```

Como usar o AWS CLI

O comando a seguir exclui um objeto chamado test.txt de um bucket chamado *amzn-s3-demo-bucket1*. Para remover uma versão específica de um objeto, você deve ser o proprietário do bucket e usar o sub-recurso de ID de versão.

```
aws s3api delete-object --bucket amzn-s3-demo-bucket1 --key test.txt --version-
id versionID
```

Para obter mais informações sobre `delete-object`, consulte delete-object na Referência de comandos da AWS CLI.

Para obter mais informações sobre como excluir versões de objetos, consulte os seguintes tópicos:

- Trabalhar com marcadores de exclusão
- Como remover marcadores de exclusão para tornar uma versão mais antiga atual
- Excluir um objeto de um bucket com exclusão de MFA habilitada

Trabalhar com marcadores de exclusão

Um marcador de exclusão no Amazon S3 é um espaço reservado (ou marcador) para um objeto com versões que foi especificado em uma solicitação `DELETE` simples. Uma solicitação `DELETE` simples é uma solicitação que não especifica um ID de versão. Como o objeto está em um bucket com versionamento habilitado, o objeto não é excluído. Mas o marcador de exclusão faz com que o Amazon S3 se comporte como se o objeto tivesse sido excluído. É possível usar a chamada de API `DELETE` do Amazon S3 em um marcador de exclusão. Para isso, será necessário fazer a solicitação `DELETE` usando um usuário ou um perfil do AWS Identity and Access Management (IAM) com as permissões adequadas.

Um marcador de exclusão tem um nome de chave (ou chave) e um ID de versão como qualquer outro objeto. Contudo, um marcador de exclusão difere de outros objetos nas seguintes maneiras:

- Um marcador de exclusão não tem dados associados a ele.
- Um marcador de exclusão não está associado a um valor da lista de controle de acesso (ACL).
- Se você emitir uma solicitação `GET` para um marcador de exclusão, a solicitação `GET` não recuperará nada porque um marcador de exclusão não tem dados. Especificamente, quando a solicitação `GET` não especifica um `versionId`, você recebe um erro 404 (não encontrado).

Os marcadores de exclusão acumulam uma cobrança mínima para armazenamento no Amazon S3. O tamanho de armazenamento de um marcador de exclusão é igual ao tamanho do nome da chave do marcador de exclusão. Um nome de chave é uma sequência de caracteres Unicode. A codificação UTF-8 para o nome da chave adiciona de 1 a 4 bytes de armazenamento ao bucket

para cada caractere no nome. Os marcadores de exclusão são armazenados na classe de armazenamento S3 Standard.

Se você quiser descobrir quantos marcadores de exclusão você tem e em qual classe de armazenamento eles estão armazenados, use a Lente de Armazenamento do Amazon S3. Para obter mais informações, consulte Avaliação de sua atividade de armazenamento e uso com a Lente de Armazenamento do Amazon S3 e Glossário de métricas de lente de armazenamento do Amazon S3.

Para obter mais informações sobre nomes de chave, consulte Nomear objetos do Amazon S3. Para obter mais informações sobre exclusão de um marcador de exclusão, consulte Gerenciamento de marcadores de exclusão.

Somente o Amazon S3 pode criar e excluir um marcador de exclusão, e ele faz isso sempre que você envia uma solicitação `DeleteObject` em um objeto em um bucket com versionamento habilitado ou suspenso. O objeto especificado na solicitação `DELETE` não é de fato excluído. Em vez disso, o marcador de exclusão torna-se a versão atual do objeto. O nome de chave (ou chave) do objeto torna-se a chave do marcador de exclusão.

Ao obter um objeto sem especificar um `versionId` na solicitação, se a versão atual for um marcador de exclusão, o Amazon S3 responderá com o seguinte:

- Um erro 404 (não encontrado)
- Um cabeçalho de resposta, `x-amz-delete-marker: true`

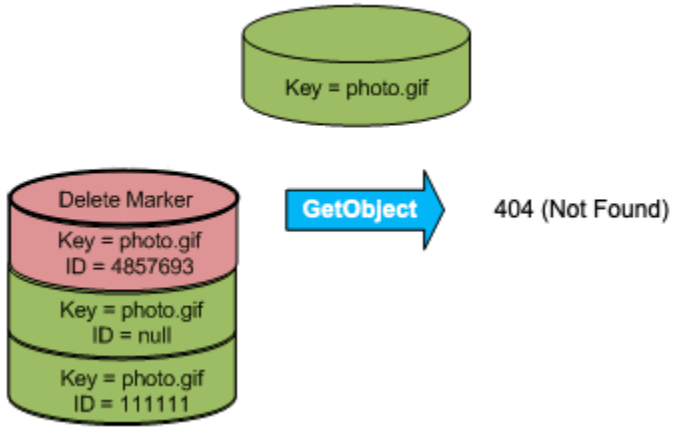
Ao obter um objeto especificando um `versionId` na solicitação, se a versão especificada for um marcador de exclusão, o Amazon S3 responderá com o seguinte:

- Um erro 405 (Método Não Permitido)
- Um cabeçalho de resposta, `x-amz-delete-marker: true`
- Um cabeçalho de resposta, `Last-Modified: timestamp` (somente ao usar as operações de API HeadObject ou GetObject)

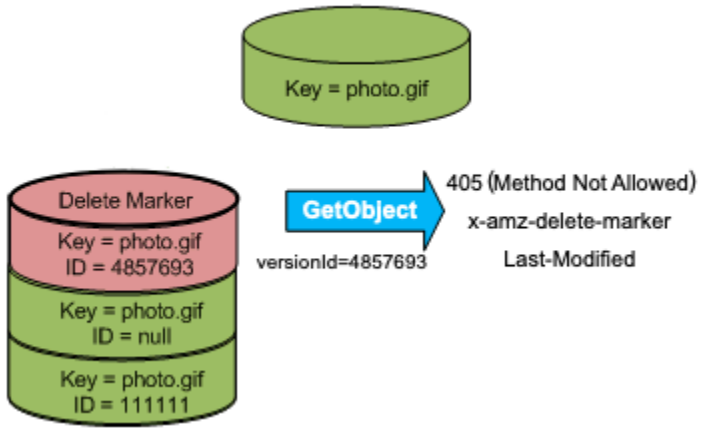
O cabeçalho de resposta `x-amz-delete-marker: true` mostra que o objeto acessado era um marcador de exclusão. Esse cabeçalho de resposta nunca retorna `false`, porque quando o valor é `false`, a versão atual ou especificada do objeto não é um marcador de exclusão.

O cabeçalho de resposta `Last-Modified` fornece a hora de criação dos marcadores de exclusão.

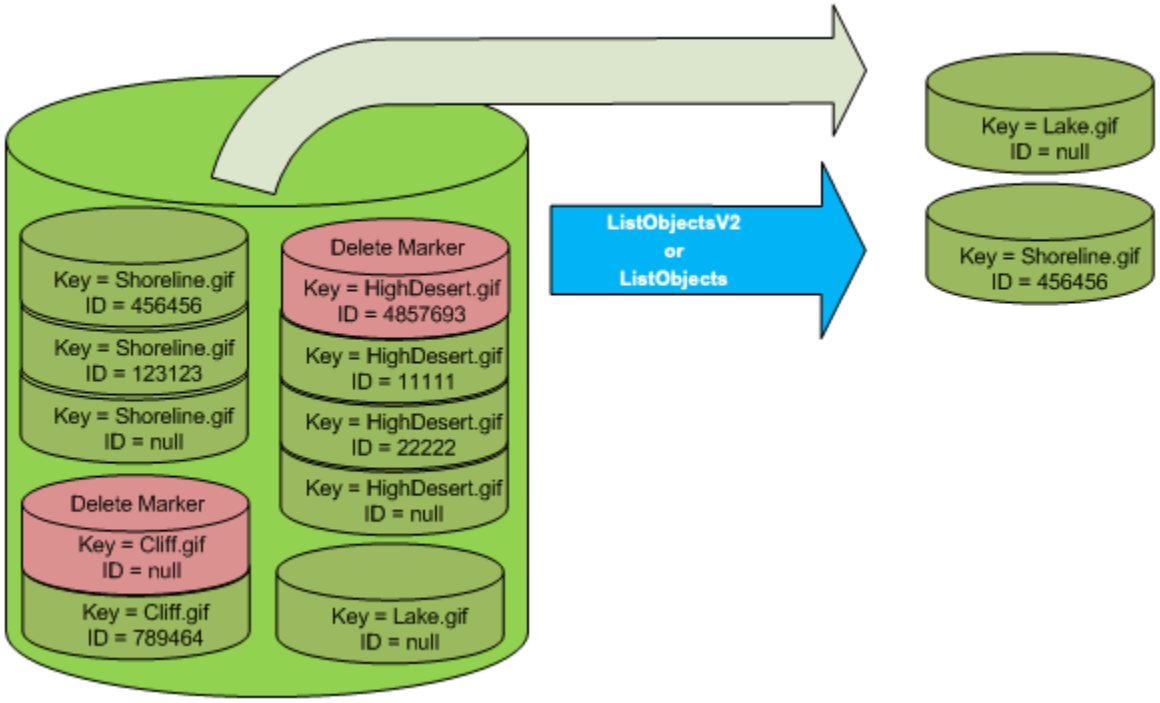
A figura a seguir mostra como uma chamada de API `GetObject` em um objeto, cuja versão atual é um marcador de exclusão, responde com um erro 404 (não encontrado), e o cabeçalho da resposta inclui `x-amz-delete-marker: true`.



Se você fizer uma chamada `GetObject` em um objeto especificando um `versionId` na solicitação e se a versão especificada for um marcador de exclusão, o Amazon S3 responderá com um erro 405 (método não permitido) e os cabeçalhos de resposta incluirão `x-amz-delete-marker: true` e `Last-Modified: timestamp`.



O único modo de listar marcadores de exclusão (e outras versões de um objeto) é usando o `versions` sub-recurso em uma solicitação ListObjectVersions. A figura a seguir mostra que uma solicitação ListObjectsV2 ou ListObjects não retorna objetos cuja versão atual é um marcador de exclusão.



Gerenciamento de marcadores de exclusão

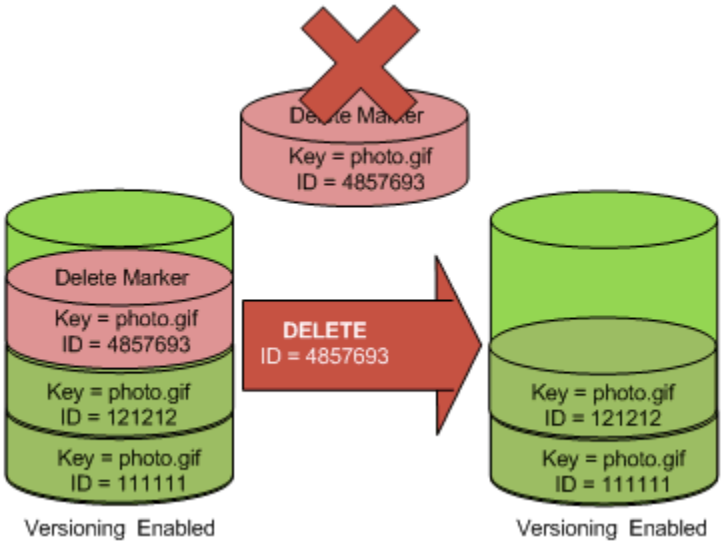
Como configurar o ciclo de vida para limpar marcadores de exclusão expirados automaticamente

Em um marcador de exclusão de objeto expirado, todas as versões de objeto são excluídas e resta apenas um único marcador de exclusão. Se a configuração de ciclo de vida estiver definida para excluir versões atuais ou a ação `ExpiredObjectDeleteMarker` estiver explicitamente definida, o Amazon S3 removerá o marcador de exclusão do objeto expirado. Para ver um exemplo, consulte Remover marcadores de exclusão de objetos expirados em um bucket com versionamento habilitado.

Como remover marcadores de exclusão para tornar uma versão mais antiga atual

Quando você exclui um objeto em um bucket ativado para versionamento, todas as versões permanecem no bucket, e o Amazon S3 cria um marcador de exclusão para o objeto. Para cancelar a exclusão do objeto, você deve excluir esse marcador de exclusão. Para obter mais informações sobre versionamento e marcadores de exclusão, consulte Reter várias versões de objetos com o Versionamento do S3.

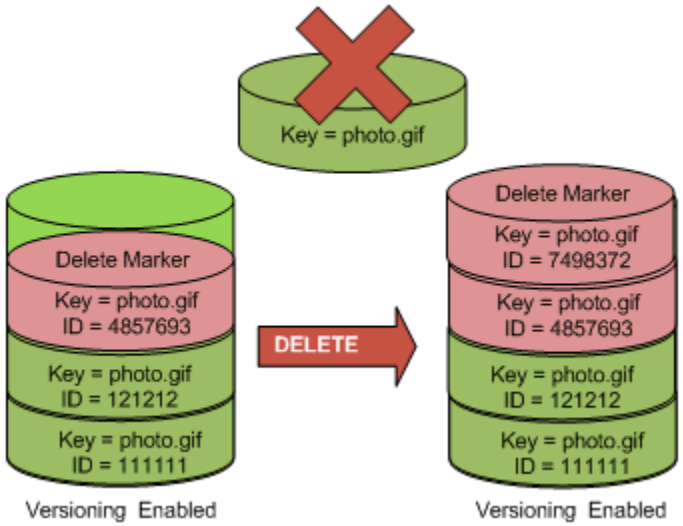
Para excluir permanentemente um marcador de exclusão, inclua seu respectivo ID de versão em uma solicitação `DeleteObject versionId`. A figura a seguir mostra como uma solicitação `DeleteObject versionId` simples remove, permanentemente, um marcador de exclusão.



O efeito da remoção do marcador de exclusão é que uma simples solicitação `GET` não recuperará o ID da versão atual do objeto (121212).

> **Note**
>
> Se você usar uma solicitação `DeleteObject` em que a versão atual seja um marcador de exclusão (sem especificar o ID da versão do marcador de exclusão), o Amazon S3 não excluirá o marcador de exclusão, mas outro marcador de exclusão `PUT`s.

Para excluir um marcador de exclusão com um ID de versão `NULL`, você deve aprovar o `NULL` como o ID da versão na solicitação `DeleteObject`. A figura a seguir mostra como uma simples solicitação `DeleteObject` feita sem um ID de versão em que a versão atual é um marcador de exclusão não remove nada. Em vez disso, ela adiciona um marcador de exclusão extra com um ID de versão exclusivo (7498372).



Uso do console do S3

Use as etapas a seguir para recuperar objetos excluídos que não são pastas do seu bucket do S3, incluindo objetos que estão dentro dessas pastas.

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Na lista Buckets, escolha o nome do bucket desejado.
3. Para ver uma lista das versões dos objetos no bucket, escolha a opção List versions (Listar versões). Você conseguirá ver os marcadores de exclusão dos objetos excluídos.
4. Para cancelar a exclusão de um objeto, você deve excluir o marcador de exclusão. Marque a caixa de seleção ao lado do delete marker (marcador de exclusão) do objeto a ser recuperado e escolha Delete (excluir).
5. Confirme a exclusão na página Delete objects (Excluir objetos).
    a. Para a opção Permanently delete objects? (Excluir objetos permanentemente?), insira **`permanently delete`**.
    b. Escolha Delete objects (Excluir objetos).

> **Note**
>
> Você não pode usar o console do Amazon S3 para cancelar a exclusão de pastas. Você deve usar a AWS CLI ou o SDK. Para ver exemplos, consulte Como faço para recuperar

um objeto do Amazon S3 que foi excluído em um bucket habilitado para versionamento? na Central de Conhecimento da AWS.

Uso dos REST API

Para remover permanentemente um marcador de exclusão

1. Defina `versionId` como o ID da versão do marcador de exclusão que você deseja remover.
2. Envie uma solicitação `DELETE Object versionId`.

Example — Remover um marcador de exclusão

O exemplo a seguir remove o marcador de exclusão de `photo.gif` com versão 4857693.

```
DELETE /photo.gif?versionId=4857693 HTTP/1.1
Host: bucket.s3.amazonaws.com
Date: Wed, 28 Oct 2009 22:32:00 GMT
Authorization: AWS AKIAIOSFODNN7EXAMPLE:0RQf4/cRonhpaBX5sCYVf1bNRuU=
```

Quando você exclui um marcador de exclusão, o Amazon S3 inclui o seguinte na resposta:

```
204 NoContent
x-amz-version-id: versionID
x-amz-delete-marker: true
```

Uso dos SDKs da AWS

Para obter informações sobre o uso de outros AWS SDKs, consulte o Centro do Desenvolvedor da AWS.

Python

O exemplo de código Python a seguir demonstra como remover um marcador de exclusão de um objeto e, portanto, transforma a versão não atual mais recente na versão atual do objeto.

```
def revive_object(bucket, object_key):
    """
    Revives a versioned object that was deleted by removing the object's active
    delete marker.
```

```
    A versioned object presents as deleted when its latest version is a delete
marker.
    By removing the delete marker, we make the previous version the latest version
    and the object then presents as *not* deleted.

    Usage is shown in the usage_demo_single_object function at the end of this
module.

    :param bucket: The bucket that contains the object.
    :param object_key: The object to revive.
    """
    # Get the latest version for the object.
    response = s3.meta.client.list_object_versions(
        Bucket=bucket.name, Prefix=object_key, MaxKeys=1
    )

    if "DeleteMarkers" in response:
        latest_version = response["DeleteMarkers"][0]
        if latest_version["IsLatest"]:
            logger.info(
                "Object %s was indeed deleted on %s. Let's revive it.",
                object_key,
                latest_version["LastModified"],
            )
            obj = bucket.Object(object_key)
            obj.Version(latest_version["VersionId"]).delete()
            logger.info(
                "Revived %s, active version is now %s  with body '%s'",
                object_key,
                obj.version_id,
                obj.get()["Body"].read(),
            )
        else:
            logger.warning(
                "Delete marker is not the latest version for %s!", object_key
            )
    elif "Versions" in response:
        logger.warning("Got an active version for %s, nothing to do.", object_key)
    else:
        logger.error("Couldn't get any version info for %s.", object_key)
```

Excluir um objeto de um bucket com exclusão de MFA habilitada

Se a configuração de versionamento do bucket tiver a exclusão de MFA ativada, o proprietário do bucket deverá incluir o cabeçalho de solicitação `x-amz-mfa` nas solicitações para excluir permanentemente uma versão de objeto ou alterar o estado de versionamento do bucket. As solicitações que incluem `x-amz-mfa` devem usar HTTPS.

O valor do cabeçalho é uma concatenação do número de série do seu dispositivo de autenticação, um espaço e o código de autenticação exibido nele. Se você não incluir esse cabeçalho, a solicitação falhará.

Para obter mais informações sobre dispositivos de autenticação, consulte Autenticação multifator.

Example — Excluir um objeto de um bucket com exclusão de MFA habilitada

O exemplo a seguir exclui `my-image.jpg` (com a versão especificada), que está em um bucket configurado com a exclusão de MFA habilitada.

Observe o espaço entre *`[SerialNumber]`* e *`[AuthenticationCode]`*. Para obter mais informações, consulte DeleteObject na Referência da API do Amazon Simple Storage Service.

```
DELETE /my-image.jpg?versionId=3HL4kqCxf3vjVBH40Nrjfkd HTTPS/1.1
Host: bucketName.s3.amazonaws.com
x-amz-mfa: 20899872 301749
Date: Wed, 28 Oct 2009 22:32:00 GMT
Authorization: AWS AKIAIOSFODNN7EXAMPLE:0RQf4/cRonhpaBX5sCYVf1bNRuU=
```

Para obter mais informações sobre ativação de exclusão de MFA, consulte Configurando a exclusão de MFA.

Configurando permissões de objeto com versão

As permissões para objetos no Amazon S3 são definidas no nível de versão. Cada versão tem seu próprio proprietário do objeto. A Conta da AWS que cria a versão do objeto é a proprietária. Assim, você pode definir diferentes permissões para diferentes versões do mesmo objeto. Para fazer isso, você deve especificar o ID da versão do objeto cujas permissões você deseja definir em uma solicitação `PUT Object versionId acl`. Para uma descrição detalhada e instruções de uso de ACLs, consulte Gerenciamento de identidade e acesso para o Amazon S3.

Example — Configuração de permissões para uma versão de objeto

A solicitação a seguir define a permissão do beneficiário, `BucketOwner@amazon.com`, como `FULL_CONTROL` na chave, `my-image.jpg`, ID de versão, `3HL4kqtJvjVBH40Nrjfkd`.

```
PUT /my-image.jpg?acl&versionId=3HL4kqtJvjVBH40Nrjfkd HTTP/1.1
Host: bucket.s3.amazonaws.com
Date: Wed, 28 Oct 2009 22:32:00 GMT
Authorization: AWS AKIAIOSFODNN7EXAMPLE:0RQf4/cRonhpaBX5sCYVf1bNRuU=
Content-Length: 124

<AccessControlPolicy>
  <Owner>
    <ID>75cc57f09aa0c8caeab4f8c24e99d10f8e7faeebf76c078efc7c6caea54ba06a</ID>
    <DisplayName>mtd@amazon.com</DisplayName>
  </Owner>
  <AccessControlList>
    <Grant>
      <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:type="CanonicalUser">
        <ID>a9a7b886d6fd24a52fe8ca5bef65f89a64e0193f23000e241bf9b1c61be666e9</ID>
        <DisplayName>BucketOwner@amazon.com</DisplayName>
      </Grantee>
      <Permission>FULL_CONTROL</Permission>
    </Grant>
  </AccessControlList>
  </AccessControlPolicy>
```

Da mesma forma, para obter permissões para uma versão específica do objeto, você deve especificar seu ID de versão em uma solicitação `GET Object versionId acl`. Você precisa incluir o ID da versão porque, por padrão, o `GET Object acl` retorna as permissões da versão atual do objeto.

Example — Recuperar permissões para uma versão especificada de objeto

No exemplo a seguir, o Amazon S3 retorna as permissões da chave, `my-image.jpg`, ID da versão, `DVBH40Nr8X8gUMLUo`.

```
GET /my-image.jpg?versionId=DVBH40Nr8X8gUMLUo&acl HTTP/1.1
Host: bucket.s3.amazonaws.com
Date: Wed, 28 Oct 2009 22:32:00 GMT
Authorization: AWS AKIAIOSFODNN7EXAMPLE:0RQf4/cRonhpaBX5sCYVf1bNRuU
```

Para obter mais informações, consulte GetObjectAcl na Referência da API do Amazon Simple Storage Service.

Trabalhar com objetos em um bucket com versionamento suspenso

No Amazon S3, você pode suspender o versionamento para parar de ter novas versões do mesmo objeto em um bucket. Você pode fazer isso porque você quer apenas uma única versão de um objeto em um bucket. Ou talvez você não queira acumular cobranças para várias versões.

Quando você suspende o versionamento, os objetos existentes em seu bucket não são alterados. O que muda é como o Amazon S3 trata os objetos em solicitações futuras. Os tópicos nesta seção explicam várias operações de objeto em um bucket suspenso de versão, incluindo adição, recuperação e exclusão de objetos.

Para obter mais informações sobre o S3 Versioning, consulte Reter várias versões de objetos com o Versionamento do S3. Para obter mais informações sobre como recuperar as versões de um objeto, consulte Recuperando versões de objeto de um bucket habilitado para versionamento.

Tópicos

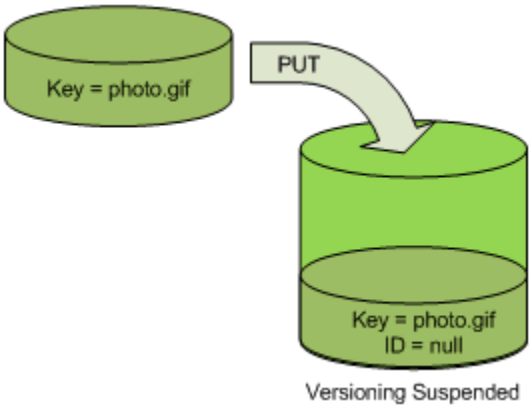
- Adicionar objetos a buckets com versionamento suspenso
- Recuperar objetos de buckets com versionamento suspenso
- Excluir objetos de buckets com versionamento suspenso

Adicionar objetos a buckets com versionamento suspenso

Você pode adicionar objetos a buckets com versionamento suspenso no Amazon S3 para criar o objeto com um ID de versão nulo ou substituir qualquer versão de objeto por um ID de versão correspondente.

Depois que você suspender o versionamento em um bucket, o Amazon S3 adicionará automaticamente um ID de versão `null` a cada objeto subsequente armazenado depois disso (usando `PUT`, `POST` ou `CopyObject`) nesse bucket.

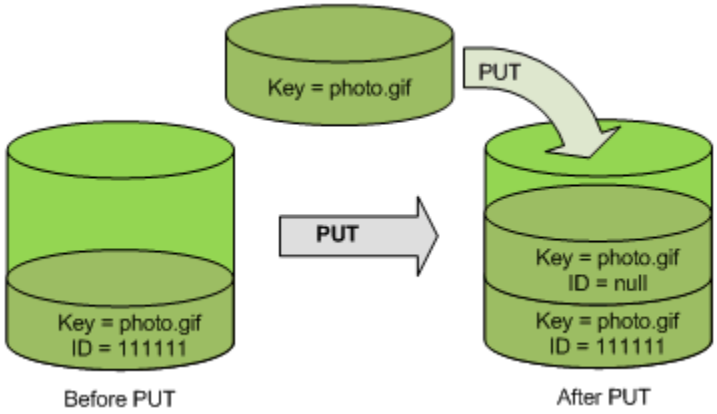
A figura a seguir mostra como o Amazon S3 adiciona um ID de versão `null` a cada objeto quando ele é adicionado a um bucket com versionamento suspenso.



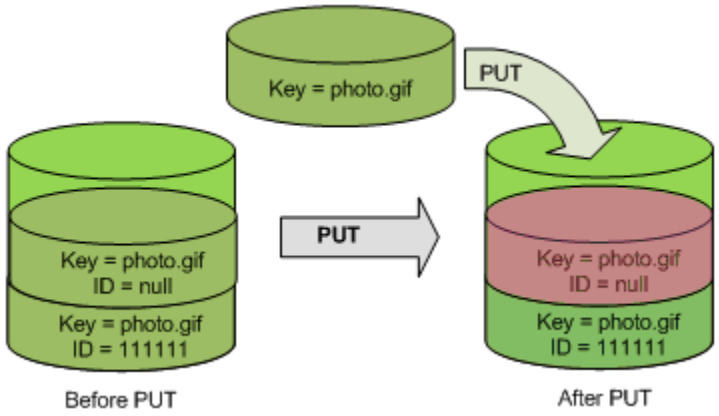
Se um versão nula já existir no bucket e você adicionar outro objeto com a mesma chave, o objeto adicionado substituirá a versão original nula.

Se existirem objetos com versões no bucket, a versão que você usa no PUT torna-se a versão atual do objeto. A figura a seguir mostra como a adição de um objeto a um bucket que contém objetos com versões não substitui o objeto já existente no bucket.

Neste caso, a versão 111111 já estava no bucket. O Amazon S3 anexa o ID de versão nula ao objeto que está sendo adicionado e armazena o objeto no bucket. A versão 111111 não é substituída.



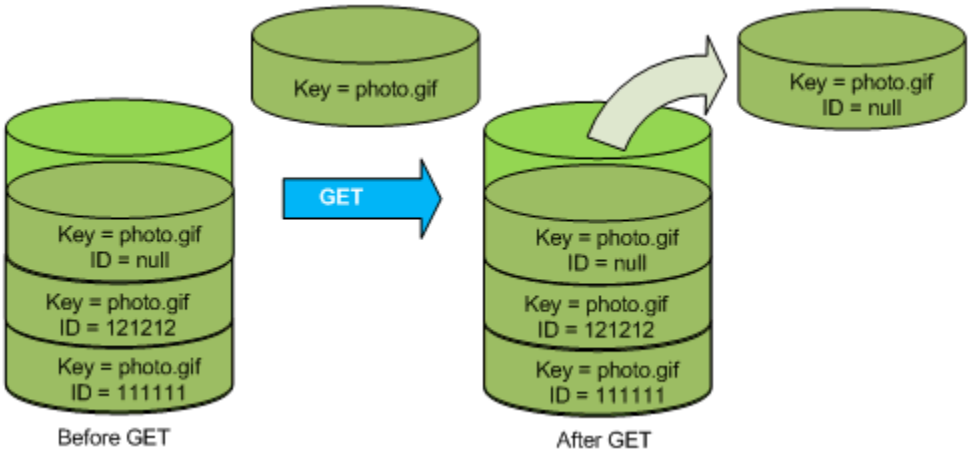
Se uma versão nula já existir em um bucket, a versão nula será substituída, como mostrado na figura a seguir.



Embora a chave e o ID (`null`) da versão nula sejam iguais antes e depois de `PUT`, o conteúdo da versão nula originalmente armazenado no bucket é substituído pelo conteúdo do objeto `PUT` no bucket.

Recuperar objetos de buckets com versionamento suspenso

Uma solicitação `GET Object` retorna a versão atual de um objeto sempre independentemente de você ter ou não ativado o versionamento de um bucket. A figura a seguir mostra como um `GET` simples retorna a versão atual de um objeto.



Excluir objetos de buckets com versionamento suspenso

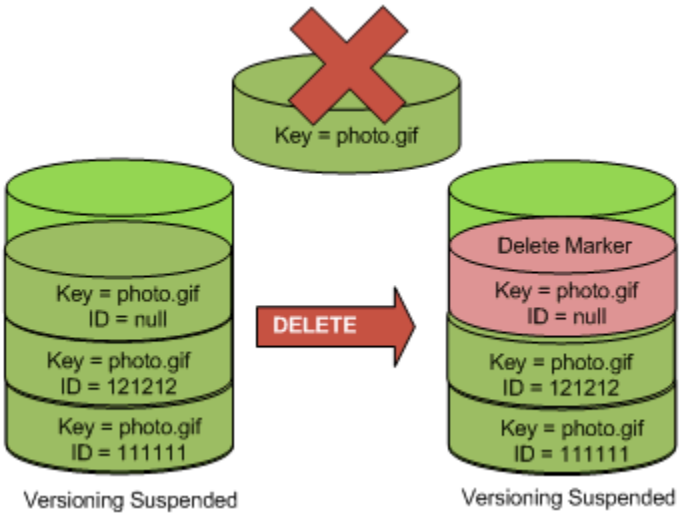
Você pode excluir objetos de buckets com versionamento suspenso para remover um objeto com um ID de versão nulo.

Se o controle de versão for suspenso para um bucket, uma `DELETE` solicitação:

- Pode remover apenas um objeto cujo ID de versão seja `null`.

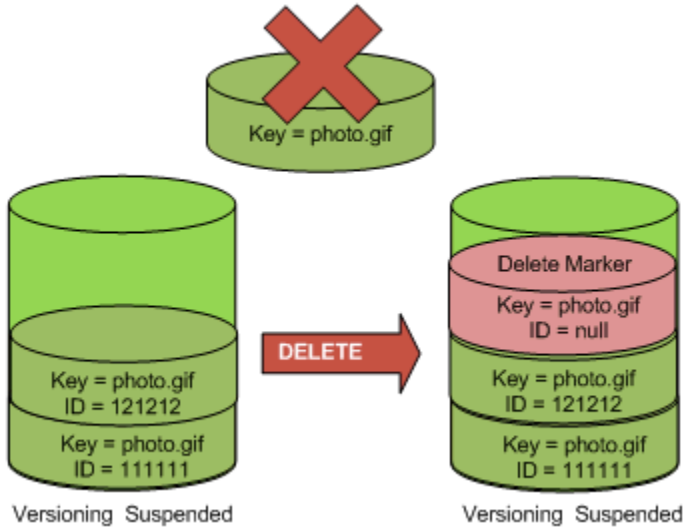
- Não removerá nada se não existir uma versão nula do objeto no bucket.
- Insere um marcador de exclusão no bucket.

Se o versionamento do bucket for suspenso, a operação removerá o objeto que tem um `versionId` nulo. Quando existe um ID de versão, o Amazon S3 insere um marcador de exclusão que se torna a versão atual do objeto. A figura a seguir mostra como um `DELETE` simples remove uma versão nula, e o Amazon S3 insere um marcador de exclusão em seu lugar com um ID de versão `null`.

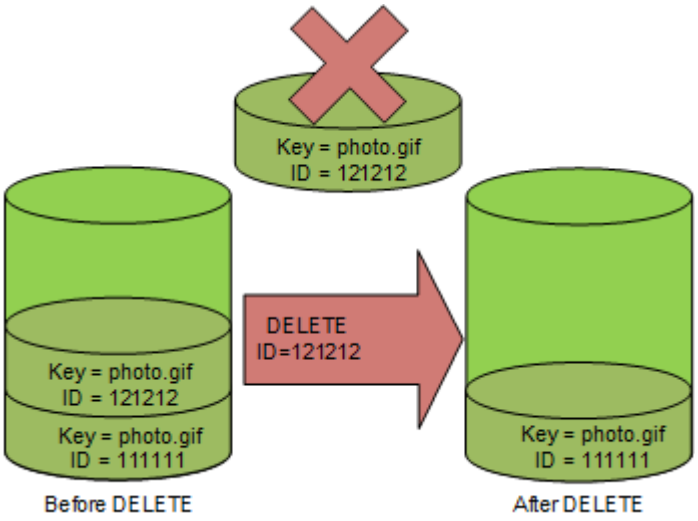


Para excluir permanentemente um objeto que tenha um `versionId`, você deve incluir o `versionId` do objeto na solicitação. Como um marcador de exclusão não contém nenhum conteúdo, você perderá o conteúdo da versão `null` quando um marcador de exclusão a substituir.

A figura a seguir mostra um bucket que não tem uma versão nula. Nesse caso, `DELETE` não remove nada. Em vez disso, o Amazon S3 apenas insere um marcador de exclusão.



Mesmo em um bucket com versionamento suspenso, o proprietário do bucket pode excluir permanentemente uma versão especificada, incluindo o ID da versão na solicitação de DELETE. A figura a seguir mostra que excluir uma versão do objeto especificada remove permanentemente essa versão do objeto. Apenas o proprietário do bucket pode excluir uma versão de objeto especificada.



Solucionar problemas de versionamento

Os tópicos a seguir podem ajudar a solucionar alguns problemas comuns de versionamento do Amazon S3.

Tópicos

- Quero recuperar objetos que foram excluídos acidentalmente em um bucket com versionamento ativado
- Quero excluir permanentemente objetos com versionamento
- Ocorreu uma degradação do desempenho depois de ativar o versionamento do bucket

Quero recuperar objetos que foram excluídos acidentalmente em um bucket com versionamento ativado

Em geral, quando as versões do objeto são excluídas dos buckets do S3, não há como o Amazon S3 recuperá-las. No entanto, se você habilitou o versionamento do S3 no bucket do S3, uma solicitação DELETE que não especifica um ID de versão não pode excluir permanentemente um objeto. Em vez disso, um marcador de exclusão é adicionado como espaço reservado. Esse marcador de exclusão torna-se a versão atual de objeto.

Para verificar se os objetos excluídos foram excluídos permanentemente ou temporariamente (com um marcador de exclusão em seu lugar), faça o seguinte:

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets.
3. Na lista Buckets, escolha o nome do bucket que contém o objeto.
4. Na lista Objetos, ative a opção Mostrar versões à direita da barra de pesquisa e, depois, pesquise o objeto excluído na barra de pesquisa. Essa alternância estará disponível somente se o versionamento tiver sido habilitado anteriormente no bucket.

   Você também pode usar o Inventário do S3 para pesquisar objetos excluídos.
5. Se você não conseguir encontrar o objeto depois de ativar Mostrar versões ou criar um relatório de inventário, e também não conseguir encontrar um marcador de exclusão do objeto, a exclusão será permanente e o objeto não poderá ser recuperado.

Você também pode verificar o status de um objeto excluído usando a operação de API `HeadObject` do AWS Command Line Interface (AWS CLI). Para fazer isso, use o comando `head-object` a seguir e substitua *`user input placeholders`* por suas próprias informações:

```
aws s3api head-object --bucket amzn-s3-demo-bucket --key index.html
```

Se você executar o comando `head-object` em um objeto com versionamento, cuja versão atual é um marcador de exclusão, você receberá um erro 404 Não encontrado. Por exemplo:

Ocorreu um erro (404) ao chamar a operação HeadObject: não encontrado

Se você executar o comando `head-object` em um objeto com versionamento e fornecer o ID da versão do objeto, o Amazon S3 recuperará os metadados do objeto, confirmando que ele ainda existe e não foi excluído permanentemente.

```
aws s3api head-object --bucket amzn-s3-demo-bucket --key index.html --
version-id versionID
```

```
{
"AcceptRanges": "bytes",
"ContentType": "text/html",
"LastModified": "Thu, 16 Apr 2015 18:19:14 GMT",
"ContentLength": 77,
```

```
"VersionId": "Zg5HyL7m.eZU9iM7AVlJkrqAiE.0UG4q",
"ETag": "\"30a6ec7e1a9ad79c203d05a589c8b400\"",
"Metadata": {}
}
```

Se o objeto for encontrado e a versão mais recente for um marcador de exclusão, a versão anterior do objeto ainda existirá. Como o marcador de exclusão é a versão atual do objeto, você pode recuperá-lo excluindo o marcador de exclusão.

Depois de remover permanentemente o marcador de exclusão, a segunda versão mais recente do objeto se torna a versão atual dele, tornando-o disponível novamente. Para obter uma descrição visual de como os objetos são recuperados, consulte Remover marcadores de exclusão.

Para remover uma versão específica de um objeto, você deve ser o proprietário do bucket. Para excluir permanentemente um marcador de exclusão, inclua seu respectivo ID de versão em uma solicitação `DeleteObject`. Para excluir o marcador de exclusão, use o comando a seguir e substitua *`user input placeholders`* por suas próprias informações:

`aws s3api delete-object --bucket` *`amzn-s3-demo-bucket`* `--key` *`index.html`* `--version-id` *`versionID`*

Para obter mais informações sobre o comando `delete-object`, consulte delete-object na Referência de comandos da AWS CLI. Para obter mais informações sobre como excluir permanentemente os marcadores de exclusão, consulte Gerenciamento de marcadores de exclusão.

Quero excluir permanentemente objetos com versionamento

Em um bucket com versionamento, uma solicitação `DELETE` sem um ID de versão não pode excluir permanentemente um objeto. Em vez disso, essa solicitação insere um marcador de exclusão.

Para excluir permanentemente objetos com versionamento, você pode escolher entre os seguintes métodos:

- Crie uma regra de ciclo de vida do S3 para excluir permanentemente as versões não atuais. Para excluir permanentemente versões não atuais de objetos, selecione Excluir permanentemente versões não atuais de objetos, e insira um número em Dias após os objetos ficarem desatualizados. Opcionalmente, você pode especificar o número de versões mais recentes a serem retidas inserindo um valor em Number of newer versions to retain (Número de versões mais novas a serem mantidas). Para obter mais informações sobre como criar essa regra, consulte Definir uma configuração de ciclo de vida do S3.

- Exclua uma versão especificada incluindo o ID da versão na solicitação DELETE. Para obter mais informações, consulte Como excluir permanentemente objetos com versionamento.
- Crie uma regra de ciclo de vida para expirar as versões atuais. Para expirar as versões atuais dos objetos, selecione Expirar versões atuais de objetos e adicione um número em Dias após a criação do objeto. Para obter mais informações sobre como criar essa regra de ciclo de vida, consulte Definir uma configuração de ciclo de vida do S3.
- Para excluir permanentemente todos os objetos com versionamento e excluir marcadores, crie duas regras de ciclo de vida: uma para expirar as versões atuais e excluir permanentemente as versões não atuais dos objetos, e outra para excluir marcadores de exclusão de objetos expirados.

Em um bucket com versionamento ativado, uma solicitação DELETE que não especifica um ID de versão pode remover somente objetos com um ID de versão NULL. Se o objeto foi carregado quando o versionamento estava ativado, uma solicitação DELETE que não especifica um ID de versão cria um marcador de exclusão desse objeto.

> **Note**
>
> Para buckets com o bloqueio de objetos do S3 ativado, uma solicitação de DELETE objeto com um ID de versão de objeto protegido causa um erro 403 Acesso negado. Uma solicitação de DELETE objeto sem um ID de versão adiciona um marcador de exclusão como a versão mais recente do objeto com uma resposta 200 OK. Objetos protegidos pelo bloqueio de objetos não podem ser excluídos permanentemente até que seus períodos de retenção e retenções legais sejam removidos. Para obter mais informações, consulte the section called “Como o bloqueio de objetos do S3 funciona”.

Ocorreu uma degradação do desempenho depois de ativar o versionamento do bucket

A degradação do desempenho poderá ocorrer em buckets com versionamento ativado se houver muitos marcadores de exclusão ou objetos com versionamento e se as práticas recomendadas não forem seguidas.

Marcadores de exclusão em excesso

Depois que você habilita o versionamento em um bucket, uma solicitação DELETE sem um ID de versão feita a um objeto cria um marcador de exclusão com um ID de versão exclusivo. As configurações do ciclo de vida com a regra Expirar versões atuais de objetos adicionam um

marcador de exclusão com um ID de versão exclusivo a cada objeto. Marcadores de exclusão excessivos podem reduzir o desempenho no bucket.

Quando o versionamento é suspenso em um bucket, o Amazon S3 marca o ID da versão como `NULL` em objetos recém-criados. Uma ação de expiração em um bucket com versionamento suspenso faz com que o Amazon S3 crie um marcador de exclusão com `NULL` como o ID da versão. Em um bucket com versionamento suspenso, um marcador de exclusão `NULL` é criado para qualquer solicitação de exclusão. Esses marcadores de exclusão `NULL` também são chamados de marcadores de exclusão de objeto expirado quando todas as versões de objeto são excluídas e resta apenas um único marcador de exclusão. Se muitos marcadores de exclusão `NULL` se acumularem, ocorrerá uma degradação do desempenho no bucket.

Objetos com versionamento em excesso

Se um bucket com versionamento ativado contiver objetos com milhões de versões, poderá ocorrer um aumento nos erros 503 Serviço indisponível. Se você perceber um aumento significativo do número de respostas HTTP 503 Serviço indisponível recebidas para solicitações `PUT` ou `DELETE` de objetos a um bucket com o versionamento ativado, talvez tenha um ou mais objetos no bucket com milhões de versões. Quando você tem objetos com milhões de versões, o Amazon S3 limita automaticamente as solicitações ao bucket. As solicitações de controle de utilização protegem o bucket de uma quantidade excessiva de tráfego de solicitação, o que pode potencialmente impedir outras solicitações feitas ao mesmo bucket.

Para determinar quais objetos têm milhões de versões, use o inventário do S3. O inventário do S3 gera um relatório que fornece uma lista de arquivos simples dos objetos em um bucket. Para obter mais informações, consulte Catalogar e analisar seus dados com o Inventário S3.

Para verificar se há um grande número de objetos com versionamento no bucket, use as métricas da Lente de Armazenamento do S3 para visualizar a Contagem de objetos da versão atual, o Número de objetos de versões não atuais e a Contagem de objetos do marcador de exclusão. Para obter mais informações sobre métricas da Lente de Armazenamento, consulte Glossário de métricas de lente de armazenamento do Amazon S3.

A equipe do Amazon S3 incentiva os clientes a investigarem aplicações que sobrescrevem repetidamente o mesmo objeto, criando potencialmente milhões de versões desse objeto, para determinar se a aplicação está funcionando conforme o esperado. Por exemplo, uma aplicação que sobrescreve o mesmo objeto a cada minuto durante uma semana pode criar mais de dez mil versões. Recomendamos armazenar menos de cem mil versões para cada objeto. Se você tiver um

caso de uso que exija milhões de versões para um ou mais objetos, entre em contato com a equipe do AWS Support a fim de obter ajuda para determinar uma solução melhor.

Práticas recomendadas

Para evitar problemas de degradação do desempenho relacionada ao versionamento, recomendamos aplicar as seguintes práticas recomendadas:

- Habilite uma regra de ciclo de vida para expirar as versões anteriores dos objetos. Por exemplo, você pode criar uma regra de ciclo de vida para expirar versões não atuais após 30 dias de inatividade do objeto. Você também poderá manter várias versões não atuais se não quiser excluir todas elas. Para obter mais informações, consulte Definir uma configuração do ciclo de vida do S3.
- Habilite uma regra de ciclo de vida para excluir marcadores de exclusão de objetos expirados que não tenham objetos de dados associados no bucket. Para obter mais informações, consulte Remover marcadores de exclusão de objeto expirado.

Para ver mais práticas recomendadas de otimização de desempenho do Amazon S3, consulte Padrões de design de melhores práticas.

Bloquear objetos com o Bloqueio de Objetos

A funcionalidade Bloqueio de Objetos do S3 pode ajudar a evitar que os objetos do Amazon S3 sejam excluídos ou substituídos por um período fixo ou indefinidamente. A funcionalidade Bloqueio de Objetos usa um modelo de gravação única e várias leituras (WORM). Você pode usar a funcionalidade Bloqueio de Objetos para ajudar a atender aos requisitos regulamentares que exigem armazenamento WORM ou para adicionar outra camada de proteção contra alterações ou exclusão de objetos.

> **Note**
>
> A funcionalidade Bloqueio de Objetos do S3 foi avaliada pela Cohasset Associates para uso em ambientes sujeitos aos regulamentos SEC 17a-4, CFTC e FINRA. Para obter mais informações sobre como a funcionalidade Bloqueio de Objetos está relacionada a essas regulamentações, consulte o documento Cohasset Associates Compliance Assessment.

O bloqueio de objetos fornece duas maneiras de gerenciar a retenção de objetos: períodos de retenção e retenções legais. Uma versão do objeto pode ter um período de retenção, uma retenção jurídica ou ambos.

- Período de retenção: um período de retenção especifica um período fixo durante o qual uma versão de objeto permanece bloqueada. Você pode definir um período de retenção exclusivo para objetos individuais. Além disso, você pode definir um período de retenção padrão em um bucket do S3. Também é possível restringir os períodos mínimo e máximo de retenção permitidos com a chave de condição `s3:object-lock-remaining-retention-days` na política do bucket. Isso ajuda você a estabelecer uma faixa de períodos de retenção e a restringir períodos de retenção que podem ser menores ou maiores do que essa faixa.
- Retenção jurídica: uma retenção jurídica oferece a mesma proteção de um período de retenção, mas sem data de expiração. Em vez disso, uma retenção legal permanecerá em vigor até você removê-la explicitamente. As retenções jurídicas independem dos períodos de retenção e são colocadas em versões de objetos individuais.

A funcionalidade Bloqueio de Objetos só funciona somente em buckets com a funcionalidade Versionamento do S3 habilitada. Quando você bloqueia uma versão do objeto, o Amazon S3 armazena as informações de bloqueio nos metadados dessa versão do objeto. A colocação de um período de retenção ou uma retenção jurídica em um objeto só protege a versão especificada na solicitação. Os períodos de retenção e as retenções jurídicas não impedem a criação de versões do objeto nem a adição de marcadores de exclusão no objeto. Para obter informações sobre o Versionamento do S3, consulte Reter várias versões de objetos com o Versionamento do S3.

Se você colocar um objeto em um bucket que já contenha um objeto protegido com o mesmo nome de chave de objeto, o Amazon S3 criará outra versão desse objeto. A versão protegida existente do objeto permanece bloqueada de acordo com a configuração da retenção.

Como o bloqueio de objetos do S3 funciona

Tópicos

- Períodos de retenção
- Modos de retenção
- Retenções legais
- Práticas recomendadas para usar a funcionalidade Bloqueio de Objetos do S3
- Permissões obrigatórias

Períodos de retenção

Um período de retenção protege uma versão do objeto por um período fixo. Quando você coloca um período de retenção em uma versão do objeto, o Amazon S3 armazena um timestamp nos metadados da versão do objeto para indicar quando o período de retenção expira. Depois que o período de retenção expirar, a versão do objeto não poderá ser substituída nem excluída.

Você pode colocar um período de retenção explicitamente em uma versão de objeto individual ou nas propriedades de um bucket para que ele se aplique automaticamente a todos os objetos no bucket. Ao aplicar um período de retenção a uma versão de objeto explicitamente, especifique a opção de Retain Until Date (Reter até uma determinada data) para a versão do objeto. O Amazon S3 armazena essa data nos metadados da versão do objeto.

Você também pode definir um período de retenção nas propriedades de um bucket. Ao definir um período de retenção em um bucket, especifique uma duração, em dias ou anos, para proteger cada versão do objeto colocada no bucket. Quando você coloca um objeto no bucket, o Amazon S3 calcula um Prazo de retenção para a versão do objeto, adicionando a duração especificada ao timestamp da criação da versão do objeto. A versão do objeto é protegida exatamente como se você tivesse colocado explicitamente um bloqueio individual com esse período de retenção na versão do objeto.

> **Note**
>
> Quando você usa PUT em uma versão de objeto que tem um modo e um período de retenção individual explícitos em um bucket, as configurações individuais da funcionalidade Bloqueio de Objetos da versão do objeto substituem qualquer configuração de retenção de propriedades do bucket.

Assim como acontece com todas as outras configurações de bloqueio de objetos, os períodos de retenção se aplicam a versões de objetos individuais. As versões diferentes de um único objeto podem ter modos e períodos de retenção diferentes.

Por exemplo, suponha que você tenha um objeto de 15 dias em um período de retenção de 30 dias e você PUT um objeto no Amazon S3 com o mesmo nome e um período de retenção de 60 dias. Nesse caso, a solicitação PUT será bem-sucedida e o Amazon S3 criará outra versão do objeto com um período de retenção de 60 dias. A versão anterior mantém o período de retenção original e se torna excluível em 15 dias.

Depois que você tiver aplicado uma configuração de retenção a uma versão do objeto, poderá estender o período de retenção. Para fazer isso, envie uma nova solicitação da funcionalidade Bloqueio de Objetos para a versão do objeto com um Prazo de retenção que seja posterior ao configurado atualmente para a versão do objeto. O Amazon S3 substitui o período de retenção existente pelo novo período mais longo. Qualquer usuário com permissões para colocar um período de retenção do objeto pode estender um período de retenção para uma versão do objeto. Para definir um período de retenção, você deve ter a permissão `s3:PutObjectRetention`.

Ao definir um período de retenção em um objeto ou bucket do S3, é necessário selecionar um dos dois modos de retenção: conformidade ou governança.

Modos de retenção

A funcionalidade Bloqueio de Objetos do S3 oferece dois modos de retenção que aplicam níveis diferentes de proteção aos objetos:

- Modo de conformidade
- Modo de governança

No modo de conformidade, uma versão do objeto protegida não pode ser substituída nem excluída por qualquer usuário, inclusive o usuário root na Conta da AWS. Quando um objeto estiver bloqueado no modo de conformidade, o modo de retenção não poderá ser alterado nem o período de retenção poderá ser encurtado. O modo de conformidade ajuda a garantir que uma versão do objeto não possa ser substituída nem excluída durante o período de retenção.

> **Note**
>
> A única maneira de excluir um objeto no modo de conformidade antes da data de retenção é excluir a Conta da AWS associada.

No modo de governança, os usuários não podem substituir nem excluir uma versão do objeto ou alterar as configurações de bloqueio, a menos que tenham permissões especiais. Com o modo de governança, você protege objetos contra a exclusão da maioria dos usuários, mas ainda pode conceder a alguns usuários permissão para alterar as configurações de retenção ou excluir objetos, caso necessário. Também é possível usar o modo de governança para testar as configurações do período de retenção antes de criar um período de retenção do modo de conformidade.

Para substituir ou remover as configurações de retenção do modo de governança, você precisa ter a permissão `s3:BypassGovernanceRetention` e incluir explicitamente `x-amz-bypass-governance-retention:true` como um cabeçalho de solicitação com qualquer solicitação que exija a substituição do modo de governança.

> **Note**
>
> Por padrão, o console do Amazon S3 inclui o cabeçalho `x-amz-bypass-governance-retention:true`. Se você tentar excluir objetos protegidos pelo modo de governança e tiver a permissão `s3:BypassGovernanceRetention`, a operação será bem-sucedida.

Retenções legais

Com a funcionalidade Bloqueio de Objetos, você também pode colocar uma retenção jurídica em uma versão de objeto. Assim como um período de retenção, uma retenção legal evita que uma versão do objeto seja substituída ou excluída. Porém, uma retenção jurídica não tem uma quantidade fixa de tempo associada e permanecerá em vigor até ser removida. As retenções legais podem ser feitas e removidas livremente por qualquer usuário com a permissão `s3:PutObjectLegalHold`.

As retenções legais independem dos períodos de retenção. Fazer uma retenção legal em uma versão do objeto não afeta o modo de retenção ou o período de retenção dessa versão do objeto.

Por exemplo, suponha que você coloque uma retenção jurídica em uma versão do objeto e que essa versão também está protegida por um período de retenção. Se o período de retenção expirar, o objeto não perderá a proteção WORM. Em vez disso, a retenção jurídica continuará protegendo o objeto até um usuário autorizado removê-la explicitamente. Da mesma maneira, se você remover uma retenção legal enquanto uma versão do objeto tiver um período de retenção em vigor, a versão do objeto continuará protegida até o período de retenção expirar.

Práticas recomendadas para usar a funcionalidade Bloqueio de Objetos do S3

Considere usar o Modo de governança se quiser proteger objetos de serem excluídos pela maioria dos usuários durante um período de retenção predefinido, mas ao mesmo tempo quiser que alguns usuários com permissões especiais tenham a flexibilidade de alterar as configurações de retenção ou excluir os objetos.

Considere usar o Modo de conformidade se você nunca quiser que nenhum usuário, incluindo o usuário raiz em sua Conta da AWS, possa excluir os objetos durante um período de retenção predefinido. Você pode usar esse modo caso precise armazenar dados de conformidade.

Você pode usar a Retenção jurídica quando não tiver certeza de quanto tempo deseja que os objetos permaneçam imutáveis. Isso pode ser devido a uma futura auditoria externa dos dados, em que você deseja manter os objetos imutáveis até que a auditoria seja concluída. Como alternativa, você pode ter um projeto em andamento que utiliza um conjunto de dados que deseja manter imutável até que o projeto seja concluído.

Permissões obrigatórias

As operações do bloqueio de objetos exigem permissões específicas. Dependendo da operação exata que você está tentando realizar, algumas das seguintes permissões poderão ser necessárias:

- `s3:BypassGovernanceRetention`
- `s3:GetBucketObjectLockConfiguration`
- `s3:GetObjectLegalHold`
- `s3:GetObjectRetention`
- `s3:PutBucketObjectLockConfiguration`
- `s3:PutObjectLegalHold`
- `s3:PutObjectRetention`

Consulte uma lista completa de permissões do Amazon S3 com descrições em Actions, resources, and condition keys for Amazon S3 na Referência de autorização do serviço.

Para ter mais informações sobre as permissões referentes a operações de API do S3 de acordo com os tipos de recurso do S3, consulte Permissões obrigatórias para operações de API do Amazon S3.

Para obter informações sobre como usar condições com permissões, consulte Exemplos de políticas de bucket usando chaves de condição.

Considerações sobre a funcionalidade Bloqueio de Objetos

A funcionalidade Bloqueio de Objetos do Amazon S3 pode ajudar a evitar que os objetos sejam excluídos ou substituídos por um período fixo ou indefinidamente.

É possível usar o console do Amazon S3, a AWS Command Line Interface (AWS CLI), os AWS SDKs ou a API REST do Amazon S3 para visualizar ou definir informações da funcionalidade Bloqueio de Objetos. Para obter informações gerais sobre os recursos da funcionalidade Bloqueio de Objetos do S3, consulte Bloquear objetos com o Bloqueio de Objetos.

Important

- Depois de habilitar a funcionalidade Bloqueio de Objetos em um bucket, não será possível desabilitá-la nem suspender o versionamento nesse bucket.
- Os buckets do S3 com funcionalidade Bloqueio de Objetos não podem ser usados como buckets de destino para logs de acesso ao servidor. Para ter mais informações, consulte the section called “Registrando acesso ao servidor”.

Tópicos

- Permissões para visualizar as informações de bloqueio
- Ignorar modo de governança
- Usar a funcionalidade Bloqueio de Objetos com a funcionalidade Replicação do S3
- Usar o Bloqueio de Objetos com criptografia
- Usar a funcionalidade Bloqueio de Objetos com a funcionalidade Inventário Amazon S3
- Gerenciar políticas da funcionalidade Ciclo de Vida do S3 com a funcionalidade Bloqueio de Objetos
- Gerenciar marcadores de exclusão com a funcionalidade Bloqueio de Objetos
- Usar a funcionalidade Lente de Armazenamento do S3 com a funcionalidade Bloqueio de Objetos
- Fazer upload de objetos em um bucket habilitado para a funcionalidade Bloqueio de Objetos
- Configurar eventos e notificações
- Definir limites para os períodos de retenção com uma política de bucket

Permissões para visualizar as informações de bloqueio

É possível visualizar de forma programática o status da funcionalidade Bloqueio de Objetos de uma versão de objeto do Amazon S3 usando as operações HeadObject ou GetObject. Ambas as operações retornam o modo de retenção, a data de retenção e o status de retenção jurídica para a

versão do objeto especificada. Além disso, é possível visualizar o status da funcionalidade Bloqueio de Objetos para vários objetos em um bucket do S3 usando a funcionalidade Inventário do S3.

Para exibir o modo e o período de retenção de uma versão do objeto, você deve ter a permissão `s3:GetObjectRetention`. Para exibir o status de retenção legal de uma versão do objeto, você deve ter a permissão `s3:GetObjectLegalHold`. Para visualizar a configuração de retenção padrão de um bucket, é necessário ter a permissão `s3:GetBucketObjectLockConfiguration`. Caso você faça uma solicitação de uma configuração da funcionalidade Bloqueio de Objetos em um bucket que não tenha a funcionalidade Bloqueio de Objetos do S3 habilitada, o Amazon S3 retornará um erro.

Ignorar modo de governança

Se você tiver a permissão `s3:BypassGovernanceRetention`, poderá realizar operações em versões de objeto bloqueadas no modo de governança como se elas estivessem desprotegidas. Essas operações incluem a exclusão de uma versão do objeto, a redução do período de retenção ou a remoção do período de retenção da funcionalidade Bloqueio de Objetos com a colocação de uma nova solicitação `PutObjectRetention` com parâmetros vazios.

Para ignorar o modo de governança, você deve indicar explicitamente na solicitação que você deseja ignorar esse modo. Para fazer isso, inclua o cabeçalho `x-amz-bypass-governance-retention:true` na solicitação da operação de API `PutObjectRetention` ou use o parâmetro equivalente com solicitações feitas por meio da AWS CLI ou dos AWS SDKs. O console do S3 aplicará automaticamente esse cabeçalho para solicitações feitas por meio do console do S3 se você tiver a permissão `s3:BypassGovernanceRetention`.

> **Note**
>
> Ignorar o modo de governança não afeta o status de retenção legal de uma versão do objeto. Caso uma versão do objeto tenha uma retenção jurídica habilitada, essa retenção permanecerá em vigor e evitará que solicitações substituam ou excluam a versão do objeto.

Usar a funcionalidade Bloqueio de Objetos com a funcionalidade Replicação do S3

Você pode usar a funcionalidade Bloqueio de Objetos com a funcionalidade Replicação do S3 para habilitar a cópia automática e assíncrona de objetos bloqueados e seus metadados de retenção em buckets do S3. Isso significa que, para objetos replicados, o Amazon S3 usa a configuração de bloqueio de objetos do bucket de origem. Em outras palavras, se o bucket de origem tiver o recurso

Bloqueio de Objetos habilitado, os buckets de destino também deverão ter esse recurso habilitado. Se um objeto for carregado diretamente no bucket de destino (fora da replicação do S3), ele usará o Bloqueio de Objetos definido no bucket de destino. Ao usar a replicação, os objetos em um bucket de origem são replicados para um ou mais buckets de destino.

Para configurar a replicação em um bucket com a funcionalidade Bloqueio de Objetos habilitada, você pode usar o console do S3, a AWS CLI, a API REST do Amazon S3 ou os AWS SDKs.

> **Note**
>
> Para usar a funcionalidade Bloqueio de Objetos com replicação, é necessário conceder duas permissões adicionais no bucket de origem do S3 no perfil do AWS Identity and Access Management (IAM) usado para configurar a replicação. As duas permissões adicionais são `s3:GetObjectRetention` e `s3:GetObjectLegalHold`. Se o perfil tiver uma instrução de permissão `s3:Get*`, essa instrução satisfará o requisito. Para ter mais informações, consulte Configurar permissões para replicação em tempo real.
> Para obter informações gerais sobre a funcionalidade Replicação do S3, consulte Replicar objetos dentro de uma região e entre regiões.
> Para obter exemplos de configuração da funcionalidade Replicação do S3, consulte Exemplos para configurar a replicação em tempo real.

Usar o Bloqueio de Objetos com criptografia

O Amazon S3 criptografa todos os objetos novos por padrão. É possível usar o Bloqueio de Objetos com objetos criptografados. Para ter mais informações, consulte Proteger dados com criptografia.

Embora o Bloqueio de Objetos possa ajudar a evitar que os objetos do Amazon S3 sejam excluídos ou substituídos, ele não oferece proteção contra a perda de acesso às chaves de criptografia ou a exclusão dessas chaves. Por exemplo, se você criptografar os objetos com a criptografia do lado do servidor do AWS KMS e a chave do AWS KMS for excluída, os objetos poderão ficar ilegíveis.

Usar a funcionalidade Bloqueio de Objetos com a funcionalidade Inventário Amazon S3

Você pode configurar a funcionalidade Inventário Amazon S3 para criar listas dos objetos em um bucket do S3 com base em uma programação definida. Você pode configurar a funcionalidade Inventário Amazon S3 para incluir os seguintes metadados da funcionalidade Bloqueio de Objetos para os objetos:

- O prazo de retenção
- O modo de retenção
- O status da retenção jurídica

Para ter mais informações, consulte Catalogar e analisar seus dados com o Inventário S3.

Gerenciar políticas da funcionalidade Ciclo de Vida do S3 com a funcionalidade Bloqueio de Objetos

As configurações de gerenciamento de ciclo de vida do objeto continuam funcionando normalmente em objetos protegidos, inclusive a colocação de marcadores de exclusão. No entanto, uma versão bloqueada de um objeto não pode ser excluída por uma política de expiração da funcionalidade Ciclo de Vida do S3. A funcionalidade Bloqueio de Objetos é mantida independentemente da classe de armazenamento em que o objeto reside, bem como durante as transições da funcionalidade Ciclo de Vida do S3 entre classes de armazenamento.

Para obter mais informações sobre como gerenciar ciclos de vida de objetos, consulte Gerenciar o ciclo de vida dos objetos.

Gerenciar marcadores de exclusão com a funcionalidade Bloqueio de Objetos

Embora possa excluir uma versão do objeto protegida, você ainda pode criar um marcador de exclusão para esse objeto. A colocação de um marcador de exclusão em um objeto não exclui o objeto nem suas versões. No entanto, isso faz com que o Amazon S3 se comporte na maioria das vezes como se o objeto tivesse sido excluído. Para obter mais informações, consulte Trabalhar com marcadores de exclusão.

> **Note**
>
> Os marcadores de exclusão não são protegidos por WORM, independentemente de qualquer período de retenção ou da retenção legal no objeto subjacente.

Usar a funcionalidade Lente de Armazenamento do S3 com a funcionalidade Bloqueio de Objetos

Para ver métricas de bytes de armazenamento e contagem de objetos com Bloqueio de Objeto habilitado, você pode usar a Lente de Armazenamento do Amazon S3. A Lente de Armazenamento

do S3 é um recurso de análise de armazenamento em nuvem que você pode usar para obter visibilidade em toda a organização sobre o uso e a atividade do armazenamento de objetos.

Para ter mais informações, consulte Usar a Lente de Armazenamento do S3 para proteger seus dados.

Para obter uma lista completa de métricas, consulte Glossário de métricas de lente de armazenamento do Amazon S3.

Fazer upload de objetos em um bucket habilitado para a funcionalidade Bloqueio de Objetos

O cabeçalho `Content-MD5` ou `x-amz-sdk-checksum-algorithm` é necessário em todas as solicitações de upload de um objeto com um período de retenção configurado usando o Bloqueio de Objetos. Esses cabeçalhos são uma forma de verificar a integridade do objeto durante o upload.

Quando um objeto é carregado com o console do Amazon S3, o S3 adiciona automaticamente o cabeçalho `Content-MD5`. Opcionalmente, você pode especificar uma função de soma de verificação adicional e um valor de soma de verificação por meio do console como o cabeçalho `x-amz-sdk-checksum-algorithm`. Se você usar a API PutObject, deverá especificar o cabeçalho `Content-MD5`, o cabeçalho `x-amz-sdk-checksum-algorithm` ou ambos para configurar o período de retenção do Bloqueio de Objetos.

Para ter mais informações, consulte Verificar a integridade do objeto no Amazon S3.

Configurar eventos e notificações

Use a funcionalidade Notificações de Eventos do Amazon S3 para rastrear o acesso e as alterações feitas nas configurações da funcionalidade Bloqueio de Objetos e nos dados usando o AWS CloudTrail. Para obter informações sobre o CloudTrail, consulte O que é AWS CloudTrail? no Guia do Usuário do AWS CloudTrail.

Você também pode usar o Amazon CloudWatch para gerar alertas com base nesses dados. Para obter informações sobre o CloudWatch, consulte O que é o Amazon CloudWatch? no Guia do usuário do Amazon CloudWatch.

Definir limites para os períodos de retenção com uma política de bucket

É possível definir os períodos de retenção mínimo e máximo permitidos para um bucket usando uma política de bucket. O período máximo de retenção é de cem anos.

O exemplo a seguir mostra uma política de bucket que usa a chave de condição `s3:object-lock-remaining-retention-days` para definir um período de retenção máximo de 10 dias.

```
{
    "Version": "2012-10-17",
    "Id": "SetRetentionLimits",
    "Statement": [
        {
            "Sid": "SetRetentionPeriod",
            "Effect": "Deny",
            "Principal": "*",
            "Action": [
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*",
            "Condition": {
                "NumericGreaterThan": {
                    "s3:object-lock-remaining-retention-days": "10"
                }
            }
        }
    ]
}
```

> **Note**
>
> Se o seu bucket for o bucket de destino de uma configuração de replicação, você poderá definir períodos de retenção mínimo e máximo permitidos para as réplicas de objetos criadas usando a replicação. Para fazer isso, você deve permitir a ação `s3:ReplicateObject` na política de bucket. Para obter mais informações sobre as permissões de replicação, consulte the section called “Configurar permissões”.

Para obter mais informações sobre políticas de bucket, consulte os seguintes tópicos:

- Actions, resources, and condition keys for Amazon S3 na Referência de autorização do serviço

  Para ter mais informações sobre as permissões referentes a operações de API do S3 de acordo com os tipos de recurso do S3, consulte Permissões obrigatórias para operações de API do Amazon S3.

- Operações com objetos
- Exemplos de políticas de bucket usando chaves de condição

Configurar a funcionalidade Bloqueio de Objetos do S3

Com a funcionalidade Bloqueio de Objetos do Amazon S3, é possível armazenar objetos em buckets de uso geral no Amazon S3 usando um modelo de gravação única e várias leituras (WORM). Você pode usar o bloqueio de objetos do S3 para evitar que um objeto seja excluído ou substituído por um período fixo ou indefinidamente. Para obter informações gerais sobre os recursos da funcionalidade Bloqueio de Objetos, consulte Bloquear objetos com o Bloqueio de Objetos.

Antes de bloquear qualquer objeto, é necessário habilitar as funcionalidades Versionamento e Bloqueio de Objetos do S3 em um bucket de uso geral. Depois, você pode definir um período de retenção, uma retenção jurídica ou ambos.

Para trabalhar com a funcionalidade Bloqueio de Objetos, é necessário ter determinadas permissões. Para obter uma lista das permissões relacionadas a várias operações da funcionalidade Bloqueio de Objetos, consulte the section called “Permissões obrigatórias”.

> **Important**
>
> - Depois de habilitar a funcionalidade Bloqueio de Objetos em um bucket, não será possível desabilitá-la nem suspender o versionamento nesse bucket.
> - Os buckets do S3 com funcionalidade Bloqueio de Objetos não podem ser usados como buckets de destino para logs de acesso ao servidor. Para ter mais informações, consulte the section called “Registrando acesso ao servidor”.

Tópicos

- Habilitar a funcionalidade Bloqueio de Objetos ao criar um bucket de uso geral do S3
- Habilitar a funcionalidade Bloqueio de Objetos em um bucket do S3 existente
- Definir ou modificar uma retenção jurídica em um objeto do S3
- Definir ou modificar um período de retenção em um objeto do S3
- Definir ou modificar um período de retenção padrão em um bucket do S3

Habilitar a funcionalidade Bloqueio de Objetos ao criar um bucket de uso geral do S3

Você pode habilitar a funcionalidade Bloqueio de Objetos ao criar um bucket de uso geral do S3 usando o console do Amazon S3, a AWS Command Line Interface (AWS CLI), os AWS SDKs ou a API REST do Amazon S3.

Uso do console do S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets de uso geral.
3. Selecione Create bucket (Criar bucket).

   A página Create bucket (Criar bucket) é aberta.
4. Para Nome do bucket, insira um nome para o bucket.

   > **Note**
   >
   > Depois de criar um bucket, não será possível mudar o nome dele. Para obter mais informações sobre como nomear buckets, consulte Regras de nomenclatura de buckets de uso geral.
5. Em Region (Região), escolha a Região da AWS onde deseja que o bucket resida.
6. Em Propriedade de Objetos, escolha desabilitar ou habilitar as listas de controle de acesso (ACLs) e controlar a propriedade de objetos carregados no bucket.
7. Em Configurações de bloqueio de acesso público para este bucket, selecione as configurações de bloqueio de acesso público que deseja aplicar ao bucket.
8. Em Versionamento de bucket, escolha Habilitado.

   A funcionalidade Bloqueio de Objetos só funciona em buckets com versionamento.
9. (Opcional) Em Tags (Etiquetas), você pode optar por adicionar etiquetas ao seu bucket. As etiquetas são pares de chave-valor usados para categorizar o armazenamento e alocar os custos.
10. Em Configurações avançadas, encontre Bloqueio de objeto e escolha Habilitar.

    Você deve reconhecer que a ativação da funcionalidade Bloqueio de Objetos permitirá permanentemente que os objetos desse bucket sejam bloqueados.

11. Escolha Criar bucket.

Uso do AWS CLI

O seguinte exemplo `create-bucket` cria um bucket do S3 chamado *amzn-s3-demo-bucket1* com a funcionalidade Bloqueio de Objetos habilitada:

```
aws s3api create-bucket --bucket amzn-s3-demo-bucket1 --object-lock-enabled-for-bucket
```

Para obter mais informações e exemplos, consulte create-bucket na Referência de comandos da AWS CLI.

> **Note**
>
> Você pode executar comandos da AWS CLI pelo console usando o AWS CloudShell. O AWS CloudShell é um shell pré-autenticado e baseado em navegador que você pode inicializar diretamente do AWS Management Console. Para obter mais informações, consulte What is CloudShell? no Guia do usuário do AWS CloudShell.

Uso da API REST

É possível usar a API REST para criar um bucket do S3 com a funcionalidade Bloqueio de Objetos habilitada. Para obter mais informações, consulte CreateBucket na Referência da API do Amazon Simple Storage Service.

Uso dos SDKs da AWS

Consulte exemplos de como habilitar o Bloqueio de Objetos ao criar um bucket do S3 com os SDKs da AWS em Code examples na Referência de API do Amazon S3.

Consulte exemplos de como obter a configuração atual do Bloqueio de Objetos com os SDKs da AWS em Code examples na Referência de API do Amazon S3.

Consulte um cenário interativo que demonstra os diferentes recursos do Bloqueio de Objetos usando os SDKs da AWS em Code examples na Referência de API do Amazon S3.

Consulte informações gerais sobre como usar diferentes SDKs da AWS em Developing with Amazon S3 using the AWS SDKs na Referência de API do Amazon S3.

Habilitar a funcionalidade Bloqueio de Objetos em um bucket do S3 existente

Você pode habilitar a funcionalidade Bloqueio de Objetos para um bucket do S3 existente usando o console do Amazon S3, a AWS CLI, os AWS SDKs ou a API REST do Amazon S3.

Uso do console do S3

> **Note**
>
> A funcionalidade Bloqueio de Objetos só funciona em buckets com versionamento.

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets.
3. Na lista Buckets, escolha o nome do bucket para o qual você deseja habilitar a funcionalidade Bloqueio de Objetos.
4. Escolha a guia Properties (Propriedades).
5. Em Propriedades, role para baixo até a seção Bloqueio de objeto e escolha Editar.
6. Em Bloqueio de objeto, escolha Habilitar.

   Você deve reconhecer que a ativação da funcionalidade Bloqueio de Objetos permitirá permanentemente que os objetos desse bucket sejam bloqueados.
7. Selecione Save changes.

Uso do AWS CLI

O seguinte exemplo de comando `put-object-lock-configuration` define um período de retenção de 50 dias da funcionalidade Bloqueio de Objetos em um bucket chamado *amzn-s3-demo-bucket1*:

```
aws s3api put-object-lock-configuration --bucket amzn-s3-demo-bucket1 --object-
lock-configuration='{ "ObjectLockEnabled": "Enabled", "Rule": { "DefaultRetention":
 { "Mode": "COMPLIANCE", "Days": 50 }}}'
```

Para obter mais informações e exemplos, consulte put-object-lock-configuration na Referência de comandos da AWS CLI.

> **Note**
>
> Você pode executar comandos da AWS CLI pelo console usando o AWS CloudShell. O AWS CloudShell é um shell pré-autenticado e baseado em navegador que você pode inicializar diretamente do AWS Management Console. Para obter mais informações, consulte What is CloudShell? no Guia do usuário do AWS CloudShell.

Uso da API REST

Você pode usar a API REST do Amazon S3 para habilitar a funcionalidade Bloqueio de Objetos em um bucket do S3 existente. Para obter mais informações, consulte PutObjectLockConfiguration na Referência da API do Amazon Simple Storage Service.

Uso dos SDKs da AWS

Consulte exemplos de como habilitar o Bloqueio de Objetos para um bucket existente do S3 com os SDKs da AWS em Code examples na Referência de API do Amazon S3.

Consulte exemplos de como obter a configuração atual do Bloqueio de Objetos com os SDKs da AWS em Code examples na Referência de API do Amazon S3.

Consulte um cenário interativo que demonstra os diferentes recursos do Bloqueio de Objetos usando os SDKs da AWS em Code examples na Referência de API do Amazon S3.

Consulte informações gerais sobre como usar diferentes SDKs da AWS em Developing with Amazon S3 using the AWS SDKs na Referência de API do Amazon S3.

Definir ou modificar uma retenção jurídica em um objeto do S3

Você pode definir ou remover uma retenção jurídica de um objeto do S3 usando o console do Amazon S3, a AWS CLI, os AWS SDKs ou a API REST do Amazon S3.

> **Important**
>
> - Se você quiser definir uma retenção jurídica em um objeto, o bucket do objeto já deverá ter a funcionalidade Bloqueio de Objetos habilitada.
> - Quando você usa PUT em uma versão de objeto que tem um modo e um período de retenção individual explícitos em um bucket, as configurações individuais da

funcionalidade Bloqueio de Objetos da versão do objeto substituem qualquer configuração de retenção de propriedades do bucket.

Para ter mais informações, consulte the section called “Retenções legais”.

Uso do console do S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets.
3. Na lista Buckets, escolha o nome do bucket que contém o objeto no qual você deseja definir ou modificar uma retenção jurídica.
4. Na lista Objetos, selecione o objeto no qual você deseja definir ou modificar uma retenção jurídica.
5. Na página Propriedades do objeto, encontre a seção Retenção jurídica do Bloqueio de objeto e escolha Editar.
6. Escolha Habilitar para definir uma retenção jurídica ou Desabilitar para remover uma retenção jurídica.
7. Selecione Save changes.

Uso do AWS CLI

O seguinte exemplo de `put-object-legal-hold` define uma retenção jurídica no objeto *`my-image.fs`* no bucket chamado *`amzn-s3-demo-bucket1`*:

```
aws s3api put-object-legal-hold --bucket amzn-s3-demo-bucket1 --key my-image.fs --
legal-hold="Status=ON"
```

O seguinte exemplo de `put-object-legal-hold` remove uma retenção jurídica do objeto *`my-image.fs`* no bucket chamado *`amzn-s3-demo-bucket1`*:

```
aws s3api put-object-legal-hold --bucket amzn-s3-demo-bucket1 --key my-image.fs --
legal-hold="Status=OFF"
```

Para obter mais informações e exemplos, consulte put-object-legal-hold na Referência de comandos da AWS CLI.

> **Note**
>
> Você pode executar comandos da AWS CLI pelo console usando o AWS CloudShell. O AWS CloudShell é um shell pré-autenticado e baseado em navegador que você pode inicializar diretamente do AWS Management Console. Para obter mais informações, consulte What is CloudShell? no Guia do usuário do AWS CloudShell.

Uso da API REST

É possível usar a API REST para definir ou modificar uma retenção jurídica em um objeto. Para obter mais informações, consulte PutObjectLegalHold na Referência da API do Amazon Simple Storage Service.

Uso dos SDKs da AWS

Consulte exemplos de como definir uma retenção legal em um objeto com os SDKs da AWS em Code examples na Referência de API do Amazon S3.

Consulte exemplos de como obter o status de retenção legal atual com os SDKs da AWS em Code examples na Referência de API do Amazon S3.

Consulte um cenário interativo que demonstra os diferentes recursos do Bloqueio de Objetos usando os SDKs da AWS em Code examples na Referência de API do Amazon S3.

Consulte informações gerais sobre como usar diferentes SDKs da AWS em Developing with Amazon S3 using the AWS SDKs na Referência de API do Amazon S3.

Definir ou modificar um período de retenção em um objeto do S3

Você pode definir ou modificar um período de retenção em um objeto do S3 usando o console do Amazon S3, a AWS CLI, os AWS SDKs ou a API REST do Amazon S3.

> **Important**
>
> - Se você quiser definir um período de retenção em um objeto, o bucket do objeto já deverá ter a funcionalidade Bloqueio de Objetos habilitada.
> - Quando você usa PUT em uma versão de objeto que tem um modo e um período de retenção individual explícitos em um bucket, as configurações individuais da

funcionalidade Bloqueio de Objetos da versão do objeto substituem qualquer configuração de retenção de propriedades do bucket.

- A única maneira de excluir um objeto no modo de conformidade antes da data de retenção é excluir a Conta da AWS associada.

Para ter mais informações, consulte Períodos de retenção.

Uso do console do S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets.
3. Na lista Buckets, escolha o nome do bucket que contém o objeto no qual você deseja definir ou modificar um período de retenção.
4. Na lista Objetos, selecione o objeto no qual você deseja definir ou modificar um período de retenção.
5. Na página Propriedades do objeto, encontre a seção Retenção de Bloqueio de objetos e escolha Editar.
6. Em Retenção, escolha Habilitar para definir um período de retenção ou Desabilitar para remover um período de retenção.
7. Se você escolher Habilitar, em Modo de retenção, escolha o Modo de governança ou o Modo de conformidade. Para ter mais informações, consulte Modos de retenção.
8. Em Prazo de retenção, escolha a data em que deseja que o período de retenção termine. Durante esse período, o objeto será protegido por WORM e não poderá ser substituído nem excluído. Para ter mais informações, consulte Períodos de retenção.
9. Selecione Save changes.

Uso do AWS CLI

O seguinte exemplo de `put-object-retention` define um período de retenção no objeto *my-image.fs* no bucket chamado *amzn-s3-demo-bucket1* até 1.º de janeiro de 2025:

```
aws s3api put-object-retention --bucket amzn-s3-demo-bucket1 --key my-image.fs --
retention='{ "Mode": "GOVERNANCE", "RetainUntilDate": "2025-01-01T00:00:00" }'
```

Para obter mais informações e exemplos, consulte put-object-retention na Referência de comandos da AWS CLI.

> **Note**
>
> Você pode executar comandos da AWS CLI pelo console usando o AWS CloudShell. O AWS CloudShell é um shell pré-autenticado e baseado em navegador que você pode inicializar diretamente do AWS Management Console. Para obter mais informações, consulte What is CloudShell? no Guia do usuário do AWS CloudShell.

Uso da API REST

É possível usar a API REST para definir um período de retenção em um objeto. Para obter mais informações, consulte PutObjectRetention na Referência da API do Amazon Simple Storage Service.

Uso dos SDKs da AWS

Consulte exemplos de como definir um período de retenção em um objeto com os SDKs da AWS em Code examples na Referência de API do Amazon S3.

Consulte exemplos de como obter o período de retenção em um objeto com os SDKs da AWS em Code examples na Referência de API do Amazon S3.

Consulte um cenário interativo que demonstra os diferentes recursos do Bloqueio de Objetos usando os SDKs da AWS em Code examples na Referência de API do Amazon S3.

Consulte informações gerais sobre como usar diferentes SDKs da AWS em Developing with Amazon S3 using the AWS SDKs na Referência de API do Amazon S3.

Definir ou modificar um período de retenção padrão em um bucket do S3

Você pode definir ou modificar um período de retenção padrão em um bucket do S3 usando o console do Amazon S3, a AWS CLI, os AWS SDKs ou a API REST do Amazon S3. Especifique uma duração, em dias ou anos, para proteger cada versão do objeto colocada no bucket.

> **Important**
>
> - Se você quiser definir um período de retenção padrão em um bucket, o bucket já deverá ter a funcionalidade Bloqueio de Objetos habilitada.

- Quando você usa PUT em uma versão de objeto que tem um modo e um período de retenção individual explícitos em um bucket, as configurações individuais da funcionalidade Bloqueio de Objetos da versão do objeto substituem qualquer configuração de retenção de propriedades do bucket.
- A única maneira de excluir um objeto no modo de conformidade antes da data de retenção é excluir a Conta da AWS associada.

Para ter mais informações, consulte Períodos de retenção.

Uso do console do S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets.
3. Na lista Buckets, escolha o nome do bucket no qual você deseja definir ou modificar um período de retenção padrão.
4. Escolha a guia Properties (Propriedades).
5. Em Propriedades, role para baixo até a seção Bloqueio de objeto e escolha Editar.
6. Em Retenção padrão, escolha Habilitar para definir uma retenção padrão ou Desabilitar para remover uma retenção padrão.
7. Se você escolher Habilitar, em Modo de retenção, escolha o Modo de governança ou o Modo de conformidade. Para ter mais informações, consulte Modos de retenção.
8. Em Período de retenção padrão, escolha o número de dias ou anos para a duração do período de retenção. Os objetos colocados nesse bucket ficarão bloqueados durante esse número de dias ou anos. Para ter mais informações, consulte Períodos de retenção.
9. Selecione Save changes.

Uso do AWS CLI

O seguinte exemplo de comando `put-object-lock-configuration` define um período de retenção de 50 dias da funcionalidade Bloqueio de Objetos no bucket chamado *`amzn-s3-demo-bucket1`* usando o modo de conformidade:

```
aws s3api put-object-lock-configuration --bucket amzn-s3-demo-bucket1 --object-
lock-configuration='{ "ObjectLockEnabled": "Enabled", "Rule": { "DefaultRetention":
 { "Mode": "COMPLIANCE", "Days": 50 }}}'
```

O seguinte exemplo de `put-object-lock-configuration` remove a configuração de retenção padrão de um bucket:

```
aws s3api put-object-lock-configuration --bucket amzn-s3-demo-bucket1 --object-lock-
configuration='{ "ObjectLockEnabled": "Enabled"}'
```

Para obter mais informações e exemplos, consulte put-object-lock-configuration na Referência de comandos da AWS CLI.

> **Note**
>
> Você pode executar comandos da AWS CLI pelo console usando o AWS CloudShell. O AWS CloudShell é um shell pré-autenticado e baseado em navegador que você pode inicializar diretamente do AWS Management Console. Para obter mais informações, consulte What is CloudShell? no Guia do usuário do AWS CloudShell.

Uso da API REST

É possível usar a API REST para definir um período de retenção padrão em um bucket do S3 disponível. Para obter mais informações, consulte PutObjectLockConfiguration na Referência da API do Amazon Simple Storage Service.

Uso dos SDKs da AWS

Consulte exemplos de como definir um período de retenção padrão em um bucket existente do S3 com os SDKs da AWS em Code examples na Referência de API do Amazon S3.

Consulte um cenário interativo que demonstra os diferentes recursos do Bloqueio de Objetos usando os SDKs da AWS em Code examples na Referência de API do Amazon S3.

Consulte informações gerais sobre como usar diferentes SDKs da AWS em Developing with Amazon S3 using the AWS SDKs na Referência de API do Amazon S3.

Fazer backup de dados do Amazon S3

O Amazon S3 é integrado nativamente ao AWS Backup, um serviço totalmente gerenciado e baseado em políticas que você pode usar para definir políticas de backup centralmente e proteger dados do Amazon S3. Depois de definir suas políticas de backup e atribuir recursos do Amazon S3 às políticas, o AWS Backup automatiza a criação de backups do Amazon S3 e os armazena com segurança em um cofre de backup criptografado designado pelo seu plano de backup.

Ao usar o AWS Backup para o Amazon S3, você pode executar as seguintes ações:

- Criar backups contínuos e backups periódicos. Backups contínuos são úteis para restauração em um ponto anterior no tempo, e backups periódicos são úteis para atender às suas necessidades de retenção de dados de longo prazo.
- Automatizar o agendamento e a retenção de backups configurando as políticas de backup de modo centralizado.
- Restaurar backups de dados do Amazon S3 em um ponto anterior no tempo que você especifica.

Com o AWS Backup, é possível usar o versionamento do S3 e a replicação do S3 para ajudar a se recuperar de exclusões acidentais e executar suas próprias operações de autorrecuperação.

Pré-requisitos

Você deve ativar o versionamento do S3 em seu bucket para o AWS Backup poder fazer backup.

> **Note**
>
> Recomendamos que você defina uma regra de validade do ciclo de vida para buckets habilitados para versionamento dos quais está sendo feito backup. Se você não definir um período de validade do ciclo de vida, os custos de armazenamento do Amazon S3 poderão aumentar, pois o AWS Backup manterá todas as versões dos dados do Amazon S3.

Começar a usar

Para começar a usar o AWS Backup para o Amazon S3, consulte Criar backups do Amazon S3 no Guia do desenvolvedor do AWS Backup.

Restrições e limitações

Para saber mais sobre as limitações, consulte Creating Amazon S3 backups (“Criar backups do Amazon S3”) no Guia do desenvolvedor do AWS Backup.

Otimização de custo

O Amazon S3 oferece uma variedade de recursos e classes de armazenamento para ajudar a otimizar os custos em todo o ciclo de vida dos dados. As classes de armazenamento oferecem a flexibilidade de gerenciar seus custos, fornecendo diferentes níveis de acesso aos dados a custos correspondentes, sem taxas iniciais ou compromisso com a quantidade de conteúdo que você armazena. Assim como outros serviços da AWS, o pagamento é conforme o uso, ou seja, você paga somente pelo que usar.

As classes de armazenamento do Amazon S3 foram criadas especificamente para fornecer o menor custo de armazenamento para diferentes padrões de acesso. Isso inclui:

- S3 Standard para armazenamento de uso geral de dados acessados com frequência.
- Amazon S3 Express One Zone para dados de alto desempenho acessados com frequência em uma única zona de disponibilidade.
- S3 Intelligent-Tiering para otimizar automaticamente os custos para dados com padrões de acesso desconhecidos ou variáveis.
- S3 Standard-IA (S3 Standard-IA) e S3 One Zone-IA (S3 One Zone-IA) para dados de longa duração, mas acessados com menos frequência.
- S3 Glacier Instant Retrieval para arquivar dados que precisam de acesso imediato.
- S3 Glacier para arquivar dados que não exigem acesso imediato, mas precisam da flexibilidade de recuperar grandes conjuntos de dados sem nenhum custo.
- S3 Glacier Deep Archive para a arquivamento de longo prazo e preservação digital com os menores custos de armazenamento na nuvem.

Você pode mover objetos para a classe de armazenamento mais econômica a qualquer momento. Além disso, o Amazon S3 oferece recursos para gerenciar o ciclo de vida dos dados. Por exemplo, é possível usar a configuração do Ciclo de Vida do S3 para automatizar a transição de objetos para classes de armazenamento mais econômicas ou para excluir automaticamente objetos expirados com base nas regras que você define.

Recursos como análise de classe de armazenamento do S3, marcação de alocação de custos e relatórios de cobrança e uso ajudam você a analisar seus padrões de custo e uso.

Tópicos

- Relatórios de uso e faturamento do Amazon S3
- Compreender e gerenciar classes de armazenamento do Amazon S3
- Gerenciar o ciclo de vida dos objetos

Relatórios de uso e faturamento do Amazon S3

Ao usar o Amazon S3, você não tem que pagar nenhuma taxa inicial nem assumir nenhum compromisso em relação à quantidade de conteúdo que armazenará. Assim como outros Serviços da AWS, você paga somente pelo que usar.

AWSA fornece os seguintes relatórios do Amazon S3:

- Relatórios de faturamento: vários relatórios que fornecem exibições de alto nível de toda a atividade dos Serviços da AWS que você está usando, incluindo o Amazon S3. A AWS sempre cobra as tarifas do Amazon S3 do proprietário do bucket do S3, a menos que o bucket tenha sido criado como um bucket de pagamento a cargo do solicitante. Para obter mais informações sobre Pagamento pelo solicitante, consulte Utilizar buckets de uso geral com pagamento pelo solicitante para transferência e uso de armazenamento. Para obter mais informações sobre relatórios de faturamento, consulte Relatórios do AWS Billing para o Amazon S3.
- Relatório de uso: um resumo das atividades de um serviço específico, agregado por hora, dia ou mês. Você pode escolher qual tipo e operação de uso incluir. Também é possível escolher a forma como os dados são agregados. Para obter mais informações, consulte Relatórios de uso da AWS para o Amazon S3.

Os tópicos seguintes fornecem informações sobre os relatórios de uso e faturamento do Amazon S3.

Tópicos

- Usar tags de alocação de custos para buckets do S3
- Relatórios do AWS Billing para o Amazon S3
- Relatórios de uso da AWS para o Amazon S3
- Como entender os relatórios de uso e faturamento da AWS para o Amazon S3
- Cobrança pelas respostas de erro do Amazon S3

Usar tags de alocação de custos para buckets do S3

Para monitorar o custo de armazenamento ou outros critérios de projetos individuais ou grupos de projetos, rotule seus buckets do Amazon S3 usando tags de alocação de custos. Uma tag de alocação de custos é um par nome-valor que você associa a um bucket do S3. Depois que você ativa as tags de alocação de custos, a AWS as utiliza para organizar os custos de recursos em seu relatório de alocação de custo. As tags de alocação de custos só podem ser usadas para identificar buckets. Para obter informações sobre tags usadas para identificar objetos, consulte Categorizar seu armazenamento usando tags.

O relatório de alocação de custos indica o uso da sua conta na AWS por categoria de produto e usuário de conta vinculado. O relatório contém os mesmos itens de linha do relatório de faturamento detalhado (consulte Como entender os relatórios de uso e faturamento da AWS para o Amazon S3) e colunas adicionais para suas chaves de tag.

A AWS fornece dois tipos de tags de alocação de custo, uma tag gerada pela AWS e tags definidas pelo usuário. A AWS define, cria e aplica a tag `createdBy` gerada pela AWS para você após um evento CreateBucket do Amazon S3. Você define, cria e aplica tags definidas pelo usuário ao seu bucket do S3.

Você deve ativar ambos os tipos de tags separadamente no console de Gerenciamento de custos e faturamento antes que elas possam aparecer em seus relatórios de faturamento. Para obter mais informações sobre etiquetas geradas pela AWS, consulte Etiquetas de alocação de custos geradas pela AWS.

- Para criar tags no console, consulte Visualizar das propriedades de um bucket de uso geral do S3.
- Para criar tags usando a API do Amazon S3, consulte Marcação de PUT bucket na Referência da API do Amazon Simple Storage Service.
- Para criar tags usando a AWS CLI, consulte put-bucket-tagging na Referência de comandos da AWS CLI.
- Para obter mais informações sobre como ativar tags, consulte Uso de tags de alocação de custos no Guia do usuário do AWS Billing.

Tags de alocação de custos definidas pelo usuário

Uma tag de alocação de custos definida pelo usuário tem os seguintes componentes:

- A chave de tags. A chave de tags é o nome da tag. Por exemplo, no projeto de tags/Trinity, o projeto é a chave. A chave de tags é uma string que diferencia maiúsculas e minúsculas que pode conter de 1 a 128 caracteres Unicode.

- O valor da tag. O valor da tag é uma string obrigatória. Por exemplo, no projeto de tags/Trinity, Trinity é o valor. O valor da tag é uma string que diferencia maiúsculas e minúsculas que pode conter de 0 a 256 caracteres Unicode.

Para obter detalhes sobre os caracteres permitidos em tags definidas pelo usuário e outras restrições, consulte Restrições de tags definidas pelo usuário no Guia do usuário do AWS Billing. Para obter mais informações sobre tags definidas pelo usuário, consulte Tags de alocação de custos definidas pelo usuário no Guia do usuário do AWS Billing.

Tags de bucket do S3

Cada bucket do S3 tem um conjunto de tags. Um conjunto de tags contém todas as tags que são atribuídas àquele bucket. Um conjunto de tags pode conter até 50 tags ou estar vazio. As chaves podem ser únicas em um conjunto de tags, mas os valores nele não precisam ser únicos. Por exemplo, você pode ter o mesmo valor nos conjuntos de tags chamados project/Trinity e cost-center/Trinity.

Em um bucket, se você adicionar uma tag que tenha a mesma chave de uma tag existente, o novo valor substituirá o antigo.

AWSA não aplica nenhum significado semântico às suas tags. Interpretamos as tags estritamente como sequências de caracteres.

Para adicionar, listar, editar ou excluir tags, você pode usar o console do Amazon S3, a AWS Command Line Interface (AWS CLI) ou a API do Amazon S3.

Mais informações

- Uso de tags de alocação de custos no Guia do usuário do AWS Billing.
- Como entender os relatórios de uso e faturamento da AWS para o Amazon S3
- Relatórios do AWS Billing para o Amazon S3

Relatórios do AWS Billing para o Amazon S3

Sua fatura mensal da AWS separa suas informações de uso e o custo por AWS service (Serviço da AWS) e por função. Há vários relatórios do AWS Billing disponíveis: o relatório mensal, o relatório de alocação de custos e os relatórios detalhados de faturamento. Para obter informações sobre como ver seus relatórios de faturamento, consulte Exibição da fatura no Guia do usuário do AWS Billing.

Para acompanhar o seu uso da AWS e fornecer as cobranças estimadas associadas à sua conta, você pode configurar Cost and Usage Reports da AWS. Para obter mais informações, consulte O que é são os Cost and Usage Reports da AWS? no Guia de exportações de dados da AWS.

Você também pode fazer download de um relatório de uso que forneça mais detalhes sobre o uso do armazenamento do Amazon S3 do que os relatórios de faturamento. Para obter mais informações, consulte Relatórios de uso da AWS para o Amazon S3.

A tabela a seguir lista as taxas associadas ao uso do Amazon S3.

Cobrança	Comentários
Armazenamento	Você paga para armazenar objetos em seu bucket do S3. A taxa cobrada depende do tamanho dos seus objetos, do tempo que você os armazenou durante o mês e das classes de armazenamento. O Amazon S3 oferece as seguintes classes de armazenam ento: S3 Standard, S3 Express One Zone, S3 Intelligent-Tiering, S3 Standard-IA (IA para acesso infrequente), S3 One Zone-IA, S3 Glacier Instant Retrieval, S3 Glacier Flexible Retrieval, S3 Glacier Deep Archive ou Reduced Redundancy Storage (RRS). Para obter mais informações sobre classes de armazenamento, consulte Compreender e gerenciar classes de armazenamento do Amazon S3. Esteja ciente de que, se a funcionalidade Versionamento do S3 estiver habilitada, você será cobrado por cada versão de um objeto

Cobrança	Comentários
	retido. Para obter mais informações sobre versionamento, consulte Como funciona o Versionamento do S3.
Buckets de uso geral	Não haverá cobrança pelos primeiros 2 mil buckets de uso geral criados em sua conta. No entanto, há uma taxa por bucket para cada bucket que você cria além dos primeiros 2 mil. Essa taxa é cobrada por bucket/mês. Consulte informações sobre o preço dos buckets de uso geral em Definição de preço do Amazon S3.
Monitoramento e automação	Você paga uma taxa mensal de monitoram ento e automação por objeto armazenado na classe de armazenamento do S3 Intelligent-Tiering para monitorar padrões de acesso e mover objetos entre camadas de acesso no S3 Intelligent-Tiering.
Solicitações	Você paga por solicitações, por exemplo, solicitações `GET`, feitas em seus buckets e objetos do S3. Isso inclui solicitações de ciclo de vida. As taxas para solicitações dependem de qual tipo de solicitação você está fazendo. Para obter informações sobre a definição de preço de solicitações, consulte Definição de preço do Amazon S3.
Recuperações	Você paga para recuperar objetos que são armazenados no armazenamento S3 Standard – IA, S3 One Zone – IA, S3 Glacier Instant Retrieval, S3 Glacier Flexible Retrieval e S3 Glacier Deep Archive.

Cobrança	Comentários
Exclusões adiantadas	Se excluir um objeto armazenado no armazenamento S3 Standard-IA, S3 One Zone-IA, S3 Glacier Instant Retrieval, S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive antes de terminado o compromisso mínimo de armazenamento, você pagará uma taxa de exclusão antecipada por esse objeto.
Gerenciamento de armazenamento	Você paga pelos recursos de gerenciamento de armazenamento (Inventário Amazon S3, análise e marcação de objetos) habilitados nos buckets de sua conta.
Largura de banda	Você paga por toda a largura de banda de entrada e de saída do Amazon S3, exceto: • Dados transferidos da Internet • Dados transferidos para uma instância do Amazon Elastic Compute Cloud (Amazon EC2), quando a instância está na mesma Região da AWS que o bucket do S3. • Dados transferidos para o Amazon CloudFront (CloudFront). Você também paga uma taxa por todos os dados transferidos usando a funcionalidade Aceleração de Transferências do Amazon S3.

Para obter informações detalhadas sobre as cobranças de uso do Amazon S3 para armazenamento, transferência de dados e serviços, consulte Definição de preço do Amazon S3 e Perguntas frequentes sobre o Amazon S3.

Para obter informações sobre como entender os códigos e as abreviações usadas nos relatórios de uso e faturamento do Amazon S3, consulte Como entender os relatórios de uso e faturamento da AWS para o Amazon S3.

Mais informações

- Relatórios de uso da AWS para o Amazon S3
- Usar tags de alocação de custos para buckets do S3
- Gerenciamento de Faturamento e Custos da AWS Billing
- Preços do Amazon S3

Relatórios de uso da AWS para o Amazon S3

Ao fazer download de um relatório de uso, você pode optar por agregar os dados de uso por hora, dia ou mês. O relatório de uso do Amazon S3 lista as operações por tipo de uso e Região da AWS. Para obter mais detalhes sobre o uso do armazenamento do Amazon S3, faça download dos relatórios de uso da AWS gerados dinamicamente. Você pode escolher qual tipo de uso, operação e período de tempo incluir. Também é possível escolher a forma como os dados são agregados. Para obter mais informações sobre os relatórios de uso, consulte AWS Usage Report no Guia do usuário de exportações de dados da AWS.

O relatório de uso do Amazon S3 inclui as seguintes informações:

- Serviço: Amazon S3
- Operação: a operação executada em seu bucket ou objeto. Para obter uma explicação detalhada das operações do Amazon S3, consulte Controle de operações em seus relatórios de uso.
- UsageType: um dos seguintes valores:
  - Um código que identifica o tipo de armazenamento
  - Um código que identifica o tipo de solicitação
  - Um código que identifica o tipo de recuperação
  - Um código que identifica o tipo de transferência de dados
  - Um código que identifica exclusões antecipadas do armazenamento S3 Intelligent-Tiering, S3 Standard – IA, S3 One Zone-Infrequent Access (S3 One Zone – IA), S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive
  - `StorageObjectCount`: a contagem de objetos armazenados em um determinado bucket

Para obter uma explicação detalhada dos tipos de uso do Amazon S3, consulte Como entender os relatórios de uso e faturamento da AWS para o Amazon S3.

- Recurso: o nome do bucket ou tabela associado ao uso listado.
- StartTime: a hora inicial do dia ao qual o uso se aplica, no Tempo Universal Coordenado (UTC).
- EndTime: a hora de término do dia ao qual o uso se aplica, no Tempo universal coordenado (UTC).
- UsageValue: um dos valores de volume a seguir: A unidade de medida comum para dados é gigabytes (GB). No entanto, dependendo do serviço e do relatório, terabytes (TB) podem aparecer.
  - O número de solicitações durante o período especificado
  - A quantidade de dados transferidos
  - A quantidade de dados armazenados em uma determinada hora
  - A quantidade de dados associados a restaurações do armazenamento de S3 Standard – IA, S3 One Zone – IA, S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive

> **Tip**
>
> Para obter informações detalhadas sobre cada solicitação recebida pelo Amazon S3 para seus objetos, ative os logs de acesso do servidor para seus buckets. Para obter mais informações, consulte Registrar em log as solicitações com registro em log de acesso ao servidor.

Você pode fazer download de um relatório de uso como um arquivo XML ou de valores separados por vírgula (CSV). A seguir há um relatório de uso de exemplo em formato CSV aberto em um aplicativo de planilha.

Service	Operation	UsageType	Resource	StartTime	EndTime	UsageValue
AmazonS3	HeadBucket	USW2-C3DataTransfer-Out-Bytes	admin-created3	6/1/2017 0:00	7/1/2017 0:00	15309
AmazonS3	PutObject	USW2-C3DataTransfer-In-Bytes	admin-created3	6/1/2017 0:00	7/1/2017 0:00	19062
AmazonS3	HeadBucket	USW2-Requests-Tier2	admin-created3	6/1/2017 0:00	7/1/2017 0:00	68
AmazonS3	PutObjectForRepl	USW1-Requests-SIA-Tier1	ca-example-bucket	6/1/2017 0:00	7/1/2017 0:00	178294
AmazonS3	PutObjectForRepl	USW1-USW2-AWS-In-Bytes	ca-example-bucket	6/1/2017 0:00	7/1/2017 0:00	387929083
AmazonS3	GetObjectForRepl	USW2-Requests-NoCharge	admin-created3	6/1/2017 0:00	7/1/2017 0:00	108
AmazonS3	GetObjectForRepl	USW2-USW1-AWS-Out-Bytes	my-test-bucket-bash	6/1/2017 0:00	7/1/2017 0:00	387910021

Para obter mais informações, consulte Como entender os relatórios de uso e faturamento da AWS para o Amazon S3.

Download do relatório de uso da AWS

Você pode fazer download de um relatório de uso como um arquivo XML ou CSV.

Para fazer download do relatório de uso

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Na barra de títulos, selecione seu nome de usuário ou ID da conta, depois escolha Gerenciamento de faturamento e custos.
3. No painel de navegação, escolha Páginas legadas e Relatórios de Custo e Uso.
4. Em Relatório de uso da AWS, selecione Criar um relatório de uso.
5. Na página Baixar relatório de uso, escolha as seguintes configurações:
   - Serviços: escolha Amazon Simple Storage Service.
   - Usage Types (Tipos de uso): para obter uma explicação detalhada sobre os tipos de uso do Amazon S3, consulte Como entender os relatórios de uso e faturamento da AWS para o Amazon S3.
   - Operation (Operação): para obter uma explicação detalhada sobre as operações do Amazon S3, consulte Controle de operações em seus relatórios de uso.
   - Time Period (Período): o período de cobertura do relatório.
   - Report Granularity (Granularidade do relatório): para que o relatório inclua subtotais por hora, dia ou mês.
6. Escolha Fazer download, selecione o formato de download (Relatório XML ou Relatório CSV) e siga as instruções para abrir ou salvar o relatório.

Mais informações

- Como entender os relatórios de uso e faturamento da AWS para o Amazon S3
- Relatórios do AWS Billing para o Amazon S3

Como entender os relatórios de uso e faturamento da AWS para o Amazon S3

Os relatórios de uso e faturamento do Amazon S3 usam códigos e abreviações. Para os tipos de uso na tabela a seguir, substitua *region*, *region1* e *region2* pelas abreviações desta lista:

- APE1: Ásia-Pacífico (Hong Kong)
- APN1: Ásia-Pacífico (Tóquio)
- APN2: Ásia-Pacífico (Seul)
- APN3: Ásia-Pacífico (Osaka)
- APS1: Ásia-Pacífico (Cingapura)
- APS2: Ásia-Pacífico (Sydney)
- APS3: Ásia-Pacífico (Mumbai)
- APS4: Ásia-Pacífico (Jacarta)
- APS5: Ásia-Pacífico (Hyderabad)
- APS6: Ásia-Pacífico (Melbourne)
- APS7: Ásia-Pacífico (Malásia)
- APS9: Ásia-Pacífico (Tailândia)
- CAN1: Canadá (Central)
- CAN2: Oeste do Canadá (Calgary)
- CNN1: China (Pequim)
- CNW1: China (Ningxia)
- AFS1: África (Cidade do Cabo)
- EUC2: Europa (Zurique)
- EUN1: UE (Estocolmo)
- EUS2: Europa (Espanha)
- EUC1: UE (Frankfurt)
- EU: UE (Irlanda)
- EUS1: Europa (Milão)
- EUW2: UE (Londres)
- EUW3: UE (Paris)

- ILC1: Israel (Tel Aviv)
- MEC1: Oriente Médio (EAU)
- MES1: Oriente Médio (Bahrein)
- MXC1: México (Centro)
- SAE1: América do Sul (São Paulo)
- UGW1: AWS GovCloud (Oeste dos EUA)
- UGE1: AWS GovCloud (Leste dos EUA)
- USE1 (ou sem prefixo): Leste dos EUA (Norte da Virgínia)
- USE2: Leste dos EUA (Ohio)
- USW1: Oeste dos EUA (Norte da Califórnia)
- USW2: Oeste dos EUA (Oregon)

Para tipos de uso de pontos de acesso multirregionais do S3 na tabela a seguir, substitua *regiongroup1* e *regiongroup2* por abreviações desta lista:

- AP: Ásia-Pacífico
- AU: Austrália
- EU: Europa
- IN: Índia
- NA: América do Norte
- SA: América do Sul

Os grupos de regiões são agrupamentos geográficos de várias Regiões da AWS. Para ter mais informações, consulte Regiões e zonas de disponibilidade. Para obter mais informações sobre preços por Região da AWS, consulte Preços do Amazon S3.

A primeira coluna da tabela a seguir indica os tipos de uso que aparecem em seus relatórios de uso e faturamento. A unidade de medida comum para dados é gigabytes (GB). No entanto, dependendo do serviço e do relatório, terabytes (TB) podem aparecer.

Tipo de uso	Unidades	Granularity	Descrição
region1-*region2*-AWS-In-A Bytes	GB	Por hora	A quantidade de dados acelerados transferi

Tipo de uso	Unidades	Granularity	Descrição
			dos de *region2* para *region1*.
region1-*region2*-AWS-In-A Bytes-T1	GB	Por hora	A quantidade de dados acelerados T1 transferi dos de *region2* para *region1*, em que T1 refere-se a solicitaç ões do CloudFront para pontos de presença (POPs) nos Estados Unidos, na Europa e no Japão.
region1-*region2*-AWS-In-A Bytes-T2	GB	Por hora	A quantidade de dados acelerados T2 transferi dos de *region2* para *region1*, em que T2 refere-se a solicitações do CloudFront para POPs em todos os outros locais da borda da AWS.
region1-*region2*-AWS-In-Bytes	GB	Por hora	A quantidade de dados transferidos de *region2* para *region1*.
region1-*region2*-AWS-Out-ABytes	GB	Por hora	A quantidade de dados acelerados transferi dos de *region1* para *region2*.

Tipo de uso	Unidades	Granularity	Descrição
region1-*region2*-AWS-Out-ABytes-T1	GB	Por hora	A quantidade de dados acelerados T1 transferidos de *region1* para *region2*, em que T1 refere-se a solicitações do CloudFront para POPs nos Estados Unidos, na Europa e no Japão.
region1-*region2*-AWS-Out-ABytes-T2	GB	Por hora	A quantidade de dados acelerados T2 transferidos de *region1* para *region2*, em que T2 refere-se a solicitações do CloudFront para POPs em todos os outros locais da borda da AWS.
region1-*region2*-AWS-Out-Bytes	GB	Por hora	A quantidade de dados transferidos de *region1* para *region2*.
region-BatchOperations-Jobs	Contagem	Por hora	O número de trabalhos de Operações em lote do S3 executados
region-BatchOperations-Objects	Contagem	Por hora	O número de Operações de objetos executadas pelas operações em lote do S3

Tipo de uso	Unidades	Granularity	Descrição
region-Bulk-Retrieval-Bytes	GB	Por hora	A quantidade de dados recuperados com solicitações em massa do S3 Glacier Flexible Retrieval ou do S3 Glacier Deep Archive
region-BytesDeleted-GDA	GB	Mensal	A quantidade de dados excluídos por uma operação DeleteObject da classe de armazenamento S3 Glacier Deep Archive.
region-BytesDeleted-GIR	GB	Mensal	A quantidade de dados excluídos por uma operação DeleteObject da classe de armazenamento S3 Glacier Instant Retrieval.
region-BytesDeleted-GLACIER	GB	Mensal	A quantidade de dados excluídos por uma operação DeleteObject da classe de armazenamento S3 Glacier Flexible Retrieval.
region-BytesDeleted-INT	GB	Mensal	A quantidade de dados excluídos por uma operação DeleteObject da classe de armazenamento S3 Intelligent-Tiering.

Tipo de uso	Unidades	Granularity	Descrição
region-BytesDeleted-RRS	GB	Mensal	A quantidade de dados excluídos por uma operação DeleteObject da classe de armazenamento Reduced Redundancy Storage (RRS).
region-BytesDeleted-SIA	GB	Mensal	A quantidade de dados excluídos por uma operação DeleteObject da classe de armazenamento S3 Standard-IA.
region-BytesDeleted-STANDARD	GB	Mensal	A quantidade de dados excluídos por uma operação DeleteObject da classe de armazenamento S3 Standard.
region-BytesDeleted-ZIA	GB	Mensal	A quantidade de dados excluídos por uma operação DeleteObject da classe de armazenamento S3 One Zone-IA.
region-C3DataTransfer-In-Bytes	GB	Por hora	A quantidade de dados transferidos para o Amazon S3 do Amazon EC2 na mesma Região da AWS

Tipo de uso	Unidades	Granularity	Descrição
region-C3DataTransfer-Out-Bytes	GB	Por hora	A quantidade de dados transferidos do Amazon S3 para o Amazon EC2 na mesma Região da AWS
region-CloudFront-In-Bytes	GB	Por hora	A quantidade de dados transferidos para uma Região da AWS de uma distribuição do CloudFront
region-CloudFront-Out-Bytes	GB	Por hora	A quantidade de dados transferidos de uma Região da AWS para uma distribuição do CloudFront
region-DataTransfer-In-Bytes	GB	Por hora	A quantidade de dados transferidos para o Amazon S3 pela Internet
region-DataTransfer-Out-Bytes	GB	Por hora	A quantidade de dados transferidos do Amazon S3 para a internet[1]
region-DataTransfer-Regional-Bytes	GB	Por hora	A quantidade de dados transferidos do Amazon S3 para os recursos da AWS dentro da mesma Região da AWS

Tipo de uso	Unidades	Granularity	Descrição
region-EarlyDelete-ByteHrs	GB-Horas	Por hora	Uso pro rata de armazenamento de objetos excluídos do armazenamento S3 Glacier Flexible Retrieval antes do término do compromisso mínimo de 90 dias[2]
region-EarlyDelete-GDA	GB-Horas	Por hora	Uso pro rata de armazenamento de objetos excluídos do armazenamento S3 Glacier Deep Archive antes do término do compromisso mínimo de 180 dias [2]
region-EarlyDelete-GIR	GB-Horas	Por hora	Uso pro rata de armazenamento de objetos excluídos do armazenamento S3 Glacier Instant Retrieval antes do término do compromisso mínimo de 90 dias.

Tipo de uso	Unidades	Granularity	Descrição
region-EarlyDelete-GIR-SmObjects	GB-Horas	Por hora	Uso pro rata de armazenamento de objetos pequenos (menores que 128 KB) que foram excluídos do S3 Glacier Instant Retrieval antes que o compromisso mínimo de 90 dias terminasse.
region-EarlyDelete-SIA	GB-Horas	Por hora	Uso pro-rata de armazenamento de objetos excluídos do S3 Standard – IA antes do término do compromisso mínimo de 30 dias[3]
region-EarlyDelete-SIA-SmObjects	GB-Horas	Por hora	Uso pro rata de armazenamento de objetos pequenos (menores que 128 KB) que foram excluídos do S3 Standard – IA antes que o compromisso mínimo de 30 dias terminasse[3]
region-EarlyDelete-ZIA	GB-Horas	Por hora	Uso pro-rata de armazenamento de objetos excluídos do S3 One Zone-IA antes do término do compromisso mínimo de 30 dias[3]

Tipo de uso	Unidades	Granularity	Descrição
region-EarlyDelete-ZIA-SmObjects	GB-Horas	Por hora	Uso pro rata de armazenamento de objetos pequenos (menores que 128 KB) excluídos do S3 One Zone-IA antes do término do compromisso mínimo de 30 dias[3]
region-Expedited-Retrieval-Bytes	GB	Por hora	A quantidade de dados recuperados com solicitações Expedited do S3 Glacier Flexible Retrieval
Global-Bucket-Hrs-FreeTier	Bucket	Mensal	O número de buckets de uso geral em sua conta dentro do nível gratuito de 2 mil buckets no nível da conta
Global-Bucket-Hrs	Bucket	Mensal	O número de buckets de uso geral em sua conta além do nível gratuito de 2 mil buckets no nível da conta
region-Inventory-Objects Listed	Objetos	Por hora	O número de objetos listados em um grupo de objetos (eles são agrupados por bucket ou prefixo) com uma lista de inventários
region-Metadata-Updates	Atualizações	Por hora	Taxa por atualização para atualizações processadas pelos metadados do S3.

Tipo de uso	Unidades	Granularity	Descrição
region-Monitoring-Automation-INT	Objetos	Por hora	O número de objetos exclusivos monitorados e autonivelados na classe de armazenamento S3 Intelligent-Tiering
region-MRAP-Out-Bytes	GB	Por hora	A quantidade de dados transferidos para fora dos buckets de uma região por meio de um endpoint de pontos de acesso multirregionais do S3 (preços de roteamento de dados MRAP).
region-MRAP-In-Bytes	GB	Por hora	A quantidade de dados transferidos para fora dos buckets de uma região por meio de um endpoint de pontos de acesso multirregionais do S3 (preços de roteamento de dados MRAP).
regiongroup1-regiongroup2- -MRAP-Out-Bytes	GB	Por hora	A quantidade de dados transferidos para fora de um bucket em *regiongroup1* por meio de um endpoint de pontos de acesso de várias regiões do S3 para um cliente em *regiongroup2* localizado fora da rede da AWS.

Tipo de uso	Unidades	Granularity	Descrição
regiongroup1-regiongroup2--MRAP-In-Bytes	GB	Por hora	A quantidade de dados transferidos de um cliente em *regiongroup2* localizado fora da rede da AWS para um bucket em *regiongroup1* por meio de um endpoint de pontos de acesso de várias regiões do S3.
region-OverwriteBytes-Copy-GDA	GB	Mensal	A quantidade de dados substituídos por uma operação CopyObject da classe de armazenamento S3 Glacier Deep Archive.
region-OverwriteBytes-Copy-GIR	GB	Mensal	A quantidade de dados substituídos por uma operação CopyObject da classe de armazenamento S3 Glacier Instant Retrieval.
region-OverwriteBytes-Copy-GLACIER	GB	Mensal	A quantidade de dados substituídos por uma operação CopyObject da classe de armazenamento S3 Glacier Flexible Retrieval.

Tipo de uso	Unidades	Granularity	Descrição
region-OverwriteBytes-Copy-INT	GB	Mensal	A quantidade de dados substituídos por uma operação CopyObject da classe de armazenamento S3 Intelligent-Tiering.
region-OverwriteBytes-Copy-RRS	GB	Mensal	A quantidade de dados sobrescritos por uma operação CopyObject da classe de armazenamento Reduced Redundancy Storage (RRS).
region-OverwriteBytes-Copy-SIA	GB	Mensal	A quantidade de dados substituídos por uma operação CopyObject da classe de armazenamento S3 Standard-IA.
region-OverwriteBytes-Copy-STANDARD	GB	Mensal	A quantidade de dados substituídos por uma operação CopyObject da classe de armazenamento S3 Standard.
region-OverwriteBytes-Copy-ZIA	GB	Mensal	A quantidade de dados substituídos por uma operação CopyObject da classe de armazenamento S3 One Zone-IA.

Tipo de uso	Unidades	Granularity	Descrição
region-OverwriteBytes-Put-GDA	GB	Mensal	A quantidade de dados substituídos por uma operação PutObject da classe de armazenamento S3 Glacier Deep Archive.
region-OverwriteBytes-Put-GIR	GB	Mensal	A quantidade de dados substituídos por uma operação PutObject da classe de armazenamento S3 Glacier Instant Retrieval.
region-OverwriteBytes-Put-GLACIER	GB	Mensal	A quantidade de dados substituídos por uma operação PutObject da classe de armazenamento S3 Glacier Flexible Retrieval.
region-OverwriteBytes-Put-INT	GB	Mensal	A quantidade de dados substituídos por uma operação PutObject da classe de armazenamento S3 Intelligent-Tiering.
region-OverwriteBytes-Put-RRS	GB	Mensal	A quantidade de dados sobrescritos por uma operação PutObject da classe de armazenamento Reduced Redundancy Storage (RRS).

Tipo de uso	Unidades	Granularity	Descrição
region-OverwriteBytes-Put-SIA	GB	Mensal	A quantidade de dados substituídos por uma operação PutObject da classe de armazenamento S3 Standard-IA.
region-OverwriteBytes-Put-STANDARD	GB	Mensal	A quantidade de dados substituídos por uma operação PutObject da classe de armazenamento S3 Standard.
region-OverwriteBytes-Put-ZIA	GB	Mensal	A quantidade de dados substituídos por uma operação PutObject da classe de armazenamento S3 One Zone-IA.
region1-*region2*-S3RTC-In-Bytes	GB	Mensal	A quantidade de dados transferidos para a funcionalidade Controle de Tempo de Replicação do S3 (S3 RTC) de *region2* para *region1* pelas operações PutObjectReplTime , GetObjectReplTime , InitiateMultipartUploadReplTime , UploadPartReplTime , CompleteMultipartUploadReplTime e WriteACLReplTime .

Tipo de uso	Unidades	Granularity	Descrição
region1-*region2*-S3RTC-Out-Bytes	GB	Mensal	A quantidade de dados transferidos para a funcionalidade Controle de Tempo de Replicação do S3 (S3 RTC) de *region1* para *region2* pelas operações PutObjectReplTime , GetObjectReplTime , InitiateMultipartUploadReplTime , UploadPartReplTime , CompleteMultipartUploadReplTime e WriteACLReplTime .
region-Requests-GDA-Tier1	Contagem	Por hora	O número de solicitações PUT, COPY, POST, CreateMultipartUpload , UploadPart ou CompleteMultipartUpload em objetos da classe S3 Glacier Deep Archive.[6]
region-Requests-GDA-Tier2	Contagem	Por hora	O número de solicitações GET e HEAD em objetos da classe S3 Glacier Deep Archive.
region-Requests-GDA-Tier3	Contagem	Por hora	O número de solicitações de restauração padrão do S3 Glacier Deep Archive

Tipo de uso	Unidades	Granularity	Descrição
region-Requests-GDA-Tier5	Contagem	Por hora	O número de solicitações de restauração em massa do S3 Glacier Deep Archive
region-Requests-GIR-Tier1	Contagem	Por hora	O número de solicitações PUT, COPY ou POST em objetos da classe S3 Glacier Instant Retrieval.
region-Requests-GIR-Tier2	Contagem	Por hora	O número de solicitações GET e todas as outras solicitações que não são da classe S3 Glacier Instant Retrieval nível 1 em objetos da classe S3 Glacier Instant Retrieval.
region-Requests-GLACIER-Tier1	Contagem	Por hora	O número de solicitações PUT, COPY, POST, CreateMultipartUpload , UploadPart ou CompleteMultipartUpload em objetos da classe S3 Glacier Flexible Retrieval.[6]
region-Requests-GLACIER-Tier2	Contagem	Por hora	O número de solicitações GET e todas as outras não listadas em objetos da classe S3 Glacier Flexible Retrieval.

Tipo de uso	Unidades	Granularity	Descrição
region-Requests-INT-Tier1	Contagem	Por hora	O número de solicitações PUT, COPY ou POST em objetos da classe S3 Intelligent-Tiering.
region-Requests-INT-Tier2	Contagem	Por hora	O número de solicitações GET e todas as outras solicitações que não são do nível 1 para objetos da classe S3 Intelligent-Tiering.
region-Requests-SIA-Tier1	Contagem	Por hora	O número de solicitações PUT, COPY ou POST em objetos da classe S3 Standard-IA.
region-Requests-SIA-Tier2	Contagem	Por hora	O número de solicitações GET e todas as outras solicitações que não são da classe S3 Glacier Instant Retrieval nível 1 em objetos da classe S3 Standard-IA.
region-Requests-Tier1	Contagem	Por hora	O número de solicitações PUT, COPY ou POST para S3 Standard, RRS e etiquetas, além de solicitações LIST para todos os buckets e objetos.

Tipo de uso	Unidades	Granularity	Descrição
region-Requests-Tier2	Contagem	Por hora	O número de solicitações GET e todas as outras solicitações que não são do nível 1.
region-Requests-Tier3	Contagem	Por hora	O número de solicitações de ciclo de vida para solicitações de restauração do S3 Glacier Flexible Retrieval ou do S3 Glacier Deep Archive e do S3 Glacier Flexible Retrieval padrão
region-Requests-Tier4	Contagem	Por hora	O número de transições do ciclo de vida para o armazenamento S3 Glacier Instant Retrieval S3 Intelligent-Tiering, S3 Standard – IA ou S3 One Zone – IA
region-Requests-Tier5	Contagem	Por hora	O número de solicitações de restauração Bulk do S3 Glacier Flexible Retrieval
region-Requests-Tier6	Contagem	Por hora	O número de solicitações de restauração Expedited do S3 Glacier Flexible Retrieval
region-Requests-Tier8	Contagem	Por hora	O número de solicitações da funcionalidade Concessões de Acesso do S3.

Tipo de uso	Unidades	Granularity	Descrição
region-Requests-XZ-Tier1	Contagem	Por hora	O número de solicitações PUT ou COPY em objetos da classe S3 Express One Zone.
region-Requests-XZ-Tier2	Contagem	Por hora	O número de solicitações GET e todas as outras solicitações que não são da classe S3 Express One Zone nível 1 em objetos da classe S3 Express One Zone.
region-Requests-ZIA-Tier1	Contagem	Por hora	O número de solicitações PUT, COPY ou POST em objetos da classe S3 One Zone-IA.
region-Requests-ZIA-Tier2	Contagem	Por hora	O número de solicitações GET e todas as outras solicitações que não são da classe S3 One Zone-IA nível 1 em objetos da classe S3 One Zone-IA.
region-Retrieval-GIR	GB	Por hora	A quantidade de dados recuperados do armazenamento S3 Glacier Instant Retrieval.
region-Retrieval-SIA	GB	Por hora	A quantidade de dados recuperados do armazenamento S3 Standard – IA

Tipo de uso	Unidades	Granularity	Descrição
region-Retrieval-XZ	GB	Por hora	A parte dos dados que excede 512 KB em determinada solicitação de recuperação (PUT ou COPY) com a classe de armazenamento S3 Express One Zone.
region-Retrieval-ZIA	GB	Por hora	A quantidade de dados recuperados do armazenamento S3 One Zone-IA
region-S3DSSE-In-Bytes	GB	Mensal	A quantidade de dados com criptografia dupla do Amazon S3.
region-S3DSSE-Out-Bytes	GB	Mensal	A quantidade de dados com criptografia dupla descriptografados pelo Amazon S3.
region-S3G-DataTransfer-In-Bytes	GB	Por hora	A quantidade de dados transferidos para o Amazon S3 para restaurar objetos do armazenamento S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive

Tipo de uso	Unidades	Granularity	Descrição
region-S3G-DataTransfer-Out-Bytes	GB	Por hora	A quantidade de dados transferidos do Amazon S3 para fazer a transição de objetos para o armazenamento S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive
region-Select-Returned-Bytes	GB	Por hora	A quantidade de dados retornados com as solicitações Select do armazenamento S3 Standard
region-Select-Returned-GIR-Bytes	GB	Por hora	A quantidade de dados retornados com solicitações Select do armazenamento S3 Glacier Instant Retrieval.
region-Select-Returned-INT-Bytes	GB	Por hora	A quantidade de dados retornados com as solicitações Select do armazenamento S3 Intelligent-Tiering
region-Select-Returned-SIA-Bytes	GB	Por hora	A quantidade de dados retornados com as solicitações Select do armazenamento S3 Standard – IA

Tipo de uso	Unidades	Granularity	Descrição
region-Select-Returned-ZIA-Bytes	GB	Por hora	A quantidade de dados retornados com as solicitações Select do armazenamento S3 One Zone-IA
region-Select-Scanned-Bytes	GB	Por hora	A quantidade de dados verificados com as solicitações Select do armazenamento S3 Standard
region-Select-Scanned-GIR-Bytes	GB	Por hora	A quantidade de dados verificados com solicitações Select do armazenamento S3 Glacier Instant Retrieval.
region-Select-Scanned-INT-Bytes	GB	Por hora	A quantidade de dados verificados com solicitações Select do armazenamento S3 Intelligent-Tiering
region-Select-Scanned-SIA-Bytes	GB	Por hora	A quantidade de dados verificados com as solicitações Select do armazenamento S3 Standard – IA
region-Select-Scanned-ZIA-Bytes	GB	Por hora	A quantidade de dados verificados com as solicitações Select do armazenamento S3 One Zone-IA

Tipo de uso	Unidades	Granularity	Descrição
region-Standard-Retrieval-Bytes	GB	Por hora	A quantidade de dados recuperados com solicitações padrão do S3 Glacier Flexible Retrieval ou do S3 Glacier Deep Archive
region-StorageAnalytics-ObjCount	Objetos	Por hora	O número de objetos exclusivos monitorados em cada configuração de análise de classe de armazenamento.
region-StorageLens-ObjCount	Objetos	Por dia	O número de objetos exclusivos em cada painel do S3 Storage Lens que são monitorados pelas recomendações e métricas avançadas do S3 Storage Lens.
region-StorageLensFreeTier-ObjCount	Objetos	Por dia	O número de objetos exclusivos em cada painel do S3 Storage Lens que são monitorados pelas métricas de uso do S3 Storage Lens.
StorageObjectCount	Contagem	Diariamente	O número de objetos armazenados em um determinado bucket
region-Tables-CompactedObjects	Objetos	Por hora	O número de objetos compactados nos buckets de tabelas do Amazon S3.

Tipo de uso	Unidades	Granularity	Descrição
region-Tables-Monitored0bjects	Objetos	Por hora	O número de objetos nos buckets de tabelas do Amazon S3.
region-Tables-ProcessedBytes	GB	Por hora	A quantidade de dados processados para compactação nos buckets de tabelas do Amazon S3.
region-Tables-Requests-Tier1	Contagem	Por hora	O número de solicitações PUT nos buckets de tabelas do Amazon S3.
region-Tables-Requests-Tier2	Contagem	Por hora	O número de solicitações GET e todas as outras solicitações que não são do nível 1 nos buckets de tabelas do Amazon S3.
region-Tables-TimedStorage-ByteHrs	GB por mês	Por dia	O número de GB-meses que os dados foram armazenados nos buckets de tabelas do Amazon S3.
region-TagStorage-TagHrs	Tag-Hours	Diariamente	O total de tags em todos os objetos no bucket informados por hora
region-TimedStorage-ByteHrs	GB por mês	Por dia	O número de GB-meses em que os dados ficaram no armazenamento S3 Standard

Tipo de uso	Unidades	Granularity	Descrição
region-TimedStorage-GDA-ByteHrs	GB por mês	Por dia	O número de GB-meses em que os dados ficaram no armazenamento S3 Glacier Deep Archive
region-TimedStorage-GDA-Staging	GB por mês	Por dia	O número de GB-meses em que os dados ficaram no armazenamento de preparação do S3 Glacier Deep Archive
region-TimedStorage-GIR-ByteHrs	GB por mês	Por dia	O número de GB-meses em que os dados ficaram no armazenamento de preparação do S3 Glacier Instant Retrieval.
region-TimedStorage-GIR-SmObjects	GB por mês	Por dia	O número de GB-meses em que objetos pequenos (menores que 128 KB) ficaram no armazenam ento S3 Glacier Instant Retrieval.
region-TimedStorage-GlacierByteHrs	GB por mês	Por dia	O número de GB-meses em que os dados ficaram no armazenamento S3 Glacier Flexible Retrieval
region-TimedStorage-GlacierStaging	GB por mês	Por dia	O número de GB-meses em que os dados ficaram no armazenamento de preparação S3 Glacier Flexible Retrieval

Tipo de uso	Unidades	Granularity	Descrição
region-TimedStorage-INT-FA-ByteHrs	GB por mês	Por dia	O número de GB-meses em que os dados ficaram armazenados no nível Frequent Access da classe de armazenamento S3 Intelligent-Tiering[5]
region-TimedStorage-INT-IA-ByteHrs	GB por mês	Por dia	O número de GB-meses em que os dados permaneceram armazenados no nível Infrequent Access do armazenamento S3 Intelligent-Tiering
region-TimedStorage-INT-AA-ByteHrs	GB por mês	Por dia	O número de GB-meses em que os dados permaneceram armazenados no nível Archive Access do armazenamento S3 Intelligent-Tiering
region-TimedStorage-INT-AIA-ByteHrs	GB por mês	Por dia	O número de GB-meses que os dados ficaram armazenados no nível Archive Instant Access do armazenamento S3 Intelligent-Tiering

Tipo de uso	Unidades	Granularity	Descrição
region-TimedStorage-INT-DAA-ByteHrs	GB por mês	Por dia	O número de GB-meses em que os dados permaneceram armazenados no nível Deep Archive Access do armazenamento S3 Intelligent-Tiering
region-TimedStorage-RRS-ByteHrs	GB por mês	Por dia	O número de GB-meses em que os dados ficaram no armazenamento Reduced Redundancy Storage (RRS)
region-TimedStorage-SIA-ByteHrs	GB por mês	Por dia	O número de GB-meses em que os dados ficaram no armazenamento S3 Standard-IA
region-TimedStorage-SIA-SmObjects	GB por mês	Por dia	O número de GB-meses em que pequenos objetos (menores que 128 KB) ficaram no armazenamento S3 Standard-IA[4]
region-TimedStorage-XZ-ByteHrs	GB por mês	Por dia	O número de GB-meses em que os dados ficaram no armazenamento S3 Express One Zone.
region-TimedStorage-ZIA-ByteHrs	GB por mês	Por dia	O número de GB-meses em que os dados ficaram no armazenamento S3 One Zone-IA

Tipo de uso	Unidades	Granularity	Descrição
region-TimedStorage-ZIA-SmObjects	GB por mês	Por dia	O número de GB-meses em que pequenos objetos (menores que 128 KB) ficaram no armazenam ento S3 One Zone-IA.
region-Upload-XZ	GB	Por hora	A quantidade de dados que excede 512 KB em determinada solicitação de upload (PUT ou COPY) com a classe S3 Express One Zone.

Observações

1. Os tipos de uso Global-Bucket-Hrs e Global-Bucket-Hrs-FreeTier se aplicam a buckets de uso geral em AWS GovCloud (US) e Regiões da AWS comerciais.
2. Caso você encerre uma transferência antes da conclusão, o volume de dados transferidos pode exceder o volume de dados recebidos pelo aplicativo. Essa discrepância pode ocorrer porque uma solicitação de encerramento de transferência não pode ser executada instantaneamente, e parte do volume de dados pode estar em trânsito com execução pendente da solicitação de encerramento. Esses dados em trânsito são faturados como dados de “saída” transferidos.
3. Quando objetos arquivados na classe de armazenamento S3 Glacier Instant Retrieval, S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive são excluídos, substituídos ou fizerem transição para outra classe de armazenamento antes do término do compromisso de armazenamento mínimo, que é de 90 dias para as classes S3 Glacier Instant Retrieval e S3 Glacier Flexible Retrieval ou de 180 dias para a classe S3 Glacier Deep Archive, há uma cobrança pro rata por gigabyte para os dias restantes.
4. Para objetos que estão na classe de armazenamento S3 Standard-IA ou S3 One Zone-IA, quando são excluídos, substituídos ou movidos para uma classe de armazenamento diferente antes de 30 dias, existe uma cobrança proporcional por gigabyte pelos dias restantes.
5. Para pequenos objetos (menores que 128 KB) que estão na classe de armazenamento S3 Standard-IA ou S3 One Zone-IA, quando são excluídos, substituídos ou movidos para uma classe

de armazenamento diferente antes de 30 dias, existe uma cobrança proporcional por gigabyte pelos dias restantes.

6. Não há tamanho mínimo de objeto faturável para objetos na classe de armazenamento S3 Intelligent-Tiering. Objetos menores do que 128 KB não são monitorados ou elegíveis para nivelamento automático. Objetos menores são sempre armazenados no nível Acesso frequente do S3 Intelligent-Tiering.
7. Quando você inicia uma solicitação `CreateMultipartUpload`, `UploadPart` ou `UploadPartCopy` para as classes de armazenamento S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive, as solicitações são cobradas de acordo com as taxas de solicitação da classe de armazenamento S3 Standard até que você conclua o upload multiparte. Quando o upload for concluído, a única solicitação `CompleteMultipartUpload` será cobrada de acordo com a taxa de PUT da classe de armazenamento S3 Glacier de destino. As partes de um upload multiparte em andamento para uma PUT na classe de armazenamento S3 Glacier Flexible Retrieval são cobradas como S3 Glacier Flexible Retrieval Staging Storage de acordo com as taxas da classe de armazenamento S3 Standard até que o upload seja concluído. De maneira semelhante, as partes de um upload multiparte em andamento para uma PUT na classe de armazenamento S3 Glacier Deep Archive são cobradas como S3 Glacier Deep Archive Staging Storage de acordo com as taxas da classe de armazenamento S3 Standard até que o upload seja concluído.
8. A classe de armazenamento S3 Express One Zone aplica uma taxa fixa por solicitação para solicitações de até 512 KB. Uma taxa adicional por GB é aplicada para a parte que exceder 512 KB em solicitações PUT e GET.
9. Para obter informações sobre os recursos compatíveis com a classe de armazenamento S3 Express One Zone, consulte Recursos do Amazon S3 não compatíveis com buckets de diretório .
10. Os tipos de uso com unidades cobrados em GB são calculados em bytes nos relatórios de uso.
11. Um GB-mês é obtido considerando o número total de GB-horas, agregando-os ao longo de um mês e, depois, dividindo-os pelo número de horas desse mês. Para saber mais, consulte Perguntas frequentes: Como serei cobrado e faturado pela utilização do Amazon S3?

> **Note**
>
> Em geral, os proprietários de bucket do S3 são cobrados pelas solicitações com respostas HTTP `200 OK` bem-sucedidas e respostas de erro `4XX` do cliente HTTP. Os proprietários de bucket não são cobrados pelas respostas de erro `5XX` do servidor HTTP, como erros HTTP `503 Slow Down`. Consulte mais informações sobre códigos de erro do S3 em HTTP `3XX` e códigos de status `4XX` que não são cobrados em Cobrança pelas respostas de erro do

Amazon S3. Consulte mais informações sobre as cobranças de um bucket de pagamento pelo solicitante em Como funcionam as cobranças de Pagamento pelo solicitante.

Controle de operações em seus relatórios de uso

As operações descrevem a ação realizada em seu objeto ou bucket da AWS pelo tipo de uso especificado. As operações são indicadas por códigos autoexplicativos, como `PutObject` ou `ListBucket`. Para ver quais ações em seu bucket geraram um tipo de uso específico, use estes códigos. Ao criar um relatório de uso, você pode optar por incluir Todas as operações ou uma operação específica, por exemplo, `GetObject`, para relatar.

Mais informações

- Relatórios de uso da AWS para o Amazon S3
- Relatórios do AWS Billing para o Amazon S3
- Preços do Amazon S3
- Perguntas frequentes sobre o Amazon S3

Cobrança pelas respostas de erro do Amazon S3

Em geral, os proprietários de bucket do S3 são cobrados pelas solicitações com respostas HTTP `200 OK` bem-sucedidas e respostas de erro `4XX` do cliente HTTP. Os proprietários de bucket não são cobrados pelas respostas de erro `5XX` do servidor HTTP, como erros HTTP `503 Slow Down`. Consulte mais informações sobre as cobranças de um bucket de pagamento pelo solicitante em Como funcionam as cobranças de Pagamento pelo solicitante.

A tabela a seguir lista códigos de erro específicos em HTTP `3XX` e códigos de status `4XX` que não são cobrados. Para buckets configurados com hospedagem de sites, a solicitação aplicável e outras cobranças ainda serão aplicadas quando o S3 retornar um documento de erro personalizado ou para redirecionamentos personalizados.

> **Note**
>
> Para `AccessDenied` (HTTP `403 Forbidden`), o S3 não cobra do proprietário do bucket quando a solicitação é iniciada fora da conta da AWS individual dele ou da organização da AWS à qual ele pertence.

Código de status HTTP	Código de erro	Descrição do código de erro	
301 Moved Permanently (301 movido permanentemente)	PermanentRedirect	O bucket que você está tentando acessar deve ser endereçado usando o endpoint especificado. Envie todas as solicitações futuras para esse endpoint.	
	PermanentRedirectControlError	A operação de API que você está tentando acessar deve ser endereçada usando o endpoint especificado. Envie todas as solicitações futuras para esse endpoint.	
307 Redirecionamento temporário	TemporaryRedirect	Será feito um redirecionamento ao bucket enquanto o servidor Sistema de Nomes de Domínio (DNS) está sendo atualizado.	
400 solicitação inválida	AuthorizationHeaderMalformed	O cabeçalho de autorização que você forneceu não é válido.	
	AuthorizationQueryParametersError	Os parâmetros da consulta de autorização que você forneceu não são válidos.	

Código de status HTTP	Código de erro	Descrição do código de erro	
	ConnectionClosedByRequester	Exibido para o chamador original quando um erro é encontrado ao ler o corpo de WriteGetObjectResponse.	
	DeviceNotActiveError	O dispositivo não está ativo no momento.	
	EndpointNotFound	Direcione as solicitações ao endpoint correto.	
	ExpiredToken	O token fornecido expirou.	
	IllegalLocationConstraintException	Você está tentando acessar um bucket de uma região diferente daquela em que o bucket existe. Para evitar esse erro, use a opção `--region`. Por exemplo: `aws s3 cp awsexample.txt s3://amzn-s3-demo-bucket/ --region ap-east-1` .	

Código de status HTTP	Código de erro	Descrição do código de erro	
	InvalidArgument	Esse erro poderá ocorrer pelos seguintes motivos: • O argumento especificado não é válido. • A solicitação não tinha o cabeçalho exigido. • O argumento especificado estava incompleto ou no formato errado. • O argumento especificado deve ter um comprimento maior ou igual a três.	
	InvalidBucketOwnerAWSAccountID	O valor do parâmetro esperado do proprietário do bucket deve ser um ID de Conta da AWS.	
	InvalidDigest	O valor de Content-MD5 ou da soma de verificação que você especificou não é válido.	
	InvalidEncryptionAlgorithmError	A solicitação de criptografia que você especificou não é válida. O valor válido é AES256.	

Código de status HTTP	Código de erro	Descrição do código de erro	
	InvalidHostHeader	Os cabeçalhos do host fornecidos na solicitação usaram o endereçamento de estilo incorreto.	
	InvalidHttpMethod	A solicitação é feita usando um método HTTP inesperado.	

Código de status HTTP	Código de erro	Descrição do código de erro	
	InvalidRequest	Esse erro poderá ocorrer pelos seguintes motivos: • A solicitação está usando a versão incorreta da assinatura. Use o `AWS4-HMAC-SHA256` (Signature versão 4). • Um ponto de acesso só pode ser criado para um bucket existente. • O ponto de acesso não está em um estado em que possa ser excluído. • Um ponto de acesso só pode ser listado para um bucket existente. • O próximo token não é válido. • Pelo menos uma ação deve ser especificada em uma regra de ciclo de vida. • Pelo menos uma regra de ciclo de vida deve ser especificada.	

Código de status HTTP	Código de erro	Descrição do código de erro	
		• O número de regras de ciclo de vida não deve exceder o limite permitido de 1.000 regras. • O intervalo do parâmetro `MaxResults` não é válido. • As solicitações SOAP devem ser feitas por meio de uma conexão HTTPS. • A Aceleração de Transferências do Amazon S3 não é compatível com buckets com nomes que não estejam em conformidade com o DNS. • A Aceleração de Transferências do Amazon S3 não é compatível com buckets com ponto (.) no nome. • O endpoint da Aceleração de	

Código de status HTTP	Código de erro	Descrição do código de erro	
		Transferências do Amazon S3 só permite solicitações no estilo virtual. • A Aceleração de Transferências do Amazon S3 não está configurada neste bucket. • A Aceleração de Transferências do Amazon S3 está desabilitada neste bucket. • A Aceleração de Transferências do Amazon S3 não é compatível com este bucket. Para obter ajuda, entre em contato com Suporte. • A Aceleração de Transferências do Amazon S3 não pode ser habilitada neste bucket. Para obter ajuda, entre em contato com Suporte. •	

Código de status HTTP	Código de erro	Descrição do código de erro	
		Valores conflitantes fornecidos em cabeçalhos HTTP e parâmetros de consulta. • Valores conflitantes fornecidos nos cabeçalhos HTTP e nos campos do formulário POST. • Solicitação CopyObject feita em objetos maiores que 5 GB.	
	InvalidSessionException	Retornado se a sessão não existir mais porque ultrapassou o limite de tempo ou expirou.	
	InvalidSignature	A assinatura da solicitação que o servidor calculou não corresponde à assinatura que você forneceu. Verifique a chave de acesso secreta da AWS e o método de assinatura. Para ter mais informações, consulte Assinar e autenticar as solicitações REST.	

Código de status HTTP	Código de erro	Descrição do código de erro	
	InvalidSOAPRequest	O corpo da solicitação SOAP não é válido.	
	InvalidStorageClass	A classe de armazenamento que você especificou não é válida.	
	InvalidTag	Sua solicitação contém uma entrada de tag que não é válida. Por exemplo, sua solicitação pode conter chaves duplicadas, chaves ou valores muito longos ou tags do sistema.	
	InvalidToken	O token fornecido foi malformado ou é inválido por algum outro motivo.	
	InvalidURI	Não foi possível analisar o URI especificado.	
	KeyTooLongError	A chave é muito longa.	
	KMS.DisabledException	A solicitação foi recusada porque a chave do KMS especificada não está habilitada.	

Código de status HTTP	Código de erro	Descrição do código de erro	
	KMS.InvalidKeyUsageException	A solicitação foi recusada por um dos seguintes motivos: • O valor KeyUsage da chave do KMS é incompatível com a operação de API. • O algoritmo de criptografia ou de assinatura especificado para a operação é incompatível com o tipo de material na chave do KMS (KeySpec). Para criptografia, descriptografia, nova criptografia e geração de chaves de dados, o KeyUsage deve ser ENCRYPT_DECRYPT. Para assinar e verificar mensagens, o KeyUsage deve ser SIGN_VERIFY. Para gerar e verificar códigos de autenticação de mensagens (MACs), o KeyUsage deve ser GENERATE_VERIFY_MAC. Para gerar segredos do	

Código de status HTTP	Código de erro	Descrição do código de erro	
		contrato de chave, o KeyUsage deve ser KEY_AGREEMENT. Para encontrar o KeyUsage de uma chave do KMS, use a operação DescribeKey. Para encontrar os algoritmos de criptografia ou de assinatura compatíveis com uma chave do KMS específica, use a operação DescribeKey.	

Código de status HTTP	Código de erro	Descrição do código de erro	
	KMS.KMSInvalidStateException	A solicitação foi recusada porque o estado do recurso especificado não é válido para essa solicitação. Essa exceção tem um dos seguintes significados: • O estado da chave do KMS não é compatível com a operação. Para encontrar o estado da chave, use a operação DescribeKey. Para ter mais informações sobre quais estados de chave são compatíveis com cada operação do KMS, consulte Key states of AWS KMS keys no Guia do desenvolvedor do AWS Key Management Service. • Em relação a operações criptográficas em chaves do KMS em armazenamentos de chaves personalizado, essa exceção represent	

Código de status HTTP	Código de erro	Descrição do código de erro	
		a uma falha geral com muitas causas possíveis. Para identificar a causa, leia a mensagem de erro que acompanha a exceção.	
	KMS.NotFoundException	A solicitação foi recusada porque não foi possível encontrar a entidade ou o recurso especificado.	
	LambdaInvalidResponse	Exibido para o chamador original quando WriteGetObjectResponse responde com ValidationError ao AWS Lambda. Leia a mensagem ValidationError para ter mais detalhes. Nem todos os casos de ValidationError geram um erro LambdaInvalidResponse.	

Código de status HTTP	Código de erro	Descrição do código de erro	
	LambdaInvocationFailed	A invocação da função do Lambda falhou. Os chamadores podem receber o erro a seguir quando o S3 Object Lambda não consegue invocar com êxito a função do Lambda configurada. A mensagem de erro pode conter detalhes sobre um eventual erro exibido pelo serviço AWS Lambda ao invocar a função (por exemplo, código de status, código de erro, mensagem de erro e ID da solicitação).	
	MalformedACLError	O ACL fornecido não foi bem formado ou não foi validado com relação a nosso esquema publicado.	
	MalformedPOSTRequest	O corpo da solicitação POST não tem dados de formulários/de várias partes bem formados.	

Código de status HTTP	Código de erro	Descrição do código de erro	
	MalformedXML	O XML fornecido não foi bem formado ou não foi validado com relação a nosso esquema publicado.	
	MaxPostPreDataLengthExceededError	Os campos de solicitação POST anteriores ao arquivo de upload eram muito grandes.	
	MetadataTooLarge	Os cabeçalhos de metadados excedem o tamanho máximo permitido de metadados.	
	MissingAttachment	Um anexo SOAP era esperado, mas nenhum foi encontrado.	
	MissingRequestBodyError	Você enviou um documento XML vazio como uma solicitação.	
	MissingSecurityHeader	Falta um cabeçalho obrigatório na solicitação.	
	NoLoggingStatusForKey	Não existe um sub-recurso de status de registro em log para uma chave.	
	NotDeviceOwnerError	O dispositivo que gerou o token não pertence ao usuário autenticado.	

Código de status HTTP	Código de erro	Descrição do código de erro	
	ResponseInterrupted	Exibido para o chamador original quando um erro é encontrado ao ler o corpo de WriteGetObjectResponse.	
	RequestHeaderSectionTooLarge	O cabeçalho da solicitação e os parâmetros de consulta usados para fazer a solicitação excedem os tamanhos máximos permitidos	
	TokenCodeInvalidError	O número de série e/ou o código de token que você forneceu não são válidos.	
	UnexpectedContent	Essa solicitação contém um conteúdo incompatível.	
	UnsupportedArgument	A solicitação continha um argumento incompatível.	
	UnsupportedSignature	A solicitação fornecida é assinada com uma versão não compatível do Security Token Service (STS) ou a versão da assinatura não é aceita.	

Código de status HTTP	Código de erro	Descrição do código de erro	
	UserKeyMustBeSpecified	A solicitação POST do bucket deve conter o nome do campo especificado. Se ele estiver especificado, confira a ordem dos campos.	
	IncorrectEndpoint	O bucket especificado existe em outra região. Direcione as solicitações ao endpoint correto.	
	ValidationError	Os erros de validação podem ser exibidos pela operação de API WriteGetObjectResponse e podem ocorrer por vários motivos. Leia a mensagem de erro para ter mais detalhes.	
403 proibido	RequestTimeTooSkewed	A diferença entre a hora da solicitação e a hora do servidor é muito grande.	

Código de status HTTP	Código de erro	Descrição do código de erro	
	SignatureDoesNotMatch	A assinatura da solicitação que o servidor calculou não corresponde à assinatura que você forneceu. Verifique a chave de acesso secreta da AWS e o método de assinatura. Consulte mais informações em Assinar e autenticar as solicitações REST e em Autenticar solicitações SOAP.	
	NotSignedUp	Sua conta não está cadastrada no serviço do Amazon S3. É necessário se cadastrar para poder usar o Amazon S3. Você pode se cadastrar no seguinte URL: https://aws.amazon.com/s3	
	InvalidSecurity	As credenciais de segurança fornecidas não são válidas.	
	InvalidPayer	Todo acesso a esse objeto foi desabilitado. Se precisar de assistência adicional, acesse Fale conosco.	

Código de status HTTP	Código de erro	Descrição do código de erro	
	InvalidAccessKeyId	O ID de chave de acesso da AWS fornecido não existe em nossos registros.	
	AccountProblem	Há um problema em sua Conta da AWS que impede a conclusão bem-sucedida da operação. Se precisar de assistênc ia adicional, acesse Fale conosco.	
	UnauthorizedAccessError	Aplicável somente nas regiões da China. Retornado quando uma solicitação é feita para um bucket que não tem uma licença ICP. Consulte mais informaçõ es em ICP Recordal.	
	UnexpectedIPError	Aplicável somente nas regiões da China. Essa solicitação foi recusada porque o IP era inesperad o.	
	MissingAuthenticat ionToken	A solicitação não foi assinada.	

Código de status HTTP	Código de erro	Descrição do código de erro	
	LambdaPermissionError	O chamador não está autorizado a invocar a função do Lambda. O chamador deve ter permissão para invocar a função do Lambda. Confira as políticas anexadas ao chamador e se elas têm permissão para usar `lambda:Invoke` para a função configurada. A mensagem de erro pode conter detalhes sobre um eventual erro exibido pelo serviço Lambda ao invocar a função (por exemplo, código de status, código de erro, mensagem de erro e ID da solicitação).	

Código de status HTTP	Código de erro	Descrição do código de erro	
404 Not Found (404 Não encontrado)	LambdaNotFound	A função do AWS Lambda não foi encontrada. A função do Lambda configurada (ou a versão ou o alias) não foi encontrada quando invocada. A configuração do ponto de acesso do S3 Object Lambda deve apontar para o ARN correto da função do Lambda. A mensagem de erro pode conter detalhes sobre um eventual erro exibido pelo serviço AWS Lambda ao invocar a função (por exemplo, código de status, código de erro, mensagem de erro e ID da solicitação).	
	NoSuchAsyncRequest	A solicitação especificada não foi encontrada.	
	NoSuchObjectLockConfiguration	O objeto especificado não tem uma configuração ObjectLock.	

Código de status HTTP	Código de erro	Descrição do código de erro	
	NoSuchUpload	O carregamento fracionado especificado não existe. O ID do carregamento pode não ser válido ou o carregamento fracionado pode ter sido anulado ou concluído.	
	NoSuchWebsiteConfiguration	O bucket especificado não tem uma configuração de site.	
	NoTransformationDefined	Nenhuma transformação encontrada para esse ponto de acesso do Object Lambda.	
	ObjectLockConfigurationNotFoundError	A configuração do Bloqueio de Objetos não existe para esse bucket.	
405 Método não permitido	MethodNotAllowed	O método especificado não é permitido neste recurso.	

Código de status HTTP	Código de erro	Descrição do código de erro	
409 Conflito	BucketAlreadyExists	O nome do bucket solicitado não está disponível. O namespace do bucket é compartilhado por todos os usuários do sistema. Especifique um nome diferente e tente novamente.	
	InvalidBucketState	A solicitação não é válida para o estado atual do bucket.	
	OperationAborted	Uma operação condicional conflitante está em andamento neste recurso. Tente novamente.	
411 Comprimento obrigatório	MissingContentLength	Você deve fornecer o cabeçalho HTTP de tamanho do conteúdo.	
412 Falha na pré-condição	RequestIsNotMultiPartContent	Uma solicitação POST de bucket deve ser do tipo dados de formulário/de várias partes.	

Código de status HTTP	Código de erro	Descrição do código de erro	
416 Intervalo solicitado não satisfatório	InvalidRange	O intervalo solicitado não é válido para a solicitação. Experimente outro intervalo.	

Compreender e gerenciar classes de armazenamento do Amazon S3

Cada objeto no Amazon S3 tem uma classe de armazenamento associada a ele. Por padrão, objetos no S3 são armazenados na classe de armazenamento S3 Standard. No entanto, o Amazon S3 oferece uma variedade de outras classes de armazenamento para os objetos que você armazena. Escolha uma classe de acordo com seu cenário de caso de uso e dos requisitos de acesso de performance. A escolha de uma classe de armazenamento desenvolvida para seu caso de uso permite otimizar os custos de armazenamento, o desempenho e a disponibilidade dos objetos. Todas essas classes de armazenamento oferecem alta durabilidade.

As seções a seguir fornecem detalhes das várias classes de armazenamento e como definir a classe de armazenamento para seus objetos.

Tópicos

- Classes de armazenamento de objetos acessados com frequência
- Classe de armazenamento para otimizar automaticamente dados com padrões de acesso alterados ou desconhecidos
- Classes de armazenamento de objetos acessados com pouca frequência
- Classes de armazenamento para objetos acessados raramente
- Classe de armazenamento para o Amazon S3 no Outposts
- Comparar as classes de armazenamento do Amazon S3
- Configurar a classe de armazenamento de um objeto
- Análise do Amazon S3 – Análise de classe de armazenamento

- Gerenciar custos de armazenamento com o Amazon S3 Intelligent-Tiering
- Noções básicas sobre as classes de armazenamento S3 Glacier para armazenamento de dados de longo prazo
- Trabalhando com objetos arquivados

Classes de armazenamento de objetos acessados com frequência

Para casos de uso nos quais a performance é importante (aqueles que exigem tempo de acesso de milissegundos) e dados acessados com frequência, o Amazon S3 fornece as seguintes classes de armazenamento:

- S3 Standard (`STANDARD`): a classe de armazenamento padrão. Se você não especificar a classe de armazenamento ao fazer upload de um objeto, o Amazon S3 atribuirá a classe S3 Standard. Para ajudar a otimizar os custos entre o S3 Standard e S3 Standard-IA, você pode usar Análise do Amazon S3 – Análise de classe de armazenamento.
- S3 Express One Zone (`EXPRESS_ONEZONE`): a classe Amazon S3 Express One Zone é uma classe de armazenamento de zona única e alta performance do Amazon S3 desenvolvida com o propósito específico de fornecer acesso consistente aos dados e com latência inferior a dez milissegundos para as aplicações mais sensíveis à latência. A classe S3 Express One Zone é a classe de armazenamento de objetos em nuvem de menor latência disponível atualmente, com velocidades de acesso aos dados até dez vezes mais rápidas e custos de solicitação 50% mais baixos do que a classe S3 Standard. Com a classe S3 Express One Zone, os dados são armazenados de forma redundante em vários dispositivos dentro de uma única zona de disponibilidade. Para obter mais informações, consulte S3 Express One Zone.
- Reduced Redundancy Storage (`REDUCED_REDUNDANCY`): a classe Reduced Redundancy Storage (RRS) foi criada para dados reproduzíveis não críticos que podem ser armazenados em níveis de redundância menores do que a classe de armazenamento S3 Standard.

  > **Important**
  >
  > Não recomendamos o uso dessa classe de armazenamento. A classe de armazenamento S3 Standard apresenta melhor custo-benefício.

  Para durabilidade, os objetos RRS têm uma perda anual média prevista de 0,01%. Se um objeto de RRS for perdido, quando forem feitas solicitações a ele, o Amazon S3 retornará um erro 405.

Classe de armazenamento para otimizar automaticamente dados com padrões de acesso alterados ou desconhecidos

A classe S3 Intelligent-Tiering (`INTELLIGENT_TIERING`) é uma classe de armazenamento do Amazon S3 projetada para otimizar os custos de armazenamento ao mover automaticamente os dados para o nível de acesso mais econômico, sem impacto na performance ou nas despesas operacionais. O S3 Intelligent-Tiering é a única classe de armazenamento na nuvem que oferece economia de custo automática ao mover dados em um nível detalhado de objeto entre níveis de acesso quando há alteração nos padrões de acesso. O S3 Intelligent-Tiering é a classe de armazenamento ideal quando você quer otimizar os custos de armazenamento dos dados com padrões de acesso desconhecidos ou variáveis. Não há taxas de recuperação para o S3 Intelligent-Tiering.

Por uma pequena taxa mensal de automação e monitoramento de objetos, o S3 Intelligent-Tiering monitora os padrões de acesso e move automaticamente os objetos que não foram acessados para níveis de acesso de custo mais baixo. A classe S3 Intelligent-Tiering oferece economia automática de custos de armazenamento em três níveis de acesso de baixa latência e alto throughput. Para dados que podem ser acessados de forma assíncrona, você pode optar por ativar os recursos de arquivamento automático na classe de armazenamento do S3 Intelligent-Tiering. O S3 Intelligent-Tiering foi projetado para oferecer 99,9 % de disponibilidade e 99,999999999 % de durabilidade.

O S3 Intelligent-Tiering armazena objetos automaticamente em três níveis de acesso:

- Acesso frequente: os objetos que foram carregados ou transferidos para o S3 Intelligent-Tiering são automaticamente armazenados no nível Acesso frequente.
- Acesso infrequente: o S3 Intelligent-Tiering move os objetos que não foram acessados durante 30 dias consecutivos para o nível Acesso infrequente.
- Acesso instantâneo ao arquivamento: com o S3 Intelligent-Tiering, todos os objetos que não foram acessados durante 90 dias consecutivos são movidos automaticamente para o nível Acesso instantâneo ao arquivamento.

Além desses três níveis, o S3 Intelligent-Tiering oferece dois níveis opcionais de acesso ao arquivamento:

- Acesso ao arquivamento: o S3 Intelligent-Tiering oferece a opção de ativar o nível Acesso ao arquivamento para dados que podem ser acessados de maneira assíncrona. Após a ativação, o

nível Archive Access arquiva os objetos que não foram acessados durante um mínimo de 90 dias consecutivos.

- Acesso profundo ao arquivamento: o S3 Intelligent-Tiering oferece a opção de ativar o nível Acesso profundo ao arquivamento para dados que podem ser acessados de maneira assíncrona. Após a ativação, o nível Deep Archive Access arquiva os objetos que não foram acessados durante um mínimo de 180 dias consecutivos.

> **Note**
>
> - Ative apenas o nível Archive Access por 90 dias se você quiser ignorar o nível Archive Instant Access. O nível Acesso ao arquivamento oferece um custo de armazenamento um pouco menor com tempos de recuperação de minutos a horas. O nível Acesso instantâneo ao arquivamento oferece acesso de milissegundos e alta performance de throughput.
> - Ative os níveis Acesso de arquivamento e Acesso de arquivamento profundo somente se seus objetos puderem ser acessados de forma assíncrona pela aplicação. Se o objeto que você está recuperando estiver armazenado nos níveis Acesso ao arquivamento ou Acesso profundo ao arquivamento, restaure o objeto usando `RestoreObject`.

Você pode migrar os dados recém-criados para o S3 Intelligent-Tiering, definindo-o como a classe de armazenamento padrão. Você também pode optar por ativar um ou ambos os níveis de acesso ao arquivamento usando a operação de API `PutBucketIntelligentTieringConfiguration`, a AWS CLI ou o console do Amazon S3. Para obter informações sobre como usar o S3 Intelligent-Tiering e ativar os níveis de acesso ao arquivamento, consulte Como usar o S3 Intelligent-Tiering.

Para acessar objetos no nível Archive Access ou Deep Archive Access, primeiro você precisa restaurá-los. Para obter mais informações, consulte Restaurar objetos dos níveis Archive Access e Deep Archive Access do S3 Intelligent-Tiering.

> **Note**
>
> Se o tamanho de um objeto for menor que 128 KB, ele não será monitorado nem qualificado para o nivelamento automático. Objetos menores são sempre armazenados no nível Acesso frequente. Para obter mais informações sobre o S3 Intelligent-Tiering, consulte Níveis de acesso do S3 Intelligent-Tiering.

Classes de armazenamento de objetos acessados com pouca frequência

As classes de armazenamento S3 Standard – IA e S3 One Zone – IA foram desenvolvidas para dados duradouros e acessados com pouca frequência. (IA é a sigla em inglês para acesso pouco frequente.) Os objetos S3 Standard – IA e S3 One Zone – IA estão disponíveis para acesso de milissegundos (o mesmo que a classe de armazenamento S3 Standard). O Amazon S3 cobra uma taxa de recuperação para esses objetos, portanto, eles são mais adequados para dados acessados com pouca frequência. Para obter informações sobre a definição de preços, consulte Definição de preços do Amazon S3.

Por exemplo, é possível escolher as classes de armazenamento S3 Standard – IA e S3 One Zone – IA para fazer o seguinte:

- Para armazenar backups.
- Para dados mais antigos acessados com pouca frequência, mas que ainda exigem acesso de milissegundos. Por exemplo, ao fazer upload de dados, é possível escolher a classe de armazenamento S3 Standard e usar a configuração de ciclo de vida para solicitar que o Amazon S3 transfira os objetos para a classe S3 Standard – IA ou S3 One Zone – IA.

  Para obter mais informações sobre gerenciamento de ciclo de vida, consulte Gerenciar o ciclo de vida dos objetos.

> **Note**
>
> As classes de armazenamento S3 Standard – IA e S3 One Zone – IA são adequadas para objetos maiores que 128 KB que você planeja armazenar por pelo menos 30 dias. Se um objeto for menor que 128 KB, o Amazon S3 cobrará por 128 KB. Se excluir um objeto antes do fim do período mínimo de duração do armazenamento de 30 dias, você será cobrado por 30 dias. Os objetos que forem excluídos, sobrescritos ou transferidos para uma classe de armazenamento diferente antes de 30 dias incorrerão na cobrança normal de uso do armazenamento mais uma cobrança proporcional pelo restante do mínimo de 30 dias. Para obter informações sobre a definição de preços, consulte Definição de preços do Amazon S3.

As diferenças entre essas classes de armazenamento são:

- S3 Standard-IA (`STANDARD_IA`): o Amazon S3 armazena dados de objetos de maneira redundante em várias zonas de disponibilidade separadas geograficamente (de maneira

semelhante à classe de armazenamento S3 Standard). Os objetos S3 Standard – IA são resistentes à perda de uma zona de disponibilidade. Essa classe de armazenamento oferece maior disponibilidade e resiliência que a classe S3 One Zone – IA. Para ajudar a otimizar os custos entre o S3 Standard e S3 Standard-IA, você pode usar Análise do Amazon S3 – Análise de classe de armazenamento.

- S3 One Zone-IA (`ONEZONE_IA`): o Amazon S3 armazena dados de objetos em apenas uma zona de disponibilidade, e isso a torna menos cara que a classe S3 Standard-IA. No entanto, os dados não são resilientes à perda física da zona de disponibilidade resultante de desastres, como terremotos e inundações. A classe de armazenamento S3 One Zone-IA é tão durável quanto a classe S3 Standard-IA, mas é menos disponível e resistente. Para uma comparação de durabilidade e disponibilidade das classes de armazenamento, consulte Comparar as classes de armazenamento do Amazon S3 no fim desta seção. Para obter informações sobre a definição de preços, consulte Definição de preços do Amazon S3. Para casos de uso de isolamento e residência de dados, você pode criar buckets de diretório em zonas locais da AWS e usar as classes de armazenamento S3 Express One Zone (`EXPRESS_ONEZONE`) e S3 One Zone-IA (`ONEZONE_IA`). Para ter mais informações sobre os buckets de diretório em zonas locais, consulte Workloads de residência de dados.

Recomendamos o seguinte:

- S3 Standard-IA (`STANDARD_IA`): use para a cópia principal ou única dos dados, que não pode ser recriada.
- S3 One Zone-IA (`ONEZONE_IA`): use se você puder recriar os dados em caso de falha da zona de disponibilidade, e para réplicas de objetos ao configurar a Replicação do S3 Entre Regiões Diferentes (CRR). Além disso, para isolamento e residência de dados, você pode criar buckets de diretório em zonas locais da AWS e usar a classe de armazenamento S3 One Zone-IA.

Classes de armazenamento para objetos acessados raramente

As classes de armazenamento S3 Glacier Instant Retrieval (`GLACIER_IR`), S3 Glacier Flexible Retrieval (`GLACIER`) e S3 Glacier Deep Archive (`DEEP_ARCHIVE`) são projetadas para arquivamento e armazenamento de dados de longo prazo a baixo custo. Essas classes de armazenamento exigem taxas de recuperação e durações mínimas de armazenamento, tornando-as mais eficazes para dados raramente acessados. Para obter mais informações sobre as classes de armazenamento do S3 Glacier, consulte Noções básicas sobre as classes de armazenamento S3 Glacier para armazenamento de dados de longo prazo.

O Amazon S3 fornece as seguintes classes de armazenamento do S3 Glacier:

- S3 Glacier Instant Retrieval (`GLACIER_IR`): use para dados de longo prazo que raramente são acessados e exigem recuperação na casa dos milissegundos. Os dados nessa classe de armazenamento ficam disponíveis para acesso em tempo real.
- S3 Glacier Flexible Retrieval (`GLACIER`): use para arquivamentos nos quais partes dos dados podem precisar ser recuperadas em questão de minutos. Os dados nessa classe de armazenamento ficam arquivados e indisponíveis para acesso em tempo real.
- S3 Glacier Deep Archive (`DEEP_ARCHIVE`): use para arquivar dados que raramente precisam ser acessados. Os dados nessa classe de armazenamento ficam arquivados e indisponíveis para acesso em tempo real.

Recuperar objetos arquivados

É possível definir a classe de armazenamento de um objeto como S3 Glacier Flexible Retrieval (`GLACIER`) ou S3 Glacier Deep Archive (`DEEP_ARCHIVE`) da mesma maneira que você faz para outras classes de armazenamento, conforme descrito na seção Configurar a classe de armazenamento de um objeto. No entanto, os objetos nas classes S3 Glacier Flexible Retrieval e S3 Glacier Deep Archive ficam arquivados e indisponíveis para acesso em tempo real. Para obter mais informações, consulte Noções básicas do armazenamento de arquivamento nas classes S3 Glacier Flexible Retrieval e S3 Glacier Deep Archive.

> **Note**
>
> Quando você usa as classes de armazenamento do S3 Glacier, os objetos permanecem no Amazon S3. Não será possível acessá-los diretamente por meio do serviço separado do Amazon S3 Glacier. Consulte informações sobre o serviço Amazon S3 Glacier no Guia do desenvolvedor do Amazon S3 Glacier.

Classe de armazenamento para o Amazon S3 no Outposts

Com o Amazon S3 on Outposts, é possível criar buckets do S3 em seus recursos do AWS Outposts, além de armazenar e recuperar objetos no ambiente on-premises para aplicações que exigem acesso a dados locais, processamento de dados local e residência de dados. É possível usar as mesmas operações de API e recursos no AWS Outposts da mesma maneira que no Amazon S3,

incluindo políticas de acesso, criptografia e marcação. Você pode usar o S3 on Outposts por meio do AWS Management Console, da AWS CLI, de AWS SDKs ou da API REST.

O S3 no Outposts fornece uma nova classe de armazenamento, o S3 Outposts (`OUTPOSTS`). A classe de armazenamento do S3 Outposts só está disponível para objetos armazenados em buckets no Outposts. Se você tentar usar essa classe de armazenamento com um bucket do S3 em uma Região da AWS, será gerado o erro `InvalidStorageClass`. Além disso, se você tentar usar outras classes de armazenamento do S3 com objetos armazenados em buckets do S3 on Outposts, ocorrerá o mesmo erro.

Os objetos armazenados na classe de armazenamento do S3 Outposts (`OUTPOSTS`) são sempre criptografados usando criptografia do lado do servidor com chaves de criptografia gerenciadas do Amazon S3 (SSE-S3). Para obter mais informações, consulte Usar a criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3).

Você também pode optar explicitamente por criptografar objetos armazenados na classe de armazenamento do S3 Outposts usando criptografia do lado do servidor com chaves de criptografia fornecidas pelo cliente (SSE-C). Para obter mais informações, consulte Como usar criptografia do lado do servidor com chaves fornecidas pelo cliente (SSE-C).

> **Note**
>
> O S3 on Outposts não é compatível com a criptografia no lado do servidor usando chaves do AWS Key Management Service (AWS KMS) (SSE-KMS).

Consulte mais informações sobre o S3 no Outposts em What is S3 on Outposts no Guia do usuário do Amazon S3 no Outposts.

Comparar as classes de armazenamento do Amazon S3

A tabela a seguir compara as classes de armazenamento, incluindo sua disponibilidade, durabilidade, duração mínima de armazenamento e outras considerações.

Storage Class	Designed for	Durability (designed for)	Availability (designed for)	Availability Zones	Min storage duration	Min billable object size	Other Considerations
STANDARD	Frequently accessed data	99.999999999%	99.99%	>= 3	None	None	None
STANDARD_IA	Long-lived, infrequently accessed data	99.999999999%	99.9%	>= 3	30 days	128 KB	Per GB retrieval fees apply.
INTELLIGENT_TIERING	Long-lived data with changing or unknown access patterns	99.999999999%	99.9%	>= 3	30 days	None	Monitoring and automation fees per object apply. No retrieval fees.
ONEZONE_IA	Long-lived, infrequently accessed, non-critical data	99.999999999%	99.5%	1	30 days	128 KB	Per GB retrieval fees apply. Not resilient to the loss of the Availability Zone.
GLACIER	Long-term data archiving with retrieval times ranging from minutes to hours	99.999999999%	99.99% (after you restore objects)	>= 3	90 days	None	Per GB retrieval fees apply. You must first restore archived objects before you can access them. For more information, see Restoring Archived Objects.
DEEP_ARCHIVE	Archiving rarely accessed data with a default retrieval time of 12 hours	99.999999999%	99.99% (after you restore objects)	>= 3	180 days	None	Per GB retrieval fees apply. You must first restore archived objects before you can access them. For more information, see Restoring Archived Objects.
RRS (Not recommended)	Frequently accessed, non-critical data	99.99%	99.99%	>= 3	None	None	None

* O S3 Glacier Flexible Retrieval requer 40 KB de metadados adicionais para cada objeto arquivado. Isso inclui 32 KB de metadados cobrados na taxa do S3 Glacier Flexible Retrieval (necessários para identificar e recuperar dados) e mais 8 KB de dados cobrados na taxa do S3 Standard. A taxa do S3 Standard é necessária para manter o nome e os metadados definidos pelo usuário para objetos arquivados no S3 Glacier Flexible Retrieval. Para obter mais informações sobre as classes de armazenamento, consulte Classes de armazenamento do Amazon S3.

** A classe S3 Glacier Deep Archive requer 40 KB de metadados adicionais para cada objeto arquivado. Isso inclui 32 KB de metadados cobrados de acordo com a taxa do S3 Glacier Deep Archive (necessários para identificar e recuperar dados) e mais 8 KB de dados cobrados na taxa do S3 Standard. A taxa do S3 Standard é necessária para manter o nome e os metadados definidos pelo usuário para objetos arquivados no Amazon S3 Glacier Deep Archive. Para obter mais informações sobre as classes de armazenamento, consulte Classes de armazenamento do Amazon S3.

Lembre-se de que todas as classes de armazenamento, exceto as classes S3 One Zone-IA (`ONEZONE_IA`) e S3 Express One Zone (`EXPRESS_ONEZONE`), foram desenvolvidas para serem resistentes à perda física de uma zona de disponibilidade resultante de desastres. Considere também os custos, além dos requisitos de performance do cenário da sua aplicação. Para obter informações sobre os preços das classes de armazenamento, consulte Definição de preços do Amazon S3.

Configurar a classe de armazenamento de um objeto

Você pode especificar uma classe de armazenamento para um objeto ao fazer upload dele. Se você não especificar, o Amazon S3 usará a classe de armazenamento padrão Amazon S3 Standard para objetos em buckets de uso geral. Também é possível alterar a classe de armazenamento de um objeto que já está armazenado em um bucket de uso geral do Amazon S3 para qualquer outra classe de armazenamento usando o console do Amazon S3, os AWS SDKs ou a AWS Command Line Interface (AWS CLI). Todas essas abordagens usam as operações de API do Amazon S3 para enviar solicitações ao Amazon S3.

> **Note**
>
> Não é possível alterar a classe de armazenamento de objetos armazenados em buckets de diretório.

É possível direcionar o Amazon S3 para alterar a classe de armazenamento de objetos automaticamente adicionando a configuração do Ciclo de Vida do S3 a um bucket. Para obter mais informações, consulte Gerenciar o ciclo de vida dos objetos.

Ao definir uma configuração de Replicação do S3, é possível definir a classe de armazenamento para objetos replicados como qualquer outra classe de armazenamento. No entanto, não é possível replicar objetos que estão armazenados nas classes de armazenamento S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive. Para obter mais informações, consulte Elementos do arquivo de configuração de replicação.

Ao definir a classe de armazenamento programaticamente, você fornece o valor da classe de armazenamento. Veja a seguir uma lista de nomes de console para classes de armazenamento com seus valores de API correspondentes:

- Reduced Redundancy Storage: `REDUCED_REDUNDANCY`
- S3 Express One Zone: `EXPRESS_ONEZONE`
- S3 Glacier Deep Archive: `DEEP_ARCHIVE`
- S3 Glacier Flexible Retrieval: `GLACIER`
- S3 Glacier Instant Retrieval: `GLACIER_IR`
- S3 Intelligent-Tiering: `INTELLIGENT_TIERING`
- S3 One Zone-IA: `ONEZONE_IA`

- S3 Standard: `STANDARD`
- S3 Standard-IA: `STANDARD_IA`

Configurar a classe de armazenamento em um novo objeto

Para definir a classe de armazenamento ao fazer upload de um objeto, você pode usar os métodos a seguir.

Uso do console do S3

Para definir a classe de armazenamento ao fazer o upload de um novo objeto no console:

1. Faça login no AWS Management Console e abra o console do Amazon S3 em: https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets de uso geral.
3. Na lista de buckets, escolha o nome do bucket no qual você deseja fazer upload de pastas ou arquivos.
4. Escolha Upload (Fazer upload).
5. Na janela Fazer upload, escolha Propriedades.
6. Na seção Classe de armazenamento, escolha uma classe de armazenamento para os arquivos que você está carregando.
7. (Opcional) Configure as propriedades adicionais para os arquivos que você está carregando. Consulte mais informações em Fazer upload de objetos.
8. Na janela Upload (Fazer upload), siga um destes procedimentos:
   - Arraste arquivos e pastas para a janela Fazer upload.
   - Escolha Adicionar arquivo ou Adicionar pasta, escolha arquivos ou pastas para fazer upload e depois escolha Abrir.
9. Na parte inferior da página, escolha Fazer upload.

Uso da API REST

É possível especificar a classe de armazenamento em um objeto ao criá-lo usando as operações de API `PutObject`, `POST Object` e `CreateMultipartUpload` e adicionar o cabeçalho da solicitação `x-amz-storage-class`. Se esse cabeçalho não for adicionado, o Amazon S3 usará a classe de armazenamento padrão, S3 Standard (`STANDARD`).

Esse exemplo de solicitação usa o comando PutObject para definir a classe de armazenamento em um novo objeto para S3 Intelligent-Tiering:

```
PUT /my-image.jpg HTTP/1.1
Host: amzn-s3-demo-bucket1.s3.Region.amazonaws.com
Date: Wed, 12 Oct 2009 17:50:00 GMT
Authorization: authorization string
Content-Type: image/jpeg
Content-Length: 11434
Expect: 100-continue
x-amz-storage-class: INTELLIGENT_TIERING
```

Como usar o AWS CLI

Esse exemplo usa o comando `put-object` para fazer upload de *my_images.tar.bz2* para *amzn-s3-demo-bucket1* na classe de armazenamento *GLACIER* :

```
aws s3api put-object --bucket amzn-s3-demo-bucket1 --key dir-1/my_images.tar.bz2 --
storage-class GLACIER --body my_images.tar.bz2
```

Se o objeto tiver mais de 5 GB, use o seguinte comando para definir a classe de armazenamento:

```
aws s3 cp large_test_file s3://amzn-s3-demo-bucket1 --storage-class GLACIER
```

Alterar a classe de armazenamento de um objeto existente

Para definir a classe de armazenamento ao fazer upload de um objeto, você pode usar os métodos a seguir.

Uso do console do S3

É possível alterar a classe de armazenamento de um objeto usando o console do Amazon S3 quando o objeto tem menos de 5 GB. Se for maior, recomendamos adicionar a configuração do ciclo de vida do S3 para alterar a classe de armazenamento do objeto.

Para alterar a classe de armazenamento de um objeto no console:

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets de uso geral.
3. Na lista de buckets, escolha o nome do bucket que contém os objetos que você deseja alterar.
4. Marque a caixa de seleção à esquerda dos nomes dos objetos que você quer alterar.
5. No menu Ações, escolha Editar classe de armazenamento na lista de opções exibida.
6. Escolha entre as classes de armazenamento disponíveis para o objeto.
7. Em Configurações adicionais de cópia, escolha se você quer Copiar configurações de origem, Não especificar configurações ou Especificar configurações. Copiar configurações de origem é a opção padrão. Se você quiser copiar o objeto somente sem os atributos das configurações de origem, escolha Não especificar configurações. Escolha Especificar configurações para especificar configurações referentes a classes de armazenamento, ACLs, tags de objeto, metadados, criptografia do lado do servidor e somas de verificação adicionais.
8. Escolha Salvar alterações no canto inferior direito. O Amazon S3 salva suas alterações.

Uso da API REST

Para alterar a classe de armazenamento de um objeto existente, use os métodos a seguir.

Esse exemplo de solicitação usa o comando `PutObject` para definir a classe de armazenamento em um objeto existente como S3 Intelligent-Tiering:

```
PUT /my-image.jpg HTTP/1.1
Host: amzn-s3-demo-bucket1.s3.Region.amazonaws.com
Date: Wed, 12 Oct 2009 17:50:00 GMT
Authorization: authorization string
Content-Type: image/jpeg
Content-Length: 11434
Expect: 100-continue
x-amz-storage-class: INTELLIGENT_TIERING
```

Como usar o AWS CLI

Esse exemplo usa o comando `cp` para alterar a classe de armazenamento de um objeto existente da classe atual para a classe de armazenamento *DEEP_ARCHIVE* :

```
aws s3 cp object_S3_URI object_S3_URI --storage-class DEEP_ARCHIVE
```

Restrição de permissões de política de acesso a uma classe de armazenamento específica

Ao conceder permissões de política de acesso para operações do Amazon S3, é possível usar a chave de condição `s3:x-amz-storage-class` para restringir qual classe de armazenamento a ser usada ao armazenar objetos obtidos por upload. Por exemplo, ao conceder a permissão `s3:PutObject`, você pode restringir uploads de objetos a uma classe de armazenamento específica. Para visualizar um exemplo de política, consulte Exemplo: restringir uploads aos objetos com uma classe de armazenamento específica.

Para obter mais informações sobre como usar condições em políticas e uma lista completa de chaves de condição do Amazon S3, consulte os seguintes tópicos:

- Actions, resources, and condition keys for Amazon S3 na Referência de autorização do serviço

  Para ter mais informações sobre as permissões referentes a operações de API do S3 de acordo com os tipos de recurso do S3, consulte Permissões obrigatórias para operações de API do Amazon S3.
- Exemplos de políticas de bucket usando chaves de condição

Análise do Amazon S3 – Análise de classe de armazenamento

Usando a análise de classe de armazenamento do Amazon S3, você pode analisar padrões de acesso de armazenamento para ajudar a decidir quando fazer a transição dos dados certos para a classe de armazenamento certa. Esse novo recurso de análise do Amazon S3 observa padrões de acesso de dados para ajudar a determinar quando fazer a transição do armazenamento STANDARD acessado menos frequentemente para a classe de armazenamento STANDARD_IA (IA, para acesso raro). Para obter mais informações sobre classes de armazenamento, consulte Compreender e gerenciar classes de armazenamento do Amazon S3.

Depois que a análise de classe de armazenamento observa os padrões incomuns de acesso a um conjunto filtrado de dados em um período, você pode usar os resultados da análise para ajudar a melhorar suas configurações de ciclo de vida. Você pode configurar a análise de classe de armazenamento para analisar todos os objetos em um bucket. Se desejar, você pode configurar

filtros para agrupar para objetos para análise por prefixo comum (ou seja, objetos que têm nomes que começam com uma string comum), por tags de objeto ou por prefixo e por tags. Você provavelmente achará que filtrar por grupos de objeto é a melhor maneira de aproveitar a análise de classe de armazenamento.

> **Important**
>
> A análise de classe de armazenamento fornece apenas recomendações para as classes IA padrão a padrão.

Você pode ter vários filtros vários de análise de classe de armazenamento por bucket, até 1.000, e receberá uma análise separada para cada filtro. As várias configurações de filtro permitem analisar grupos específicos de objetos para melhorar suas configurações de ciclo de vida que fazem a transição de objetos para STANDARD_IA.

A análise de classe de armazenamento fornece visualizações de uso de armazenamento no console do Amazon S3 que são atualizadas diariamente. Também é possível exportar esses dados de uso diário para um bucket do S3 e visualizá-los em uma aplicação de planilha ou com ferramentas de business intelligence, como o QuickSight.

Há custos associados à análise da classe de armazenamento. Para ter informações sobre preços, consulte Gerenciamento e insights em Definição de preço do Amazon S3.

Tópicos

- Como configurar a análise de classe de armazenamento?
- Como usar a análise de classe de armazenamento?
- Como exportar dados de análise de classe de armazenamento?
- Configurar análise de classe de armazenamento

Como configurar a análise de classe de armazenamento?

Para configurar a análise de classe de armazenamento, configure os dados de objeto que você deseja analisar. Você pode configurar a análise de classe de armazenamento para fazer o seguinte:

- Analisar o conteúdo completo de um bucket.

  Você receberá uma análise para todos os objetos no bucket.

- Analisar objetos agrupados por prefixo e por tags.

  Você pode configurar filtros que agrupam objetos para análise por prefixo, por tags de objeto ou por uma combinação de prefixo e tags. Você recebe uma análise separada para cada filtro configurado. Você pode ter várias configurações de filtro por bucket, até 1.000.
- Exportar dados de análise.

  Quando você configura a análise de classe de armazenamento para um bucket ou filtro, pode optar por exportar os dados de análise para um arquivo todo dia. A análise do dia é adicionada ao arquivo para formar um registro histórico de análise para o filtro configurado. O arquivo é atualizado diariamente no destino escolhido por você. Ao selecionar dados para exportar, especifique um bucket de destino e um prefixo de destino opcional onde o arquivo é gravado.

Você pode usar o console do Amazon S3, a API REST, a AWS CLI ou os AWS SDKs para configurar a análise de classe de armazenamento.

- Para obter informações sobre como configurar a análise de classe de armazenamento no console do Amazon S3, consulte Configurar análise de classe de armazenamento.
- Para usar a API do Amazon S3, use a API REST PutBucketAnalyticsConfiguration, ou equivalente, na AWS CLI ou nos AWS SDKs.

Como usar a análise de classe de armazenamento?

Você usa a análise de classe de armazenamento para observar os padrões de acesso de dados ao longo do tempo e coletar informações para ajudar a melhorar o gerenciamento de ciclo de vida do armazenamento STANDARD_IA. Depois de configurar um filtro, você começará a ver a análise de dados baseada no filtro no console do Amazon S3 entre 24 e 48 horas. Contudo, a análise de classe de armazenamento observa os padrões de acesso de um conjunto de dados filtrado por 30 dias ou mais para coletar informações para análise antes de oferecer um resultado. A análise continua sendo executada após o resultado inicial e atualiza o resultado à medida que os padrões de acesso mudam

A primeira vez que você configura um filtro, o console do Simple Storage Service (Amazon S3) pode levar algum tempo para analisar os dados.

A análise de classe de armazenamento observa os padrões de acesso de um conjunto de dados de objeto filtrado por 30 dias ou mais para coletar informações suficientes para a análise. Após a análise de classe de armazenamento coletar informações suficientes, você verá uma mensagem no console do Amazon S3 informando que a análise está incompleta.

Quando a análise de classe de armazenamento é executada em busca de objetos acessados raramente, o conjunto filtrado de objetos agrupados com base na data de upload no Amazon S3 é observado. A análise de classe de armazenamento determina se a faixa etária é acessada raramente observando os seguintes fatores do conjunto de dados filtrado:

- Objetos na classe de armazenamento STANDARD que têm mais de 128 KB.
- Quanto armazenamento total médio você tem por faixa etária.
- Número médio de bytes transferidos para fora (não frequência) por faixa etária.
- Os dados de exportação de análise incluem somente solicitações com dados pertinentes para a análise de classe de armazenamento. Isso pode causar diferenças no número de solicitações e nos bytes totais de upload e solicitação em comparação com o que é mostrado nas métricas de armazenamento ou rastreado por seus próprios sistemas internos.
- As solicitações GET e PUT com falha não são contadas para análise. Contudo, você verá as solicitações com falha nas métricas de armazenamento.

Quanto armazenamento eu recuperei?

O console do Amazon S3 mostra em um gráfico quanto de armazenamento no conjunto de dados filtrado foi recuperado durante o período de observação.

Que porcentagem do armazenamento eu recuperei?

O console do Amazon S3 também mostra em um gráfico que porcentagem do armazenamento no conjunto de dados filtrado foi recuperado durante o período de observação.

Como mencionado anteriormente neste tópico, quando a análise de classe de armazenamento é executada em busca de objetos acessados raramente, o conjunto filtrado de objetos agrupados com base na data de upload no Amazon S3 é observado. A análise de classe de armazenamento usa as seguintes faixas etárias de objeto predefinidas:

- Objetos do Amazon S3 com menos de 15 dias
- Objetos do Amazon S3 de 15 a 29 dias
- Objetos do Amazon S3 de 30 a 44 dias
- Objetos do Amazon S3 de 45 a 59 dias
- Objetos do Amazon S3 de 60 74 dias
- Objetos do Amazon S3 de 75 a 89 dias
- Objetos do Amazon S3 de 90 a 119 dias

- Objetos do Amazon S3 de 120 a 149 dias
- Objetos do Amazon S3 de 150 a 179 dias
- Objetos do Amazon S3 de 180 a 364 dias
- Objetos do Amazon S3 de 365 a 729 dias
- Objetos do Amazon S3 com 730 dias ou mais

Geralmente, leva cerca de 30 dias para observar os padrões de acesso e coletar informações suficientes para gerar um resultado de análise. Pode levar mais de 30 dias, dependendo do padrão de acesso exclusivo dos dados. No entanto, depois de configurar um filtro, você começará a ver a análise de dados baseada no filtro no console do Amazon S3 entre 24 e 48 horas. Você pode visualizar a análise de acesso do objeto diariamente dividida por faixa etária no console do Amazon S3.

Quanto do armazenamento é acessado raramente?

O console do Amazon S3 mostra os padrões de acesso agrupados pelos grupos etários de objetos predefinidos. O texto Frequently accessed (Acessado com frequência) ou Infrequently accessed (Acessado com pouca frequência) mostrado é uma ajuda visual para ajudá-lo no processo de criação do ciclo de vida.

Como exportar dados de análise de classe de armazenamento?

Você pode optar por exportar os relatórios de análise de classe de armazenamento para um arquivo sem formatação de valores separados por vírgula (CSV). Os relatórios são atualizados diariamente e se baseiam nos filtros de faixa etária de objeto que você configura. Ao usar o console do Amazon S3, você pode escolher a opção de exportação de relatório quando cria um filtro. Ao selecionar dados para exportar, especifique um bucket de destino e um prefixo de destino opcional onde o arquivo é gravado. Você pode exportar os dados para um bucket de destino em uma conta diferente. O bucket de destino deve estar na mesma região que o bucket que você configura para ser analisado.

Você deve criar uma política de bucket no bucket de destino para conceder permissões ao Amazon S3 para verificar se a Conta da AWS é proprietária do bucket e para gravar objetos no bucket no local definido. Para ver um exemplo de política, consulte Conceder permissões para o Inventário do S3 e análises do S3.

Após configurar relatórios de análise de classe de armazenamento, você começará a receber o relatório exportado diariamente após 24 horas. Depois disso, o Amazon S3 continuará monitorando e fornecendo exportações diárias.

Você pode abrir o arquivo CSV em uma aplicação de planilha ou importar o arquivo para outras aplicações, como o Amazon QuickSight. Para obter informações sobre como usar os arquivos do Amazon S3 com o Amazon QuickSight, consulte Criar um conjunto de dados usando arquivos do Amazon S3 no Guia do usuário do Amazon QuickSight.

Os dados no arquivo exportado são classificados por data na faixa etária de objeto conforme exibido nos exemplos a seguir. Se a classe de armazenamento é STANDARD, a linha também contém dados para as colunas `ObjectAgeForSIATransition` e `RecommendedObjectAgeForSIATransition`.

Date	ConfigId	Filter	StorageClass	ObjectAge	ObjectCount	DataUploaded_MB	Storage_MB	DataRetrieved_MB	GetRequestCount	CumulativeAccessRatio	ObjectAgeForSIATransition	RecommendedObjectAgeForSIATransition
8/17/2021	SalesMaterial	SalesMaterial	STANDARD	000-014			0.4313			0		
9/2/2021	SalesMaterial	SalesMaterial	STANDARD	000-014						0.04096734		
8/22/2021	SalesMaterial	SalesMaterial	STANDARD	000-014			0.4313			0		
8/25/2021	SalesMaterial	SalesMaterial	STANDARD	000-014			0.4313			0		
9/6/2021	SalesMaterial	SalesMaterial	STANDARD	000-014						0.04096734		
8/30/2021	SalesMaterial	SalesMaterial	STANDARD	000-014						0.04096734		
8/28/2021	SalesMaterial	SalesMaterial	STANDARD	000-014						0.04096734		
8/21/2021	SalesMaterial	SalesMaterial	STANDARD	000-014			0.4313			0		
9/5/2021	SalesMaterial	SalesMaterial	STANDARD	000-014						0.04096734		

No final do relatório, a faixa etária de objeto é fornecida como ALL. As linhas ALL contêm totais cumulativos, incluindo objetos menores que 128 KB, para todas as faixas etárias desse dia.

8/24/2021	SalesMaterial	SalesMaterial	STANDARD	ALL	3		0.4599			0	000-014
9/3/2021	SalesMaterial	SalesMaterial	STANDARD	ALL	3		0.4599			0.02426125	015-029
8/28/2021	SalesMaterial	SalesMaterial	STANDARD	ALL	3		0.4599			0.03545875	015-029
8/17/2021	SalesMaterial	SalesMaterial	STANDARD	ALL	3		0.4599			0	000-014
8/25/2021	SalesMaterial	SalesMaterial	STANDARD	ALL	3		0.4599			0	000-014
9/6/2021	SalesMaterial	SalesMaterial	STANDARD	ALL	3		0.4599			0.0209529	015-029
9/4/2021	SalesMaterial	SalesMaterial	STANDARD	ALL	3		0.4599			0.02304819	015-029
8/22/2021	SalesMaterial	SalesMaterial	STANDARD	ALL	3		0.4599			0	000-014
8/21/2021	SalesMaterial	SalesMaterial	STANDARD	ALL	3		0.4599			0	000-014
8/30/2021	SalesMaterial	SalesMaterial	STANDARD	ALL	3		0.4599			0.03073092	015-029
8/20/2021	SalesMaterial	SalesMaterial	STANDARD	ALL	3		0.4599			0	000-014

A próxima seção descreve as colunas usadas no relatório.

Layout de arquivos exportados

A tabela a seguir descreve o layout de arquivo de exportação de análise da classe de armazenamento do Amazon S3.

Configurar análise de classe de armazenamento

Usando a ferramenta de análise de classe de armazenamento do Amazon S3, é possível analisar padrões de acesso de armazenamento para ajudar a decidir quando fazer a transição dos dados certos para a classe de armazenamento certa. A análise de classe de armazenamento observa padrões de acesso de dados para ajudar você a determinar quando fazer a transição do armazenamento STANDARD, acessado menos frequentemente, para a classe de armazenamento STANDARD_IA (IA, para acesso raro). Para obter mais informações sobre STANDARD_IA, consulte as perguntas frequentes do Amazon S3 e Compreender e gerenciar classes de armazenamento do Amazon S3.

Para configurar a análise de classe de armazenamento, configure os dados de objeto que você deseja analisar. Você pode configurar a análise de classe de armazenamento para fazer o seguinte:

- Analisar o conteúdo completo de um bucket.

  Você receberá uma análise para todos os objetos no bucket.

- Analisar objetos agrupados por prefixo e por tags.

  Você pode configurar filtros que agrupam objetos para análise por prefixo, por tags de objeto ou por uma combinação de prefixo e tags. Você recebe uma análise separada para cada filtro configurado. Você pode ter várias configurações de filtro por bucket, até 1.000.

- Exportar dados de análise.

  Quando você configura a análise de classe de armazenamento para um bucket ou filtro, pode optar por exportar os dados de análise para um arquivo todo dia. A análise do dia é adicionada ao arquivo para formar um registro histórico de análise para o filtro configurado. O arquivo é atualizado diariamente no destino escolhido por você. Ao selecionar dados para exportar, especifique um bucket de destino e um prefixo de destino opcional onde o arquivo é gravado.

Você pode usar o console do Amazon S3, a API REST, a AWS CLI ou os AWS SDKs para configurar a análise de classe de armazenamento.

> **Important**
>
> A análise da classe de armazenamento não fornece recomendações de transições para as classes de armazenamento ONEZONE_IA ou S3 Glacier Flexible Retrieval.
> Se você quiser configurar a análise de classe de armazenamento para exportar suas descobertas como um arquivo.csv e o bucket de destino usar criptografia de bucket padrão com uma AWS KMS key, atualize a política de chaves do AWS KMS para conceder permissão ao Amazon S3 para criptografar o arquivo.csv. Para instruções, consulte Conceder permissão para que o Amazon S3 use a sua chave gerenciada pelo cliente para criptografia.

Para obter mais informações sobre análises, consulte Análise do Amazon S3 – Análise de classe de armazenamento.

Uso do console do S3

Para configurar a análise de classe de armazenamento

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets de uso geral ou Buckets de diretórios.
3. Na lista de buckets, escolha o nome do bucket para o qual você deseja configurar a análise de classe de armazenamento.
4. Escolha a guia Metrics.
5. Em Storage Class Analysis (Análise de classe de armazenamento), escolha Create analytics configuration (Criar configuração de análise).
6. Digite um nome para o filtro. Se você quiser analisar o bucket todo, deixe o campo Prefix (Prefixo) vazio.
7. No campo Prefix (Prefixo) digite o texto para o prefixo para os objetos que você deseja analisar.
8. Para adicionar uma tag, escolha Add tag. Insira uma chave e um valor para a tag. Você pode inserir um prefixo e várias tags.
9. Opcionalmente, você pode escolher Enable (Habilitar) em Export CSV (Exportar CSV) para exportar relatórios de análise para um arquivo simples com valores separados por vírgula (.csv). Escolha um bucket de destino onde o arquivo pode ser armazenado. Você pode digitar um prefixo para o bucket de destino. O bucket de destino deve estar na mesma Região da AWS que o bucket para o qual você está configurando a análise. O bucket de destino pode estar em uma Conta da AWS diferente.

   Se o bucket de destino do arquivo .csv usar criptografia de bucket padrão com uma chave de KMS, você deverá atualizar a política de chaves do AWS KMS para conceder permissão do Amazon S3 para criptografar o arquivo .csv. Para instruções, consulte Conceder permissão para que o Amazon S3 use a sua chave gerenciada pelo cliente para criptografia.
10. Selecione Create Configuration (Criar configuração).

O Amazon S3 cria uma política de bucket no bucket de destino que concede ao Amazon S3 permissão para gravação. Isso permitirá gravar os dados de exportação no bucket.

Se ocorrer um erro quando você tentar criar a política de bucket, serão fornecidas instruções sobre como resolvê-lo. Por exemplo, se você escolher um bucket de destino em outra Conta da AWS e não tiver permissões para ler e gravar na política de bucket, verá a mensagem a seguir. Você deve pedir

ao proprietário do bucket de destino para adicionar a política de bucket exibida ao bucket de destino. Se a política não for adicionada ao bucket de destino, você não terá os dados de exportação porque o Amazon S3 não terá permissão para gravar no bucket de destino. Se o bucket de origem for de uma conta diferente da conta do usuário atual, o ID de conta correto do bucket de origem deverá ser substituído na política.

Para obter informações sobre os dados exportados e como o filtro funciona, consulte Análise do Amazon S3 – Análise de classe de armazenamento.

Uso dos REST API

Para configurar a Análise de classe de armazenamento usando a API REST, use PutBucketAnalyticsConfiguration. Você também pode usar a operação equivalente com a AWS CLI ou os AWS SDKs.

Você pode usar as seguintes APIs REST para trabalhar com a Análise de classe de armazenamento:

- Configuração de DELETE Bucket Analytics
- Configuração de GET Bucket Analytics
- Listar configuração de análise de bucket

Gerenciar custos de armazenamento com o Amazon S3 Intelligent-Tiering

A classe de armazenamento S3 Intelligent-Tiering foi projetada para otimizar os custos de armazenamento movendo automaticamente os dados para o nível de acesso ao armazenamento de melhor custo-benefício quando os padrões de acesso mudam, sem sobrecarga operacional nem impacto na performance. Por uma cobrança pequena mensal de automação e monitoramento de objetos, o S3 Intelligent-Tiering monitora os padrões de acesso e move automaticamente os objetos que não foram acessados para níveis de acesso de baixo custo.

O S3 Intelligent-Tiering oferece economia automática de custos de armazenamento em três níveis de acesso de baixa latência e alta taxa de transferência. Para dados que podem ser acessados de forma assíncrona, você pode optar por ativar os recursos de arquivamento automático na classe de armazenamento do S3 Intelligent-Tiering. Não há cobranças de recuperação no S3 Intelligent-Tiering. Se um objeto no nível Infrequent Access ou Archive Instant Access for acessado posteriormente, ele será automaticamente movido de volta para o nível Frequent Access. Nenhuma cobrança adicional de nível se aplica quando objetos são movidos entre os níveis de acesso na classe de armazenamento do S3 Intelligent-Tiering.

O S3 Intelligent-Tiering é a classe de armazenamento recomendada para dados com padrões de acesso desconhecidos, alterados ou imprevisíveis, independentemente do tamanho do objeto ou do período de retenção, como data lakes, análise de dados e novas aplicações.

A classe de armazenamento S3 Intelligent-Tiering oferece suporte a todos os recursos do Amazon S3, inclusive:

- S3 Inventory, para verificar a camada de acesso de objetos
- S3 Replication, para replicação de dados em qualquer Região da AWS.
- S3 Storage Lens, para exibição de métricas de uso de armazenamento e atividade
- Criptografia do lado do servidor, para proteção de dados de objetos.
- Bloqueio de objeto do S3, para evitar exclusão acidental de dados.
- AWS PrivateLink, para acessar o Amazon S3 por um endpoint privado em uma nuvem privada virtual (VPC).

Para obter informações sobre como usar o S3 Intelligent-Tiering, consulte as seguintes seções:

Tópicos

- Como o S3 Intelligent-Tiering funciona
- Como usar o S3 Intelligent-Tiering
- Como gerenciar o S3 Intelligent-Tiering

Como o S3 Intelligent-Tiering funciona

A classe de armazenamento Amazon S3 Intelligent-Tiering armazena objetos automaticamente em três níveis de acesso. Um nível é otimizado para acesso frequente, um nível de menor custo é otimizado para acesso pouco frequente e outro nível de baixo custo é otimizado para dados raramente acessados. Por uma cobrança mensal baixa de automação e monitoramento de objetos, o S3 Intelligent-Tiering monitora os padrões de acesso e move automaticamente para o nível Infrequent Access os objetos que não foram acessados por 30 dias consecutivos. Após 90 dias sem acesso, os objetos são movidos para a camada Archive Instant Access sem causar impacto na performance ou sobrecarga operacional.

Para obter o menor custo de armazenamento para dados que levem de minutos a horas para serem acessados, ative recursos de arquivamento a fim de adicionar mais dois níveis de acesso. Você pode rebaixar os objetos para o nível Acesso ao arquivamento, para o nível Acesso profundo ao

arquivamento ou para ambos. Com o Archive Access, o S3 Intelligent-Tiering move os objetos que não foram acessados por no mínimo 90 dias consecutivos para o nível Archive Access. Com o Deep Archive Access, o S3 Intelligent-Tiering move os objetos para o nível Deep Archive Access depois de no mínimo 180 dias consecutivos sem acesso. Para os dois níveis, é possível configurar o número de dias sem acesso com base nas suas necessidades.

As ações a seguir constituem um acesso que impede rebaixar os objetos para o nível Archive Access ou Deep Archive Access:

- Baixar ou copiar um objeto por meio do console do Amazon S3.
- Invocar CopyObject, UploadPartCopy ou replicar objetos com a replicação em lote do S3. Nesses casos, os objetos de origem das operações de cópia ou replicação são hierarquizados.
- Invocar GetObject, PutObject, RestoreObject, CompleteMultipartUpload, ListParts ou SelectObjectContent

Por exemplo, se os objetos forem acessados por meio de `SelectObjectContent` antes do número especificado de dias sem acesso (por exemplo, 180 dias), essa ação redefinirá o timer. Os objetos não serão movidos para o nível Archive Access ou Deep Archive Access até que o tempo depois da última solicitação `SelectObjectContent` atinge o número de dias especificado.

Se um objeto no nível Infrequent Access ou Archive Instant Access for acessado posteriormente, ele será automaticamente movido de volta para o nível Frequent Access.

As ações a seguir constituem um acesso que automaticamente move os objetos do nível Infrequent Access ou Archive Instant de volta para o nível Frequent Access:

- Baixar ou copiar um objeto por meio do console do Amazon S3.
- Invocar CopyObject, UploadPartCopy ou replicar objetos com a replicação em lote. Nesses casos, os objetos de origem das operações de cópia ou replicação são hierarquizados.
- Invocar GetObject, PutObject, RestoreObject, CompleteMultipartUpload ou ListParts.

Outras ações não constituem um acesso que automaticamente mova os objetos do nível Infrequent Access ou Archive Instant Access de volta para o nível Frequent Access. Veja a seguir uma amostra, não uma lista definitiva, destas ações:

- Invocar HeadObject, GetObjectTagging, PutObjectTagging, ListObjects, ListObjectsV2 ou ListObjectVersio

- Invocar SelectObjectContent não constitui acesso que hierarquiza objetos até um nível Frequent Access. Além disso, ele não impede a hierarquização de objetos do nível Frequent Access para o nível Infrequent Access e, depois, para o nível Archive Instant.

É possível usar o S3 Intelligent-Tiering como sua classe de armazenamento padrão para dados recém-criados especificando `INTELLIGENT-TIERING` no cabeçalho de solicitação `x-amz-storage-class` ao chamar as operações `PutObject`, `CopyObject` ou `CreateMultipartUpload`. O S3 Intelligent-Tiering foi projetado para oferecer 99,9% de disponibilidade e 99,9999999% de durabilidade.

> **Note**
>
> Se o tamanho do objeto for menor que 128 KB, ele não será monitorado nem qualificado para o nivelamento automático. Objetos menores são sempre armazenados no nível Acesso frequente.

Níveis de acesso do S3 Intelligent-Tiering

A seção a seguir explica os diferentes níveis de acesso automático e opcional. Ao mover objetos entre os níveis de acesso, a classe de armazenamento permanece a mesma (S3 Intelligent-Tiering).

Nível de Acesso frequente (automático)

Este é o nível de acesso padrão no qual qualquer objeto criado ou transicionado para o S3 Intelligent-Tiering inicia seu ciclo de vida. Um objeto permanecerá neste nível enquanto estiver sendo acessado. O nível Frequent Access oferece baixa latência e throughput de alto desempenho.

Nível de Acesso infrequente (automático)

Se um objeto não for acessado por 30 dias consecutivos, o objeto se moverá para o nível de Acesso infrequente. O nível Infrequent Access oferece baixa latência e throughput de alto desempenho.

Nível Archive Instant Access (automático)

Se o objeto não for acessado por 90 dias consecutivos, ele será movido para o nível Archive Instant Access. O nível de acesso de arquivamento instantâneo oferece baixa latência e throughput de alto desempenho.

Nível de Acesso de arquivamento (opcional)

O S3 Intelligent-Tiering oferece a opção de ativar o nível Archive Access para dados que podem ser acessados de maneira assíncrona. Após a ativação, o nível Archive Access arquiva os objetos que não foram acessados durante um mínimo de 90 dias consecutivos. Você pode estender o último tempo de acesso para arquivamento para um máximo de 730 dias. O nível Archive Access tem a mesma performance que a classe de armazenamento do S3 Glacier Flexible Retrieval.

Os tempos de recuperação comuns para esse nível de acesso podem variar de três a cinco horas. Se você iniciar a solicitação de restauração usando o Operações em Lote do S3, a restauração começará em minutos. Para receber mais informações sobre as opções e prazos de recuperação, consulte the section called “Restaurar objetos dos níveis Archive Access e Deep Archive Access do S3 Intelligent-Tiering”.

> **Note**
>
> Ative apenas o nível Archive Access por 90 dias se você quiser ignorar o nível Archive Instant Access. O nível Archive Access oferece um custo de armazenamento um pouco menor com tempos de recuperação de minutos a horas. O nível Acesso instantâneo ao arquivamento oferece acesso de milissegundos e alta performance de throughput.

Nível Acesso de arquivamento profundo (opcional)

O S3 Intelligent-Tiering oferece a opção de ativar o nível Deep Archive Access para dados que podem ser acessados de maneira assíncrona. Após a ativação, o nível Deep Archive Access arquiva os objetos que não foram acessados durante um mínimo de 180 dias consecutivos. Você pode estender o último tempo de acesso para arquivamento para um máximo de 730 dias. O nível de Acesso de arquivamento profundo tem a mesma performance que a classe de armazenamento S3 Glacier Deep Archive.

A recuperação padrão de objetos desse nível de acesso ocorre em até 12 horas. Se você iniciar a solicitação de restauração usando o Operações em Lote do S3, a restauração começará em nove horas. Para receber mais informações sobre as opções e prazos de recuperação, consulte the section called “Restaurar objetos dos níveis Archive Access e Deep Archive Access do S3 Intelligent-Tiering”.

> **Note**
>
> Ative os níveis Acesso de arquivamento e Acesso de arquivamento profundo somente se seus objetos puderem ser acessados de forma assíncrona pela aplicação. Se o objeto que você está recuperando estiver armazenado nos níveis de acesso Archive ou Deep Archive, será necessário primeiro restaurar o objeto usando a operação `RestoreObject`.

Como usar o S3 Intelligent-Tiering

Você pode usar a classe de armazenamento S3 Intelligent-Tiering para otimizar automaticamente os custos de armazenamento. O S3 Intelligent-Tiering oferece economia de custo automática ao mover dados em um nível detalhado de objeto entre níveis de acesso quando há alteração nos padrões de acesso. Para dados que podem ser acessados de forma assíncrona, você pode optar por habilitar o arquivamento automático na classe de armazenamento do S3 Intelligent-Tiering usando o AWS Management Console, a AWS CLI ou a API do Amazon S3.

Como mover dados para o S3 Intelligent-Tiering

Há duas maneiras de mover dados para o S3 Intelligent-Tiering. É possível fazer upload de objetos diretamente no S3 Intelligent-Tiering pelo console ou programaticamente usando uma operação PUT. Para ter mais informações, consulte Configurar a classe de armazenamento de um objeto. Também é possível definir as configurações do Ciclo de Vida do S3 para fazer a transição de objetos do S3 Standard ou S3 Standard-Infrequent Access para o S3 Intelligent-Tiering.

Carregar dados para o S3 Intelligent-Tiering usando o Direct PUT

Quando você carrega um objeto para a classe de armazenamento do S3 Intelligent-Tiering usando a operação de API PUT, você especifica S3 Intelligent-Tiering no cabeçalho da solicitação de `x-amz-storage-class`.

A seguinte solicitação armazena a imagem, `my-image.jpg`, no bucket `myBucket`. A solicitação usa o cabeçalho `x-amz-storage-class` para solicitar que o objeto seja armazenado usando a classe de armazenamento do S3 Intelligent-Tiering.

Example

```
PUT /my-image.jpg HTTP/1.1
Host: myBucket.s3.<Region>.amazonaws.com (http://amazonaws.com/)
Date: Wed, 1 Sep 2021 17:50:00 GMT
```

```
Authorization: authorization string
Content-Type: image/jpeg
Content-Length: 11434
Expect: 100-continue
x-amz-storage-class: INTELLIGENT_TIERING
```

Como fazer transição de dados para o S3 Intelligent-Tiering do S3 Standard ou do S3 Standard-Infrequent Access usando o S3 Lifecycle

É possível adicionar regras a uma configuração do S3 Lifecycle para solicitar que o Amazon S3 faça a transição de objetos de uma classe de armazenamento para outra. Para obter informações sobre transições suportadas e restrições relacionadas, consulte Como fazer transição de objetos usando o S3 Lifecycle.

É possível especificar configurações de ciclo de vida do S3 no nível do bucket ou do prefixo. Nesta regra de configuração do S3 Lifecycle, o filtro especifica um prefixo das chaves (`documents/`). Portanto, a regra aplica-se a objetos com o prefixo de nome de chave `documents/`, como `documents/doc1.txt` e `documents/doc2.txt`. A regra especifica uma ação de `Transition` direcionando o Amazon S3 para fazer a transição de objetos para a classe de armazenamento do S3 Intelligent-Tiering 0 dia após a criação. Nesse caso, os objetos são elegíveis para transição para o S3 Intelligent-Tiering à meia-noite UTC, após a criação.

Example

```
<LifecycleConfiguration>
  <Rule>
    <ID>ExampleRule</ID>
    <Filter>
       <Prefix>documents/</Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>0</Days>
      <StorageClass>INTELLIGENT_TIERING</StorageClass>
    </Transition>
 </Rule>
</LifecycleConfiguration>
```

Um bucket com versionamento habilitado mantém uma versão atual do objeto e versões desatualizadas do objeto (se disponíveis). Você pode definir regras separadas de ciclo de vida para versões atuais e não atuais do objeto.

Para ter mais informações, consulte Elementos de configuração do ciclo de vida.

Habilitar níveis Archive Access e Deep Archive Access do S3 Intelligent-Tiering

Para obter o custo de armazenamento mais baixo sobre dados que podem ser acessados de minutos a horas, você pode ativar um ou ambos os níveis de acesso de arquivo criando uma configuração no nível de bucket, prefixo ou etiqueta de objeto usando o AWS Management Console, a AWS CLI ou a API do Amazon S3.

Uso do console do S3

Para habilitar o arquivamento automático do S3 Intelligent-Tiering

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Na lista de Buckets, escolha o nome do bucket desejado.
3. Escolha Properties (Propriedades).
4. Navegue até a seção S3 Intelligent-Tiering Archive configurations (Configurações do S3 Intelligent-Tiering) e escolha Create configuration (Criar configuração).
5. Na seção Archive configuration settings (Definições de configuração do arquivamento), especifique um nome de configuração descritiva para a configuração de arquivamento do S3 Intelligent-Tiering.
6. Em Choose a configuration scope (Escolher um escopo de configuração), escolha um escopo de configuração a ser usado. Opcionalmente, você pode limitar o escopo de configuração a objetos especificados em um bucket usando um prefixo compartilhado, uma etiqueta de objeto ou uma combinação dos dois.
    a. Para limitar o escopo da configuração, selecione Limit the scope of this configuration using one or more filters (Limitar o escopo dessa configuração usando um ou mais filtros).
    b. Para limitar o escopo da configuração usando um único prefixo, insira o prefixo em Prefix (Prefixo).
    c. Para limitar o escopo da configuração usando etiquetas de objeto, selecione Add tag (Adicionar etiqueta) e insira um valor para Key (Chave).
7. Em Status, selecione Enable (Habilitar).
8. Na seção Archive settings (Configurações de arquivamento), selecione um ou ambos os níveis de Acesso de arquivamento a serem ativados.

9. Escolha Criar.

Como usar a AWS CLI

Você pode usar os seguintes comandos da AWS CLI para gerenciar as configurações do S3 Intelligent-Tiering:

- `delete-bucket-intelligent-tiering-configuration`
- `get-bucket-intelligent-tiering-configuration`
- `list-bucket-intelligent-tiering-configurations`
- `put-bucket-intelligent-tiering-configuration`

Consulte instruções sobre como configurar a AWS CLI em Developing with Amazon S3 using the AWS CLI na Referência de API do Amazon S3.

Ao usar a AWS CLI, você não pode especificar a configuração como um arquivo XML. Você deve especificar o JSON em vez disso. A seguir, está um exemplo de configuração XML do S3 Intelligent-Tiering e JSON equivalente que você pode especificar em um comando da AWS CLI.

O exemplo a seguir coloca uma configuração do S3 Intelligent-Tiering no bucket especificado.

Example **`put-bucket-intelligent-tiering-configuration`**

JSON

```
{
  "Id": "string",
  "Filter": {
    "Prefix": "string",
    "Tag": {
      "Key": "string",
      "Value": "string"
    },
    "And": {
      "Prefix": "string",
      "Tags": [
        {
          "Key": "string",
          "Value": "string"
        }
```

```
        ...
      ]
    }
  },
  "Status": "Enabled"|"Disabled",
  "Tierings": [
    {
      "Days": integer,
      "AccessTier": "ARCHIVE_ACCESS"|"DEEP_ARCHIVE_ACCESS"
    }
    ...
  ]
}
```

XML

```
PUT /?intelligent-tiering&id=Id HTTP/1.1
Host: Bucket.s3.amazonaws.com
<?xml version="1.0" encoding="UTF-8"?>
<IntelligentTieringConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
   <Id>string</Id>
   <Filter>
      <And>
         <Prefix>string</Prefix>
         <Tag>
            <Key>string</Key>
            <Value>string</Value>
         </Tag>
         ...
      </And>
      <Prefix>string</Prefix>
      <Tag>
         <Key>string</Key>
         <Value>string</Value>
      </Tag>
   </Filter>
   <Status>string</Status>
   <Tiering>
      <AccessTier>string</AccessTier>
      <Days>integer</Days>
   </Tiering>
   ...
</IntelligentTieringConfiguration>
```

Usando a operação PUT da API

Você pode usar a operação `PutBucketIntelligentTieringConfiguration` para um bucket especificado e até 1.000 configurações do S3 Intelligent-Tiering por bucket. Você pode definir quais objetos em um bucket são elegíveis para os níveis de Acesso de arquivamento usando um prefixo compartilhado ou uma etiqueta de objeto. Usar um prefixo compartilhado ou etiqueta de objeto permite que você alinhe aplicações comerciais, fluxos de trabalho ou organizações internas específicas. Você também tem a flexibilidade de ativar o nível de Acesso de arquivamento, o nível Acesso de arquivamento profundo ou ambos.

Começar a usar o S3 Intelligent-Tiering

Para saber mais sobre como usar o S3 Intelligent-Tiering, consulte Tutorial: Começar a usar o S3 Intelligent-Tiering.

Como gerenciar o S3 Intelligent-Tiering

A classe de armazenamento do S3 Intelligent-Tiering oferece redução automática de custos de armazenamento em três níveis de acesso de baixa latência e alto throughput. Também oferece recursos de arquivo opcionais para ajudar você a obter os menores custos de armazenamento na nuvem para dados que podem ser acessados de minutos a horas.

Identificar quais objetos do nível de acesso do S3 Intelligent-Tiering estão armazenados

Para receber uma lista dos objetos e dos metadados correspondentes, incluindo o nível S3 Intelligent-Tiering Access, você pode usar o Inventário Amazon S3 . O Inventário S3 fornece arquivos de saída CSV, ORC ou Parquet que listam seus objetos e os metadados correspondentes. Você pode receber esses relatórios de inventário diariamente ou semanalmente para um bucket do Amazon S3 ou um prefixo compartilhado. (Prefixo compartilhado refere-se a objetos que tenham nomes que começam com uma string em comum.)

Visualizar o status do arquivo de um objeto no S3 Intelligent-Tiering

Para receber uma notificação quando um objeto na classe de armazenamento do S3 Intelligent-Tiering for movido ao nível Archive Access ou ao Deep Archive Access, você pode configurar notificações de evento do S3. Para obter mais informações, consulte Habilitar notificações de eventos.

O Amazon S3 pode publicar notificações de eventos em um tópico do Amazon Simple Notification Service (Amazon SNS), em uma fila do Amazon Simple Queue Service (Amazon SQS) ou em uma

função do AWS Lambda. Para ter mais informações, consulte Notificações de eventos do Amazon S3.

Veja a seguir um exemplo de mensagem que o Amazon S3 envia para publicar um evento `s3:IntelligentTiering`. Para ter mais informações, consulte the section called “Estrutura de mensagens de evento”.

```
{
   "Records":[
      {
         "eventVersion":"2.3",
         "eventSource":"aws:s3",
         "awsRegion":"us-west-2",
         "eventTime":"1970-01-01T00:00:00.000Z",
         "eventName":"IntelligentTiering",
         "userIdentity":{
            "principalId":"s3.amazonaws.com"
         },
         "requestParameters":{
            "sourceIPAddress":"s3.amazonaws.com"
         },
         "responseElements":{
            "x-amz-request-id":"C3D13FE58DE4C810",
            "x-amz-id-2":"FMyUVURIY8/IgAtTv8xRjskZQpcIZ9KG4V5Wp6S7S/
JRWeUWerMUE5JgHvANOjpD"
         },
         "s3":{
            "s3SchemaVersion":"1.0",
            "configurationId":"testConfigRule",
            "bucket":{
               "name":"amzn-s3-demo-bucket",
               "ownerIdentity":{
                  "principalId":"A3NL1KOZZKExample"
               },
               "arn":"arn:aws:s3:::amzn-s3-demo-bucket"
            },
            "object":{
               "key":"HappyFace.jpg",
               "size":1024,
               "eTag":"d41d8cd98f00b204e9800998ecf8427e",
            }
         },
         "intelligentTieringEventData":{
```

```
            "destinationAccessTier": "ARCHIVE_ACCESS"
            }
      }
   ]
}
```

Você também pode usar uma solicitação do objeto HEAD para visualizar o status de arquivamento de um objeto. Se um objeto for armazenado usando a classe de armazenamento do S3 Intelligent-Tiering e estiver no momento em um dos níveis de arquivamento, a resposta de objeto HEAD mostrará o nível de arquivamento atual. Para mostrar o nível de arquivamento, a solicitação usa o cabeçalho x-amz-archive-status.

A solicitação de objeto HEAD a seguir retorna os metadados de um objeto (nesse caso, *my-image.jpg*).

Example

```
HEAD /my-image.jpg HTTP/1.1
Host: bucket.s3.region.amazonaws.com
Date: Wed, 28 Oct 2009 22:32:00 GMT
Authorization: AWS AKIAIOSFODNN7EXAMPLE:02236Q3V0RonhpaBX5sCYVf1bNRuU=
```

Você também pode usar solicitações de objetos HEAD para monitorar o status de uma solicitação `restore-object`. Se a restauração do arquivo estiver em andamento, a resposta de objeto HEAD incluirá o cabeçalho x-amz-restore.

O exemplo de resposta de objeto HEAD a seguir mostra um objeto arquivado usando o S3 Intelligent-Tiering com uma solicitação de restauração em andamento.

Example

```
HTTP/1.1 200 OK
x-amz-id-2: FSVaTMjrmBp3Izs1NnwBZeu7M19iI8UbxMbi0A8AirHANJBo+hEftBuiESACOMJp
x-amz-request-id: E5CEFCB143EB505A
Date: Fri, 13 Nov 2020 00:28:38 GMT
Last-Modified: Mon, 15 Oct 2012 21:58:07 GMT
ETag: "1accb31fcf202eba0c0f41fa2f09b4d7"
x-amz-storage-class: 'INTELLIGENT_TIERING'
x-amz-archive-status: 'ARCHIVE_ACCESS'
x-amz-restore: 'ongoing-request="true"'
x-amz-restore-request-date: 'Fri, 13 Nov 2020 00:20:00 GMT'
Accept-Ranges: bytes
```

```
Content-Type: binary/octet-stream
Content-Length: 300
Server: AmazonS3
```

Restaurar objetos dos níveis Archive Access e Deep Archive Access do S3 Intelligent-Tiering

Para acessar objetos nos níveis S3 Intelligent-Tiering Archive Access e Deep Archive Access, você deve iniciar uma solicitação de restauração e esperar até que o objeto seja movido para o nível Frequent Access. Para obter mais informações sobre objetos arquivados, consulte the section called "Trabalhando com objetos arquivados".

Quando você restaura dos níveis Acesso de arquivamento ou Acesso de arquivamento profundo, o objeto faz a transição de volta para o nível Acesso frequente. Depois, se o objeto não for acessado durante 30 dias consecutivos, ele se moverá automaticamente para o nível Infrequent Access (Acesso infrequente). Depois, após um período mínimo de 90 dias consecutivos sem acesso, o objeto é transferido ao nível Archive Access. Depois de um período mínimo de 180 dias consecutivos sem acesso, o objeto é transferido automaticamente ao nível Deep Archive Access. Para ter mais informações, consulte the section called "Como o S3 Intelligent-Tiering funciona".

Você pode restaurar um objeto arquivado usando o console do Amazon S3, o Operações em Lote do S3, a API REST do Amazon S3, os SDKs da AWS ou a AWS Command Line Interface (AWS CLI). Para ter mais informações, consulte the section called "Trabalhando com objetos arquivados".

Noções básicas sobre as classes de armazenamento S3 Glacier para armazenamento de dados de longo prazo

É possível usar as classes de armazenamento S3 Glacier do Amazon S3 para fornecer soluções econômicas para armazenar dados de longo prazo que não são acessados com frequência. As classes de armazenamento do S3 Glacier são:

- S3 Glacier Instant Retrieval
- S3 Glacier Flexible Retrieval
- S3 Glacier Deep Archive

Escolha uma dessas classes de armazenamento com base na frequência com que você acessa seus dados e na rapidez com que precisa recuperá-los. Cada uma dessas classes de armazenamento oferece a mesma durabilidade e resiliência que a classe de armazenamento S3 Standard, mas com custos de armazenamento mais baixos. Para obter mais informações sobre as

classes de armazenamento do S3 Glacier, consulte https://aws.amazon.com/s3/storage-classes/glacier/.

Tópicos

- Comparar as classes de armazenamento do S3 Glacier
- S3 Glacier Instant Retrieval
- S3 Glacier Flexible Retrieval
- S3 Glacier Deep Archive
- Noções básicas do armazenamento de arquivamento nas classes S3 Glacier Flexible Retrieval e S3 Glacier Deep Archive
- Diferenças entre essas classes de armazenamento e o serviço S3 Glacier

Comparar as classes de armazenamento do S3 Glacier

Cada classe de armazenamento do S3 Glacier tem uma duração de armazenamento mínima para todos os objetos. Se excluir, substituir ou fizer a transição de um objeto para outra classe de armazenamento antes do período mínimo, você receberá uma cobrança pelo período restante dessa duração.

Algumas classes de armazenamento do S3 Glacier são de arquivamento, o que significa que os objetos armazenados nessas classes são arquivados e não ficam disponíveis para acesso em tempo real. Para obter mais informações, consulte Noções básicas do armazenamento de arquivamento nas classes S3 Glacier Flexible Retrieval e S3 Glacier Deep Archive.

As classes de armazenamento projetadas para padrões de acesso menos frequentes com tempos de recuperação mais longos oferecem custos de armazenamento mais baixos. Para obter informações sobre preços, consulte https://aws.amazon.com/s3/pricing/.

A tabela a seguir resume os principais pontos a serem considerados ao escolher uma classe de armazenamento do S3 Glacier:

S3 Glacier Instant Retrieval

Recomendamos usar a classe S3 Glacier Instant Retrieval para dados de longo prazo que são acessados uma vez por trimestre e exigem tempos de recuperação na casa dos milissegundos. Essa classe de armazenamento é ideal para casos de uso sensíveis à performance, como hospedagem de imagens, aplicações de compartilhamento de arquivos e armazenamento de registros médicos para acesso durante consultas.

A classe de armazenamento S3 Glacier Instant Retrieval oferece acesso em tempo real aos objetos com a mesma latência e performance de throughput que a classe de armazenamento S3 Standard-IA. Em comparação com a classe S3 Standard-IA, a classe S3 Glacier Instant Retrieval oferece custos de armazenamento mais baixos e custos de acesso aos dados mais altos.

Há um tamanho de objeto mínimo de 128 KB para dados armazenados na classe de armazenamento S3 Glacier Instant Retrieval. Essa classe de armazenamento também tem um período mínimo de armazenamento de 90 dias.

S3 Glacier Flexible Retrieval

Recomendamos usar a classe S3 Glacier Flexible Retrieval para arquivar dados que são acessados uma ou duas vezes por ano e não exigem acesso imediato. A classe S3 Glacier Flexible Retrieval oferece tempos de recuperação flexíveis para ajudar você a equilibrar os custos, com tempos de acesso que variam de alguns minutos a horas, e recuperações em massa gratuitas. Essa classe de armazenamento é ideal para backup e recuperação de desastres.

Os objetos na classe S3 Glacier Flexible Retrieval ficam arquivados e não estão disponíveis para acesso em tempo real. Para obter mais informações, consulte Noções básicas do armazenamento de arquivamento nas classes S3 Glacier Flexible Retrieval e S3 Glacier Deep Archive. Para acessar esses objetos, primeiro inicie uma solicitação de restauração que cria uma cópia temporária do objeto que você poderá acessar quando a solicitação for concluída. Para mais informações, consulte Trabalhando com objetos arquivados. Ao restaurar um objeto, é possível escolher um nível de recuperação adequado ao seu caso de uso, com custos mais baixos para tempos de restauração mais longos.

Os seguintes níveis de recuperação estão disponíveis para a classe S3 Glacier Flexible Retrieval:

- Recuperação expressa: normalmente, leva de 1 a 5 minutos para restaurar um objeto. As recuperações expressas estão sujeitas à demanda. Portanto, para garantir que você tenha tempos de restauração confiáveis e previsíveis, recomendamos que compre capacidade de recuperação provisionada. Para obter mais informações, consulte Capacidade provisionada.
- Recuperação padrão: normalmente, leva de 3 a 5 horas para restaurar um objeto, ou de 1 minuto a 5 horas usando a funcionalidade Operações em Lote do S3. Para obter mais informações, consulte Restaurar objetos com operações em lote.
- Recuperação em massa: normalmente, leva de 5 a 12 horas para restaurar um objeto. As recuperações em massa são gratuitas.

A duração mínima de armazenamento para objetos na classe de armazenamento S3 Glacier Flexible Retrieval é de 90 dias.

A classe S3 Glacier Flexible Retrieval requer 40 KB de metadados adicionais para cada objeto. Isso inclui 32 KB de metadados necessários para identificar e recuperar os dados, que são cobrados segundo a taxa padrão da classe S3 Glacier Flexible Retrieval. São necessários mais 8 KB de dados para manter o nome e os metadados definidos pelo usuário para objetos arquivados, que são cobrados segundo a taxa da classe S3 Standard.

S3 Glacier Deep Archive

Recomendamos usar a classe S3 Glacier Deep Archive para arquivar dados que são acessados menos de uma vez por ano. Essa classe de armazenamento foi projetada para reter conjuntos de dados por vários anos a fim de atender aos requisitos de conformidade, podendo também ser usada para backup ou recuperação de desastres ou para qualquer dado acessado com baixa frequência que você possa esperar até 72 horas para recuperar. O S3 Glacier Deep Archive é a opção de armazenamento com o menor custo na AWS.

Os objetos na classe S3 Glacier Deep Archive ficam arquivados e não estão disponíveis para acesso em tempo real. Para obter mais informações, consulte Noções básicas do armazenamento de arquivamento nas classes S3 Glacier Flexible Retrieval e S3 Glacier Deep Archive. Para acessar esses objetos, primeiro inicie uma solicitação de restauração que cria uma cópia temporária do objeto que você poderá acessar quando a solicitação for concluída. Para mais informações, consulte Trabalhando com objetos arquivados. Ao restaurar um objeto, é possível escolher um nível de recuperação adequado ao seu caso de uso, com custos mais baixos para tempos de restauração mais longos.

Os seguintes níveis de recuperação estão disponíveis para a classe S3 Glacier Deep Archive:

- Recuperação padrão: normalmente, leva até 12 horas para restaurar um objeto, ou de 9 a 12 horas usando a funcionalidade Operações em Lote do S3. Para obter mais informações, consulte Restaurar objetos com operações em lote.
- Recuperação em massa: normalmente, leva até 48 horas para restaurar um objeto por uma fração do custo do nível de recuperação Standard.

A duração mínima de armazenamento para objetos na classe de armazenamento S3 Glacier Deep Archive é de 180 dias.

A classe S3 Glacier Deep Archive requer 40 KB de metadados adicionais para cada objeto. Isso inclui 32 KB de metadados necessários para identificar e recuperar os dados, que são cobrados segundo a taxa padrão da classe S3 Glacier Deep Archive. São necessários mais 8 KB de dados para manter o nome e os metadados definidos pelo usuário para objetos arquivados, que são cobrados segundo a taxa da classe S3 Standard.

Noções básicas do armazenamento de arquivamento nas classes S3 Glacier Flexible Retrieval e S3 Glacier Deep Archive

As classe S3 Glacier Flexible Retrieval e S3 Glacier Deep Archive são classes de armazenamento para arquivamento. Isso significa que, quando você armazena um objeto nessas classes de armazenamento, esse objeto é arquivado e não pode ser acessado diretamente. Para acessar um objeto arquivado, envie uma solicitação de restauração para ele e aguarde até que o serviço restaure o objeto. A solicitação de restauração restaura uma cópia temporária do objeto, e essa cópia é excluída após a duração especificada na solicitação. Para obter mais informações, consulte Trabalhando com objetos arquivados.

A transição de objetos para a classe de armazenamento S3 Glacier Deep Archive é apenas unidirecional.

Se você quiser mudar a classe de armazenamento de um objeto arquivado em outra classe de armazenamento, deverá usar a operação de restauração para fazer primeiro uma cópia temporária do objeto. Depois, use a operação de cópia para substituir o objeto especificando S3 Standard, S3 Intelligent-Tiering, S3 Standard – IA, S3 One Zone – IA, S3 Glacier Instant Retrieval, S3 Glacier Flexible Retrieval ou armazenamento de redundância reduzida como a classe de armazenamento.

> **Note**
>
> A aplicação da operação Copy a objetos restaurados não é permitida no console do Amazon S3 em objetos nas classes de armazenamento S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive. Para esse tipo de operação de cópia, use a AWS Command Line Interface (AWS CLI), AWS SDKs ou a API REST.

Você pode restaurar objetos arquivados nessas classes de armazenamento com até 1.000 transações por segundo (TPS) de solicitações de restauração de objetos por conta, por Região da AWS.

Considerações sobre custos

Se você estiver planejando arquivar dados acessados com pouca frequência por um período de meses ou anos, as classes de armazenamento S3 Glacier Flexible Retrieval e S3 Glacier Deep Archive podem reduzir seus custos de armazenamento. No entanto, para garantir que a classe de armazenamento S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive seja apropriada para você, considere o seguinte:

- Cobranças de sobrecarga de armazenamento: cada objeto arquivado requer 40 KB de metadados adicionais. Isso inclui 32 KB de metadados necessários para identificar e recuperar os dados, que são cobrados segundo a taxa padrão da respectiva classe de armazenamento. São necessários mais 8 KB de dados para manter o nome e os metadados definidos pelo usuário para objetos arquivados, que são cobrados segundo a taxa da classe S3 Standard.

  Se você estiver arquivando objetos pequenos, considere esses encargos de armazenamento. Considere também a possibilidade de agregar vários objetos pequenos em um número menor de objetos grandes para reduzir os gastos adicionais.
- Preços do carregamento fracionado: os objetos em S3-storage-class-glacier; e S3 Glacier Deep Archive são cobrados segundo as taxas da classe de armazenamento S3 Standard quando você usa carregamentos fracionados para fazer upload deles. Para obter mais informações, consulte Multipart upload e definição de preço.
- Cobranças de armazenamento de no mínimo 30 dias: o S3 Glacier Flexible Retrieval e o S3 Glacier Deep Archive são soluções de arquivamento de longo prazo. O período mínimo de duração de armazenamento é de 90 dias para a classe de armazenamento S3 Glacier Flexible Retrieval e 180 dias para o S3 Glacier Deep Archive. A exclusão de dados arquivados nessas classes de armazenamento não incorrerá em cobrança se os objetos que você excluir estiverem arquivados por mais do que o período mínimo de duração do armazenamento. Se você excluir ou substituir um objeto arquivado dentro do período mínimo de duração do arquivamento, o Amazon S3 cobrará pelo restante dessa duração.
- Cobranças de recuperação de dados: quando você restaura objetos arquivados no S3 Glacier Flexible Retrieval e no S3 Glacier Deep Archive, há cobranças de recuperação de dados por solicitação. Essas cobranças variam de acordo com o nível de recuperação escolhido ao iniciar uma restauração. Para obter informações sobre a definição de preços, consulte Definição de preços do Amazon S3.
- Ciclo de Vida do S3: quando você restaura objetos arquivados no S3 Glacier Flexible Retrieval e no S3 Glacier Deep Archive, há cobranças de recuperação de dados por solicitação. Essas

cobranças variam de acordo com o nível de recuperação escolhido ao iniciar uma restauração. Para obter informações sobre a definição de preços, consulte Definição de preços do Amazon S3.

Restaurar objetos arquivados

Os objetos arquivados não podem ser acessados em tempo real. Primeiro inicie uma solicitação de restauração e, em seguida, aguarde até que uma cópia temporária do objeto esteja disponível pelo tempo que você especificar na solicitação. Depois de receber uma cópia temporária do objeto restaurado, a classe de armazenamento do objeto continuará sendo S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive. (Uma solicitação de operação de API HeadObject ou GetObject retornará o S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive como a classe de armazenamento.)

> **Note**
>
> Ao restaurar um arquivamento, você paga pelo arquivamento (taxa de S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive) e por uma cópia restaurada temporariamente (taxa de armazenamento de S3 Standard). Para obter mais informações sobre definição de preços, consulte Definição de preços do Amazon S3.

Você pode restaurar uma cópia do objeto programaticamente ou usando o console do Amazon S3. O Amazon S3 só processa uma solicitação de restauração por vez por objeto. Para obter mais informações, consulte Restaurar um objeto arquivado.

Diferenças entre essas classes de armazenamento e o serviço S3 Glacier

As classes de armazenamento do S3 Glacier fazem parte do serviço Amazon S3 e armazenam dados como objetos em buckets do S3. Você pode gerenciar objetos nessas classes de armazenamento usando o console do S3 ou usando as APIs ou SDKs do S3 de maneira programática. Ao armazenar objetos nas classes de armazenamento do S3 Glacier, você pode usar os recursos do S3, como criptografia avançada, marcação de objetos e configurações da funcionalidade Ciclo de Vida do S3, para ajudar a gerenciar a acessibilidade e o custo dos dados.

> **Important**
>
> Recomendamos usar as classes de armazenamento do S3 Glacier no serviço Amazon S3 para todos os seus dados de longo prazo.

O Amazon S3 Glacier (S3 Glacier) é um serviço separado que armazena dados na forma de arquivamento dentro de cofres. Esse serviço não é compatível com os recursos do Amazon S3 e oferece suporte ao console para operações de upload e download de dados. Não recomendamos usar o serviço S3 Glacier para dados de longo prazo. Os dados armazenados nesse serviço não podem ser acessados pelo serviço Amazon S3. Para obter informações sobre o serviço S3 Glacier, consulte o Guia do desenvolvedor do Amazon S3 Glacier. Para transferir dados do serviço Amazon S3 Glacier para uma classe de armazenamento no Amazon S3, consulte Transferência de dados de cofres do Amazon S3 Glacier para o Amazon S3 na Biblioteca de Soluções da AWS.

Trabalhando com objetos arquivados

Para reduzir os custos de armazenamento de objetos acessados com pouca frequência, você pode arquivar esses objetos. Quando você arquiva um objeto, ele é movido para um armazenamento de baixo custo, o que significa que não é possível acessá-lo em tempo real.

Embora os objetos arquivados não estejam acessíveis em tempo real, você pode restaurá-los em minutos ou horas, dependendo da classe de armazenamento. Você pode restaurar um objeto arquivado usando o console do Amazon S3, o Operações em Lote do S3, a API REST, os AWS SDKs e a AWS Command Line Interface (AWS CLI). Para obter instruções, consulte Restaurar um objeto arquivado.

Os objetos do Amazon S3 nas seguintes classes ou níveis de armazenamento são arquivados e não podem ser acessados em tempo real:

- A classe de armazenamento S3 Glacier Flexible Retrieval
- A classe de armazenamento S3 Glacier Deep Archive
- O nível Acesso ao arquivamento do S3 Intelligent-Tiering
- O nível de acesso de arquivamento profundo do S3 Intelligent-Tiering

Para restaurar objetos arquivados, você deve fazer o seguinte:

- Para objetos nas classes de armazenamento S3 Glacier Flexible Retrieval e S3 Glacier Deep Archive, você deve iniciar a solicitação de restauração e aguardar até que uma cópia temporária do objeto esteja disponível. Se for criada uma cópia temporária do objeto restaurado, a classe de armazenamento do objeto permanecerá a mesma. (Uma solicitação de operação de API HeadObject ou GetObject retornará S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive como a classe de armazenamento.)

- Para objetos nos níveis Acesso de arquivamento e Acesso de arquivamento profundo do S3 Intelligent-Tiering, você deve iniciar a solicitação de restauração e esperar até que o objeto seja movido para o nível Acesso frequente.

Para obter mais informações sobre como todas as classes de armazenamento do Amazon S3 se comparam, consulte Compreender e gerenciar classes de armazenamento do Amazon S3. Para obter mais informações sobre o S3 Intelligent-Tiering, consulte the section called “Como o S3 Intelligent-Tiering funciona”.

O tempo necessário para concluir um trabalho de restauração depende da classe ou do nível de armazenamento de arquivo usado e da opção de recuperação especificada: expressa (disponível apenas para o S3 Glacier Flexible Retrieval e o S3 Intelligent-Tiering Archive Access), padrão ou em massa. Para ter mais informações, consulte Noções básicas sobre as opções de recuperação de arquivos.

Você pode ser notificado quando sua restauração for concluída usando as Notificações de Eventos do Amazon S3. Para ter mais informações, consulte Notificações de eventos do Amazon S3.

Restaurar objetos do S3 Glacier

Quando você usa o S3 Glacier Flexible Retrieval ou o S3 Glacier Deep Archive, o Amazon S3 restaura uma cópia temporária do objeto somente pela duração especificada. Depois disso, ele exclui a cópia restaurada do objeto. Você pode modificar o período de validade de uma cópia restaurada reenviando uma solicitação de restauração. Nesse caso, o Amazon S3 atualiza o período de expiração relativo à hora atual.

> **Note**
>
> Ao restaurar um objeto arquivado do S3 Glacier Flexible Retrieval ou do S3 Glacier Deep Archive, você paga pelo objeto arquivado e pela cópia restaurada temporariamente. Para obter mais informações sobre preços, consulte Preços do Amazon S3.

O Amazon S3 calcula o tempo de validade da cópia do objeto restaurado adicionando o número de dias especificado na solicitação de restauração à hora de conclusão da restauração solicitada. Depois, o Amazon S3 arredonda a hora resultante para o próximo dia à meia-noite do Tempo Universal Coordenado (UTC). Por exemplo, suponha que a cópia de um objeto restaurado tenha sido criada em 15 de outubro de 2012, às 10h30 UTC, e o período de restauração tenha sido especificado

como três dias. Nesse caso, a cópia restaurada expira em 19 de outubro de 2012, à 0h UTC, hora em que o Amazon S3 vai excluir a cópia do objeto.

Restaurar objetos do S3 Intelligent-Tiering

Quando você está restaurando um objeto dos níveis S3 Intelligent-Tiering Archive Access ou S3 Intelligent-Tiering Deep Archive Access, o objeto volta para o nível S3 Intelligent-Tiering Frequent Access. Se o objeto não for acessado depois de 30 dias consecutivos, ele será movido automaticamente para o nível Acesso infrequente. Depois de um período mínimo de 90 dias consecutivos sem acesso, o objeto é movido para o nível Acesso ao arquivamento do S3 Intelligent-Tiering. Se o objeto não for acessado depois de um período mínimo de 180 dias consecutivos, ele será movido para o nível Acesso profundo ao arquivamento.

> **Note**
>
> Ao contrário das classes de armazenamento S3 Glacier Flexible Retrieval e S3 Glacier Deep Archive, as solicitações de restauração para objetos S3 Intelligent-Tiering não aceitam o valor `Days`.

Usar o recurso Operações em Lote do S3 com solicitações de restauração

Para restaurar mais de um objeto do Amazon S3 com uma única solicitação, é possível usar operações em lote do S3. Você fornece às operações em lote do S3 uma lista de objetos nos quais operar. O S3 Batch Operations chama a respectiva operação de API para executar a operação especificada. Um único trabalho de operações em lote pode realizar a operação especificada em bilhões de objetos contendo exabytes de dados.

Tópicos

- Noções básicas sobre as opções de recuperação de arquivos
- Restaurar um objeto arquivado

Noções básicas sobre as opções de recuperação de arquivos

Veja a seguir as opções de recuperação disponíveis ao restaurar um objeto arquivado no Amazon S3:

- Expressa: acesse rapidamente os dados armazenados na classe de armazenamento S3 Glacier Flexible Retrieval ou no nível S3 Intelligent-Tiering Archive Access. É possível usar essa opção quando solicitações urgentes ocasionais para um subconjunto de arquivos for solicitado. Para todos os objetos arquivados, exceto os maiores (mais de 250 MB), os dados acessados por meio de recuperações expressas geralmente são disponibilizados dentro de um a cinco minutos.

  > **Note**
  >
  > As recuperações expressas são um recurso premium e são cobradas de acordo com a taxa de solicitação e recuperação expressas.
  > Para receber informações sobre a definição de preço do Amazon S3, consulte Definição de preço do Amazon S3.

  A capacidade provisionada ajuda a garantir que a capacidade de recuperação para recuperações expressas do S3 Glacier Flexible Retrieval esteja disponível quando você precisar dela. Para ter mais informações, consulte Capacidade provisionada.

- Padrão: acesse qualquer um dos objetos arquivados em algumas horas. Padrão é a opção assumida para solicitações de recuperação que não especificam a opção de recuperação.
  As recuperações padrão geralmente terminam em até 3 a 5 horas para objetos armazenados na classe de armazenamento S3 Glacier Flexible Retrieval ou no nível Archive Access do S3 Intelligent-Tiering. Normalmente, essas recuperações terminam em até 12 horas para objetos armazenados na classe de armazenamento S3 Glacier Deep Archive ou no nível S3 Intelligent-Tiering Deep Archive Access. As recuperações padrão são gratuitas para objetos armazenados na classe S3 Intelligent-Tiering.

  > **Note**
  >
  > - Para objetos armazenados na classe de armazenamento S3 Glacier Flexible Retrieval ou no nível S3 Intelligent-Tiering Archive Access, as recuperações padrão iniciadas por meio da operação de restauração de Operações em Lote do S3 normalmente se iniciam em minutos e terminam em três a cinco horas.
  > - Para objetos na classe de armazenamento S3 Glacier Deep Archive ou no nível S3 Intelligent-Tiering Deep Archive Access, as recuperações padrão iniciadas por meio da operação de restauração de Operações em Lote normalmente se iniciam em nove horas e terminam em doze horas.

- Em massa: acesse os dados usando a opção de recuperação de menor custo do Amazon S3 Glacier. Com as recuperações em massa, você pode recuperar grandes quantidades de dados por um baixo custo, até mesmo petabytes.

  Para objetos armazenados na classe de armazenamento S3 Glacier Flexible Retrieval ou no nível S3 Intelligent-Tiering Archive Access, as recuperações em massa normalmente terminam em cinco a doze horas. Para objetos armazenados na classe de armazenamento S3 Glacier Deep Archive ou no nível S3 Intelligent-Tiering Deep Archive Access, essas recuperações normalmente terminam em 48 horas.

  As recuperações em massa são gratuitas para objetos armazenados na classe de armazenamento S3 Glacier Flexible Retrieval ou S3 Intelligent-Tiering.

A tabela a seguir resume as opções de recuperação de arquivos. Para obter mais informações sobre preços, consulte Preços do Amazon S3.

Para fazer uma recuperação de `Expedited`, `Standard` ou `Bulk`, defina o elemento `Tier` da solicitação na solicitação da operação de API REST de RestoreObject que você deseja, ou o equivalente na AWS Command Line Interface (AWS CLI) ou em AWS SDKs. Se você adquiriu a capacidade provisionada, todas as recuperações expressas serão automaticamente fornecidas por meio de sua capacidade provisionada.

Capacidade provisionada

A capacidade provisionada ajuda a garantir que a capacidade de recuperação para recuperações aceleradas do S3 Glacier Flexible Retrieval esteja disponível quando você precisar. Cada unidade de capacidade garante que pelo menos três recuperações expressas possam ser realizadas a cada cinco minutos e fornece até 150 megabytes por segundo (MB/s) de throughput de recuperação.

Se a workload exigir acesso altamente confiável e previsível a um subconjunto de dados em minutos, considere adquirir a capacidade de recuperação provisionada. Sem capacidade provisionada, as recuperações expressas podem não ser aceitas durante períodos de alta demanda. Se precisar de acesso a recuperações expressas em qualquer circunstâncias, recomendamos que você compre a capacidade de recuperação provisionada.

As unidades de capacidade provisionada são alocadas a uma Conta da AWS. Portanto, o solicitante da recuperação rápida de dados deve comprar a unidade de capacidade provisionada, não o proprietário do bucket.

É possível comprar a capacidade provisionada usando o console do Amazon S3, o console do Amazon S3 Glacier, a operação Purchase Provisioned Capacity da API REST, os AWS SDKs ou a AWS CLI. Para obter informações sobre a definição de preços da capacidade provisionada, consulte Definição de preço do Amazon S3.

Taxas de solicitações de iniciação de restauração do S3 Glacier

Quando você inicia solicitações de restauração de objetos que estão armazenados nas classes de armazenamento S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive, uma cota de solicitações de recuperação é aplicada para sua Conta da AWS. O S3 Glacier comporta solicitações de restauração em uma taxa de até 1.000 transações por segundo. Se essa taxa for excedida, as solicitações consideradas válidas em outros aspectos terão a utilização controlada ou serão rejeitadas, e o Amazon S3 retornará um erro `ThrottlingException`.

Opcionalmente, você também pode usar o recurso Operações em Lote do S3 para recuperar um grande número de objetos armazenados nas classes S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive com uma única solicitação. Para ter mais informações, consulte Executar operações de objetos em massa com o Operações em Lote.

Restaurar um objeto arquivado

Os objetos do Amazon S3 nas seguintes classes ou níveis de armazenamento são arquivados e não podem ser acessados em tempo real:

- A classe de armazenamento S3 Glacier Flexible Retrieval
- A classe de armazenamento S3 Glacier Deep Archive
- O nível Acesso ao arquivamento do S3 Intelligent-Tiering
- O nível de acesso de arquivamento profundo do S3 Intelligent-Tiering

Os objetos do Amazon S3 armazenados nas classes de armazenamento S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive não são acessíveis imediatamente. Para acessar um objeto nessas classes de armazenamento, você deve restaurar uma cópia temporária dele no bucket do S3 para uma duração especificada (número de dias). Se você quiser uma cópia permanente do objeto, restaure o objeto e crie uma cópia dele no bucket do Amazon S3. O console do Amazon S3 não comporta a cópia de objetos restaurados. Para esse tipo de operação de cópia, use a AWS Command Line Interface (AWS CLI), AWS SDKs ou a API REST. A menos que você faça uma cópia e altere a classe de armazenamento, o objeto ainda será armazenado nas classes de armazenamento S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive. Para receber informações

sobre como usar essas classes de armazenamento, consulte Classes de armazenamento para objetos acessados raramente.

Para acessar objetos nos níveis S3 Intelligent-Tiering Archive Access e Deep Archive Access, você deve iniciar a solicitação de restauração e esperar até que o objeto seja movido para o nível Frequent Access para acessá-lo. Quando você restaura dos níveis Acesso de arquivamento ou Acesso de arquivamento profundo, o objeto faz a transição de volta para o nível Acesso frequente. Para receber informações sobre como usar essas classes de armazenamento, consulte Classe de armazenamento para otimizar automaticamente dados com padrões de acesso alterados ou desconhecidos.

Para receber informações gerais sobre objetos arquivados, consulte Trabalhando com objetos arquivados.

> **Note**
>
> - Ao restaurar um objeto arquivado das classes de armazenamento S3 Glacier Flexible Retrieval ou do S3 Glacier Deep Archive, você paga pelo objeto arquivado e pela cópia restaurada temporariamente.
> - Quando você restaura um objeto do S3 Intelligent-Tiering, não há cobranças para recuperações padrão ou em massa.
> - As solicitações de restauração subsequentes chamadas em objetos arquivados que já estão sendo restaurados são cobradas como uma solicitação `GET`. Para obter mais informações sobre preços, consulte Preços do Amazon S3.

Restaurar um objeto arquivado

Você pode restaurar um objeto arquivado usando o console do Amazon S3, a API REST do Amazon S3, os AWS SDKs, a AWS Command Line Interface (AWS CLI) ou o Operações em Lote do S3.

Uso do console do S3

Restaurar objetos usando o console do Amazon S3

Use o procedimento a seguir para restaurar um objeto que foi arquivado na classe de armazenamento S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive ou no nível de armazenamento S3 Intelligent-Tiering Archive Access ou Deep Archive Access.

Para restaurar um objeto arquivado

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets de uso geral.
3. Na lista de buckets, escolha o nome do bucket que contém os objetos que você deseja restaurar.
4. Na lista Objects (Objetos), selecione o objeto ou os objetos que você deseja restaurar, selecione Actions (Ações) e escolha Initiate restore (Iniciar restauração).
5. Se você estiver restaurando do S3 Glacier Flexible Retrieval ou do S3 Glacier Deep Archive, insira o número de dias em que deseja que seus dados arquivados fiquem acessíveis na caixa Número de dias em que a cópia restaurada fica disponível.
6. Em Nível de recuperação, siga um destes procedimentos:

   - Selecione Recuperação em massa ou Recuperação padrão e, depois, escolha Iniciar restauração.
   - Escolha Expedited retrieval (Recuperação acelerada) (disponível somente para o S3 Glacier Flexible Retrieval ou S3 Intelligent-Tiering Archive Access). Se você estiver restaurando um objeto no S3 Glacier Flexible Retrieval, poderá escolher se deseja comprar capacidade provisionada para recuperação expressa. Se quiser comprar capacidade provisionada, vá para a próxima etapa. Caso contrário, selecione Iniciar restauração.

   > **Note**
   >
   > Os objetos dos níveis S3 Intelligent-Tiering Archive Access e Deep Archive Access são restaurados automaticamente para o nível Frequent Access.

7. (Opcional) Se você estiver restaurando um objeto no S3 Glacier Flexible Retrieval e escolher Recuperação expressa, poderá escolher se deseja comprar capacidade provisionada. A capacidade provisionada só está disponível para objetos no S3 Glacier Flexible Retrieval. Se você tiver a capacidade provisionada, escolha Iniciar restauração para iniciar uma recuperação provisionada.

   Se você tiver a capacidade provisionada, todas as recuperações expressas serão atendidas pela capacidade provisionada. Para ter mais informações, consulte Capacidade provisionada.

- Se você não tiver a capacidade provisionada e não desejar comprá-la, selecione Iniciar restauração.
- Se você não tiver capacidade provisionada mas quiser comprar unidades de capacidade provisionada (PCUs), selecione Comprar PCUs. Na caixa de diálogo Comprar PCUs, escolha quantas PCUs você deseja comprar, confirme a compra e selecione Comprar PCUs. Ao receber a mensagem Compra realizada, selecione Iniciar restauração para iniciar a recuperação provisionada.

Uso do AWS CLI

Restaurar objetos do S3 Glacier Flexible Retrieval ou do S3 Glacier Deep Archive

O exemplo a seguir usa o comando `restore-object` para restaurar o objeto *`dir1/example.obj`* no bucket *`amzn-s3-demo-bucket`* por 25 dias.

```
aws s3api restore-object --bucket amzn-s3-demo-bucket --key dir1/example.obj --restore-request '{"Days":25,"GlacierJobParameters":{"Tier":"Standard"}}'
```

Se a sintaxe JSON usada no exemplo resultar em um erro em um cliente Windows, substitua a solicitação de restauração pela seguinte sintaxe:

```
--restore-request Days=25,GlacierJobParameters={"Tier"="Standard"}
```

Restaurar objetos do S3 Intelligent-Tiering Archive Access e Deep Archive Access

O exemplo a seguir usa o comando `restore-object` para restaurar o objeto *`dir1/example.obj`* no bucket *`amzn-s3-demo-bucket`* no nível Frequent Access.

```
aws s3api restore-object --bucket amzn-s3-demo-bucket --key dir1/example.obj --restore-request '{}'
```

> **Note**
>
> Ao contrário das classes de armazenamento S3 Glacier Flexible Retrieval e S3 Glacier Deep Archive, as solicitações de restauração para objetos S3 Intelligent-Tiering não aceitam o valor `Days`.

Monitorar o status da restauração

Para monitorar o status da solicitação `restore-object`, use o seguinte comando `head-object`:

```
aws s3api head-object --bucket amzn-s3-demo-bucket --key dir1/example.obj
```

Para obter mais informações, consulte restore-object na Referência de comandos da AWS CLI.

Uso da API REST

O Amazon S3 fornece uma operação de API para que você inicie a restauração de um objeto arquivado. Para obter mais informações, consulte RestoreObject na Referência da API do Amazon Simple Storage Service.

Uso dos SDKs da AWS

Consulte exemplos de como restaurar objetos arquivados no S3 Glacier Flexible Retrieval ou no S3 Glacier Deep Archive com os SDKs da AWS em Exemplos de código na Referência de API do Amazon S3.

Usar o Operações em Lote do S3

Para restaurar mais de um objeto arquivado com uma única solicitação, você pode usar o Operações em Lote do S3. Você fornece às operações em lote do S3 uma lista de objetos nos quais operar. O S3 Batch Operations chama a respectiva operação de API para executar a operação especificada. Um único trabalho de operações em lote pode realizar a operação especificada em bilhões de objetos contendo exabytes de dados.

Para criar um trabalho de operações em lote, você deve ter um manifesto que contenha somente os objetos a serem restaurados. Você pode criar um manifesto usando o Inventário S3 ou fornecer um arquivo CSV com as informações necessárias. Para ter mais informações, consulte the section called “Especificar um manifesto”.

Antes de criar e executar trabalhos de operações em lote no S3, você deve conceder permissões ao Amazon S3 para realizar essas operações em seu nome. Para ver as permissões necessárias, consulte the section called “Conceder permissões”.

> **Note**
>
> Os trabalhos de operações em lote podem operar em objetos das classes de armazenamento S3 Glacier Flexible Retrieval e S3 Glacier Deep Archive ou em objetos

dos níveis S3 Intelligent-Tiering Archive Access e Deep Archive Access. As operações em lote não podem operar nos dois tipos de objetos arquivados no mesmo trabalho. Para restaurar objetos de ambos os tipos, você deve criar trabalhos de Operações em lote separados.
Para receber mais informações sobre o uso de operações em lote para restauração de objetos de arquivo, consulte the section called “Restaurar objetos”.

Como criar um trabalho de operações em lote de iniciar restauração no S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação esquerdo, escolha Batch Operations (Operações em lote).
3. Escolha Criar trabalho.
4. Para Região da AWS, escolha a região onde você deseja criar o trabalho.
5. Em Formato do manifesto, selecione o tipo de manifesto a ser usado.
   - Se você escolher Relatório de inventário do S3, insira o caminho para o objeto `manifest.json` que o Amazon S3 gerou como parte do relatório de inventário em formato CSV. Se você quiser usar uma versão de manifesto que não seja a mais recente, insira o ID da versão do objeto `manifest.json`.
   - Se você selecionar CSV, insira o caminho para o objeto do manifesto formatado em CSV. O objeto do manifesto deve seguir o formato descrito no console. Se você quiser usar outra versão que não seja a mais recente, poderá incluir o ID da versão do objeto de manifesto.
6. Escolha Próximo.
7. Na seção Operação, escolha Restaurar.
8. Na seção Restaurar, em Restaurar origem, selecione Glacier Flexible Retrieval ou Glacier Deep Archive ou Nível Intelligent-Tiering Archive Access ou Deep Archive Access.

   Se você escolheu Glacier Flexible Retrieval ou Glacier Deep Archive, insira um número para Número de dias em que a cópia restaurada fica disponível.

   Em Nível de recuperação, selecione o nível que você deseja usar.
9. Escolha Próximo.
10.

Na página Configurar opções adicionais, preencha as seguintes seções:

- Na seção Opções adicionais, forneça uma descrição para o trabalho e especifique um número de prioridade para ele. Números maiores indicam uma prioridade mais alta. Para ter mais informações, consulte the section called “Atribuir prioridade aos trabalhos”.
- Na seção Relatório de conclusão, selecione se as operações em lote devem criar um relatório de conclusão. Para receber mais informações sobre relatórios de conclusão, consulte the section called “Relatórios de conclusão”.
- Na seção Permissões, você deve conceder permissões ao Amazon S3 para realizar operações em lote em seu nome. Para ver as permissões necessárias, consulte the section called “Conceder permissões”.
- (Opcional) Na seção Tags de trabalho, adicione tags em pares de chave-valor. Para ter mais informações, consulte the section called “Usar tags”.

Quando terminar, escolha Próximo.

11. Na página Review (Examinar), verifique as configurações. Se precisar fazer alterações, escolha Previous (Anterior). Caso contrário, selecione Criar trabalho.

Para receber mais informações sobre operações em lote, consulte Restaurar objetos com operações em lote e Criar um trabalho de operações em lote do S3.

Verificar o status de restauração e a data de expiração

Você pode verificar o status de uma solicitação de restauração ou a data de expiração usando o console do Amazon S3, as Notificações de eventos do Amazon S3, a AWS CLI ou a API REST do Amazon S3.

> **Note**
>
> Os objetos restaurados das classes de armazenamento S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive são armazenados apenas pelo número de dias que você especificar. Os procedimentos abaixo retornarão a data de expiração dessas cópias.
> Os objetos restaurados dos níveis de armazenamento S3 Intelligent-Tiering Archive Access e Deep Archive Access não têm datas de expiração e, em vez disso, são movidos para o nível Frequent Access.

Uso do console do S3

Como conferir o status de restauração e a data de validade de um objeto no console do Amazon S3

1. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets de uso geral.
3. Na lista de buckets, selecione o nome do bucket que contém os objetos que você está restaurando.
4. Na lista Objetos, selecione o objeto que você está restaurando. A página de detalhes do objeto é exibida.

    - Se a restauração não estiver concluída, você verá uma seção que indica Restauração em andamento na parte superior da página.
    - Se a restauração estiver concluída, você verá uma seção que indica Restauração concluída na parte superior da página. Se você estiver restaurando por meio do S3 Glacier Flexible Retrieval ou do S3 Glacier Deep Archive, essa seção também exibirá a Data de expiração da restauração. O Amazon S3 removerá a cópia restaurada do objeto arquivado nessa data.

Usar Notificações de eventos do Amazon S3

Você pode receber notificações sobre a conclusão da restauração de um objeto usando a ação `s3:ObjectRestore:Completed` com o recurso Notificações de eventos do Amazon S3. Para obter mais informações sobre como habilitar notificações de eventos, consulte Usar o Amazon SQS, o Amazon SNS e o AWS Lambda. Para obter mais informações sobre os vários tipos de evento `ObjectRestore`, consulte the section called “Tipos de evento compatíveis com SQS, SNS e Lambda”.

Uso do AWS CLI

Confira o status de restauração e a data de validade de um objeto com a AWS CLI.

O exemplo a seguir usa o comando `head-object` para visualizar metadados referentes ao objeto *`dir1/example.obj`* no bucket *`amzn-s3-demo-bucket`*. Quando você executa esse comando em um objeto que está sendo restaurado, o Amazon S3 retorna se a restauração está em andamento e (se aplicável) a data de validade.

```
aws s3api head-object --bucket amzn-s3-demo-bucket --key dir1/example.obj
```

Saída esperada (restauração em andamento):

```
{
    "Restore": "ongoing-request=\"true\"",
    "LastModified": "2020-06-16T21:55:22+00:00",
    "ContentLength": 405,
    "ETag": "\"b662d79adeb7c8d787ea7eafb9ef6207\"",
    "VersionId": "wbYaE2vtOV0iIBXrOqGAJt3fP1cHB8Wi",
    "ContentType": "binary/octet-stream",
    "ServerSideEncryption": "AES256",
    "Metadata": {},
    "StorageClass": "GLACIER"
}
```

Saída esperada (restauração concluída):

```
{
    "Restore": "ongoing-request=\"false\", expiry-date=\"Wed, 12 Aug 2020 00:00:00 GMT
\"",
    "LastModified": "2020-06-16T21:55:22+00:00",
    "ContentLength": 405,
    "ETag": "\"b662d79adeb7c8d787ea7eafb9ef6207\"",
    "VersionId": "wbYaE2vtOV0iIBXrOqGAJt3fP1cHB8Wi",
    "ContentType": "binary/octet-stream",
    "ServerSideEncryption": "AES256",
    "Metadata": {},
    "StorageClass": "GLACIER"
}
```

Para obter mais informações sobre `head-object`, consulte head-object na Referência de comandos da AWS CLI.

Uso da API REST

O Amazon S3 fornece uma operação de API para você recuperar metadados do objeto. Para conferir o status da restauração e a data de validade de um objeto arquivado usando a API REST, consulte HeadObject na Referência da API do Amazon Simple Storage Service.

Atualizar a velocidade de uma restauração em andamento

Atualize a velocidade da restauração enquanto ela está em andamento.

Para atualizar uma restauração em andamento para um nível mais rápido

1. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets.
3. Na lista Buckets, escolha o nome do bucket que contém os objetos que você deseja restaurar.
4. Na lista Objetos, selecione o objeto que você está restaurando. A página de detalhes do objeto é exibida. Na página de detalhes do objeto, selecione Fazer upgrade do nível de recuperação. Para obter informações sobre como verificar o status de restauração de um objeto, consulte Verificar o status de restauração e a data de expiração.
5. Escolha o nível para o qual você deseja atualizar e selecione Iniciar restauração.

Gerenciar o ciclo de vida dos objetos

O Ciclo de Vida do S3 ajuda você a armazenar objetos de forma econômica durante todo o respectivo ciclo de vida deles ao fazer a transição para classes de armazenamento de menor custo ou excluir objetos expirados em seu nome. Para gerenciar o ciclo de vida dos objetos, crie uma configuração do Ciclo de Vida do S3 para o bucket. Uma configuração do Amazon S3 Lifecycle é um conjunto de regras que define as ações aplicadas pelo Amazon S3 a um grupo de objetos. Existem dois tipos de ações:

- Ações de transição: estas ações definem quando os objetos fazem a transição para outra classe de armazenamento. Por exemplo, você pode optar por fazer a transição de objetos para a classe de armazenamento S3 Standard – IA 30 dias após a criação deles ou arquivar objetos para a classe de armazenamento do S3 Glacier Flexible Retrieval um ano após a sua criação. Para obter mais informações, consulte Compreender e gerenciar classes de armazenamento do Amazon S3.

  Há custos associados a solicitações de transição do ciclo de vida. Para obter informações sobre a definição de preços, consulte Definição de preços do Amazon S3.
- Ações de validade: estas ações definem quando os objetos perdem a validade. O Amazon S3 exclui os objetos expirados em seu nome. Por exemplo, você pode optar por expirar os objetos armazenados após um período de conformidade regulamentar. Para obter mais informações, consulte Expirando objetos.

  Há possíveis custos associados à validade do ciclo de vida somente quando você encerra objetos em uma classe de armazenamento com uma duração mínima de armazenamento. Para obter mais informações, consulte Cobrança da duração mínima de armazenamento.

> **Important**
>
> Buckets de uso geral: você não pode usar uma política de bucket para evitar exclusões ou transições por meio de uma regra da funcionalidade Ciclo de Vida do S3. Por exemplo, mesmo que a política de bucket negue todas as ações para todas as entidades principais, a configuração do ciclo de vida do S3 ainda funcionará normalmente.

Objetos existentes e novos

Quando você adiciona uma configuração do ciclo de vida a um bucket, as regras de configuração se aplicam aos objetos existentes e aos objetos que serão adicionados no futuro. Por exemplo, se você adicionar uma regra de configuração da funcionalidade Ciclo de Vida hoje com uma ação de expiração que faz com que os objetos expirem 30 dias após sua criação, o Amazon S3 organizará para exclusão todos os objetos existentes com mais de 30 dias.

Alterações no faturamento

Se houver algum atraso entre quando um objeto se tornar elegível para uma ação de ciclo de vida e quando o Amazon S3 transferir ou expirar seu objeto, as alterações de faturamento serão aplicadas assim que o objeto se tornar qualificado para a ação de ciclo de vida. Por exemplo, se um objeto estiver programado para perder a validade e o Amazon S3 não o descontinuar imediatamente, você não receberá cobrança pelo armazenamento após o fim da validade.

A única exceção a esse comportamento é se você tiver uma regra de ciclo de vida para a classe de armazenamento S3 Intelligent-Tiering. Nesse caso, as alterações no faturamento não acontecerão até que o objeto tenha feito a transição para o S3 Intelligent-Tiering. Para obter mais informações sobre regras do Amazon S3 Lifecycle, consulte Elementos de configuração do ciclo de vida.

> **Note**
>
> Não há nenhuma cobrança de recuperação de dados para transições de ciclo de vida. No entanto, há cobranças de ingestão por solicitação ao usar regras de `PUT`, `COPY` ou ciclo de vida para transferir dados a qualquer classe de armazenamento do S3. Considere o custo de ingestão ou transição antes de transferir objetos a qualquer classe de armazenamento. Para obter mais informações sobre considerações de custo, consulte Definição de preço do Amazon S3.

Monitorar o efeito de regras de ciclo de vida

Para monitorar o efeito das atualizações feitas pelas regras de ciclo de vida ativas, consulte the section called “Como monitorar as ações realizadas pelas minhas regras de ciclo de vida?”.

Gerenciar o ciclo de vida completo dos objetos

Com as regras de configuração de ciclo de vida do S3, é possível solicitar que o Amazon S3 faça a transição de objetos para classes de armazenamento menos caras, arquive-os ou os exclua. Por exemplo:

- Se você fizer upload periódico de logs em um bucket, é possível que seu aplicativo precise deles por uma semana ou um mês. Depois disso, você pode excluí-los.
- Alguns documentos são acessados frequentemente por um período limitado. Depois disso, eles serão acessados com pouca frequência. Em algum ponto, você pode não precisar de acesso em tempo real a esses objetos, mas sua organização ou as regulamentações podem exigir que você os arquive por um período específico. Depois disso, é possível excluí-los.
- É possível fazer upload de alguns tipos de dados no Amazon S3 para fins de arquivamento. Por exemplo, é possível arquivar mídias digitais, registros financeiros e prontuários médicos, dados não processados de sequência genômica, backups de banco de dados de longo prazo e dados que devem ser retidos para conformidade regulatória.

Ao combinar ações do ciclo de vida do S3 para gerenciar o ciclo de vida completo de um objeto. Por exemplo, suponha que os objetos criados tenham um ciclo de vida bem definido. No início, os objetos são acessados com frequência em um período de 30 dias. Depois disso, eles são acessados com pouca frequência por 90 dias. Depois desse período, eles não são mais necessário. Portanto, é possível optar por arquivá-los ou excluí-los.

Nesse cenário, você pode criar uma regra do S3 Lifecycle especificando a ação de transição inicial para armazenamento S3 Intelligent-Tiering, S3 Standard – IA ou S3 One Zone – IA, outra ação de transição para o armazenamento S3 Glacier Flexible Retrieval para arquivamento e uma ação de expiração. Ao mover objetos de uma classe de armazenamento para outra, você evita os custos de armazenamento. Para obter mais informações sobre considerações de custo, consulte Definição de preço do Amazon S3.

Tópicos

- Transição de objetos usando o Amazon S3 Lifecycle
- Expirando objetos

- Definir uma configuração do Ciclo de Vida do S3 em um bucket
- Como o Ciclo de Vida do S3 interage com outras configurações de bucket
- Configurar notificações de evento do Ciclo de Vida do S3
- Elementos de configuração do ciclo de vida
- Como o Amazon S3 lida com conflitos nas configurações do ciclo de vida
- Exemplos de configurações do Ciclo de Vida do S3
- Solucionar problemas de ciclo de vida do Amazon S3

Transição de objetos usando o Amazon S3 Lifecycle

É possível adicionar ações de transição a uma configuração do Ciclo de Vida do S3 para solicitar que o Amazon S3 mova objetos para outra classe de armazenamento do Amazon S3. Para obter mais informações sobre classes de armazenamento, consulte Compreender e gerenciar classes de armazenamento do Amazon S3. Alguns exemplos de quando você pode usar as configurações do ciclo de vida do S3 dessa maneira incluem:

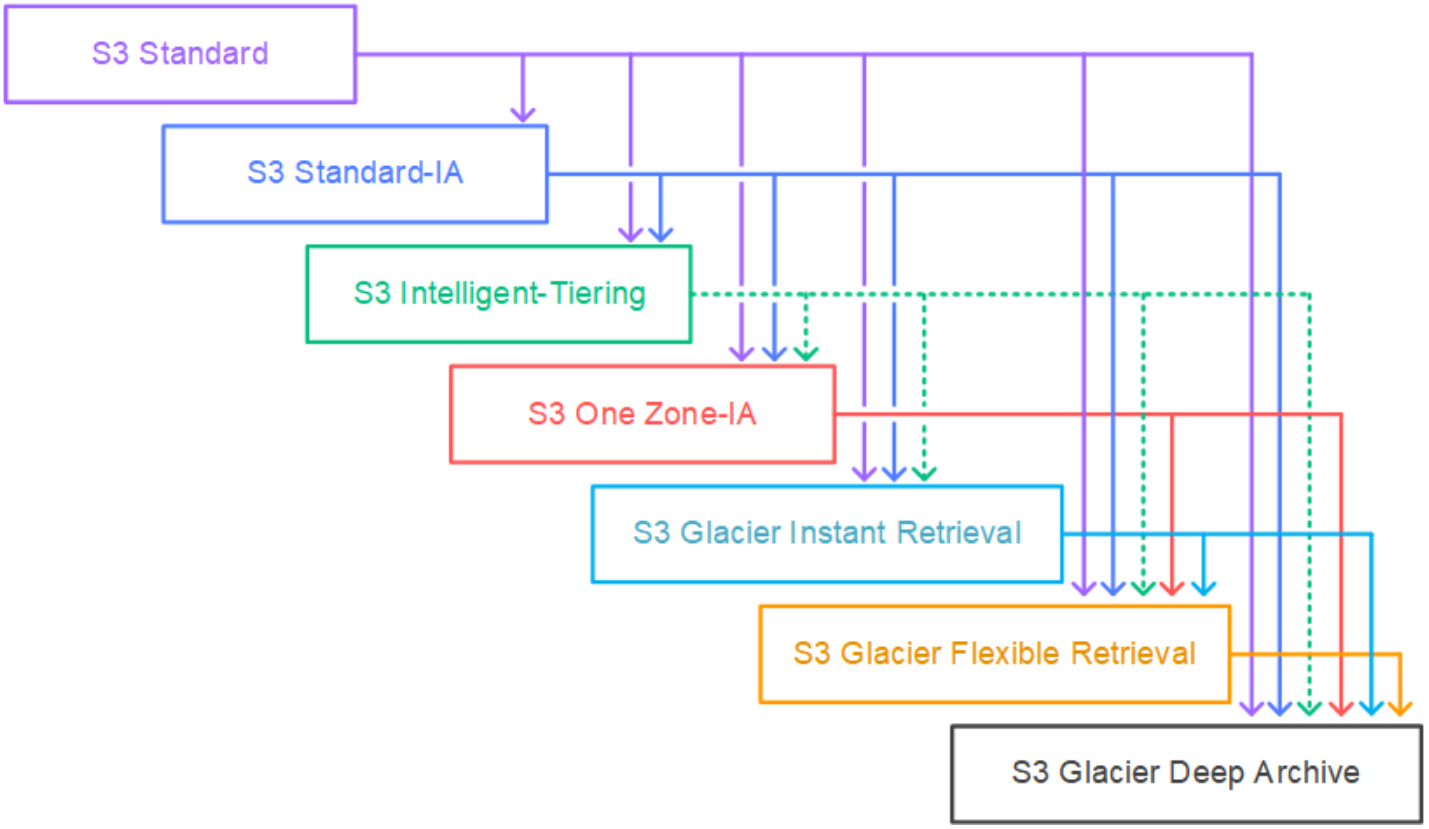
- Quando você sabe que os objetos são acessados com pouca frequência, você pode fazer a transição para a classe de armazenamento S3 Standard – IA.
- Convém arquivar objetos que não precisam de acesso em tempo real às classes de armazenamento S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive.

> **Note**
>
> Os objetos criptografados permanecem criptografados durante todo o processo de transição da classe de armazenamento.

Transições aceitas

Em uma configuração do S3 Lifecycle, você pode definir regras para fazer a transição de objetos de uma classe de armazenamento para outra a fim de economizar custos de armazenamento. Quando você desconhece os padrões de acesso dos objetos ou os padrões de acesso mudam com o passar do tempo, é possível fazer a transição para os objetos para a classe de armazenamento S3 Intelligent-Tiering para economizar automaticamente. Para obter informações sobre classes de armazenamento, consulte Compreender e gerenciar classes de armazenamento do Amazon S3.

O Amazon S3 da suporte a um modelo de cachoeira para fazer a transição entre classes de armazenamento, conforme mostrado no diagrama a seguir.



Transições de ciclo de vida com suporte

O Amazon S3 oferece suporte às seguintes transições do ciclo de vida entre as classes de armazenamento usando uma configuração do ciclo de vida do S3.

- Da classe de armazenamento S3 Standard para as classes S3 Standard-IA, S3 Intelligent-Tiering, S3 One Zone-IA, S3 Glacier Instant Retrieval, S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive.
- Da classe de armazenamento S3 Standard-IA para S3 Intelligent-Tiering, S3 One Zone-IA, S3 Glacier Instant Retrieval, S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive.
- A classe de armazenamento S3 Intelligent-Tiering pode fazer a transição para diferentes classes de armazenamento dependendo do nível de acesso da classe S3 Intelligent-Tiering. As transições a seguir são possíveis para cada nível de acesso.
  - Níveis Frequent Access ou Infrequent Access para as classes de armazenamento S3 One Zone-IA, S3 Glacier Instant Retrieval, S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive.

  - Nível Archive Instant Access para as classes de armazenamento S3 Glacier Instant Retrieval, S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive.
  - Nível Archive Access para as classes de armazenamento S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive.
  - Nível Deep Archive Access para as classes de armazenamento S3 Glacier Deep Archive.
- Da classe de armazenamento S3 One Zone-IA para S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive.
- Da classe de armazenamento S3 Glacier Instant Retrieval para S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive.
- A classe de armazenamento S3 Glacier Flexible Retrieval para a classe de armazenamento S3 Glacier Deep Archive.

> **Note**
>
> Para buckets com versionamento habilitado ou suspenso, é possível fazer a transição de objetos com status de replicação `Pending`.

Restrições e considerações relativas a transições

As transições da classe de armazenamento do ciclo de vida têm as seguintes restrições:

Por padrão, objetos com menos de 128 KB não farão a transição para nenhuma classe de armazenamento

O Amazon S3 aplica um comportamento padrão às configurações de ciclo de vida do S3 que não permite a transferência de objetos com menos de 128 KB para nenhuma classe de armazenamento. Não recomendamos fazer a transição de objetos com menos de 128 KB porque é cobrada uma taxa de solicitação de transição para cada objeto. Isso significa que, para objetos menores, os custos de transição podem exceder as economias obtidas com o armazenamento. Para ter mais informações sobre os custos de solicitação de transição, consulte Solicitações e recuperações de dados na guia Armazenamento e solicitações da página Definição de preço do Amazon S3.

Para permitir a transição de objetos menores, é possível adicionar um filtro de tamanho de objeto às suas regras de transição de ciclo de vida que especifique um tamanho mínimo (`ObjectSizeGreaterThan`) ou máximo (`ObjectSizeLessThan`) personalizado. Para obter mais informações, consulte Exemplo: permitir que objetos com menos de 128 KB sejam transferidos.

> **Note**
>
> Em setembro de 2024, o Amazon S3 atualizou o comportamento de transição padrão para objetos pequenos, da seguinte forma:
>
> - Comportamento de transição padrão atualizado: desde setembro de 2024, o comportamento padrão não permite a transferência de objetos com menos de 128 KB para nenhuma classe de armazenamento.
> - Comportamento de transição padrão anterior: antes de setembro de 2024, o comportamento padrão permitia que objetos com menos de 128 KB fossem transferidos somente para as classes de armazenamento S3 Glacier e S3 Glacier Deep Archive.
>
> As configurações criadas antes de setembro de 2024 retêm o comportamento de transição anterior, a menos que você as modifique. Ou seja, se você criar, editar ou excluir regras, o comportamento de transição padrão da configuração mudará para o comportamento atualizado. Se seu caso de uso exigir, será possível alterar o comportamento de transição padrão para que objetos com menos de 128 KB façam a transição para o S3 Glacier e o S3 Glacier Deep Archive. Para isso, use o cabeçalho `x-amz-transition-default-minimum-object-size` opcional em uma solicitação PutBucketLifecycleConfiguration.

Os objetos devem ser armazenados pelo menos 30 dias antes de fazer a transição para S3 Standard-IA ou S3 One Zone-IA.

Antes de fazer a transição de objetos para S3 Standard-IA ou S3 One Zone-IA, é necessário armazená-los pelo menos 30 dias no Amazon S3. Por exemplo, você não pode criar uma regra de ciclo de vida para fazer a transição de objetos para a classe de armazenamento S3 Standard – IA um dia depois de criá-los. O Amazon S3 não faz essa transição nos primeiros 30 dias porque os objetos mais recentes geralmente são acessados com mais frequência ou excluídos mais cedo do que o adequado para o armazenamento S3 Standard-IA ou S3 One Zone-IA.

Da mesma forma, se você estiver fazendo a transição de objetos não atuais (em buckets com versões), poderá fazer a transição somente de objetos que não são atuais pelo menos 30 dias para armazenamento S3 Standard – IA ou S3 One Zone – IA. Para obter uma lista da duração mínima de armazenamento para todas as classes de armazenamento, consulte Comparar as classes de armazenamento do Amazon S3.

Você incorrerá em cobrança se fizer a transição antes da duração mínima de armazenamento dos objetos

Algumas classes de armazenamento têm uma duração mínima de armazenamento de objetos. Se você fizer a transição de objetos dessas classes de armazenamento antes da duração mínima, receberá uma cobrança referente ao restante dessa duração. Para ter mais informações sobre quais classes de armazenamento têm durações mínimas de armazenamento, consulte Comparar as classes de armazenamento do Amazon S3.

Não é possível criar uma única regra de ciclo de vida que transfira objetos de uma classe de armazenamento para outra antes do término do período mínimo de duração do armazenamento.

Por exemplo, o S3 Glacier Instant Retrieval tem uma duração mínima de armazenamento de noventa dias. Não é possível especificar uma regra de ciclo de vida que transfira objetos para o S3 Glacier Instant Retrieval após quatro dias e, em seguida, transfira objetos para o S3 Glacier Deep Archive após vinte dias. Nesse caso, a transição do S3 Glacier Deep Archive deve ocorrer após pelo menos 94 dias.

É possível especificar duas regras para realizar isso, mas é necessário arcar com as cobranças de duração mínima de armazenamento. Para obter mais informações sobre considerações de custo, consulte Definição de preço do Amazon S3.

Para ter mais informações sobre a criação de um ciclo de vida do S3, consulte Definir uma configuração do Ciclo de Vida do S3 em um bucket.

Transição para as classes de armazenamento S3 Glacier Flexible Retrieval e S3 Glacier Deep Archive (arquivamento de objetos)

Usando a configuração do S3 Lifecycle, você pode fazer a transição de objetos para as classes de armazenamento S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive para arquivamento.

Para que você arquive objetos, reveja as seguintes seções para considerações relevantes.

Considerações gerais

Veja a seguir as considerações gerais que você deve fazer antes de arquivar objetos:

- Os objetos criptografados permanecem criptografados durante todo o processo de transição da classe de armazenamento.
- Os objetos armazenados nas classes de armazenamento S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive não estão disponíveis em tempo real.

Os objetos arquivados são objetos do Amazon S3, mas para acessar um objeto arquivado, primeiro você deve restaurar uma cópia temporária dele. A cópia restaurada do objeto fica disponível somente pelo tempo que você especifica na solicitação de restauração. Depois disso, o Amazon S3 exclui a cópia temporária e o objeto permanece arquivado no S3 Glacier Flexible Retrieval.

Você pode restaurar um objeto usando o console do Amazon S3 ou, programaticamente, usando bibliotecas wrapper dos AWS SDKs ou a API REST do Amazon S3 em seu código. Para obter mais informações, consulte Restaurar um objeto arquivado.

- Os objetos armazenados na classe de armazenamento S3 Glacier Flexible Retrieval só podem ser transferidos para a classe de armazenamento S3 Glacier Deep Archive.

  Você pode usar uma regra de configuração do S3 Lifecycle somente para converter a classe de armazenamento de um objeto do S3 Glacier Flexible Retrieval para a classe de armazenamento S3 Glacier Deep Archive. Se quiser alterar a classe de armazenamento de um objeto armazenado no S3 Glacier Flexible Retrieval para uma classe de armazenamento diferente do S3 Glacier Deep Archive, use a operação de restauração para fazer uma cópia temporária do objeto primeiro. Depois, use a operação de cópia para substituir o objeto especificando S3 Standard, S3 Intelligent-Tiering, S3 Standard – IA, S3 One Zone – IA ou Reduced Redundancy como a classe de armazenamento.

- A transição de objetos para a classe de armazenamento S3 Glacier Deep Archive é apenas unidirecional.

  Não é possível usar uma regra de configuração do S3 Lifecycle para converter a classe de armazenamento de um objeto do S3 Glacier Deep Archive para qualquer outra classe de armazenamento. Se você quiser mudar a classe de armazenamento de um objeto arquivado em outra classe de armazenamento, deverá usar a operação de restauração para fazer primeiro uma cópia temporária do objeto. Depois, use a operação de cópia para substituir o objeto especificando S3 Standard, S3 Intelligent-Tiering, S3 Standard – IA, S3 One Zone – IA, S3 Glacier Instant Retrieval, S3 Glacier Flexible Retrieval ou armazenamento de redundância reduzida como a classe de armazenamento.

> **Note**
>
> A aplicação da operação Copy a objetos restaurados não é permitida no console do Amazon S3 em objetos nas classes de armazenamento S3 Glacier Flexible Retrieval ou

S3 Glacier Deep Archive. Para esse tipo de operação de cópia, use a AWS Command Line Interface(AWS CLI), AWS SDKs ou a API REST.

Os objetos armazenados nas classes de armazenamento S3 Glacier Flexible Retrieval e S3 Glacier Deep Archive são visíveis e ficam disponíveis somente por meio do Amazon S3. Eles não estão disponíveis por meio do serviço separado do Amazon S3 Glacier.

Esses são objetos do Amazon S3 e você só pode acessá-los usando o console do Amazon S3 ou a API do Amazon S3. Você não pode acessar os objetos arquivados por meio do console separado do Amazon S3 Glacier ou da API do Amazon S3 Glacier.

Considerações sobre custos

Se você estiver planejando arquivar dados acessados com pouca frequência por um período de meses ou anos, as classes de armazenamento S3 Glacier Flexible Retrieval e S3 Glacier Deep Archive podem reduzir seus custos de armazenamento. No entanto, para garantir que a classe de armazenamento S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive seja apropriada para você, considere o seguinte:

- Cobranças extras de armazenamento: quando você faz a transição de objetos para a classe de armazenamento S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive, uma quantidade fixa de armazenamento é adicionada a cada objeto para acomodar metadados para gerenciar o objeto.
  - Para cada objeto arquivado no S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive, o Amazon S3 usa 8 KB de armazenamento para o nome do objeto e outros metadados. O Amazon S3 armazena esses metadados de modo que você possa obter uma lista em tempo real de seus objetos arquivados usando a API do Amazon S3. Para obter mais informações, consulte GET bucket (listar objetos). Você é cobrado conforme as taxas do S3 Standard nesse armazenamento adicional.
  - Para cada objeto arquivado no S3 Glacier Flexible Retrieval ou no S3 Glacier Deep Archive, o Amazon S3 adiciona 32 KB de armazenamento para indexação e metadados relacionados. Esses dados adicionais são necessários para identificar e recuperar seu objeto. As taxas do S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive são cobradas por esse armazenamento adicional.

Se você estiver arquivando objetos pequenos, considere esses encargos de armazenamento. Considere também a possibilidade de agregar vários objetos pequenos em um número menor de objetos grandes para reduzir os gastos adicionais.

- Número de dias que você pretende manter objetos arquivados: o S3 Glacier Flexible Retrieval e o S3 Glacier Deep Archive são soluções de arquivamento de longo prazo. O período mínimo de duração de armazenamento é de 90 dias para a classe de armazenamento S3 Glacier Flexible Retrieval e 180 dias para o S3 Glacier Deep Archive. A exclusão de dados arquivados no Amazon S3 Glacier não incorrerá em cobrança se os objetos que você excluir estiverem arquivados por mais do que o período mínimo de duração do armazenamento. Se você excluir ou substituir um objeto arquivado dentro do período mínimo de duração do arquivamento, o Amazon S3 cobrará uma taxa pro rata pela exclusão antecipada. Para obter informações sobre a taxa de exclusão antecipada, consulte a pergunta “Como é a cobrança pela exclusão de objetos do Amazon S3 Glacier com menos de 90 dias? de arquivamento?” nas Perguntas frequentes sobre o Amazon S3.
- Cobranças de solicitações de transição do S3 Glacier Flexible Retrieval e do S3 Glacier Deep Archive: cada objeto que você transitar para a classe de armazenamento S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive constitui uma solicitação de transição. Há um custo para cada solicitação desse tipo. Se você pretende fazer a transição de um grande número de objetos, considere os custos de solicitação. Se você estiver arquivando uma mistura de objetos que inclui objetos pequenos, especialmente objetos com menos de 128 KB, recomendamos usar o filtro de tamanho do objeto do ciclo de vida para remover objetos pequenos da transição e reduzir os custos da solicitação.
- Cobranças de restauração de dados do S3 Glacier Flexible Retrieval e S3 Glacier Deep Archive: o S3 Glacier Flexible Retrieval e o S3 Glacier Deep Archive foram projetados para arquivamento de dados de longo prazo que você acessa com pouca frequência. Para obter informações sobre cobranças de restauração de dados, consulte a pergunta “Quanto custa recuperar dados do Amazon S3 Glacier?”. nas Perguntas frequentes sobre o Amazon S3. Para obter informações sobre como restaurar dados do Amazon S3 Glacier, consulte Restaurar um objeto arquivado.

> **Note**
>
> O Ciclo de Vida do S3 faz a transição de objetos para o S3 Glacier Flexible Retrieval e o S3 Glacier Deep Archive de forma assíncrona. Pode haver um atraso entre a data de transição na regra de configuração do S3 Lifecycle e a data de transição física. Nesse caso, você

recebe a cobrança da taxa padrão da classe de armazenamento da qual fez a transição com base na data de transição especificada na regra.

A página de detalhes de produto do Amazon S3 fornece informações sobre preços e exemplos de cálculo para arquivamento de objetos no Amazon S3. Para obter mais informações, consulte os tópicos a seguir:

- “Como é calculada a cobrança do armazenamento de objetos do Amazon S3 arquivados no Amazon S3 Glacier?” nas Perguntas frequentes sobre o Amazon S3.
- “Como é feita a cobrança pela exclusão de objetos do Amazon S3 Glacier com menos de 90 dias de arquivamento?” nas Perguntas frequentes sobre o Amazon S3.
- “Quanto custa a recuperação de dados do Amazon S3 Glacier?” nas Perguntas frequentes sobre o Amazon S3.
- Definição de preço do Amazon S3 para custos de armazenamento das diferentes classes de armazenamento.

Restaurar objetos arquivados

Os objetos arquivados não podem ser acessados em tempo real. Primeiro inicie uma solicitação de restauração e, em seguida, aguarde até que uma cópia temporária do objeto esteja disponível pelo tempo que você especificar na solicitação. Depois de receber uma cópia temporária do objeto restaurado, a classe de armazenamento do objeto continuará sendo S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive. (Uma solicitação de operação de API HeadObject ou GetObject retornará o S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive como a classe de armazenamento.)

> **Note**
>
> Ao restaurar um arquivamento, você paga pelo arquivamento (taxa de S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive) e por uma cópia restaurada temporariamente (taxa de armazenamento de S3 Standard). Para obter mais informações sobre definição de preços, consulte Definição de preços do Amazon S3.

Você pode restaurar uma cópia do objeto programaticamente ou usando o console do Amazon S3. O Amazon S3 só processa uma solicitação de restauração por vez por objeto. Para obter mais informações, consulte Restaurar um objeto arquivado.

Expirando objetos

É possível adicionar ações de transição a uma configuração do Ciclo de Vida do S3 para solicitar que o Amazon S3 exclua objetos no final de sua vida útil. Quando um objeto atinge o fim de seu ciclo de vida, com base na respectiva configuração de ciclo de vida, o Amazon S3 realiza uma ação `Expiration` de acordo com o estado do Versionamento do S3 no qual o bucket está:

- Bucket sem versionamento: o Amazon S3 coloca o objeto em uma fila para remoção e o remove de maneira assíncrona, eliminando-o permanentemente.
- Bucket com versionamento habilitado: se a versão atual do objeto não for um marcador de exclusão, o Amazon S3 adicionará um com um ID exclusivo de versão. Isso torna a versão atual desatualizada, e o marcador de exclusão se torna a versão atual.
- Bucket com versionamento suspenso: o Amazon S3 cria um marcador de exclusão com ID de versão nulo. Esse marcador de exclusão substitui qualquer versão de objeto por um ID de versão nulo na hierarquia de versões, que exclui o objeto.

Para um bucket com versionamento (ou seja, versionamento habilitado ou suspenso), há várias considerações que orientam como o Amazon S3 trata a ação `Expiration`. Para buckets com versionamento habilitado ou suspenso, o seguinte se aplica:

- A expiração do objeto se aplica somente à versão atual de um objeto (não afeta versões desatualizadas de objetos).
- O Amazon S3 não realizará ações se houver uma ou mais versões de objeto e se o marcador de exclusão estiver na versão atual.
- Se a versão atual do objeto for a única versão do objeto e também houver um marcador de exclusão (também chamado de marcador de exclusão de objeto expirado, onde todas as versões do objeto são excluídas e você tem somente um marcador de exclusão restante), o Amazon S3 removerá o marcador de exclusão de objeto expirado. Você também pode usar a ação `Expiration` para instruir o Amazon S3 a remover os marcadores de exclusão do objeto expirado. Por exemplo, consulte Remover marcadores de exclusão de objetos expirados em um bucket com versionamento habilitado.
- Você pode usar o elemento de ação `NoncurrentVersionExpiration` para instruir o Amazon S3 a excluir permanentemente versões de objetos desatualizadas. Esses objetos excluídos não podem ser recuperados. Esse prazo de validade pode se basear em determinado número de dias desde o momento em que os objetos se tornam desatualizados. Além do número de dias, você também pode fornecer um número máximo de versões desatualizadas que devem ser

retidas (entre 1 e 100). Esse valor especifica quantas versões desatualizadas mais recentes devem existir antes que o Amazon S3 possa executar a ação associada em uma determinada versão. Para especificar o número máximo de versões não atuais, também é necessário fornecer um elemento `Filter`. Se não especificar um elemento `Filter`, o Amazon S3 gerará um erro `InvalidRequest` quando você fornecer um número máximo de versões não atuais. Para obter mais informações sobre como usar o elemento de ação `NoncurrentVersionExpiration`, consulte the section called “Elementos para descrever ações de ciclo de vida”.

- O Amazon S3 não realiza nenhuma ação em versões não atuais de objetos que tenham a configuração de Bloqueio de Objetos do S3 aplicada.
- Em relação a objetos com o status de replicação `Pending`, o Amazon S3 não realiza nenhuma ação em versões atuais ou não atuais dos objetos.

Para obter mais informações, consulte Reter várias versões de objetos com o Versionamento do S3.

> **Important**
>
> Quando você tem várias regras em uma configuração do ciclo de vida do S3, um objeto pode se tornar elegível para várias ações do ciclo de vida do S3 no mesmo dia. Nesses casos, o Amazon S3 segue estas regras gerais:
>
> - A exclusão permanente tem precedência sobre a transição.
> - A transição tem precedência sobre a criação de marcadores de exclusão.
> - Quando um objeto é elegível para transição às classes S3 Glacier Flexible Retrieval e S3 Standard-IA (ou S3 One Zone-IA), o Amazon S3 escolhe a transição para a classe S3 Glacier Flexible Retrieval.
>
> Para obter exemplos, consulte Exemplos de filtros sobrepostos e ações de ciclo de vida conflitantes.

Objetos existentes e novos

Quando você adiciona uma configuração do ciclo de vida a um bucket, as regras de configuração se aplicam aos objetos existentes e aos objetos que serão adicionados no futuro. Por exemplo, se você adicionar uma regra de configuração da funcionalidade Ciclo de Vida hoje com uma ação de expiração que faz com que os objetos com um prefixo específico expirem 30 dias após sua criação,

o Amazon S3 organizará para exclusão todos os objetos existentes com o prefixo especificado e com mais de 30 dias.

> **Important**
>
> Você não pode usar uma política de bucket para evitar exclusões ou transições por meio de uma regra de ciclo de vida do S3. Por exemplo, mesmo que a política de bucket negue todas as ações para todas as entidades principais, a configuração do ciclo de vida do S3 ainda funcionará normalmente.

Como descobrir quando os objetos expiram

Para descobrir quando a versão atual de um objeto está programada para expirar, use as operações de API HeadObject ou GetObject. Essas operações de API exibem os cabeçalhos de resposta que fornecem a data e a hora em que não é mais possível armazenar a versão atual do objeto em cache.

> **Note**
>
> - Pode haver um atraso entre a data de expiração e a data em que o Amazon S3 remove um objeto. Você não será cobrado pela validade ou tempo de armazenamento associado a um objeto que expirou.
> - Antes de atualizar, desabilitar ou excluir regras de ciclo de vida, use as operações de API `LIST` (como ListObjectsV2, ListObjectVersions e ListMultipartUploads) ou Catalogar e analisar seus dados com o Inventário S3 para verificar se o Amazon S3 fez a transição e descontinuou os objetos elegíveis com base em seus casos de uso.

Cobrança da duração mínima de armazenamento

Se você criar uma regra de expiração do S3 Lifecycle que fará com que os objetos que estiveram no armazenamento S3 Standard – IA ou S3 One Zone – IA por menos de 30 dias expirem, você será cobrado por 30 dias. Se criar uma regra de validade do Lifecycle que resulte na expiração de objetos armazenados na classe S3 Glacier Flexible Retrieval por pelo menos 90 dias, você será cobrado por 90 dias. Se você criar uma regra de expiração do ciclo de vida que faça com que os objetos que estiveram no armazenamento do S3 Glacier Deep Archive por menos de 180 dias expirem, será cobrado por 180 dias.

Para obter mais informações, consulte Preço do Amazon S3.

Definir uma configuração do Ciclo de Vida do S3 em um bucket

É possível definir uma configuração do Ciclo de Vida do Amazon S3 em um bucket usando o console do Amazon S3, a AWS Command Line Interface (AWS CLI), os SDKs da AWS ou a API REST do Amazon S3. Para obter informações sobre a configuração do S3 Lifecycle, consulte Gerenciar o ciclo de vida dos objetos.

> **Note**
>
> Para visualizar ou editar a configuração do ciclo de vida de um bucket de diretório, use a AWS CLI, os AWS SDKs ou a API REST do Amazon S3. Para obter mais informações, consulte Trabalhar com o S3 Lifecycle para buckets de diretório.

Na configuração do Ciclo de Vida do S3, você usa regras de ciclo de vida para definir ações que você deseja que o Amazon S3 realize durante a vida útil de um objeto. Por exemplo, é possível definir regras para fazer a transição de objetos a outra classe de armazenamento, arquivá-los ou expirá-los (excluí-los) após um período especificado.

Considerações sobre o Ciclo de Vida do S3

Antes de definir uma configuração de ciclo de vida, observe o seguinte:

Atraso de propagação da configuração do ciclo de vida

Quando você adiciona uma configuração do S3 Lifecycle a um bucket, costuma haver algum atraso antes que uma configuração nova ou atualizada do ciclo de vida seja totalmente propagada para todos os sistemas do Amazon S3. Considere um atraso de alguns minutos antes que a configuração entre totalmente em vigor. Esse atraso também pode ocorrer quando você exclui uma configuração do S3 Lifecycle.

Atraso na transição ou na expiração

Há um atraso entre quando uma regra do ciclo de vida é cumprida e quando a ação para a regra é concluída. Por exemplo, suponha que um conjunto de objetos tenha expirado por uma regra de ciclo de vida em 1.º de janeiro. Mesmo que a regra de expiração tenha sido cumprida em 1º de janeiro, o Amazon S3 pode não excluir esses objetos até dias ou até semanas depois. Esse atraso ocorre porque o ciclo de vida do S3 enfileira objetos para transições ou expirações de forma assíncrona.

No entanto, as alterações no faturamento geralmente são aplicadas quando a regra do ciclo de vida é cumprida, mesmo que a ação não seja concluída. Consulte mais informações em Alterações no faturamento. Para monitorar o efeito das atualizações feitas pelas regras de ciclo de vida ativas, consulte the section called “Como monitorar as ações realizadas pelas minhas regras de ciclo de vida?”

Atualizar, desabilitar ou excluir regras de ciclo de vida

Quando você desabilita ou exclui regras de ciclo de vida, o Amazon S3 para de programar a exclusão ou transição de novos objetos depois de um pequeno atraso. Todos os objetos que já foram agendados não são agendados e não são excluídos ou transicionados.

> **Note**
>
> Antes de atualizar, desabilitar ou excluir regras de ciclo de vida, use as operações de API `LIST` (como ListObjectsV2, ListObjectVersions e ListMultipartUploads) ou Catalogar e analisar seus dados com o Inventário S3 para verificar se o Amazon S3 fez a transição e descontinuou os objetos elegíveis com base em seus casos de uso. Se você estiver enfrentando problemas com a atualização, a desabilitação ou a exclusão de regras de ciclo de vida, consulte Solucionar problemas de ciclo de vida do Amazon S3.

Objetos existentes e novos

Quando você adiciona uma configuração do ciclo de vida a um bucket, as regras de configuração se aplicam aos objetos existentes e aos objetos que serão adicionados no futuro. Por exemplo, se você adicionar uma regra de configuração da funcionalidade Ciclo de Vida hoje com uma ação de expiração que faz com que os objetos com um prefixo específico expirem 30 dias após sua criação, o Amazon S3 organizará para exclusão todos os objetos existentes com o prefixo especificado e com mais de 30 dias.

Monitorar o efeito de regras de ciclo de vida

Para monitorar o efeito das atualizações feitas pelas regras de ciclo de vida ativas, consulte the section called “Como monitorar as ações realizadas pelas minhas regras de ciclo de vida?”

Alterações no faturamento

Pode haver um atraso entre o momento em que as regras de configuração da funcionalidade Ciclo de Vida são satisfeitas e o momento em que a ação, ativada pela satisfação da regra, é tomada. No

entanto, as alterações na cobrança acontecem assim que a regra de configuração da funcionalidade Ciclo de Vida é satisfeita, mesmo que a ação ainda não tenha sido tomada.

Por exemplo, não haverá cobrança pelo armazenamento após o tempo de expiração do objeto, mesmo que o objeto não seja excluído imediatamente. Da mesma maneira, assim que o tempo de transição do objeto terminar, você receberá cobrança segundo as taxas de armazenamento da classe S3 Glacier Flexible Retrieval, mesmo que a transição do objeto para a classe de armazenamento S3 Glacier Flexible Retrieval não seja feita imediatamente.

No entanto, as transições do ciclo de vida para a classe de armazenamento S3 Intelligent-Tiering são a exceção. As alterações no faturamento só acontecerão depois da transição do objeto para a classe de armazenamento S3 Intelligent-Tiering.

Regras múltiplas ou conflitantes

Quando você tem várias regras em uma configuração do ciclo de vida do S3, um objeto pode se tornar elegível para várias ações do ciclo de vida do S3 no mesmo dia. Nesses casos, o Amazon S3 segue estas regras gerais:

- A exclusão permanente tem precedência sobre a transição.
- A transição tem precedência sobre a criação de marcadores de exclusão.
- Quando um objeto é elegível para transição às classes S3 Glacier Flexible Retrieval e S3 Standard-IA (ou S3 One Zone-IA), o Amazon S3 escolhe a transição para a classe S3 Glacier Flexible Retrieval.

Para obter exemplos, consulte Exemplos de filtros sobrepostos e ações de ciclo de vida conflitantes.

Como definir uma configuração do Ciclo de Vida do S3

É possível definir uma configuração da funcionalidade Ciclo de Vida do Amazon S3 em um bucket de uso geral usando o console do Amazon S3, a AWS Command Line Interface (AWS CLI), os AWS SDKs ou a API REST do Amazon S3.

Consulte informações sobre modelos e exemplos do AWS CloudFormation em Trabalhar com modelos do AWS CloudFormation e AWS::S3::Bucket no Guia do usuário do AWS CloudFormation.

Uso do console do S3

É possível definir regras de ciclo de vida para todos os objetos ou para um subconjunto de objetos em um bucket usando um prefixo compartilhado (nomes de objetos que começam com uma string

comum) ou uma tag. Na regra de ciclo de vida, é possível definir ações específicas para versões atuais e não atuais do objeto. Para obter mais informações, consulte:

- Gerenciar o ciclo de vida dos objetos
- Reter várias versões de objetos com o Versionamento do S3

Como criar uma regra de ciclo de vida

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets de uso geral.
3. Na lista de buckets, escolha o nome do bucket para o qual você deseja criar uma regra de ciclo de vida.
4. Escolha a guia Management (Gerenciamento) e escolha Create lifecycle rule (Criar regra de ciclo de vida).
5. Em Lifecycle rule name (Nome da regra do ciclo de vida), insira um nome para sua regra.

   O nome deve ser exclusivo dentro do bucket.
6. Escolha o escopo da regra do ciclo de vida:

   - Para aplicar essa regra de ciclo de vida a todos os objetos com um prefixo ou uma tag específica, escolha Limitar o escopo a prefixos ou tags específicos.
     - Para limitar o escopo por prefixo, em Prefix (Prefixo), insira o prefixo.
     - Para limitar o escopo por tag, escolha Add tag (Adicionar tag) e insira a chave e o valor da tag.

     Para obter mais informações sobre prefixos de nome de objeto, consulte Nomear objetos do Amazon S3. Para obter mais informações sobre tags de objeto, consulte Categorizar seu armazenamento usando tags.
   - Para aplicar essa regra de ciclo de vida a todos os objetos no bucket, escolha Esta regra se aplica a todos os objetos no bucket e Eu reconheço que esta regra se aplica a todos os objetos no bucket.
7. Para filtrar uma regra por tamanho de objeto, selecione Especificar o tamanho mínimo do objeto, Especificar o tamanho máximo do objeto ou as duas opções.

- Ao especificar um valor para Tamanho mínimo do objeto ou Tamanho máximo do objeto, o valor deverá ser maior que 0 byte e no máximo 5 TB. É possível especificar esse valor em bytes, KB, MB ou GB.
- Ao especificar ambos os valores, o tamanho máximo do objeto deverá ser maior que o tamanho mínimo do objeto.

> **Note**
>
> Os filtros Tamanho mínimo do objeto e Tamanho máximo do objeto excluem os valores especificados. Por exemplo, se você definir um filtro para expirar objetos que tenham um Tamanho mínimo do objeto de 128 KB, os objetos com exatamente 128 KB não expirarão. Em vez disso, a regra se aplica somente a objetos com tamanho maior que 128 KB.

8. Em Lifecycle rule actions (Ações de regra do ciclo de vida), escolha as ações que você deseja que sua regra de ciclo de vida execute:

   - Transição de versões atuais de objetos entre classes de armazenamento
   - Transição de versões anteriores de objetos entre classes de armazenamento
   - Expirar as versões atuais dos objetos

   > **Note**
   >
   > Para buckets que não têm o versionamento do S3 habilitado, a expiração das versões atuais faz com que o Amazon S3 exclua permanentemente os objetos. Para obter mais informações, consulte the section called “Ações de ciclo de vida e estado de versionamento do bucket”.

   - Excluir permanentemente versões anteriores de objetos
   - Excluir marcadores de exclusão expirados ou multipart uploads incompletos

   Dependendo das ações que você escolher, diferentes opções serão exibidas.

9. Para fazer a transição de versões atuais de objetos entre classes de armazenamento, em Transição de versões atuais de objetos entre classes de armazenamento, faça o seguinte:

a. Em Transições de classe de armazenamento, escolha a classe de armazenamento para a qual fazer a transição. Consulte uma lista de possíveis transições em the section called "Transições de ciclo de vida com suporte". É possível escolher entre as seguintes classes de armazenamento:

   - S3 Standard – IA
   - S3 Intelligent-Tiering
   - S3 One Zone-IA
   - S3 Glacier Instant Retrieval
   - S3 Glacier Flexible Retrieval
   - S3 Glacier Deep Archive

b. Em Days after object creation (Dias após a criação do objeto), insira o número de dias após a criação para fazer a transição do objeto.

Para obter mais informações sobre classes de armazenamento, consulte Compreender e gerenciar classes de armazenamento do Amazon S3. É possível definir transições para a versão atual ou as versões anteriores do objeto, ou para ambas. O versionamento permite que você mantenha várias versões de um objeto em um bucket. Para obter mais informações sobre versionamento, consulte Uso do console do S3.

> **Important**
>
> Quando você escolhe a classe de armazenamento S3 Glacier Instant Retrieval, S3 Glacier Flexible Retrieval ou Glacier Deep Archive, os objetos permanecem no Amazon S3. Não será possível acessá-los diretamente por meio do serviço separado do Amazon S3 Glacier. Para obter mais informações, consulte Transição de objetos usando o Amazon S3 Lifecycle.

10. Para fazer a transição de versões não atuais de objetos entre classes de armazenamento, em Transição de versões não atuais de objetos entre classes de armazenamento, faça o seguinte:

    a. Em Transições de classe de armazenamento, escolha a classe de armazenamento para a qual fazer a transição. Consulte uma lista de possíveis transições em the section called "Transições de ciclo de vida com suporte". É possível escolher entre as seguintes classes de armazenamento:

- S3 Standard – IA
- S3 Intelligent-Tiering
- S3 One Zone-IA
- S3 Glacier Instant Retrieval
- S3 Glacier Flexible Retrieval
- S3 Glacier Deep Archive

b. Em Dias após o objeto ficar desatualizado, insira o número de dias após a criação para fazer a transição do objeto.

11. Para expirar as versões atuais dos objetos, em Expire current versions of objects (Expirar versões atuais de objetos), em Number of days after object creation (Número de dias após a criação do objeto), insira o número de dias.

> **Important**
>
> Em um bucket sem versionamento, a ação de expiração faz com que o Amazon S3 remova permanentemente o objeto. Para obter mais informações sobre ações de ciclo de vida, consulte Elementos para descrever ações de ciclo de vida.

12. Para excluir permanentemente versões anteriores de objetos, em Permanently delete previous versions of objects (Excluir permanentemente versões desatualizadas de objetos), em Days after objects become noncurrent (Dias após os objetos ficarem desatualizados), insira o número de dias. Opcionalmente, você pode especificar o número de versões mais recentes a serem retidas inserindo um valor em Number of newer versions to retain (Número de versões mais novas a serem mantidas).
13. Em Delete expired delete markers or incomplete multipart uploads (Excluir marcadores de exclusão expirados ou multipart uploads incompletos), escolha Delete expired object delete markers (Excluir marcadores de exclusão de objetos expirados) e Delete incomplete multipart uploads (Excluir multipart uploads incompletos). Depois, insira o número de dias após o início do multipart upload que você deseja encerrar e limpar multipart uploads incompletos.

    Para obter mais informações sobre multipart uploads, consulte Carregar e copiar objetos usando upload fracionado no Amazon S3.
14. Selecione Criar regra.

Se a regra não contiver erros, o Amazon S3 a habilitará e você poderá vê-la na guia Management (Gerenciamento) em Lifecycle rules (Regras de ciclo de vida).

Usar o AWS CLI

Use os comandos da AWS CLI a seguir para gerenciar as configurações do S3 Lifecycle:

- `put-bucket-lifecycle-configuration`
- `get-bucket-lifecycle-configuration`
- `delete-bucket-lifecycle`

Consulte instruções sobre como configurar a AWS CLI em Developing with Amazon S3 using the AWS CLI na Referência de API do Amazon S3.

A configuração do ciclo de vida do Amazon S3 é um arquivo XML. Porém, ao usar a AWS CLI, você não pode especificar o formado XML. Em vez disso, você deve especificar o formato JSON. Veja a seguir exemplos de configurações de ciclo de vida em XML e as configurações JSON equivalentes que podem ser especificadas em um comando da AWS CLI.

Considere o seguinte exemplo de configuração do S3 Lifecycle.

Example Exemplo 1

Example

XML

```
<LifecycleConfiguration>
    <Rule>
        <ID>ExampleRule</ID>
        <Filter>
           <Prefix>documents/</Prefix>
        </Filter>
        <Status>Enabled</Status>
        <Transition>
           <Days>365</Days>
           <StorageClass>GLACIER</StorageClass>
        </Transition>
        <Expiration>
             <Days>3650</Days>
```

```
        </Expiration>
    </Rule>
</LifecycleConfiguration>
```

JSON

```
{
    "Rules": [
        {
            "Filter": {
                "Prefix": "documents/"
            },
            "Status": "Enabled",
            "Transitions": [
                {
                    "Days": 365,
                    "StorageClass": "GLACIER"
                }
            ],
            "Expiration": {
                "Days": 3650
            },
            "ID": "ExampleRule"
        }
    ]
}
```

Example Exemplo 2

Example

XML

```
<LifecycleConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
    <Rule>
        <ID>id-1</ID>
        <Expiration>
            <Days>1</Days>
        </Expiration>
        <Filter>
            <And>
```

```
                <Prefix>myprefix</Prefix>
                <Tag>
                    <Key>mytagkey1</Key>
                    <Value>mytagvalue1</Value>
                </Tag>
                <Tag>
                    <Key>mytagkey2</Key>
                    <Value>mytagvalue2</Value>
                </Tag>
            </And>
        </Filter>
        <Status>Enabled</Status>
    </Rule>
</LifecycleConfiguration>
```

JSON

```
{
    "Rules": [
        {
            "ID": "id-1",
            "Filter": {
                "And": {
                    "Prefix": "myprefix",
                    "Tags": [
                        {
                            "Value": "mytagvalue1",
                            "Key": "mytagkey1"
                        },
                        {
                            "Value": "mytagvalue2",
                            "Key": "mytagkey2"
                        }
                    ]
                }
            },
            "Status": "Enabled",
            "Expiration": {
                "Days": 1
            }
        }
    ]
```

```
}
```

Teste o comando `put-bucket-lifecycle-configuration` da seguinte forma.

Como testar a configuração

1. Salve a configuração de ciclo de vida JSON em um arquivo (por exemplo, *`lifecycle.json`*).
2. Execute o comando da AWS CLI a seguir para definir a configuração do ciclo de vida no bucket. Substitua os *`user input placeholders`* por suas próprias informações.

```
$ aws s3api put-bucket-lifecycle-configuration  \
--bucket amzn-s3-demo-bucket  \
--lifecycle-configuration file://lifecycle.json
```

3. Para verificar, recupere a configuração do S3 Lifecycle usando o comando `get-bucket-lifecycle-configuration` da AWS CLI da seguinte maneira:

```
$ aws s3api get-bucket-lifecycle-configuration  \
--bucket amzn-s3-demo-bucket
```

4. Para excluir a configuração do S3 Lifecycle, use o comando `delete-bucket-lifecycle` da AWS CLI da seguinte maneira:

```
aws s3api delete-bucket-lifecycle \
--bucket amzn-s3-demo-bucket
```

Uso dos SDKs da AWS

Java

Use o AWS SDK para Java para gerenciar a configuração do S3 Lifecycle de um bucket. Para obter mais informações sobre o gerenciamento da configuração do ciclo de vida do S3, consulte Gerenciar o ciclo de vida dos objetos.

> **Note**
>
> Quando você adiciona uma configuração do Ciclo de Vida do S3 a um bucket, o Amazon S3 substitui a configuração do Ciclo de Vida atual do bucket, se houver. Para atualizar

uma configuração, recupere a configuração, faça as alterações desejadas e adicione a configuração revisada ao bucket.

O exemplo a seguir mostra como usar o AWS SDK para Java para adicionar, atualizar e excluir a configuração do ciclo de vida de um bucket. O exemplo faz o seguinte:

- Adiciona a configuração do ciclo de vida a um bucket.
- Recupera a configuração do ciclo de vida e a atualiza adicionando outra regra.
- Adiciona a configuração do ciclo de vida modificada ao bucket. O Amazon S3 substitui a configuração existente.
- Recupera a configuração novamente e verifica se ela tem o número certo de regras imprimindo o número de regras.
- Exclui a configuração do ciclo de vida e verifica se ela foi excluída ao tentar recuperá-la novamente.

Consulte instruções sobre como criar e testar uma amostra funcional em Getting Started no Guia do desenvolvedor do AWS SDK para Java.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.BucketLifecycleConfiguration;
import com.amazonaws.services.s3.model.BucketLifecycleConfiguration.Transition;
import com.amazonaws.services.s3.model.StorageClass;
import com.amazonaws.services.s3.model.Tag;
import com.amazonaws.services.s3.model.lifecycle.LifecycleAndOperator;
import com.amazonaws.services.s3.model.lifecycle.LifecycleFilter;
import com.amazonaws.services.s3.model.lifecycle.LifecyclePrefixPredicate;
import com.amazonaws.services.s3.model.lifecycle.LifecycleTagPredicate;

import java.io.IOException;
import java.util.Arrays;

public class LifecycleConfiguration {
```

```
        public static void main(String[] args) throws IOException {
                Regions clientRegion = Regions.DEFAULT_REGION;
                String bucketName = "*** Bucket name ***";

                // Create a rule to archive objects with the "glacierobjects/"
prefix to Glacier
                // immediately.
                BucketLifecycleConfiguration.Rule rule1 = new
BucketLifecycleConfiguration.Rule()
                                .withId("Archive immediately rule")
                                .withFilter(new LifecycleFilter(new
LifecyclePrefixPredicate("glacierobjects/")))
                                .addTransition(new
Transition().withDays(0).withStorageClass(StorageClass.Glacier))
                                .withStatus(BucketLifecycleConfiguration.ENABLED);

                // Create a rule to transition objects to the Standard-Infrequent
Access storage
                // class
                // after 30 days, then to Glacier after 365 days. Amazon S3 will
delete the
                // objects after 3650 days.
                // The rule applies to all objects with the tag "archive" set to
"true".
                BucketLifecycleConfiguration.Rule rule2 = new
BucketLifecycleConfiguration.Rule()
                                .withId("Archive and then delete rule")
                                .withFilter(new LifecycleFilter(new
LifecycleTagPredicate(new Tag("archive", "true"))))
                                .addTransition(new Transition().withDays(30)

.withStorageClass(StorageClass.StandardInfrequentAccess))
                                .addTransition(new
Transition().withDays(365).withStorageClass(StorageClass.Glacier))
                                .withExpirationInDays(3650)
                                .withStatus(BucketLifecycleConfiguration.ENABLED);

                // Add the rules to a new BucketLifecycleConfiguration.
                BucketLifecycleConfiguration configuration = new
BucketLifecycleConfiguration()
                                .withRules(Arrays.asList(rule1, rule2));

                try {
```

```
                        AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                                        .withCredentials(new
ProfileCredentialsProvider())
                                        .withRegion(clientRegion)
                                        .build();

                        // Save the configuration.
                        s3Client.setBucketLifecycleConfiguration(bucketName,
configuration);

                        // Retrieve the configuration.
                        configuration =
s3Client.getBucketLifecycleConfiguration(bucketName);

                        // Add a new rule with both a prefix predicate and a tag
predicate.
                        configuration.getRules().add(new
BucketLifecycleConfiguration.Rule().withId("NewRule")
                                        .withFilter(new LifecycleFilter(new
LifecycleAndOperator(
                                                        Arrays.asList(new
LifecyclePrefixPredicate("YearlyDocuments/"),
                                                                        new
LifecycleTagPredicate(new Tag(

   "expire_after",

   "ten_years"))))))
                                        .withExpirationInDays(3650)

.withStatus(BucketLifecycleConfiguration.ENABLED));

                        // Save the configuration.
                        s3Client.setBucketLifecycleConfiguration(bucketName,
configuration);

                        // Retrieve the configuration.
                        configuration =
s3Client.getBucketLifecycleConfiguration(bucketName);

                        // Verify that the configuration now has three rules.
                        configuration =
s3Client.getBucketLifecycleConfiguration(bucketName);
```

```
                        System.out.println("Expected # of rules = 3; found: " +
 configuration.getRules().size());

                        // Delete the configuration.
                        s3Client.deleteBucketLifecycleConfiguration(bucketName);

                        // Verify that the configuration has been deleted by
 attempting to retrieve it.
                        configuration =
 s3Client.getBucketLifecycleConfiguration(bucketName);
                        String s = (configuration == null) ? "No configuration
 found." : "Configuration found.";
                        System.out.println(s);
                } catch (AmazonServiceException e) {
                        // The call was transmitted successfully, but Amazon S3
 couldn't process
                        // it, so it returned an error response.
                        e.printStackTrace();
                } catch (SdkClientException e) {
                        // Amazon S3 couldn't be contacted for a response, or the
 client
                        // couldn't parse the response from Amazon S3.
                        e.printStackTrace();
                }
        }
}
```

.NET

Use o AWS SDK para .NET para gerenciar a configuração do S3 Lifecycle em um bucket. Para obter mais informações sobre o gerenciamento da configuração do ciclo de vida, consulte Gerenciar o ciclo de vida dos objetos.

> **Note**
>
> Quando você adiciona uma configuração do ciclo de vida, o Amazon S3 substitui a configuração existente no bucket especificado. Para atualizar uma configuração, recupere a configuração do ciclo de vida, faça as alterações e, depois, adicione a configuração revisada ao bucket.

O exemplo a seguir mostra como usar o AWS SDK para .NET para adicionar, atualizar e excluir uma configuração do ciclo de vida de um bucket. O exemplo de código faz o seguinte:

- Adiciona a configuração do ciclo de vida a um bucket.
- Recupera a configuração do ciclo de vida e a atualiza adicionando outra regra.
- Adiciona a configuração do ciclo de vida modificada ao bucket. O Amazon S3 substitui a configuração do ciclo de vida existente.
- Recupera a configuração novamente e a verifica imprimindo o número de regras na configuração.
- Exclui a configuração do Lifecycle e verifica a exclusão.

Consulte informações sobre como configurar e executar exemplos de código, em Getting Started with the AWS SDK para .NET no Guia do desenvolvedor do AWS SDK para .NET.

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Collections.Generic;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class LifecycleTest
    {
        private const string bucketName = "*** bucket name ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 client;
        public static void Main()
        {
            client = new AmazonS3Client(bucketRegion);
            AddUpdateDeleteLifecycleConfigAsync().Wait();
        }

        private static async Task AddUpdateDeleteLifecycleConfigAsync()
        {
            try
            {
```

```
                var lifeCycleConfiguration = new LifecycleConfiguration()
                {
                    Rules = new List<LifecycleRule>
                        {
                            new LifecycleRule
                            {
                                 Id = "Archive immediately rule",
                                 Filter = new LifecycleFilter()
                                 {
                                     LifecycleFilterPredicate = new
LifecyclePrefixPredicate()
                                     {
                                         Prefix = "glacierobjects/"
                                     }
                                 },
                                 Status = LifecycleRuleStatus.Enabled,
                                 Transitions = new List<LifecycleTransition>
                                 {
                                      new LifecycleTransition
                                      {
                                           Days = 0,
                                           StorageClass = S3StorageClass.Glacier
                                      }
                                  },
                            },
                            new LifecycleRule
                            {
                                 Id = "Archive and then delete rule",
                                  Filter = new LifecycleFilter()
                                 {
                                     LifecycleFilterPredicate = new
LifecyclePrefixPredicate()
                                     {
                                         Prefix = "projectdocs/"
                                     }
                                 },
                                 Status = LifecycleRuleStatus.Enabled,
                                 Transitions = new List<LifecycleTransition>
                                 {
                                      new LifecycleTransition
                                      {
                                           Days = 30,
                                           StorageClass =
S3StorageClass.StandardInfrequentAccess
```

```
                                    },
                                    new LifecycleTransition
                                    {
                                      Days = 365,
                                      StorageClass = S3StorageClass.Glacier
                                    }
                                },
                                Expiration = new LifecycleRuleExpiration()
                                {
                                     Days = 3650
                                }
                            }
                        }
                };

                // Add the configuration to the bucket.
                await AddExampleLifecycleConfigAsync(client,
lifeCycleConfiguration);

                // Retrieve an existing configuration.
                lifeCycleConfiguration = await RetrieveLifecycleConfigAsync(client);

                // Add a new rule.
                lifeCycleConfiguration.Rules.Add(new LifecycleRule
                {
                    Id = "NewRule",
                    Filter = new LifecycleFilter()
                    {
                        LifecycleFilterPredicate = new LifecyclePrefixPredicate()
                        {
                            Prefix = "YearlyDocuments/"
                        }
                    },
                    Expiration = new LifecycleRuleExpiration()
                    {
                        Days = 3650
                    }
                });

                // Add the configuration to the bucket.
                await AddExampleLifecycleConfigAsync(client,
lifeCycleConfiguration);

                // Verify that there are now three rules.
```

```
                lifeCycleConfiguration = await RetrieveLifecycleConfigAsync(client);
                Console.WriteLine("Expected # of rulest=3; found:{0}",
lifeCycleConfiguration.Rules.Count);

                // Delete the configuration.
                await RemoveLifecycleConfigAsync(client);

                // Retrieve a nonexistent configuration.
                lifeCycleConfiguration = await RetrieveLifecycleConfigAsync(client);

            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered ***. Message:'{0}' when writing
an object", e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
writing an object", e.Message);
            }
        }

        static async Task AddExampleLifecycleConfigAsync(IAmazonS3 client,
LifecycleConfiguration configuration)
        {

            PutLifecycleConfigurationRequest request = new
PutLifecycleConfigurationRequest
            {
                BucketName = bucketName,
                Configuration = configuration
            };
            var response = await client.PutLifecycleConfigurationAsync(request);
        }

        static async Task<LifecycleConfiguration>
RetrieveLifecycleConfigAsync(IAmazonS3 client)
        {
            GetLifecycleConfigurationRequest request = new
GetLifecycleConfigurationRequest
            {
                BucketName = bucketName
            };
```

```
            var response = await client.GetLifecycleConfigurationAsync(request);
            var configuration = response.Configuration;
            return configuration;
        }

        static async Task RemoveLifecycleConfigAsync(IAmazonS3 client)
        {
            DeleteLifecycleConfigurationRequest request = new
 DeleteLifecycleConfigurationRequest
            {
                BucketName = bucketName
            };
            await client.DeleteLifecycleConfigurationAsync(request);
        }
    }
}
```

Ruby

É possível usar o AWS SDK para Ruby para gerenciar uma configuração do Ciclo de Vida do S3 em um bucket usando a classe AWS::S3::BucketLifecycleConfiguration. Para obter mais informações sobre o gerenciamento da configuração do ciclo de vida do S3, consulte Gerenciar o ciclo de vida dos objetos.

Uso da API REST

Os tópicos a seguir na Referência da API do Amazon Simple Storage Service descrevem as operações da API REST relacionada à configuração do Ciclo de Vida do S3:

- PutBucketLifecycleConfiguration
- GetBucketLifecycleConfiguration
- DeleteBucketLifecycle

Solução de problemas de ciclo de vida do S3

Consulte problemas comuns que podem ocorrer ao trabalhar com o ciclo de vida do S3 em the section called “Solucionar problemas de ciclo de vida”.

Como o Ciclo de Vida do S3 interage com outras configurações de bucket

Além de configurações do S3 Lifecycle, você pode associar outras configurações a seu bucket. Esta seção explica como a configuração do S3 Lifecycle está relacionada a outras configurações de bucket.

Ciclo de Vida do S3 e Versionamento do S3

Você pode adicionar configurações de ciclo de vida do S3 a buckets com e sem versionamento. Para obter mais informações, consulte Reter várias versões de objetos com o Versionamento do S3.

Um bucket com versionamento habilitado mantém uma versão atual do objeto e versões desatualizadas do objeto (se disponíveis). Você pode definir regras separadas de ciclo de vida para versões atuais e não atuais do objeto.

Para obter mais informações, consulte Elementos de configuração do ciclo de vida.

> **Important**
>
> Quando você tem várias regras em uma configuração do ciclo de vida do S3, um objeto pode se tornar elegível para várias ações do ciclo de vida do S3 no mesmo dia. Nesses casos, o Amazon S3 segue estas regras gerais:
>
> - A exclusão permanente tem precedência sobre a transição.
> - A transição tem precedência sobre a criação de marcadores de exclusão.
> - Quando um objeto está qualificado para uma transição S3 Glacier Flexible Retrieval e S3 Standard – IA (ou S3 One Zone – IA), o Amazon S3 escolhe a transição do S3 Glacier Flexible Retrieval.
>
> Para obter exemplos, consulte Exemplos de filtros sobrepostos e ações de ciclo de vida conflitantes.

Configuração do Ciclo de Vida do S3 em buckets com MFA habilitada

Não é possível usar a configuração do ciclo de vida do S3 em buckets com autenticação multifator configurada para exclusão da MFA. Para obter mais informações, consulte Configurando a exclusão de MFA.

Ciclo de Vida do S3 e registro em log

As ações de Ciclo de Vida do Amazon S3 não são capturadas pelo registro em log no nível do objeto do AWS CloudTrail. O CloudTrail captura solicitações de API feitas para endpoints externos do Amazon S3, enquanto as ações do Ciclo de Vida do S3 são realizadas usando endpoints internos do Amazon S3.

É possível habilitar logs de acesso ao servidor do Amazon S3 em um bucket do S3 para capturar ações relacionadas ao Ciclo de Vida do S3, como transições de objetos para outra classe de armazenamento e expirações de objetos que resultam em exclusão permanente ou lógica. Para obter mais informações, consulte the section called “Registrando acesso ao servidor”.

Se o registro em logs estiver ativado em seu bucket, os logs de acesso do servidor do Amazon S3 relatarão os resultados das seguintes operações.

Log de operação	Descrição
`S3.EXPIRE.OBJECT`	O Amazon S3 exclui permanentemente o objeto devido à ação `Expiration` do ciclo de vida.
`S3.CREATE.DELETEMARKER`	O Amazon S3 exclui logicamente a versão atual adicionando o marcador de exclusão em um bucket com versionamento habilitado.
`S3.TRANSITION_SIA.OBJECT`	O Amazon S3 faz a transição do objeto para a classe de armazenamento S3 Standard – IA.
`S3.TRANSITION_ZIA.OBJECT`	O Amazon S3 faz a transição do objeto para a classe de armazenamento S3 One Zone – IA.
`S3.TRANSITION_INT.OBJECT`	O Amazon S3 faz a transição do objeto para a classe de armazenamento S3 Intelligent-Tierin g.
`S3.TRANSITION_GIR.OBJECT`	O Amazon S3 inicia a transição do objeto para a classe de armazenamento S3 Glacier Instant Retrieval.

Log de operação	Descrição
`S3.TRANSITION.OBJECT`	O Amazon S3 inicia a transição do objeto para a classe de armazenamento S3 Glacier Flexible Retrieval.
`S3.TRANSITION_GDA.OBJECT`	O Amazon S3 inicia a transição do objeto para a classe de armazenamento S3 Glacier Deep Archive.
`S3.DELETE.UPLOAD`	O Amazon S3 interrompe o carregamento fracionado incompleto.

> **Note**
>
> Os registros do log de acesso ao servidor do Amazon S3 são entregues com base no melhor esforço e não podem ser usados para uma contabilização completa de todas as solicitações do Amazon S3.

Configurar notificações de evento do Ciclo de Vida do S3

Para receber uma notificação quando o Amazon S3 exclui um objeto ou o transiciona para outra classe de armazenamento do Amazon S3 ao seguir uma regra do Ciclo de Vida do S3, é possível configurar uma notificação de eventos do Amazon S3.

É possível receber notificações para os seguintes eventos do Ciclo de Vida do S3:

- Eventos de transição: ao usar o tipo de evento `s3:LifecycleTransition`, você poderá receber uma notificação quando um objeto for transferido para outra classe de armazenamento do Amazon S3 por uma configuração do Ciclo de Vida do S3.
- Eventos de expiração (exclusão): ao usar os tipos de evento `LifecycleExpiration`, você poderá receber notificações sempre que o Amazon S3 excluir um objeto com base na configuração do Ciclo de Vida do S3.

  Há dois tipos de evento de expiração:

- O tipo de evento `s3:LifecycleExpiration:Delete` notifica você quando um objeto em um bucket sem versionamento é excluído. `s3:LifecycleExpiration:Delete` também notifica quando uma versão de objeto é excluída permanentemente por uma configuração do Ciclo de Vida do S3.
- O tipo de evento `s3:LifecycleExpiration:DeleteMarkerCreated` notifica você quando o Ciclo de Vida do S3 cria um marcador de exclusão depois que uma versão atual de um objeto no bucket com versionamento é excluída. O Ciclo de vida do S3 define o horário de criação do marcador de exclusão como 00:00 UTC (meia-noite) do dia atual. Esse horário de criação pode ser diferente do horário do evento na notificação `s3:LifecycleExpiration:DeleteMarkerCreated` que o S3 envia. Para obter mais informações, consulte the section called “Excluir versões de objeto”.

O Amazon S3 pode publicar notificações de eventos em um tópico do Amazon Simple Notification Service (Amazon SNS), em uma fila do Amazon Simple Queue Service (Amazon SQS) ou em uma função do AWS Lambda. Para obter mais informações, consulte Notificações de eventos do Amazon S3.

Consulte instruções sobre como configurar Notificações de Eventos do Amazon S3 em Usar o Amazon SQS, o Amazon SNS e o AWS Lambda.

Veja a seguir um exemplo de mensagem que o Amazon S3 envia para publicar um evento `s3:LifecycleExpiration:Delete`. Para obter mais informações, consulte the section called “Estrutura de mensagens de evento”.


```
{
   "Records":[
      {
         "eventVersion":"2.3",
         "eventSource":"aws:s3",
         "awsRegion":"us-west-2",
         "eventTime":"1970-01-01T00:00:00.000Z",
         "eventName":"LifecycleExpiration:Delete",
         "userIdentity":{
            "principalId":"s3.amazonaws.com"
         },
         "requestParameters":{
            "sourceIPAddress":"s3.amazonaws.com"
         },
         "responseElements":{
```

```
            "x-amz-request-id":"C3D13FE58DE4C810",
            "x-amz-id-2":"FMyUVURIY8/IgAtTv8xRjskZQpcIZ9KG4V5Wp6S7S/
JRWeUWerMUE5JgHvANOjpD"
         },
         "s3":{
            "s3SchemaVersion":"1.0",
            "configurationId":"testConfigRule",
            "bucket":{
               "name":"amzn-s3-demo-bucket",
               "ownerIdentity":{
                  "principalId":"A3NL1KOZZKExample"
               },
               "arn":"arn:aws:s3:::amzn-s3-demo-bucket"
            },
            "object":{
               "key":"expiration/delete",
               "sequencer":"0055AED6DCD90281E5",
            }
         }
      }
   ]
}
```

As mensagens que o Amazon S3 envia para publicar um evento `s3:LifecycleTransition` também incluem as seguintes informações:

```
"lifecycleEventData":{
    "transitionEventData": {
        "destinationStorageClass": the destination storage class for the object
    }
}
```

Elementos de configuração do ciclo de vida

Uma configuração do Ciclo de Vida do S3 consiste em regras de ciclo de vida que incluem vários elementos que descrevem as ações que o Amazon S3 realiza e a vida útil dos objetos. Você especifica uma configuração do Ciclo de Vida do Amazon S3 como XML, que é composta por uma ou mais regras do Ciclo de Vida, em que cada regra consiste em um ou mais elementos.

```
<LifecycleConfiguration>
    <Rule>
```

```
          <Element>
     </Rule>
     <Rule>
          <Element>
          <Element>
     </Rule>
</LifecycleConfiguration>
```

Cada regra consiste no seguinte:

- Metadados de regra que incluem um ID de regra e um status que indica se a regra está habilitada ou desabilitada. Se uma regra estiver desativada, o Amazon S3 não executará as ações especificadas nela.
- Um filtro que identifica os objetos aos quais a regra se aplica. Você pode especificar um filtro usando o tamanho do objeto, o prefixo de chave do objeto, uma ou mais tags de objeto ou uma combinação de filtros.
- Uma ou mais ações de transição ou expiração com uma data ou um período no ciclo de vida do objeto quando você deseja que o Amazon S3 realize a ação especificada.

Tópicos

- Elemento ID
- Elemento Status
- Elemento Filter
- Elementos para descrever ações de ciclo de vida
- Como adicionar filtros a regras de ciclo de vida

As seções a seguir descrevem os elementos XML em uma configuração de ciclo de vida do S3. Para obter configurações de exemplo, consulte Exemplos de configurações do Ciclo de Vida do S3.

Elemento ID

Uma configuração do ciclo de vida do S3 pode ter até 1.000 regras. Este limite não é ajustável. O elemento `<ID>` identifica uma regra com exclusividade. O tamanho do ID está limitado a 255 caracteres.

Elemento Status

O valor do elemento `<Status>` pode ser `Enabled` ou `Disabled`. Se uma regra estiver desativada, o Amazon S3 não executará as ações definidas nela.

Elemento Filter

Uma regra do Ciclo de Vida do S3 pode ser aplicada a todos os objetos ou a um subconjunto de objetos em um bucket com base no elemento `<Filter>` especificado na regra.

É possível filtrar objetos por prefixo das chaves, por tag de objeto ou por uma combinação dos dois (neste último caso, o Amazon S3 usa uma operação AND lógica para combinar os filtros). Consulte exemplos e mais informações sobre filtros em Como adicionar filtros a regras de ciclo de vida.

- Especificação de um filtro usando prefixos de chave: este exemplo mostra uma regra do S3 Lifecycle que se aplica a um subconjunto de objetos com base no prefixo de nome de chave (`logs/`). Por exemplo, a regra de ciclo de vida se aplica aos objetos `logs/mylog.txt`, `logs/temp1.txt` e `logs/test.txt`. A regra não se aplica ao objeto `example.jpg`.

```
<LifecycleConfiguration>
    <Rule>
        <Filter>
           <Prefix>logs/</Prefix>
        </Filter>
        transition/expiration actions
         ...
    </Rule>
    ...
</LifecycleConfiguration>
```

  Caso queira aplicar uma ação de ciclo de vida a um subconjunto de objetos com base em prefixos de nome de chave diferentes, especifique regras separadas. Em cada regra, especifique um filtro com base em prefixo. Por exemplo, para descrever uma ação de ciclo de vida para objetos com prefixos de chave `projectA/` e `projectB/`, especifique duas regras da seguinte forma:

```
<LifecycleConfiguration>
    <Rule>
        <Filter>
           <Prefix>projectA/</Prefix>
        </Filter>
        transition/expiration actions
```

```
        ...
    </Rule>

    <Rule>
        <Filter>
           <Prefix>projectB/</Prefix>
        </Filter>
        transition/expiration actions
        ...
    </Rule>
</LifecycleConfiguration>
```

Para obter mais informações sobre chaves de objeto, consulte Nomear objetos do Amazon S3.

- Especificação de um filtro com base em tags de objeto: no exemplo a seguir, a regra de ciclo de vida especifica um filtro com base em uma tag (*key*) e valor (*value*). A regra aplica-se somente a um subconjunto de objetos com a tag específica.

```
<LifecycleConfiguration>
    <Rule>
        <Filter>
           <Tag>
              <Key>key</Key>
              <Value>value</Value>
           </Tag>
        </Filter>
        transition/expiration actions
        ...
    </Rule>
</LifecycleConfiguration>
```

Você pode especificar um filtro com base em várias tags. Você deve encapsular as tags no elemento <And>, como mostrado no exemplo a seguir. A regra instrui o Amazon S3 a executar ações de ciclo de vida em objetos com duas tags (com a chave e o valor específicos da tag).

```
<LifecycleConfiguration>
    <Rule>
      <Filter>
         <And>
            <Tag>
               <Key>key1</Key>
               <Value>value1</Value>
```

```
            </Tag>
            <Tag>
               <Key>key2</Key>
               <Value>value2</Value>
            </Tag>
             ...
         </And>
      </Filter>
      transition/expiration actions
    </Rule>
</Lifecycle>
```

A regra de ciclo de vida se aplica a objetos que têm ambas as tags especificadas. O Amazon S3 realiza uma operação AND lógica. Observe o seguinte:

- Cada tag deve corresponder exatamente a ambos: à chave e ao valor. Se você especificar somente um elemento <Key> e nenhum elemento <Value>, a regra será aplicada apenas aos objetos que corresponderem à chave da tag e que não tenham um valor especificado.
- A regra se aplica a um subconjunto de objetos que tem todas as tags especificadas na regra. Se um objeto tiver tags adicionais especificadas, a regra ainda será aplicada.

> **Note**
>
> Quando você especifica várias tags em um filtro, cada chave de tag deve ser exclusiva.

- Especificação de um filtro com base no prefixo e em uma ou mais tags: em uma regra de ciclo de vida, você pode especificar um filtro com base no prefixo de chaves e em uma ou mais tags. Além disso, você deve incluir tudo isso no elemento <And>, como mostrado a seguir.

```
<LifecycleConfiguration>
    <Rule>
        <Filter>
          <And>
             <Prefix>key-prefix</Prefix>
             <Tag>
                <Key>key1</Key>
                <Value>value1</Value>
             </Tag>
             <Tag>
                <Key>key2</Key>
                <Value>value2</Value>
```

```
            </Tag>
             ...
          </And>
        </Filter>
        <Status>Enabled</Status>
        transition/expiration actions
    </Rule>
</LifecycleConfiguration>
```

O Amazon S3 combina esses filtros usando uma operação AND lógica. Isto é, a regra aplica-se ao subconjunto de objetos com o prefixo de chave especificado e as tags especificadas. Um filtro pode ter somente um prefixo e zero ou mais tags.

- Você pode especificar um filtro vazio e, nesse caso, a regra se aplicará a todos os objetos do bucket.

```
<LifecycleConfiguration>
    <Rule>
        <Filter>
        </Filter>
        <Status>Enabled</Status>
        transition/expiration actions
    </Rule>
</LifecycleConfiguration>
```

- Para filtrar uma regra por tamanho do objeto, você pode especificar um tamanho mínimo (`ObjectSizeGreaterThan`), um tamanho máximo (`ObjectSizeLessThan`) ou um intervalo de tamanhos de objeto.

  Os valores de tamanho de objeto estão em bytes. Por padrão, objetos com menos de 128 KB não serão transferidos para nenhuma classe de armazenamento, a menos que você especifique um tamanho mínimo menor (`ObjectSizeGreaterThan`) ou máximo (`ObjectSizeLessThan`). Para ter mais informações, consulte Exemplo: permitir que objetos com menos de 128 KB sejam transferidos.

```
                <LifecycleConfiguration>
    <Rule>
        <Filter>
            <ObjectSizeGreaterThan>500</ObjectSizeGreaterThan>
        </Filter>
        <Status>Enabled</Status>
```

```
        transition/expiration actions
    </Rule>
</LifecycleConfiguration>
```

> **Note**
>
> Os filtros `ObjectSizeGreaterThan` e `ObjectSizeLessThan` excluem os valores especificados. Por exemplo, se você definir objetos com tamanho de 128 KB a 1.024 KB para mover da classe de armazenamento S3 Standard para a classe de armazenamento S3 Standard-IA, os objetos que têm exatamente 1.024 KB e 128 KB não farão a transição para S3 Standard-IA. Em vez disso, a regra se aplicará somente a objetos maiores que 128 KB e menores que 1.024 KB de tamanho.

Se você estiver especificando um intervalo de tamanho de objeto, o número inteiro `ObjectSizeGreaterThan` deve ser menor que o valor de `ObjectSizeLessThan`. Ao usar mais de um filtro, é necessário fazer a quebra dos filtros em um elemento `<And>`. O exemplo a seguir mostra como especificar objetos em um intervalo entre 500 e 64.000 bytes.

```
<LifecycleConfiguration>
    <Rule>
        <Filter>
            <And>
                <Prefix>key-prefix</Prefix>
                <ObjectSizeGreaterThan>500</ObjectSizeGreaterThan>
                <ObjectSizeLessThan>64000</ObjectSizeLessThan>
            </And>
        </Filter>
        <Status>Enabled</Status>
        transition/expiration actions
    </Rule>
</LifecycleConfiguration>
```

Elementos para descrever ações de ciclo de vida

Você pode instruir o Amazon S3 a executar ações específicas no ciclo de vida de um objeto, especificando uma ou mais das seguintes ações predefinidas em uma regra de ciclo de vida do S3. O efeito dessas ações depende do estado do versionamento de seu bucket.

- Elemento de ação **`Transition`**: você especifica a ação `Transition` para fazer a transição de objetos de uma classe de armazenamento para outra. Para obter mais informações sobre transição de objetos, consulte Transições aceitas. Quando uma data ou um período especificado no ciclo de vida do objeto é atingido, o Amazon S3 executa a transição.

  Para um bucket com versões (versionamento ativado ou suspenso no bucket), a ação `Transition` aplica-se à versão do objeto atual. Para gerenciar versões desatualizadas, o Amazon S3 define a ação `NoncurrentVersionTransition` (descrita posteriormente neste tópico).

- Elemento de ação **`Expiration`**: a ação `Expiration` descontinua objetos identificados na regra e se aplica a objetos qualificados em qualquer uma das classes de armazenamento do Amazon S3. Para obter mais informações sobre classes de armazenamento, consulte Compreender e gerenciar classes de armazenamento do Amazon S3. O Amazon S3 deixa todos os objetos expirados indisponíveis. A remoção permanente dos objetos depende do estado de versionamento do bucket.
  - Bucket sem versionamento: a ação `Expiration` resulta na remoção permanente do objeto pelo Amazon S3.
  - Bucket com versão: para um bucket com versão (ou seja, versionamento ativado ou suspenso), há várias considerações que orientam como o Amazon S3 trata a ação `Expiration`. Para buckets com versionamento habilitado ou suspenso, o seguinte se aplica:
    - A ação `Expiration` se aplica somente à versão atual (não afeta versões não atuais do objeto).
    - O Amazon S3 não realizará ações se houver uma ou mais versões de objeto e se o marcador de exclusão estiver na versão atual.
    - Se a versão atual do objeto for a única versão do objeto e também houver um marcador de exclusão (também chamado de marcador de exclusão de objeto expirado, onde todas as versões do objeto são excluídas e você tem somente um marcador de exclusão restante), o Amazon S3 removerá o marcador de exclusão de objeto expirado. Você também pode usar a ação Expiration para instruir o Amazon S3 a remover os marcadores de exclusão do objeto expirado. Para ver um exemplo, consulte Remover marcadores de exclusão de objetos expirados em um bucket com versionamento habilitado.

  Para ter mais informações, consulte Reter várias versões de objetos com o Versionamento do S3.

Ao configurar o Amazon S3 para gerenciar a expiração, considere também:

- Bucket com versionamento ativado

  Se a versão atual do objeto não for um marcador de exclusão, o Amazon S3 adicionará um com um ID exclusivo de versão. Isso torna a versão atual desatualizada, e o marcador de exclusão se torna a versão atual.

- Bucket com versionamento suspenso

  Em um bucket com versionamento suspenso, a ação de expiração faz com que o Amazon S3 crie um marcador de exclusão com `null` como ID de versão. Esse marcador de exclusão substitui qualquer versão de objeto por um ID de versão nulo na hierarquia de versões, que exclui o objeto.

Além disso, o Amazon S3 fornece as seguintes ações que você pode usar para gerenciar versões de objeto não atuais em um bucket com versão (isto é, buckets com versionamento ativado e suspenso).

- Elemento de ação **`NoncurrentVersionTransition`**: use essa ação para especificar quando o Amazon S3 deve realizar a transição de objetos para a classe de armazenamento especificada. Essa transição pode se basear em determinado número de dias desde o momento em que os objetos se tornam desatualizados (`<NoncurrentDays>`). Além do número de dias, você também pode especificar o número de versões desatualizadas (`<NewerNoncurrentVersions>`) que devem ser retidas (entre 1 e 100). Esse valor determina quantas versões desatualizadas mais recentes devem existir antes que o Amazon S3 possa fazer a transição de determinada versão. O Amazon S3 fará a transição de qualquer versão adicional não atual que ultrapasse o número especificado para reter. Para que a transição ocorra, os valores `<NoncurrentDays>` e `<NewerNoncurrentVersions>` devem ser excedidos.

  Para especificar o número de versões desatualizadas que devem ser retidas, também é necessário fornecer um elemento `<Filter>`. Se você não especificar um elemento `<Filter>`, o Amazon S3 gerará um erro `InvalidRequest` quando você especificar o número de versões desatualizadas.

  Para obter mais informações sobre transição de objetos, consulte Transições aceitas. Para obter detalhes sobre como o Amazon S3 calcula a data para especificar o número de dias na ação `NoncurrentVersionTransition`, consulte Regras de ciclo de vida: com base na idade de um objeto.

- Elemento de ação **`NoncurrentVersionExpiration`**: use essa ação para especificar que o Amazon S3 exclua permanentemente versões de objetos não atuais. Esses objetos excluídos não podem ser recuperados. Esse prazo de validade pode se basear em determinado número de dias desde o momento em que os objetos se tornam desatualizados (`<NoncurrentDays>`). Além do número de dias, você também pode especificar o número de versões desatualizadas (`<NewerNoncurrentVersions>`) que devem ser retidas (entre 1 e 100). Esse valor especifica quantas versões desatualizadas mais recentes devem existir antes que o Amazon S3 possa prescrever determinada versão. O Amazon S3 excluirá permanentemente qualquer versão adicional não atual que ultrapasse o número especificado para reter. Para que a exclusão ocorra, os valores `<NoncurrentDays>` e `<NewerNoncurrentVersions>` devem ser excedidos.

  Para especificar o número de versões desatualizadas que devem ser retidas, também é necessário fornecer um elemento `<Filter>`. Se você não especificar um elemento `<Filter>`, o Amazon S3 gerará um erro `InvalidRequest` quando você especificar o número de versões desatualizadas.

  A remoção atrasada de objetos não atuais pode ser útil quando é necessário corrigir exclusões ou substituições acidentais. Por exemplo, você pode configurar uma regra de expiração para excluir versões não atuais cinco dias após ficarem nesse estado. Por exemplo, imagine que, em 1.º/1/2014, às 10h30 UTC, você crie um objeto denominado `photo.gif` (ID de versão 111111). Em 2/1/2014, às 11h30 UTC, você exclui acidentalmente `photo.gif` (ID de versão 111111), o que cria um marcador de exclusão com um novo ID de versão (como ID de versão 4857693). Agora você tem cinco dias para recuperar a versão original de `photo.gif` (ID de versão 111111) até que a exclusão seja permanente. Em 8/1/2014, à 0h UTC, a regra de ciclo de vida para expiração executa e exclui permanentemente `photo.gif` (ID de versão 111111), cinco dias depois de se tornar uma versão não atual.

  Para obter detalhes sobre como o Amazon S3 calcula a data para especificar o número de dias em uma ação `NoncurrentVersionExpiration`, consulte Regras de ciclo de vida: com base na idade de um objeto.

  > **Note**
  >
  > As configurações de ciclo de vida de expiração do objeto não removem carregamentos fracionados incompletos. Para remover carregamentos fracionados incompletos, você deve usar a ação de configuração de ciclo de vida `AbortIncompleteMultipartUpload`, que é descrita posteriormente nesta seção.

Além das ações de transição e expiração, você pode usar as ações de configuração de ciclo de vida a seguir para instruir o Amazon S3 a interromper carregamentos fracionados incompletos.

- Elemento de ação**`AbortIncompleteMultipartUpload`**: use esse elemento para definir o tempo máximo (em dias) em que você deseja permitir que os carregamentos fracionados continuem em andamento. Se os carregamentos fracionados aplicáveis (determinados pelo `prefix` de nome de chave especificado na regra de ciclo de vida) não forem concluídos no período predefinido, o Amazon S3 interromperá os carregamentos fracionados incompletos. Para ter mais informações, consulte Abortar um multipart upload.

  > **Note**
  >
  > Não é possível especificar essa ação de ciclo de vida em uma regra que tenha um filtro que use tags de objeto.

- Elemento de ação **`ExpiredObjectDeleteMarker`**: em um bucket com versionamento habilitado, um marcador de exclusão sem versões não atuais é chamado de marcador de exclusão de objeto expirado. Você pode usar essa ação de ciclo de vida para instruir o Amazon S3 a remover marcadores de exclusão de objeto expirado. Para obter um exemplo, consulte Remover marcadores de exclusão de objetos expirados em um bucket com versionamento habilitado.

  > **Note**
  >
  > Não é possível especificar essa ação de ciclo de vida em uma regra que tenha um filtro que use tags de objeto.

Como o Amazon S3 calcula quanto tempo um objeto ficou desatualizado

Em um bucket com versionamento habilitado, é possível ter várias versões de um objeto. Há sempre uma versão atual e zero ou mais versões desatualizadas. Sempre que você faz upload de um objeto, a versão atual é retida como a versão não atual e a versão recém-adicionada, a sucessora, se torna a versão atual. Para determinar o número de dias que um objeto fica desatualizado, o Amazon S3 observa quando o sucessor foi criado. O Amazon S3 usa o número de dias desde que o sucessor foi criado como o número de dias que um objeto fica desatualizado.

Restaurar versões anteriores de um objeto ao usar configurações do S3 Lifecycle

Como explicado em Restaurar versões anteriores, você pode usar qualquer um dos dois métodos seguintes para recuperar versões anteriores de um objeto:

- Método 1: copiar uma versão não atual do objeto no mesmo bucket. O objeto copiado torna-se a versão atual desse objeto e todas as versões são preservadas.
- Método 2: excluir permanentemente a versão atual do objeto. Ao excluir a versão atual do objeto, você acaba transformando a versão não atual na versão atual do objeto.

Quando você estiver usando regras de configuração do S3 Lifecycle com buckets habilitados para versionamento, a prática recomendada é usar o método 1.
O S3 Lifecycle opera sob um modelo de consistência final. Existe a possibilidade de uma versão atual excluída permanentemente não desaparecer enquanto as alterações não forem propagadas para todos os sistemas do Amazon S3. (Por isso, temporariamente, o Amazon S3 pode não perceber essa exclusão.) Entretanto, a regra de ciclo de vida configurada para a validade de objetos desatualizados pode remover permanentemente objetos desatualizados, inclusive aquele que você deseja restaurar. Portanto, copiar a versão antiga, como recomendado no método 1, é uma alternativa mais confiável.

Ações de ciclo de vida e estado de versionamento do bucket

Regras de ciclo de vida: com base na idade de um objeto

É possível especificar um período, em número de dias desde a criação (ou modificação) do objeto, no qual o Amazon S3 pode realizar a ação especificada.

Quando você especificar o número de dias nas ações `Transition` e `Expiration` em uma configuração de ciclo de vida do S3, observe o seguinte:

- O valor que você especifica é o número de dias que devem transcorrer desde a criação do objeto para que a ação ocorra.
- O Amazon S3 calcula o tempo, adicionando o número de dias especificado na regra ao momento de criação do objeto e arredondando o tempo resultante para a meia-noite UTC do próximo dia. Por exemplo, se um objeto foi criado em 15/1/2014, às 10h30 UTC, e você especificar três dias em uma regra de transição, a data de transição do objeto será calculada como 19/1/2014, 0h UTC.

> **Note**
>
> O Amazon S3 mantém apenas a data da última modificação para cada objeto. Por exemplo, o console do Amazon S3 mostra a data Última modificação no painel Propriedades do objeto. Quando você cria inicialmente um objeto, essa data reflete a data em que o objeto é criado. Se você substituir o objeto, a data será alterada conforme necessário. Portanto, a data de criação é idêntica à data da Última modificação.

Ao especificar o número de dias nas ações `NoncurrentVersionTransition` e `NoncurrentVersionExpiration` em uma configuração de ciclo de vida, observe o seguinte:

- O valor que você especifica é o número de dias que devem transcorrer desde o momento em que a versão do objeto se torna desatualizada (ou seja, quando o objeto é sobrescrito ou excluído) para que o Amazon S3 execute a ação em um ou mais objetos especificados.
- O Amazon S3 calcula o tempo, adicionando o número de dias especificado na regra ao momento em que a nova versão sucessora do objeto é criada e arredondando o tempo resultante para a meia-noite UTC do próximo dia. Por exemplo, no seu bucket, suponha que a versão atual de um objeto foi criada em 1º./1/2014, às 10h30 UTC. Se a nova versão do objeto que substitui a atual tiver sido criada em 15/1/2014, às 10h30 UTC, e você especificar uma regra de transição de três dias, a data de transição do objeto será calculada como 19/1/2014, 0h UTC.

Regras de ciclo de vida: com base em uma data especificada

Ao especificar uma ação em uma regra de ciclo de vida do S3, é possível especificar uma data em que deseja que o Amazon S3 realize a ação. Quando a data especificada chegar, o Amazon S3 aplicará a ação a todos os objetos qualificados (com base nos critérios de filtro).

Se você especificar uma ação do S3 Lifecycle com uma data no passado, todos os objetos qualificados estarão imediatamente qualificados para essa ação de ciclo de vida.

> **Important**
>
> A ação com base em data não é uma ação única. O Amazon S3 continuará aplicando a ação com base em data mesmo após a data ter passado, contanto que o status da regra seja `Enabled`.
>
> Por exemplo, imagine que você especifique uma ação `Expiration` com base em data para excluir todos os objetos (supondo que nenhum filtro seja especificado na regra). Na

data especificada, o Amazon S3 expira todos os objetos no bucket. O Amazon S3 também continuará invalidando todos os objetos que você criar no bucket. Para interromper a ação de ciclo de vida, você deve remover a ação da regra de ciclo de vida, desabilitar a regra ou excluir a regra da configuração de ciclo de vida.

O valor de data deve estar em conformidade com o formato ISO 8601. A hora é sempre meia-noite (UTC).

> **Note**
>
> Não é possível criar regras de ciclo de vida com base em data usando o console do Amazon S3, mas você pode visualizar, desabilitar ou excluir essas regras.

Como adicionar filtros a regras de ciclo de vida

Os filtros são um elemento opcional das regras de ciclo de vida que você pode usar para especificar a quais objetos a regra se aplica.

Os elementos a seguir podem ser usados para filtrar objetos:

Prefixo de chaves

É possível filtrar objetos com base em um prefixo. Caso queira aplicar uma ação de ciclo de vida a um subconjunto de objetos com diferentes prefixos, crie regras separadas para cada ação.

Tags de objeto

É possível filtrar objetos com base em uma ou mais tags. Cada tag deve corresponder exatamente à chave e ao valor e, se você especificar várias tags, cada chave de tag deve ser exclusiva. Um filtro com várias tags de objeto se aplica a um subconjunto de objetos que tenha todas as tags especificadas. Se um objeto tiver tags adicionais especificadas, o filtro ainda será aplicado.

> **Note**
>
> Se você especificar somente um elemento `Key` e nenhum elemento `Value`, a regra será aplicada apenas aos objetos que corresponderem à chave da tag e que não tenham um valor especificado.

Tamanho mínimo ou máximo do objeto

É possível filtrar objetos com base no tamanho. É possível especificar um tamanho mínimo (`ObjectSizeGreaterThan`), um tamanho máximo (`ObjectSizeLessThan`) ou um intervalo de tamanhos de objeto no mesmo filtro. Os valores de tamanho de objeto estão em bytes. O tamanho máximo do filtro é 5 TB. O Amazon S3 aplica um tamanho mínimo padrão de objeto à configuração do ciclo de vida. Para obter mais informações, consulte Exemplo: permitir que objetos com menos de 128 KB sejam transferidos.

É possível combinar diferentes elementos de filtro e, nesse caso, o Amazon S3 usa um `AND` lógico.

Exemplos de filtro

Os exemplos a seguir mostram como você pode usar elementos de filtro diferentes:

- Especificação de um filtro usando prefixos de chave: este exemplo mostra uma regra do S3 Lifecycle que se aplica a um subconjunto de objetos com base no prefixo de nome de chave (`logs/`). Por exemplo, a regra de ciclo de vida se aplica aos objetos `logs/mylog.txt`, `logs/temp1.txt` e `logs/test.txt`. A regra não se aplica ao objeto `example.jpg`.

```
<LifecycleConfiguration>
    <Rule>
        <Filter>
           <Prefix>logs/</Prefix>
        </Filter>
        transition/expiration actions
         ...
    </Rule>
    ...
</LifecycleConfiguration>
```

> **Note**
>
> Se você tiver um ou mais prefixos que comecem com os mesmos caracteres, poderá incluir todos esses prefixos em sua regra especificando um prefixo parcial sem barra (`/`) no filtro. Por exemplo, suponha que você tenha estes prefixos:
>
> ```
> sales1999/
>                sales2000/
> ```

```
                sales2001/
```

Para incluir todos os três prefixos na regra, especifique `sales` como prefixo na regra de ciclo de vida.

Caso queira aplicar uma ação de ciclo de vida a um subconjunto de objetos com base em prefixos de nome de chave diferentes, especifique regras separadas. Em cada regra, especifique um filtro com base em prefixo. Por exemplo, para descrever uma ação de ciclo de vida para objetos com prefixos de chave `projectA/` e `projectB/`, especifique duas regras da seguinte forma:

```
<LifecycleConfiguration>
    <Rule>
        <Filter>
           <Prefix>projectA/</Prefix>
        </Filter>
        transition/expiration actions
         ...
    </Rule>

    <Rule>
        <Filter>
           <Prefix>projectB/</Prefix>
        </Filter>
        transition/expiration actions
         ...
    </Rule>
</LifecycleConfiguration>
```

Para obter mais informações sobre chaves de objeto, consulte Nomear objetos do Amazon S3.

- Especificação de um filtro com base em tags de objeto: no exemplo a seguir, a regra de ciclo de vida especifica um filtro com base em uma tag (*key*) e valor (*value*). A regra aplica-se somente a um subconjunto de objetos com a tag específica.

```
<LifecycleConfiguration>
    <Rule>
        <Filter>
           <Tag>
              <Key>key</Key>
              <Value>value</Value>
```

```
            </Tag>
        </Filter>
        transition/expiration actions
        ...
    </Rule>
</LifecycleConfiguration>
```

Você pode especificar um filtro com base em várias tags. Você deve encapsular as tags no elemento <And>, como mostrado no exemplo a seguir. A regra instrui o Amazon S3 a executar ações de ciclo de vida em objetos com duas tags (com a chave e o valor específicos da tag).

```
<LifecycleConfiguration>
    <Rule>
      <Filter>
         <And>
            <Tag>
               <Key>key1</Key>
               <Value>value1</Value>
            </Tag>
            <Tag>
               <Key>key2</Key>
               <Value>value2</Value>
            </Tag>
             ...
         </And>
      </Filter>
      transition/expiration actions
    </Rule>
</Lifecycle>
```

A regra de ciclo de vida se aplica a objetos que têm ambas as tags especificadas. O Amazon S3 realiza uma operação AND lógica. Observe o seguinte:

- Cada tag deve corresponder exatamente a ambos: à chave e ao valor. Se você especificar somente um elemento <Key> e nenhum elemento <Value>, a regra será aplicada apenas aos objetos que corresponderem à chave da tag e que não tenham um valor especificado.
- A regra se aplica a um subconjunto de objetos que tem todas as tags especificadas na regra. Se um objeto tiver tags adicionais especificadas, a regra ainda será aplicada.

> **Note**
>
> Quando você especifica várias tags em um filtro, cada chave de tag deve ser exclusiva.

- Especificação de um filtro com base no prefixo e em uma ou mais tags: em uma regra de ciclo de vida, você pode especificar um filtro com base no prefixo de chaves e em uma ou mais tags. Além disso, você deve incluir tudo isso no elemento <And>, como mostrado a seguir.

```
<LifecycleConfiguration>
    <Rule>
        <Filter>
          <And>
             <Prefix>key-prefix</Prefix>
             <Tag>
                <Key>key1</Key>
                <Value>value1</Value>
             </Tag>
             <Tag>
                <Key>key2</Key>
                <Value>value2</Value>
             </Tag>
              ...
          </And>
        </Filter>
        <Status>Enabled</Status>
        transition/expiration actions
    </Rule>
</LifecycleConfiguration>
```

  O Amazon S3 combina esses filtros usando uma operação AND lógica. Isto é, a regra aplica-se ao subconjunto de objetos com o prefixo de chave especificado e as tags especificadas. Um filtro pode ter somente um prefixo e zero ou mais tags.

- Especificar um filtro vazio: é possível especificar um filtro vazio e, nesse caso, a regra se aplica a todos os objetos no bucket.

```
<LifecycleConfiguration>
    <Rule>
        <Filter>
        </Filter>
        <Status>Enabled</Status>
```

```
        transition/expiration actions
    </Rule>
</LifecycleConfiguration>
```

- Especificar um filtro de tamanho de objeto: para filtrar uma regra por tamanho do objeto, é possível especificar um tamanho mínimo (`ObjectSizeGreaterThan`), um tamanho máximo (`ObjectSizeLessThan`) ou um intervalo de tamanhos de objeto.

  Os valores de tamanho de objeto estão em bytes. O tamanho máximo do filtro é 5 TB. Algumas classes de armazenamento têm limitações mínimas de tamanho. Para obter mais informações, consulte Comparar as classes de armazenamento do Amazon S3.

```
<LifecycleConfiguration>
    <Rule>
        <Filter>
            <ObjectSizeGreaterThan>500</ObjectSizeGreaterThan>
        </Filter>
        <Status>Enabled</Status>
        transition/expiration actions
    </Rule>
</LifecycleConfiguration>
```

> **Note**
>
> Os filtros `ObjectSizeGreaterThan` e `ObjectSizeLessThan` excluem os valores especificados. Por exemplo, se você definir objetos com tamanho de 128 KB a 1.024 KB para mover da classe de armazenamento S3 Standard para a classe de armazenamento S3 Standard-IA, os objetos que têm exatamente 1.024 KB e 128 KB não farão a transição para S3 Standard-IA. Em vez disso, a regra se aplicará somente a objetos maiores que 128 KB e menores que 1.024 KB de tamanho.

  Se você estiver especificando um intervalo de tamanho de objeto, o número inteiro `ObjectSizeGreaterThan` deve ser menor que o valor de `ObjectSizeLessThan`. Ao usar mais de um filtro, é necessário fazer a quebra dos filtros em um elemento `<And>`. O exemplo a seguir mostra como especificar objetos em um intervalo entre 500 e 64.000 bytes.

```
<LifecycleConfiguration>
    <Rule>
```

```
        <Filter>
            <And>
                <Prefix>key-prefix</Prefix>
                <ObjectSizeGreaterThan>500</ObjectSizeGreaterThan>
                <ObjectSizeLessThan>64000</ObjectSizeLessThan>
            </And>
        </Filter>
        <Status>Enabled</Status>
        transition/expiration actions
    </Rule>
</LifecycleConfiguration>
```

Como o Amazon S3 lida com conflitos nas configurações do ciclo de vida

Geralmente, o ciclo de vida do Amazon S3 otimiza o custo. Por exemplo, se duas políticas de expiração se sobrepuserem, a mais curta será honrada para que os dados não sejam armazenados por mais tempo do que o esperado. Do mesmo modo, se duas políticas de transição se sobrepuserem, o ciclo de vida do S3 irá fazer a transição dos seus objetos para a classe de armazenamento de menor custo.

Nos dois casos, o ciclo de vida do S3 tenta escolher o caminho com menos custo para você. Uma exceção a essa regra geral é com a classe de armazenamento S3 Intelligent-Tiering. O S3 Intelligent-Tiering é favorecido pelo Ciclo de Vida do S3 em qualquer classe de armazenamento, além das classes de armazenamento S3 Glacier e S3 Glacier Deep Archive.

Quando você tem várias regras em uma configuração do ciclo de vida do S3, um objeto pode se tornar elegível para várias ações do ciclo de vida do S3 no mesmo dia. Nesses casos, o Amazon S3 segue estas regras gerais:

- A exclusão permanente tem precedência sobre a transição.
- A transição tem precedência sobre a criação de marcadores de exclusão.
- Quando um objeto é elegível para transição às classes S3 Glacier Flexible Retrieval e S3 Standard-IA (ou S3 One Zone-IA), o Amazon S3 escolhe a transição para a classe S3 Glacier Flexible Retrieval.

Exemplos de filtros sobrepostos e ações de ciclo de vida conflitantes

Você pode especificar uma configuração de ciclo de vida do S3 em que especifica prefixos ou ações sobrepostos. Os exemplos a seguir mostram como o Amazon S3 resolve possíveis conflitos.

Example 1: prefixos sobrepostos (nenhum conflito)

O exemplo de configuração a seguir tem duas regras especificando prefixos sobrepostos da seguinte maneira:

- A primeira regra especifica um filtro vazio, indicando todos os objetos no bucket.
- A segunda regra especifica um prefixo de nome de chave (`logs/`) indicando somente um subconjunto de objetos.

A Regra 1 solicita que o Amazon S3 exclua todos os objetos um ano após a criação. A Regra 2 solicita que o Amazon S3 faça a transição de um subconjunto de objetos para a classe de armazenamento do S3 Standard – IA 30 dias após a criação.

```
<LifecycleConfiguration>
  <Rule>
    <ID>Rule 1</ID>
    <Filter>
    </Filter>
    <Status>Enabled</Status>
    <Expiration>
      <Days>365</Days>
    </Expiration>
  </Rule>
  <Rule>
    <ID>Rule 2</ID>
    <Filter>
      <Prefix>logs/</Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <StorageClass>STANDARD_IA</StorageClass>
      <Days>30</Days>
    </Transition>
   </Rule>
</LifecycleConfiguration>
```

Como não há conflito nesse caso, o Amazon S3 fará a transição dos objetos com o prefixo `logs/` para a classe de armazenamento S3 Standard – IA 30 dias após a criação. Ao atingir um ano após a criação, qualquer objeto será excluído.

Example 2: ações de ciclo de vida conflitantes

Nesta configuração de exemplo, há duas regras que levam o Amazon S3 a executar ao mesmo tempo duas diferentes ações no mesmo conjunto de objetos na vida útil do objeto:

- Ambas as regras especificam o mesmo prefixo de nome de chave, de modo que ambas as regras se aplicam ao mesmo conjunto de objetos.
- Ambas as regras especificam os mesmos 365 dias após a criação de objeto quando as regras se aplicam.
- Uma regra leva o Amazon S3 a fazer a transição de objetos para a classe de armazenamento S3 Standard – IA e outra regra quer que o Amazon S3 expire os objetos ao mesmo tempo.

```
<LifecycleConfiguration>
  <Rule>
    <ID>Rule 1</ID>
    <Filter>
      <Prefix>logs/</Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Expiration>
      <Days>365</Days>
    </Expiration>
  </Rule>
  <Rule>
    <ID>Rule 2</ID>
    <Filter>
      <Prefix>logs/</Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <StorageClass>STANDARD_IA</StorageClass>
      <Days>365</Days>
    </Transition>
   </Rule>
</LifecycleConfiguration>
```

Nesse caso, como você deseja que os objetos percam a validade (sejam removidos), não faz sentido mudar a classe de armazenamento, então o Amazon S3 simplesmente escolhe a ação de validade desses objetos.

Example 3: prefixos sobrepostos que resultam em ações de ciclo de vida conflitantes

Neste exemplo, a configuração tem duas regras, que especificam prefixos sobrepostos da seguinte maneira:

- A regra 1 especifica um prefixo vazio (indicando todos os objetos).
- A regra 2 especifica um prefixo de nome de chave (`logs/`) que identifica um subconjunto de todos os objetos.

Para o subconjunto de objetos com o prefixo de nome de chave `logs/`, as ações do S3 Lifecycle em ambas as regras se aplicam. Uma regra direciona o Amazon S3 a fazer a transição de objetos dez dias após a criação, e outra regra direciona o Amazon S3 a fazer a transição de objetos 365 dias após a criação.

```
<LifecycleConfiguration>
  <Rule>
    <ID>Rule 1</ID>
    <Filter>
      <Prefix></Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <StorageClass>STANDARD_IA</StorageClass>
      <Days>10</Days>
    </Transition>
  </Rule>
  <Rule>
    <ID>Rule 2</ID>
    <Filter>
      <Prefix>logs/</Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <StorageClass>STANDARD_IA</StorageClass>
      <Days>365</Days>
    </Transition>
   </Rule>
```

```
</LifecycleConfiguration>
```

Nesse caso, o Amazon S3 escolhe fazer a transição dos objetos 10 dias após a criação.

Example 4: filtragem baseada em tags e ações de ciclo de vida conflitantes resultantes

Suponha que você tenha a seguinte configuração de ciclo de vida do S3 que tem duas regras, cada uma especificando um filtro de tag:

- A regra 1 especifica um filtro baseado em tag (`tag1/value1`). Essa regra direciona o Amazon S3 para fazer a transição de objetos para a classe de armazenamento S3 Glacier Flexible Retrieval 365 dias após a criação.
- A regra 2 especifica um filtro baseado em tag (`tag2/value2`). Essa regra leva o Amazon S3 a expirar objetos 14 dias após a criação.

A configuração do S3 Lifecycle é apresentada como a seguir.

```
<LifecycleConfiguration>
  <Rule>
    <ID>Rule 1</ID>
    <Filter>
      <Tag>
         <Key>tag1</Key>
         <Value>value1</Value>
      </Tag>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <StorageClass>GLACIER</StorageClass>
      <Days>365</Days>
    </Transition>
  </Rule>
  <Rule>
    <ID>Rule 2</ID>
    <Filter>
      <Tag>
         <Key>tag2</Key>
         <Value>value2</Value>
      </Tag>
    </Filter>
    <Status>Enabled</Status>
    <Expiration>
```

```
      <Days>14</Days>
    </Expiration>
   </Rule>
</LifecycleConfiguration>
```

Se um objeto tiver as duas etiquetas, o Amazon S3 precisará decidir qual regra seguir. Nesse caso, o Amazon S3 expira o objeto 14 dias após a criação. O objeto é removido e, portanto, a ação de transição não é aplicada.

Exemplos de configurações do Ciclo de Vida do S3

Esta seção fornece exemplos de configuração do ciclo de vida do S3. Cada exemplo mostra como você pode especificar o XML em cada um dos cenários de exemplo.

Tópicos

- Arquivar todos os objetos em até um dia após a criação
- Desabilitar temporariamente as regras de ciclo de vida
- Rebaixar uma classe de armazenamento pela duração do ciclo de vida de um objeto
- Especificar várias regras
- Especificar uma regra de ciclo de vida para um bucket com versionamento habilitado
- Remover marcadores de exclusão de objetos expirados em um bucket com versionamento habilitado
- Configuração do Ciclo de Vida para anular carregamentos fracionados
- Expirar objetos desatualizados que não têm data
- Exemplo: permitir que objetos com menos de 128 KB sejam transferidos

Arquivar todos os objetos em até um dia após a criação

Cada regra do S3 Lifecycle inclui um filtro que pode ser usado para identificar um subconjunto de objetos em seu bucket ao qual a regra do S3 Lifecycle se aplica. As configurações de ciclo de vida do S3 a seguir mostram exemplos de como você pode especificar um filtro.

- Nesta regra de configuração do S3 Lifecycle, o filtro especifica um prefixo das chaves (`tax/`). Portanto, a regra aplica-se a objetos com o prefixo de nome de chave `tax/`, como `tax/doc1.txt` e `tax/doc2.txt`.

A regra especifica duas ações que direcionam o Amazon S3 a fazer o seguinte:

- Faça a transição de objetos para a classe de armazenamento S3 Glacier Flexible Retrieval 365 dias (um ano) após a criação.
- Exclua objetos (a ação `Expiration`) 3.650 dias (10 anos) após a criação.

```
<LifecycleConfiguration>
  <Rule>
    <ID>Transition and Expiration Rule</ID>
    <Filter>
       <Prefix>tax/</Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>365</Days>
      <StorageClass>GLACIER</StorageClass>
    </Transition>
    <Expiration>
      <Days>3650</Days>
    </Expiration>
  </Rule>
</LifecycleConfiguration>
```

Em vez de especificar a idade do objeto em termos de dias após a criação, você pode especificar uma data para cada ação. No entanto, você não pode usar `Date` e `Days` na mesma regra.

- Se você quiser que a regra do S3 Lifecycle se aplique a todos os objetos no bucket, especifique um prefixo vazio. Na configuração a seguir, a regra especifica uma ação `Transition` que direciona o Amazon S3 para fazer a transição de objetos para a classe de armazenamento S3 Glacier Flexible Retrieval 0 dia após a criação. Essa regra significa que os objetos são elegíveis para arquivamento na classe S3 Glacier Flexible Retrieval à meia-noite (UTC) após a criação. Para obter mais informações sobre restrições de ciclo de vida, consulte Restrições e considerações relativas a transições.

```
<LifecycleConfiguration>
  <Rule>
    <ID>Archive all object same-day upon creation</ID>
    <Filter>
      <Prefix></Prefix>
    </Filter>
    <Status>Enabled</Status>
```

```
    <Transition>
      <Days>0</Days>
      <StorageClass>GLACIER</StorageClass>
    </Transition>
  </Rule>
</LifecycleConfiguration>
```

- Você pode especificar zero ou um prefixo de nome de chave ou zero ou mais tags de objeto em um filtro. O exemplo de código a seguir aplica a regra do S3 Lifecycle a um subconjunto de objetos com prefixo das chaves `tax/` e a objetos que têm duas etiquetas com uma chave e um valor específicos. Ao especificar mais de um filtro, você deve incluir o elemento <And> conforme mostrado (o Amazon S3 aplica um elemento AND lógico para combinar as condições de filtro especificadas).

```
...
<Filter>
   <And>
      <Prefix>tax/</Prefix>
      <Tag>
         <Key>key1</Key>
         <Value>value1</Value>
      </Tag>
      <Tag>
         <Key>key2</Key>
         <Value>value2</Value>
      </Tag>
    </And>
</Filter>
...
```

- Você pode filtrar objetos com base apenas nas tags. Por exemplo, a regra do S3 Lifecycle a seguir aplica-se a objetos que tenham duas etiquetas especificadas (não especifica nenhum prefixo).

```
...
<Filter>
   <And>
      <Tag>
         <Key>key1</Key>
         <Value>value1</Value>
      </Tag>
      <Tag>
```

```
          <Key>key2</Key>
          <Value>value2</Value>
       </Tag>
    </And>
</Filter>
...
```

> **Important**
>
> Quando você tem várias regras em uma configuração do ciclo de vida do S3, um objeto pode se tornar elegível para várias ações do ciclo de vida do S3 no mesmo dia. Nesses casos, o Amazon S3 segue estas regras gerais:
>
> - A exclusão permanente tem precedência sobre a transição.
> - A transição tem precedência sobre a criação de marcadores de exclusão.
> - Quando um objeto é elegível para transição para as classes S3 Glacier Flexible Retrieval e S3 Standard-IA (ou S3 One Zone-IA), o Amazon S3 escolhe a transição para a classe S3 Glacier Flexible Retrieval.
>
> Para obter exemplos, consulte Exemplos de filtros sobrepostos e ações de ciclo de vida conflitantes.

Desabilitar temporariamente as regras de ciclo de vida

É possível desabilitar temporariamente uma regra do Ciclo de Vida do S3 usando o elemento `status`. Isso pode ser útil se você quiser testar novas regras ou solucionar problemas com sua configuração, sem substituir as regras existentes. A configuração do S3 Lifecycle a seguir especifica duas regras:

- Na regra 1, o Amazon S3 faz a transição de objetos com o prefixo `logs/` para a classe de armazenamento S3 Glacier Flexible Retrieval logo após a criação.
- Na regra 2, o Amazon S3 faz a transição de objetos com o prefixo `documents/` para a classe de armazenamento S3 Glacier Flexible Retrieval logo após a criação.

Na configuração, a regra 1 é habilitada e a regra 2 é desabilitada. O Amazon S3 ignora a regra desabilitada.

```
<LifecycleConfiguration>
  <Rule>
    <ID>Rule1</ID>
    <Filter>
      <Prefix>logs/</Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>0</Days>
      <StorageClass>GLACIER</StorageClass>
    </Transition>
  </Rule>
  <Rule>
    <ID>Rule2</ID>
    <Filter>
      <Prefix>documents/</Prefix>
    </Filter>
    <Status>Disabled</Status>
    <Transition>
      <Days>0</Days>
      <StorageClass>GLACIER</StorageClass>
    </Transition>
  </Rule>
</LifecycleConfiguration>
```

Rebaixar uma classe de armazenamento pela duração do ciclo de vida de um objeto

Neste exemplo, você usa a configuração do S3 Lifecycle para rebaixar a classe de armazenamento de objetos pela sua vida útil. O rebaixamento pode ajudar a reduzir os custos de armazenamento. Para obter mais informações sobre a definição de preços, consulte Definição de preços do Amazon S3.

A configuração do S3 Lifecycle a seguir especifica uma regra que se aplica a objetos com o prefixo de nome de chave `logs/`. A regra especifica as seguintes ações:

- Duas ações de transição:
  - Transição de objetos para a classe de armazenamento S3 Standard – IA 30 dias após a criação.

  - Faça a transição de objetos para a classe de armazenamento S3 Glacier Flexible Retrieval 90 dias após a criação.
- Uma ação de expiração que leva o Amazon S3 a excluir esses objetos um ano após a criação.

```
<LifecycleConfiguration>
  <Rule>
    <ID>example-id</ID>
    <Filter>
       <Prefix>logs/</Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>30</Days>
      <StorageClass>STANDARD_IA</StorageClass>
    </Transition>
    <Transition>
      <Days>90</Days>
      <StorageClass>GLACIER</StorageClass>
    </Transition>
    <Expiration>
      <Days>365</Days>
    </Expiration>
  </Rule>
</LifecycleConfiguration>
```

Note

Você pode usar uma regra para descrever todas as ações do S3 Lifecycle se todas as ações se aplicarem ao mesmo conjunto de objetos (identificados pelo filtro). Caso contrário, você pode adicionar várias regras com cada uma especificando um filtro diferente.

Important

Quando você tem várias regras em uma configuração do ciclo de vida do S3, um objeto pode se tornar elegível para várias ações do ciclo de vida do S3 no mesmo dia. Nesses casos, o Amazon S3 segue estas regras gerais:

  - A exclusão permanente tem precedência sobre a transição.

- A transição tem precedência sobre a criação de marcadores de exclusão.
- Quando um objeto é elegível para transição para as classes S3 Glacier Flexible Retrieval e S3 Standard-IA (ou S3 One Zone-IA), o Amazon S3 escolhe a transição para a classe S3 Glacier Flexible Retrieval.

Para obter exemplos, consulte Exemplos de filtros sobrepostos e ações de ciclo de vida conflitantes.

Especificar várias regras

Você pode especificar várias regras se quiser diferentes ações do S3 Lifecycle de diferentes objetos. A configuração do S3 Lifecycle a seguir tem duas regras:

- A regra 1 se aplica a objetos com prefixo de nome de chave `classA/`. Com ela, o Amazon S3 faz a transição de objetos para a classe de armazenamento S3 Glacier Flexible Retrieval um ano após a criação e expira esses objetos dez anos após a criação.
- A regra 2 se aplica a objetos com prefixo de nome de chave `classB/`. Ela direciona o Amazon S3 para fazer a transição de objetos para a classe de armazenamento S3 Standard – IA 90 dias após a criação e excluí-los um ano após a criação.

```
<LifecycleConfiguration>
    <Rule>
        <ID>ClassADocRule</ID>
        <Filter>
           <Prefix>classA/</Prefix>
        </Filter>
        <Status>Enabled</Status>
        <Transition>
           <Days>365</Days>
           <StorageClass>GLACIER</StorageClass>
        </Transition>
        <Expiration>
             <Days>3650</Days>
        </Expiration>
    </Rule>
    <Rule>
        <ID>ClassBDocRule</ID>
```

```
        <Filter>
            <Prefix>classB/</Prefix>
        </Filter>
        <Status>Enabled</Status>
        <Transition>
           <Days>90</Days>
           <StorageClass>STANDARD_IA</StorageClass>
        </Transition>
        <Expiration>
             <Days>365</Days>
        </Expiration>
    </Rule>
</LifecycleConfiguration>
```

Important

Quando você tem várias regras em uma configuração do ciclo de vida do S3, um objeto pode se tornar elegível para várias ações do ciclo de vida do S3 no mesmo dia. Nesses casos, o Amazon S3 segue estas regras gerais:

- A exclusão permanente tem precedência sobre a transição.
- A transição tem precedência sobre a criação de marcadores de exclusão.
- Quando um objeto é elegível para transição para as classes S3 Glacier Flexible Retrieval e S3 Standard-IA (ou S3 One Zone-IA), o Amazon S3 escolhe a transição para a classe S3 Glacier Flexible Retrieval.

Para obter exemplos, consulte Exemplos de filtros sobrepostos e ações de ciclo de vida conflitantes.

Especificar uma regra de ciclo de vida para um bucket com versionamento habilitado

Suponha que você tenha um bucket com versionamento habilitado, ou seja, para cada objeto, há uma versão atual e zero ou mais versões desatualizadas. (Para obter mais informações sobre o versionamento do S3, consulte Reter várias versões de objetos com o Versionamento do S3.)

No exemplo a seguir, você deseja manter o equivalente a um ano de histórico e reter cinco versões desatualizadas. As configurações do S3 Lifecycle permitem manter de 1 a 100 versões de qualquer objeto. Esteja ciente de que mais de cinco versões desatualizadas mais recentes devem existir antes

que o Amazon S3 possa prescrever determinada versão. O Amazon S3 excluirá permanentemente qualquer versão adicional não atual que ultrapasse o número especificado para reter. Para que a exclusão ocorra, os valores `NoncurrentDays` e `NewerNoncurrentVersions` devem ser excedidos.

Para economizar em custos de armazenamento, você deseja migrar as versões desatualizadas para o S3 Glacier Flexible Retrieval 30 dias depois de se tornarem desatualizadas (supondo que sejam dados frios, que você não precisa acessar em tempo real). Além disso, diante da expectativa de que a frequência de acesso das versões atuais diminua 90 dias após a criação, você pode optar por mover esses objetos para a classe de armazenamento S3 Standard-IA.

```
<LifecycleConfiguration>
    <Rule>
        <ID>sample-rule</ID>
        <Filter>
           <Prefix></Prefix>
        </Filter>
        <Status>Enabled</Status>
        <Transition>
           <Days>90</Days>
           <StorageClass>STANDARD_IA</StorageClass>
        </Transition>
        <NoncurrentVersionTransition>
            <NoncurrentDays>30</NoncurrentDays>
            <StorageClass>GLACIER</StorageClass>
        </NoncurrentVersionTransition>
       <NoncurrentVersionExpiration>
            <NewerNoncurrentVersions>5</NewerNoncurrentVersions>
            <NoncurrentDays>365</NoncurrentDays>
       </NoncurrentVersionExpiration>
    </Rule>
</LifecycleConfiguration>
```

Remover marcadores de exclusão de objetos expirados em um bucket com versionamento habilitado

Um bucket com versionamento habilitado mantém uma versão atual e nenhuma ou mais versões desatualizadas de cada objeto. Ao excluir um objeto, observe o seguinte:

- Se você não especificar um ID de versão na solicitação de exclusão, o Amazon S3 adicionará um marcador de exclusão em vez de excluir o objeto. A versão atual do objeto se torna desatualizada, e o marcador de exclusão se torna a versão atual.
- Se você especificar um ID de versão na solicitação de exclusão, o Amazon S3 excluirá permanentemente a versão do objeto (um marcador de exclusão não é criado).
- Um marcador de exclusão sem versões desatualizadas é chamado de marcador de exclusão do objeto expirado.

Este exemplo mostra um cenário que pode criar marcadores de exclusão de objetos expirados em seu bucket e como você pode usar a configuração de ciclo de vida do S3 para que o Amazon S3 remova os marcadores de exclusão de objetos expirados.

Suponha que você crie uma configuração da funcionalidade Ciclo de Vida do S3 que use a ação `NoncurrentVersionExpiration` para remover as versões desatualizadas 30 dias após se tornarem desatualizadas e reter dez versões desatualizadas, como mostrado a seguir. Esteja ciente de que mais de dez versões desatualizadas mais recentes devem existir antes que o Amazon S3 possa prescrever determinada versão. O Amazon S3 excluirá permanentemente qualquer versão adicional não atual que ultrapasse o número especificado para reter. Para que a exclusão ocorra, os valores `NoncurrentDays` e `NewerNoncurrentVersions` devem ser excedidos.

```
<LifecycleConfiguration>
    <Rule>
        ...
        <NoncurrentVersionExpiration>
            <NewerNoncurrentVersions>10</NewerNoncurrentVersions>
            <NoncurrentDays>30</NoncurrentDays>
        </NoncurrentVersionExpiration>
    </Rule>
</LifecycleConfiguration>
```

A ação `NoncurrentVersionExpiration` não se aplica às versões de objeto atualizadas. Ela remove apenas versões desatualizadas.

Para versões atuais do objeto, existem as opções abaixo para gerenciar o ciclo de vida. Tudo vai depender de as versões atuais seguirem um ciclo de vida bem definido:

- As versões atuais do objeto seguem um ciclo de vida bem definido.

Nesse caso, você pode usar a configuração de ciclo de vida do S3 com a ação `Expiration` para que o Amazon S3 remova as versões atuais, conforme exibido no exemplo a seguir.

```
<LifecycleConfiguration>
    <Rule>
        ...
        <Expiration>
           <Days>60</Days>
        </Expiration>
        <NoncurrentVersionExpiration>
            <NewerNoncurrentVersions>10</NewerNoncurrentVersions>
            <NoncurrentDays>30</NoncurrentDays>
        </NoncurrentVersionExpiration>
    </Rule>
</LifecycleConfiguration>
```

Neste exemplo, o Amazon S3 remove as versões atualizadas 60 dias após serem criadas adicionando um marcador de exclusão para cada uma das versões atualizadas do objeto. Esse processo torna a versão atual do objeto desatualizada, e o marcador de exclusão torna-se a versão atual. Para ter mais informações, consulte Reter várias versões de objetos com o Versionamento do S3.

> **Note**
>
> Não é possível especificar uma tag `Days` e uma `ExpiredObjectDeleteMarker` na mesma regra. Com a especificação da etiqueta `Days`, o Amazon S3 executará automaticamente a limpeza `ExpiredObjectDeleteMarker` assim que os marcadores de exclusão tiverem idade suficiente para satisfazer os critérios de idade. Para limpar marcadores de exclusão assim que eles se tornarem a única versão, crie uma regra separada contendo apenas a etiqueta `ExpiredObjectDeleteMarker`.

A ação `NoncurrentVersionExpiration` na mesma configuração do S3 Lifecycle remove os objetos desatualizados 30 dias após se tornarem desatualizados. Assim, neste exemplo, todas as versões de objeto são permanentemente removidas 90 dias após a criação do objeto. Esteja ciente de que, nesse exemplo, mais de dez versões desatualizadas mais recentes devem existir antes que o Amazon S3 possa prescrever determinada versão. O Amazon S3 excluirá permanentemente qualquer versão adicional não atual que ultrapasse o número especificado para reter. Para que

a exclusão ocorra, os valores `NoncurrentDays` e `NewerNoncurrentVersions` devem ser excedidos.

Embora marcadores de exclusão de objetos expirados sejam criados durante esse o processo, o Amazon S3 detecta e remove os marcadores de exclusão de objetos expirados para você.

- As versões atuais do objeto não têm um ciclo de vida bem definido.

  Neste caso, convém remover os objetos manualmente quando não forem mais necessários criando um marcador de exclusão com uma ou mais versões desatualizadas. Se a configuração do S3 Lifecycle com a ação `NoncurrentVersionExpiration` remover todas as versões desatualizadas, agora você terá marcadores de exclusão de objetos expirados.

  Especificamente para este cenário, a configuração do S3 Lifecycle fornece uma ação `Expiration` que você pode usar para remover os marcadores de exclusão de objetos expirados.

```
<LifecycleConfiguration>
    <Rule>
       <ID>Rule 1</ID>
        <Filter>
          <Prefix>logs/</Prefix>
        </Filter>
        <Status>Enabled</Status>
        <Expiration>
           <ExpiredObjectDeleteMarker>true</ExpiredObjectDeleteMarker>
        </Expiration>
        <NoncurrentVersionExpiration>
            <NewerNoncurrentVersions>10</NewerNoncurrentVersions>
            <NoncurrentDays>30</NoncurrentDays>
        </NoncurrentVersionExpiration>
    </Rule>
</LifecycleConfiguration>
```

Ao definir o elemento `ExpiredObjectDeleteMarker` como `true` na ação `Expiration`, você faz o Amazon S3 remover os marcadores de exclusão de objetos expirados.

> **Note**
>
> Ao usar a ação `ExpiredObjectDeleteMarker` do S3 Lifecycle, a regra não pode especificar um filtro baseado em etiqueta.

Configuração do Ciclo de Vida para anular carregamentos fracionados

Você pode usar as operações de API REST de carregamento fracionado do Amazon S3 para carregar objetos grandes em partes. Para obter mais informações sobre multipart uploads, consulte Carregar e copiar objetos usando upload fracionado no Amazon S3.

Usando a configuração do S3 Lifecycle, você pode levar o Amazon S3 a interromper carregamentos fracionados incompletos (identificados pelo prefixo de nome de chave especificado na regra) se eles não forem concluídos em um número especificado de dias após a inicialização. Ao interromper um carregamento fracionado, o Amazon S3 exclui todas as partes associadas ao carregamento fracionado. Esse processo ajuda a controlar os custos de armazenamento, garantindo que você não tenha carregamentos fracionados incompletos com partes que estão armazenadas no Amazon S3.

> **Note**
>
> Ao usar a ação `AbortIncompleteMultipartUpload` do S3 Lifecycle, a regra não pode especificar um filtro baseado em etiqueta.

Veja a seguir um exemplo de configuração de ciclo de vida do S3 que especifica uma regra com a ação `AbortIncompleteMultipartUpload`. Essa ação solicita que o Amazon S3 interrompa carregamentos fracionados incompletos sete dias após a inicialização.

```
<LifecycleConfiguration>
    <Rule>
        <ID>sample-rule</ID>
        <Filter>
           <Prefix>SomeKeyPrefix/</Prefix>
        </Filter>
        <Status>rule-status</Status>
        <AbortIncompleteMultipartUpload>
          <DaysAfterInitiation>7</DaysAfterInitiation>
        </AbortIncompleteMultipartUpload>
    </Rule>
```

```
</LifecycleConfiguration>
```

Expirar objetos desatualizados que não têm data

É possível criar regras que fazem a transição de objetos com base somente no tamanho. Você pode especificar um tamanho mínimo (`ObjectSizeGreaterThan`), um tamanho máximo (`ObjectSizeLessThan`) ou um intervalo de tamanhos de objeto em bytes. Ao usar mais de um filtro, como prefixo e regra de tamanho, é necessário quebrar os filtros em um elemento `<And>`.

```
<LifecycleConfiguration>
  <Rule>
    <ID>Transition with a prefix and based on size</ID>
    <Filter>
       <And>
          <Prefix>tax/</Prefix>
          <ObjectSizeGreaterThan>500</ObjectSizeGreaterThan>
       </And>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>365</Days>
      <StorageClass>GLACIER</StorageClass>
    </Transition>
  </Rule>
</LifecycleConfiguration>
```

Se você especificar um intervalo usando os elementos `ObjectSizeGreaterThan` e `ObjectSizeLessThan`, o tamanho máximo do objeto deverá ser maior que o tamanho mínimo do objeto. Ao usar mais de um filtro, é necessário fazer a quebra dos filtros em um elemento `<And>`. O exemplo a seguir mostra como especificar objetos em um intervalo entre 500 e 64.000 bytes. Quando você especifica um intervalo, os filtros `ObjectSizeGreaterThan` e `ObjectSizeLessThan` excluem os valores especificados. Para ter mais informações, consulte the section called “Elemento Filter”.

```
<LifecycleConfiguration>
    <Rule>
        ...
          <And>
             <ObjectSizeGreaterThan>500</ObjectSizeGreaterThan>
             <ObjectSizeLessThan>64000</ObjectSizeLessThan>
          </And>
```

```
    </Rule>
</LifecycleConfiguration>
```

Você também pode criar regras para expirar especificamente objetos desatualizados que não têm nenhum dado, incluindo objetos de marcador de exclusão desatualizados criados em um bucket com versionamento habilitado. O exemplo a seguir usa a ação `NoncurrentVersionExpiration` para remover as versões desatualizadas 30 dias após se tornarem desatualizadas e reter dez versões desatualizadas. Ele também usa o elemento `0bjectSizeLessThan` para filtrar somente objetos sem nenhum dado.

Esteja ciente de que mais de dez versões desatualizadas mais recentes devem existir antes que o Amazon S3 possa prescrever determinada versão. O Amazon S3 excluirá permanentemente qualquer versão adicional não atual que ultrapasse o número especificado para reter. Para que a exclusão ocorra, os valores `NoncurrentDays` e `NewerNoncurrentVersions` devem ser excedidos.

```
<LifecycleConfiguration>
  <Rule>
    <ID>Expire noncurrent with size less than 1 byte</ID>
    <Filter>
       <ObjectSizeLessThan>1</ObjectSizeLessThan>
    </Filter>
    <Status>Enabled</Status>
    <NoncurrentVersionExpiration>
       <NewerNoncurrentVersions>10</NewerNoncurrentVersions>
       <NoncurrentDays>30</NoncurrentDays>
    </NoncurrentVersionExpiration>
  </Rule>
</LifecycleConfiguration>
```

Exemplo: permitir que objetos com menos de 128 KB sejam transferidos

O Amazon S3 aplica um comportamento padrão às configurações de ciclo de vida que não permite a transferência de objetos com menos de 128 KB para nenhuma classe de armazenamento. Para permitir a transição de objetos menores, adicione um filtro de tamanho mínimo (`0bjectSizeGreaterThan`) ou tamanho máximo (`0bjectSizeLessThan`) à configuração que especifique um tamanho menor. O seguinte exemplo permite fazer a transição de qualquer objeto com menos de 128 KB para a classe de armazenamento S3 Glacier Instant Retrieval:

```
<LifecycleConfiguration>
```

```
  <Rule>
    <ID>Allow small object transitions</ID>
    <Filter>
          <ObjectSizeGreaterThan>1</ObjectSizeGreaterThan>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>365</Days>
      <StorageClass>GLACIER_IR</StorageClass>
    </Transition>
  </Rule>
</LifecycleConfiguration>
```

Note

Em setembro de 2024, o Amazon S3 atualizou o comportamento de transição padrão para objetos pequenos, da seguinte forma:

- Comportamento de transição padrão atualizado: desde setembro de 2024, o comportamento padrão não permite a transferência de objetos com menos de 128 KB para nenhuma classe de armazenamento.
- Comportamento de transição padrão anterior: antes de setembro de 2024, o comportamento padrão permitia que objetos com menos de 128 KB fossem transferidos somente para as classes de armazenamento S3 Glacier e S3 Glacier Deep Archive.

As configurações criadas antes de setembro de 2024 retêm o comportamento de transição anterior, a menos que você as modifique. Ou seja, se você criar, editar ou excluir regras, o comportamento de transição padrão da configuração mudará para o comportamento atualizado. Se seu caso de uso exigir, será possível alterar o comportamento de transição padrão para que objetos com menos de 128 KB façam a transição para o S3 Glacier e o S3 Glacier Deep Archive. Para fazer isso, use o cabeçalho opcional `x-amz-transition-object-size-minimum-default` em uma solicitação PutBucketLifecycleConfiguration.

O exemplo a seguir mostra como usar o cabeçalho `x-amz-transition-object-size-minimum-default` em uma solicitação PutBucketLifecycleConfiguration para aplicar o comportamento de transição padrão `varies_by_storage_class` a uma configuração da funcionalidade Ciclo de Vida do S3. Esse comportamento permite fazer a transição de objetos com

menos de 128 KB para as classes de armazenamento S3 Glacier ou S3 Glacier Deep Archive. Por padrão, todas as outras classes de armazenamento evitarão transições menores que 128 KB. Ainda é possível usar filtros personalizados para alterar o tamanho mínimo de transição para qualquer classe de armazenamento. Os filtros personalizados sempre têm precedência sobre o comportamento de transição padrão:

```
HTTP/1.1 200
x-amz-transition-object-size-minimum-default: varies_by_storage_class
<?xml version="1.0" encoding="UTF-8"?>
...
```

Solucionar problemas de ciclo de vida do Amazon S3

As informações a seguir podem ajudar você a solucionar problemas comuns com as regras de ciclo de vida do Amazon S3.

Tópicos

- Executei uma operação de lista no bucket e vi objetos que achei que estavam expirados ou que tinham sido transferidos de acordo com uma regra de ciclo de vida.
- Como monitorar as ações realizadas pelas minhas regras de ciclo de vida?
- Minha quantidade de objetos do S3 ainda aumenta, mesmo depois de configurar as regras do ciclo de vida em um bucket habilitado para versionamento.
- Como esvaziar meu bucket do S3 usando regras de ciclo de vida?
- Minha fatura do Amazon S3 aumentou após a transição de objetos para uma classe de armazenamento de menor custo.
- Eu atualizei minha política de bucket, mas meus objetos do S3 ainda estão sendo excluídos pelas regras de ciclo de vida expiradas.
- Posso recuperar objetos do S3 que expiraram pelas regras do ciclo de vida do S3?
- Por que minhas ações do ciclo de vida de expiração e transição não estão ocorrendo?
- Como faço para excluir um prefixo da minha regra de ciclo de vida?
- Como faço para incluir vários prefixos na minha regra de ciclo de vida?

Executei uma operação de lista no bucket e vi objetos que achei que estavam expirados ou que tinham sido transferidos de acordo com uma regra de ciclo de vida.

As transições de objetos e as expirações de objetos do ciclo de vida do S3 são operações assíncronas. Portanto, pode haver um atraso entre o momento em que os objetos são elegíveis para expiração ou transição e o momento em que eles realmente são transferidos ou expirados. As alterações no faturamento são aplicadas assim que a regra do ciclo de vida é cumprida, mesmo que a ação não seja concluída. A única exceção a esse comportamento é se você tiver uma regra de ciclo de vida definida para transição à classe de armazenamento S3 Intelligent-Tiering. Nesse caso, as alterações no faturamento não acontecerão até que o objeto tenha feito a transição para o S3 Intelligent-Tiering. Para obter mais informações sobre mudanças no faturamento, consulte Definir a configuração do ciclo de vida em um bucket.

> **Note**
>
> O Amazon S3 não faz a transição de objetos com menos de 128 KB da classe de armazenamento S3 Standard ou S3 Standard-IA para a classe de armazenamento S3 Intelligent-Tiering, S3 Standard-IA ou S3 One Zone-IA.

Como monitorar as ações realizadas pelas minhas regras de ciclo de vida?

Para monitorar as ações realizadas por regras de ciclo de vida, use os seguintes recursos:

- Notificações de eventos do S3: é possível configurar notificações de eventos do S3 para receber notificações sobre qualquer evento de transição ou expiração do ciclo de vida do S3.
- Logs de acesso ao servidor do S3: é possível habilitar logs de acesso ao servidor para os buckets do S3 a fim de capturar ações relacionadas ao ciclo de vida do S3, como transições de objetos para outra classe de armazenamento e expirações de objeto. Para obter mais informações, consulte Ciclo de vida e log.

Para visualizar diariamente as mudanças em seu armazenamento causadas pelas ações do ciclo de vida, recomendamos usar os painéis da Lente de Armazenamento do S3 em vez de usar as métricas do Amazon CloudWatch. No painel da Lente de Armazenamento, é possível visualizar as seguintes métricas, que monitoram a quantidade ou tamanho do objeto:

- Bytes da versão atual

- Contagem de objetos da versão atual
- Bytes de versão não atual
- Número de objetos de versões não atuais
- Contagem de objetos do marcador de exclusão
- Bytes de armazenamento do marcador de exclusão
- Bytes de uploads incompletos de várias partes
- Contagem de objetos de multipart upload incompletos

Minha quantidade de objetos do S3 ainda aumenta, mesmo depois de configurar as regras do ciclo de vida em um bucket habilitado para versionamento.

Quando um objeto está expirado em um bucket com versionamento habilitado, ele não é completamente excluído do bucket. Em vez disso, um marcador de exclusão é criado como a versão mais recente do objeto. Os marcadores de exclusão ainda são contados como objetos. Portanto, se uma regra de ciclo de vida for criada para expirar somente nas versões atuais, a contagem de objetos no bucket do S3 realmente aumentará em vez de diminuir.

Por exemplo, digamos que um bucket do S3 tenha o versionamento ativado com 100 objetos, e uma regra de ciclo de vida esteja configurada para expirar as versões atuais do objeto após sete dias. Após o sétimo dia, a quantidade de objetos aumenta para 200 porque 100 marcadores de exclusão são criados além dos 100 objetos originais, que agora são as versões não atuais. Para obter mais informações sobre as ações da regra de configuração do ciclo de vida do S3 para buckets com versionamento ativado, consulte Definir a configuração do ciclo de vida em um bucket.

Para remover objetos permanentemente, adicione uma configuração de ciclo de vida adicional para excluir as versões anteriores dos objetos, os marcadores de exclusão expirados e os uploads incompletos de várias partes. Para obter instruções sobre como criar regras de ciclo de vida, consulte Definir a configuração do ciclo de vida em um bucket.

> **Note**
>
> - O Amazon S3 arredonda a data de transição ou expiração de um objeto para a meia-noite UTC do dia seguinte.
>
> Ao avaliar objetos com relação às ações do ciclo de vida, o Amazon S3 usa o horário de criação do objeto em UTC. Por exemplo, considere um bucket sem versionamento com

uma regra de ciclo de vida configurada para expirar objetos após um dia. Suponha que um objeto tenha sido criado em 1.º de janeiro às 17h05, Horário de Verão do Pacífico (PDT), que corresponde a 2 de janeiro às 0h05 UTC. O objeto tem um dia de vida às 0h05 UTC de 3 de janeiro, o que o torna elegível para expiração quando o ciclo de vida do S3 avalia os objetos às 0h00 UTC de 4 de janeiro.

Como as ações do ciclo de vida do Amazon S3 ocorrem de forma assíncrona, pode haver algum atraso entre a data especificada na regra do ciclo de vida e a transição física real do objeto. Consulte mais informações em Atraso na transição ou na expiração.

Para obter mais informações, consulte Regras de ciclo de vida: com base na idade de um objeto.

- Para objetos S3 protegidos pelo bloqueio de objetos, as versões atuais não são excluídas permanentemente. Em vez disso, um marcador de exclusão é adicionado aos objetos, tornando-os não atuais. As versões não atuais são então preservadas e não expiram permanentemente.

Como esvaziar meu bucket do S3 usando regras de ciclo de vida?

As regras do ciclo de vida do S3 são uma ferramenta eficaz para esvaziar um bucket do S3 com milhões de objetos. Para excluir um grande número de objetos do bucket do S3, use estes dois pares de regras de ciclo de vida:

- Expire as versões atuais dos objetos e Exclua permanentemente as versões anteriores dos objetos
- Exclua marcadores de exclusão expirados e Exclua uploads incompletos de várias partes

Para ver as etapas de como criar regras de configuração de ciclo de vida, consulte Definir a configuração do ciclo de vida em um bucket.

> **Note**
>
> Para objetos S3 protegidos pelo bloqueio de objetos, as versões atuais não são excluídas permanentemente. Em vez disso, um marcador de exclusão é adicionado aos objetos, tornando-os não atuais. As versões não atuais são então preservadas e não expiram permanentemente.

Minha fatura do Amazon S3 aumentou após a transição de objetos para uma classe de armazenamento de menor custo.

Há vários motivos pelos quais sua fatura pode aumentar após a transição de objetos para uma classe de armazenamento de menor custo:

- Sobrecarga do S3 Glacier cobra por objetos pequenos

  Para cada objeto que é transferido para o S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive, uma sobrecarga total de 40 KB é associada a essa atualização de armazenamento. Como parte da sobrecarga de 40 KB, 8 KB são usados para armazenar os metadados e o nome do objeto. Esses 8 KB são cobrados de acordo com as tarifas do S3 Standard. Os 32 KB restantes são usados para indexação e metadados relacionados. Esses 32 KB são cobrados de acordo com os preços do S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive.

  Portanto, se você estiver armazenando muitos objetos menores, não recomendamos o uso de transições de ciclo de vida. Em vez disso, para reduzir as despesas adicionais, considere a possibilidade de agregar vários objetos menores em um número menor de objetos grandes antes de armazená-los no Amazon S3. Para obter mais informações sobre as considerações de custo, consulte Transição para as classes de armazenamento S3 Glacier Flexible Retrieval e S3 Glacier Deep Archive (arquivamento de objetos).
- Cobranças de armazenamento mínimo

  Algumas classes de armazenamento do S3 têm requisitos mínimos de duração de armazenamento. Os objetos que são excluídos, substituídos ou transferidos dessas classes antes que a duração mínima seja cumprida recebem uma cobrança proporcional de taxa de exclusão ou transição antecipada. Esses requisitos de duração mínima de armazenamento são os seguintes:
  - S3 Standard-IA e S3 One Zone-IA: 30 dias
  - S3 Glacier Flexible Retrieval e S3 Glacier Instant Retrieval: 90 dias
  - S3 Glacier Deep Archive: 180 dias

  Para obter mais informações sobre esses requisitos, consulte a seção Restrições de Transição de objetos usando o ciclo de vida do S3. Para obter informações gerais sobre preços do S3, consulte Preços do Amazon S3 e a Calculadora de preços da AWS.
- Custos de transição do ciclo de vida

  Cada vez que um objeto é transferido para uma classe de armazenamento diferente por uma regra de ciclo de vida, o Amazon S3 considera essa transição como uma solicitação de

transição. Os custos dessas solicitações de transição são adicionais aos custos dessas classes de armazenamento. Se você pretende fazer a transição de um grande número de objetos, considere os custos de solicitação ao fazer a transição para um nível mais baixo. Para obter mais informações, consulte Definição de preço do Amazon S3.

Eu atualizei minha política de bucket, mas meus objetos do S3 ainda estão sendo excluídos pelas regras de ciclo de vida expiradas.

As declarações `Deny` em uma política de bucket não evitam a expiração dos objetos definidos em uma regra de ciclo de vida. As ações do ciclo de vida (como transições ou expirações) não usam a operação `DeleteObject` do S3. Em vez disso, as ações do ciclo de vida do S3 são executadas usando endpoints internos do S3. (Para obter mais informações, consulte Ciclo de vida e log.)

Para evitar que a regra de ciclo de vida realize qualquer ação, você deve editar, excluir ou desativar a regra.

Posso recuperar objetos do S3 que expiraram pelas regras do ciclo de vida do S3?

A única maneira de recuperar objetos que expiraram pelo ciclo de vida do S3 é por meio do versionamento, que deve estar em vigor antes que os objetos se tornem elegíveis para expiração. Você não pode desfazer as operações de expiração que são executadas pelas regras do ciclo de vida. Se os objetos forem excluídos permanentemente pelas regras de ciclo de vida do S3 em vigor, você não poderá recuperá-los. Para ativar o versionamento em um bucket, consulte the section called “Reter várias versões de objetos”.

Se você aplicou o versionamento ao bucket e as versões não atuais dos objetos ainda estão intactas, é possível restaurar as versões anteriores dos objetos expirados. Para obter mais informações sobre o comportamento das ações e os estados de versionamento do ciclo de vida do S3, consulte a tabela de estados de Ações de ciclo de vida e estado de versionamento do bucket em Elementos de configuração do ciclo de vida.

> **Note**
>
> Se o bucket do S3 estiver protegido pelo AWS Backup ou pela Replicação do S3, você também poderá usar esses recursos para recuperar os objetos expirados.

Por que minhas ações do ciclo de vida de expiração e transição não estão ocorrendo?

Para um bucket com versionamento habilitado ou suspenso, as seguintes considerações indicam como o Amazon S3 lida com a ação de expiração:

- A expiração do objeto se aplica somente à versão atual de um objeto (não afeta versões desatualizadas de objetos).
- O Amazon S3 não realizará ações se houver uma ou mais versões de objeto e se o marcador de exclusão estiver na versão atual.
- O Amazon S3 não realiza nenhuma ação em versões não atuais de objetos que tenham o Bloqueio de Objetos do S3 aplicado.
- Em relação a objetos com o status de replicação `PENDING`, o Amazon S3 não realiza nenhuma ação em versões atuais ou não atuais dos objetos.

As transições da classe de armazenamento do ciclo de vida têm as seguintes restrições:

- Por padrão, objetos com menos de 128 KB não farão a transição para nenhuma classe de armazenamento.
- Os objetos devem ser armazenados pelo menos trias dias antes de fazer a transição para S3 Standard-IA ou S3 One Zone-IA.
- Não é possível fazer a transição de objetos com status de replicação `PENDING` em buckets com versionamento habilitado ou suspenso.

Como faço para excluir um prefixo da minha regra de ciclo de vida?

O S3 Lifecycle não comporta a exclusão de prefixos em suas regras. Em vez disso, use tags para marcar todos os objetos que você deseja incluir na regra. Para ter mais informações sobre como usar tags em regras de ciclo de vida, consulte the section called “Arquivar todos os objetos em até um dia após a criação”.

Como faço para incluir vários prefixos na minha regra de ciclo de vida?

O S3 Lifecycle não comporta a inclusão de vários prefixos em suas regras. Em vez disso, use tags para marcar todos os objetos que você deseja incluir na regra. Para ter mais informações sobre como usar tags em regras de ciclo de vida, consulte the section called “Arquivar todos os objetos em até um dia após a criação”.

No entanto, se você tiver um ou mais prefixos que comecem com os mesmos caracteres, poderá incluir todos esses prefixos em sua regra especificando um prefixo parcial sem barra (`/`) no filtro. Por exemplo, suponha que você tenha estes prefixos:

```
sales1999/
sales2000/
sales2001/
```

Para incluir todos os três prefixos na regra, especifique `<Prefix>sales</Prefix>` na regra de ciclo de vida.

Registrar em log e monitorar no Amazon S3

O monitoramento é uma parte importante para manter a confiabilidade, a disponibilidade e a performance do Amazon S3 e das soluções da AWS. Recomendamos coletar dados de monitoramento de todas as partes de sua solução da AWS para que possa depurar mais facilmente uma falha multiponto, caso ocorra. Antes de começar a monitorar o Amazon S3, crie um plano de monitoramento que inclua as respostas para as seguintes perguntas:

- Quais são seus objetivos de monitoramento?
- Quais recursos você vai monitorar?
- Com que frequência você vai monitorar esses recursos?
- Quais ferramentas de monitoramento você usará?
- Quem realizará o monitoramento das tarefas?
- Quem deve ser notificado quando algo der errado?

Para obter mais informações sobre registro em log e monitoramento no Amazon S3, consulte os tópicos a seguir.

> **Note**
>
> Para obter mais informações sobre o uso da classe de armazenamento Amazon S3 Express One Zone com buckets de diretório, consulte S3 Express One Zone e Trabalhar com buckets de diretório.

O monitoramento é uma parte importante para manter a confiabilidade, a disponibilidade e a performance do Amazon S3 e das soluções da AWS. É necessário coletar dados de monitoramento de todas as partes de sua solução da AWS para depurar uma falha de vários pontos com mais facilidade, caso ocorra. A AWS fornece várias ferramentas para monitorar seus recursos do Amazon S3 e responder a possíveis incidentes.

Alarmes do Amazon CloudWatch

Com o uso de alarmes do Amazon CloudWatch, você observa uma única métrica durante um período especificado. Se a métrica exceder determinado limite, uma notificação será enviada para um tópico do Amazon SNS ou para uma política do AWS Auto Scaling. Os alarmes do

CloudWatch não invocam ações só porque estão em um determinado estado. O estado deve ter sido alterado e mantido por uma quantidade especificada de períodos. Para obter mais informações, consulte Monitoramento de métricas com o Amazon CloudWatch.

Logs do AWS CloudTrail

O CloudTrail fornece um registro de ações executadas por um usuário, uma função ou um produto da AWS no Amazon S3. Usando as informações coletadas pelo CloudTrail, é possível determinar a solicitação feita para o Amazon S3, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e detalhes adicionais. Para obter mais informações, consulte Registrar chamadas de API do Amazon S3 em log usando AWS CloudTrail.

Amazon GuardDuty

O Amazon GuardDuty é um serviço de detecção de ameaças que monitora continuamente contas, contêineres, workloads e dados no ambiente da AWS para identificar possíveis ameaças ou riscos à segurança nos buckets do S3. O GuardDuty também fornece um contexto detalhado sobre as ameaças detectadas. O GuardDuty monitora os logs de gerenciamento do AWS CloudTrail em busca de ameaças e mostra informações relevantes de segurança. Por exemplo, o GuardDuty inclui fatores de uma solicitação de API, como o usuário que fez a solicitação, o local de onde ela foi feita e a API específica solicitada, que podem ser incomuns em seu ambiente. A Proteção do S3 no GuardDuty monitora os eventos de dados do S3 coletados pelo CloudTrail e identifica comportamentos possivelmente anômalos e mal-intencionados em todos os buckets do S3 do ambiente.

Logs de acesso do Amazon S3

Os logs de acesso ao servidor fornecem registros detalhados das solicitações feitas a um bucket. Os logs de acesso ao servidor são úteis para muitos aplicativos. Por exemplo, as informações do log de acesso podem ser úteis em auditorias de segurança e acesso. Para obter mais informações, consulte Registrar em log as solicitações com registro em log de acesso ao servidor.

AWS Trusted Advisor

O Trusted Advisor conta com as práticas recomendadas aprendidas com o atendimento a centenas de milhões de clientes da AWS. O Trusted Advisor inspeciona seu ambiente da AWS e faz recomendações quando há oportunidades para economizar dinheiro, melhorar a performance e a disponibilidade do sistema e ajuda a corrigir falhas de segurança. Todos os clientes da AWS têm acesso a cinco verificações do Trusted Advisor. Os clientes com um plano de suporte Business ou Enterprise podem ver todas as verificações do Trusted Advisor.

A Trusted Advisor tem as seguintes verificações relacionadas ao Amazon S3:

- Configuração de registro em log de buckets do Amazon S3.
- Verificações de segurança para buckets do Amazon S3 que têm permissões de acesso livre.
- Verificações de tolerância a falhas para buckets do Amazon S3 que não têm versionamento habilitado ou têm versionamento suspenso.

Para obter mais informações, consulte AWS Trusted Advisor no Guia do usuário do Suporte.

Amazon S3 Storage Lens

A Lente de Armazenamento do Amazon S3 é um recurso de análise de armazenamento em nuvem que você pode usar para obter visibilidade em toda a organização sobre o uso e a atividade do armazenamento de objetos. Use as métricas da Lente de Armazenamento do S3 para gerar insights resumidos, como descobrir quanto armazenamento você tem em toda a organização ou quais são os buckets e prefixos que mais crescem. Você também pode usar as métricas da Lente de Armazenamento do S3 para identificar oportunidades de otimização de custos, implementar práticas recomendadas de proteção e segurança de dados, e melhorar a performance das workloads de aplicações.

A Lente de Armazenamento do S3 agrega suas métricas e exibe as informações na seção “Snapshot da conta” na página Buckets do console do Amazon S3. A Lente de Armazenamento do S3 também oferece um painel interativo para visualizar insights e tendências, sinalizar discrepâncias e receber recomendações para otimizar os custos de armazenamento e aplicar as práticas recomendadas de proteção de dados. O painel tem opções de detalhamento para gerar e visualizar insights no nível da organização, conta, Região da AWS, classe de armazenamento, bucket, prefixo ou grupo de Lente de Armazenamento. Para obter mais informações, consulte Noções básicas sobre o Amazon S3 Storage Lens.

Inventário do Amazon S3

A funcionalidade Inventário Amazon S3 gera uma lista de objetos e metadados que você pode usar para consultar e gerenciar os objetos. Você pode usar esse relatório de inventário para gerar dados granulares, como tamanho do objeto, data da última modificação, status de criptografia e outros campos. Esses relatórios são disponibilizados diária ou semanalmente para fornecer automaticamente a lista mais recente.

Por exemplo, você pode usar a funcionalidade Inventário Amazon S3 para auditar e gerar relatórios de status da replicação e criptografia dos objetos a fim de atender às necessidades dos negócios, de conformidade e regulatórias. Também é possível usar a funcionalidade Inventário Amazon S3 para simplificar e acelerar os fluxos de trabalho de negócios e os trabalhos de big

data, o que proporciona uma alternativa programada para as operações síncronas da API `List` do Amazon S3. A funcionalidade Inventário Amazon S3 não usa as operações da API `List` para auditar os objetos e não afeta a taxa de solicitação do bucket. Para obter mais informações, consulte Catalogar e analisar seus dados com o Inventário S3.

Notificações de eventos do Amazon S3

Com a funcionalidade Notificações de Eventos do Amazon S3, você recebe notificações quando certos eventos ocorrem no bucket do S3. Para habilitar notificações, adicione uma configuração de notificação que identifique os eventos que deseja que o Amazon S3 publique. Para obter mais informações, consulte Notificações de eventos do Amazon S3.

Amazon S3 e AWS X-Ray

O AWS X-Ray se integra ao Amazon S3 para rastrear solicitações precedentes para atualizar os buckets do S3 da aplicação. Se um serviço rastreia solicitações usando o X-Ray SDK, o Amazon S3 pode enviar os cabeçalhos de rastreamento para assinantes de eventos downstream, como o Λ, o Amazon SQS e o Amazon SNS. O X-Ray permite mensagens de rastreamento para notificações de eventos do Amazon S3. É possível usar o X-Ray para visualizar o mapa de conexões entre o Amazon S3 e outros serviços que a aplicação usa. Para ter mais informações, consulte Amazon S3 and X-Ray.

As melhores práticas de segurança a seguir também abordam registros em logs e monitoramento:

- Identify and audit all your Amazon S3 buckets
- Implement monitoring using Amazon Web Services monitoring tools
- Habilitar AWS Config
- Enable Amazon S3 server access logging
- Use CloudTrail
- Monitor Amazon Web Services security advisories

Tópicos

- Ferramentas de monitoramento
- Opções de registro em log para o Amazon S3
- Registrar chamadas de API do Amazon S3 em log usando AWS CloudTrail
- Registrar em log as solicitações com registro em log de acesso ao servidor

- Monitoramento de métricas com o Amazon CloudWatch
- Notificações de eventos do Amazon S3
- Avaliação de sua atividade de armazenamento e uso com a Lente de Armazenamento do Amazon S3
- Catalogar e analisar seus dados com o Inventário S3

Ferramentas de monitoramento

A AWS fornece várias ferramentas que você pode usar para monitorar o Amazon S3. É possível configurar algumas dessas ferramentas para fazer o monitoramento em seu lugar, e, ao mesmo tempo, algumas das ferramentas exigem intervenção manual. Recomendamos que as tarefas de monitoramento sejam automatizadas ao máximo possível.

Ferramentas de monitoramento automatizadas

É possível usar as seguintes ferramentas automatizadas de monitoramento para supervisionar o Amazon S3 e gerar relatórios quando algo estiver errado:

- Amazon CloudWatch Alarms: observe uma única métrica ao longo de um período que você especificar e realize uma ou mais ações com base no valor da métrica em relação a um limite ao longo de vários períodos. A ação é uma notificação enviada para um tópico do Amazon Simple Notification Service (Amazon SNS) ou uma política do Amazon EC2 Auto Scaling. Os alarmes do CloudWatch não invocam ações só porque estão em um determinado estado. O estado deve ter sido alterado e mantido por uma quantidade especificada de períodos. Para obter mais informações, consulte Monitoramento de métricas com o Amazon CloudWatch.
- AWS CloudTrailMonitoramento de log: compartilhe arquivos de log entre contas, monitore os arquivos de log do CloudTrail em tempo real enviando-os para o CloudWatch Logs, escreva aplicações de processamento de logs em Java e confirme se os arquivos de log não foram alterados após a entrega pelo CloudTrail. Para obter mais informações, consulte Registrar chamadas de API do Amazon S3 em log usando AWS CloudTrail.

Ferramentas de monitoramento manual

Outra parte importante do monitoramento do Amazon S3 é o monitoramento manual dos itens que os alarmes do CloudWatch não abrangem. O Amazon S3, o CloudWatch, o Trusted Advisor e outros painéis do AWS Management Console fornecem uma visão rápida do estado do ambiente da AWS.

Você pode permitir o registro em log de acesso ao servidor, que acompanha as solicitações de acesso ao seu bucket. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso, como solicitante, nome do bucket, horário da solicitação, ação da solicitação, status de resposta e código de erro, se houver. Para obter mais informações, consulte Registrar em log as solicitações com registro em log de acesso ao servidor.

- O painel do Amazon S3 mostra o seguinte:
  - Seus buckets, objetos e propriedades que contêm
- A página inicial do CloudWatch mostra o seguinte:
  - Alertas e status atual
  - Gráficos de alertas e recursos
  - Estado de integridade do serviço

  Além disso, é possível usar o CloudWatch para fazer o seguinte:
  - Criar painéis personalizados para monitorar os serviços com os quais você se preocupa.
  - Colocar em gráfico dados de métrica para solucionar problemas e descobrir tendências.
  - Pesquise e procure todas as métricas de recursos da AWS.
  - Criar e editar alertas para ser notificado sobre problemas.
- O AWS Trusted Advisor pode ajudar a monitorar os recursos da AWS para melhorar a performance, a confiabilidade, a segurança e a economia. Quatro verificações do Trusted Advisor estão disponíveis a todos os usuários; mais de 50 verificações estão disponíveis para usuários com um plano de suporte Business ou Enterprise. Para obter mais informações, consulte AWS Trusted Advisor.

  O Trusted Advisor tem essas verificações que se referem ao Amazon S3:
  - Verificações da configuração de registro em log dos buckets do Amazon S3.
  - Verificações de segurança para buckets do Amazon S3 que têm permissões de acesso livre.
  - Verificações de tolerância a falhas para buckets do Amazon S3 que não têm versionamento habilitado ou têm versionamento suspenso.

Opções de registro em log para o Amazon S3

É possível registrar as ações que são realizadas por usuários, perfis ou Serviços da AWS em recursos do Amazon S3 e manter registros de log para fins de auditoria e conformidade. Para fazer isso, você pode usar o registro em log de acesso ao servidor, o registro em log do AWS CloudTrail

ou uma combinação de ambos. Recomendamos que você use o CloudTrail para registrar em log ações por bucket e objeto para seus recursos do Amazon S3. Para obter mais informações sobre cada opção, consulte as seguintes seções:

- Registrar em log as solicitações com registro em log de acesso ao servidor
- Registrar chamadas de API do Amazon S3 em log usando AWS CloudTrail

A tabela a seguir lista as principais propriedades dos logs do CloudTrail e dos logs de acesso ao servidor do Amazon S3. Analise a tabela e as observações para garantir que o CloudTrail atenda aos seus requisitos de segurança.

Propriedades de log	AWS CloudTrail	Logs do servidor do Amazon S3
Pode ser encaminhado para outros sistemas (Amazon CloudWatch Logs, Amazon CloudWatch Events)	Sim	No
Entregue logs para mais de um destino (por exemplo, envie os mesmos logs para dois buckets diferentes)	Sim	No
Ative logs para um subconjunto de objetos (prefixo)	Sim	No
Entrega de logs entre contas (bucket de origem e de destino pertencentes a contas diferentes)	Sim	No
Validação de integridade do arquivo de log usando assinatura digital ou hashing	Sim	No
Padrão ou opção de criptografia para arquivos de log	Sim	No

Propriedades de log	AWS CloudTrail	Logs do servidor do Amazon S3
Operações de objeto (usando APIs do Amazon S3)	Sim	Sim
Operações de bucket (usando APIs do Amazon S3)	Sim	Sim
UI pesquisável para logs	Sim	No
Campos para parâmetros de bloqueio de objetos, propriedades selecionadas do Amazon S3 para registros de log	Sim	No
Campos de `Object Size`, `Total Time`, `Turn-Around Time` e `HTTP Referer` para registros de log	Não	Sim
Transições, expirações e restaurações do ciclo de vida	Não	Sim
Registro de chaves em uma operação de exclusão em lote	Sim	Sim
Falhas de autenticação[1]	Não	Sim
Contas em que logs são entregues	Proprietário do bucket[2] e solicitante	Somente proprietário do bucket
Performance and Cost	AWS CloudTrail	Amazon S3 Server Logs

Propriedades de log	AWS CloudTrail	Logs do servidor do Amazon S3
Preço	Os eventos de gerenciamento (primeira entrega) são gratuitos. Os eventos de dados incorrem em uma taxa, além do armazenamento de logs	Nenhum custo adicional além do armazenamento de logs
Velocidade da entrega de logs	Eventos de dados a cada 5 minutos; eventos de gerenciamento a cada 15 minutos	Em algumas horas
Formato do log	JSON	Arquivo de log com registros delimitados por novas linhas e separados por espaços

Observações

1. O CloudTrail não entrega logs para solicitações com falha de autenticação (nas quais as credenciais fornecidas não são válidas) ou que falham devido a redirecionamento (código de erro `301 Moved Permanently`). No entanto, ele inclui logs para solicitações nas quais a autorização falha (`AccessDenied`) e as solicitações são feitas por usuários anônimos.
2. O proprietário do bucket do S3 recebe logs do CloudTrail quando a conta não tem acesso total ao objeto na solicitação. Para obter mais informações, consulte Ações em nível de objeto do Amazon S3 em cenários entre contas.
3. O S3 não é compatível com a entrega de logs do CloudTrail ou logs de acesso ao servidor ao solicitante ou ao proprietário do bucket para solicitações de endpoint da VPC quando a política de endpoint da VPC as nega ou para solicitações que falham antes da política da VPC ser avaliada.

Registrar chamadas de API do Amazon S3 em log usando AWS CloudTrail

O Amazon S3 é integrado ao AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, um perfil ou um AWS service (Serviço da AWS). O CloudTrail captura todas as chamadas de API para o Amazon S3 como eventos. As chamadas capturadas incluem aquelas do console do Amazon S3 e as chamadas de código para as operações de API do Amazon S3. Ao fazer uso das informações coletadas pelo CloudTrail, é possível determinar a solicitação feita ao Amazon S3, o endereço IP que a realizou, quando ela foi feita e detalhes adicionais.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar o seguinte:

- Se a solicitação foi feita com credenciais de usuário raiz ou credenciais de usuário.
- Se a solicitação foi feita em nome de um usuário do Centro de Identidade do IAM.
- Se a solicitação foi feita com credenciais de segurança temporárias de um perfil ou de um usuário federado.
- Se a solicitação foi feita por outro AWS service (Serviço da AWS).

Quando a Conta da AWS é criada, o CloudTrail torna-se ativo nela e você tem acesso automático ao Histórico de eventos do CloudTrail. O Histórico de eventos do CloudTrail fornece um registro visualizável, pesquisável, baixável e imutável dos últimos 90 dias de eventos de gerenciamento gravados em uma Região da AWS. Para obter mais informações, consulte Trabalhar com histórico de eventos do CloudTrail no Guia do usuário do AWS CloudTrail. Não há cobranças do CloudTrail pela visualização do Histórico de eventos.

Para obter um registro contínuo de eventos em sua Conta da AWS nos últimos 90 dias, crie uma trilha ou um armazenamento de dados de eventos do CloudTrail Lake.

Trilhas do CloudTrail

> Uma trilha permite que o CloudTrail entregue arquivos de log a um bucket do Amazon S3. As trilhas criadas usando o AWS Management Console são de várias regiões. Só é possível criar uma trilha de região única ou de várias regiões usando a AWS CLI. Criar uma trilha de várias regiões é uma prática recomendada, pois você captura atividades em todas as Regiões da AWS da conta. Ao criar uma trilha de região única, é possível visualizar somente os eventos registrados na Região da AWS da trilha. Para obter mais informações sobre trilhas, consulte Criar

uma trilha para a Conta da AWS e Criar uma trilha para uma organização no Guia do usuário do AWS CloudTrail.

Uma cópia dos eventos de gerenciamento em andamento pode ser entregue no bucket do Amazon S3 sem nenhum custo via CloudTrail com a criação de uma trilha; no entanto, há cobranças de armazenamento do Amazon S3. Para obter mais informações sobre os preços do CloudTrail, consulte Preços do AWS CloudTrail. Para receber informações sobre a definição de preços do Amazon S3, consulte Definição de preços do Amazon S3.

Armazenamentos de dados de eventos do CloudTrail Lake

O CloudTrail Lake permite executar consultas baseadas em SQL nos eventos. O CloudTrail Lake converte eventos existentes em formato JSON baseado em linhas para o formato Apache ORC. O ORC é um formato colunar de armazenamento otimizado para recuperação rápida de dados. Os eventos são agregados em armazenamentos de dados de eventos, que são coleções imutáveis de eventos baseados nos critérios selecionados com a aplicação de seletores de eventos avançados. Os seletores que aplicados a um armazenamento de dados de eventos controlam quais eventos persistem e estão disponíveis para consulta. Para obter mais informações sobre o CloudTrail Lake, consulte Trabalhar com o AWS CloudTrail Lake, no Guia do usuário do AWS CloudTrail.

Os armazenamentos de dados de eventos e consultas do CloudTrail Lake incorrem em custos. Ao criar um armazenamento de dados de eventos, você escolhe a opção de preço que deseja usar para ele. A opção de preço determina o custo para a ingestão e para o armazenamento de eventos, e o período de retenção padrão e máximo para o armazenamento de dados de eventos. Para obter mais informações sobre os preços do CloudTrail, consulte Preços do AWS CloudTrail.

Você pode armazenar arquivos de log no bucket pelo tempo que desejar, mas também pode definir regras do ciclo de vida do Amazon S3 para arquivar ou excluir os arquivos de log automaticamente. Por padrão, os arquivos de log são criptografados usando-se Server-Side Encryption (SSE - Criptografia do lado do servidor) do Amazon S3.

Usar logs do CloudTrail com logs de acesso ao servidor do Amazon S3 e CloudWatch Logs

Os logs do AWS CloudTrail fornecem os registros das ações tomadas por um usuário, uma função ou um produto da AWS no Amazon S3, enquanto os logs de acesso do servidor do Amazon S3 oferecem registros das solicitações feitas a um bucket do S3. Para obter mais informações sobre

como os diferentes registros funcionam e as propriedades, a performance e os custos deles, consulte the section called “Opções de registro em log”.

Você pode usar os logs do AWS CloudTrail em conjunto com os logs de acesso ao servidor do Amazon S3. Os logs do CloudTrail fornecem rastreamento detalhado de API para operações no nível de bucket e objeto do Amazon S3. Os logs de acesso ao servidor do Amazon S3 fornecem visibilidade em operações no nível de objeto em seus dados no Amazon S3. Para obter mais informações sobre logs de acesso ao servidor, consulte Registrar em log as solicitações com registro em log de acesso ao servidor.

Você também pode usar logs do CloudTrail junto com o Amazon CloudWatch para Amazon S3. A integração do CloudTrail com o CloudWatch Logs entrega as atividades de API no nível do bucket do S3 capturadas pelo CloudTrail a um stream de logs do CloudWatch no grupo de logs do CloudWatch especificado. Você pode criar alarmes do CloudWatch para monitoramento de atividade específica de API e receber notificações por e-mail quando a atividade específica de API ocorrer. Para obter mais informações sobre alarmes do CloudWatch para monitorar atividades específicas da API, consulte o Guia do usuário do AWS CloudTrail. Para obter mais informações sobre como usar o CloudWatch com o Amazon S3, consulte Monitoramento de métricas com o Amazon CloudWatch.

> **Note**
>
> O S3 não é compatível com a entrega de logs do CloudTrail ao solicitante ou ao proprietário do bucket para solicitações de endpoint da VPC quando a política de endpoint da VPC as nega.

Rastreamento do CloudTrail com chamadas de API SOAP do Amazon S3

O CloudTrail rastreia as chamadas de API SOAP do Amazon S3. O suporte de SOAP via HTTP do Amazon S3 está obsoleto, mas continua disponível via HTTPS. Consulte mais informações sobre o suporte de SOAP do Amazon S3 em Appendix: SOAP API na Referência de API do Amazon S3.

> **Important**
>
> Os novos recursos do Amazon S3 não são compatíveis com o SOAP. Recomendamos usar a API REST ou os AWS SDKs.

A tabela a seguir mostra ações do SOAP do Amazon S3 monitoradas pelo registro em log do CloudTrail.

Nome da API SOAP	Nome do evento da API usado no log do CloudTrail
ListAllMyBuckets	`ListBuckets`
CreateBucket	`CreateBucket`
DeleteBucket	`DeleteBucket`
GetBucketAccessControlPolicy	`GetBucketAcl`
SetBucketAccessControlPolicy	`PutBucketAcl`
GetBucketLoggingStatus	`GetBucketLogging`
SetBucketLoggingStatus	`PutBucketLogging`

Para obter mais informações sobre o CloudTrail e o Amazon S3, consulte os seguintes tópicos:

Tópicos

- Eventos do CloudTrail no Amazon S3
- Entradas de arquivo de log do CloudTrail para Amazon S3 e S3 on Outposts
- Habilitar o log de eventos do CloudTrail para buckets e objetos do S3
- Identificar solicitações do Amazon S3 usando o CloudTrail

Eventos do CloudTrail no Amazon S3

Important

O Amazon S3 agora aplica criptografia do lado do servidor com chaves gerenciadas do Amazon S3 (SSE-S3) como nível básico de criptografia para cada bucket no Amazon S3. Desde 5 de janeiro de 2023, todos os novos uploads de objetos para o Amazon S3 são automaticamente criptografados sem custo adicional e sem impacto na performance. O status de criptografia automática para a configuração de criptografia padrão do bucket do S3

e para novos uploads de objetos está disponível em logs do AWS CloudTrail, no Inventário do S3, na Lente de Armazenamento do S3, no console do Amazon S3 e como cabeçalho adicional de resposta da API do Amazon S3 na AWS Command Line Interface e em AWS SDKs. Para obter mais informações, consulte Perguntas frequentes sobre criptografia padrão.

Esta seção fornece informações sobre os eventos que o S3 registra em log no CloudTrail.

Eventos de dados do Amazon S3 no CloudTrail

Os Eventos de dados fornecem informações sobre as operações de recursos realizadas em um recurso (por exemplo, leitura ou gravação em um objeto do Amazon S3). Também são conhecidas como operações de plano de dados. Eventos de dados geralmente são atividades de alto volume. Por padrão, o CloudTrail não registra eventos de dados em log. O Histórico de eventos do CloudTrail não registra eventos de dados.

Há cobranças adicionais para eventos de dados. Para obter mais informações sobre os preços do CloudTrail, consulte Preços do AWS CloudTrail.

É possível registrar em log eventos de dados para os tipos de recurso do Amazon S3 usando o console do CloudTrail, a AWS CLI ou as operações de API do CloudTrail. Para obter mais informações sobre como registrar eventos de dados em log, consulte Registrar eventos de dados com o AWS Management Console e Registrar eventos de dados com a AWS Command Line Interface no Guia do usuário do AWS CloudTrail.

A tabela a seguir lista o tipo de recurso do Amazon S3 para o qual você pode registrar eventos de dados em log. A coluna Tipo de evento de dados (console) mostra o valor a ser escolhido na lista Tipo de evento de dados no console do CloudTrail. A coluna do valor resources.type mostra o valor de `resources.type` que você especificaria ao configurar seletores de eventos avançados usando a AWS CLI ou as APIs do CloudTrail. A coluna APIs de dados registradas no CloudTrail mostra as chamadas de API registradas no CloudTrail para o tipo de recurso.

Tipo de evento de dados (console)	valor resources.type	APIs de dados registradas no CloudTrail
S3	`AWS::S3::Object`	• AbortMultipartUpload • CompleteMultipartUpload

Tipo de evento de dados (console)	valor resources.type	APIs de dados registradas no CloudTrail
		• CopyObject • CreateMultipartUpload • DeleteObject • DeleteObjectTagging • DeleteObjects • GetObject • GetObjectAcl • GetObjectAttributes • GetObjectLegalHold • GetObjectRetention • GetObjectTagging • GetObjectTorrent • HeadObject • HeadBucket • ListObjectVersions • ListObjects • ListParts • PutObject • PutObjectAcl • PutObjectLegalHold • PutObjectRetention • PutObjectTagging • RestoreObject • SelectObjectContent • UploadPart • UploadPartCopy

Tipo de evento de dados (console)	valor resources.type	APIs de dados registradas no CloudTrail
S3 Express One Zone	`AWS::S3Express::Object`	• AbortMultipartUpload • CompleteMultipartUpload • CreateSession • CopyObject • CreateMultipartUpload • DeleteObject • DeleteObjects • GetObject • GetObjectAttributes • HeadBucket • HeadObject • ListObjectsV2 • ListParts • PutObject • UploadPart • UploadPartCopy

Tipo de evento de dados (console)	valor resources.type	APIs de dados registradas no CloudTrail
Ponto de acesso do S3	`AWS::S3::Access Point`	• AbortMultipartUpload • CompleteMultipartUpload • CopyObject (somente cópias da mesma região) • CreateMultipartUpload • DeleteObject • DeleteObjectTagging • GetBucketAcl • GetBucketCors • GetBucketLocation • GetBucketNotificationConfiguration • GetBucketPolicy • GetObject • GetObjectAcl • GetObjectAttributes • GetObjectLegalHold • GetObjectRetention • GetObjectTagging • HeadBucket • HeadObject • ListObjects • ListObjectsV2 • ListObjectVersions • ListParts • Presign • PutObject • PutObjectLegalHold

Tipo de evento de dados (console)	valor resources.type	APIs de dados registradas no CloudTrail
		• PutObjectRetention • PutObjectAcl • PutObjectTagging • RestoreObject • UploadPart • UploadPartCopy (somente cópias da mesma região)

Tipo de evento de dados (console)	valor resources.type	APIs de dados registradas no CloudTrail
S3 Object Lambda	`AWS::S3ObjectLambda::AccessPoint`	• AbortMultipartUpload • CompleteMultipartUpload • CopyObject (somente cópias da mesma região) • CreateMultipartUpload • DeleteObject • DeleteObjectTagging • GetObject • GetObjectAcl • GetObjectLegalHold • GetObjectRetention • GetObjectTagging • HeadObject • ListObjects • ListObjectVersions • ListParts • PutObject • PutObjectLegalHold • PutObjectRetention • PutObjectAcl • PutObjectTagging • RestoreObject • UploadPart • WriteGetObjectResponse

Tipo de evento de dados (console)	valor resources.type	APIs de dados registradas no CloudTrail
S3 Outposts	`AWS::S3Outposts::Object`	• AbortMultipartUpload • CompleteMultipartUpload • CopyObject (somente cópias da mesma região) • CreateMultipartUpload • DeleteObject • DeleteObjectTagging • GetObject • GetObjectTagging • HeadObject • ListObjects • ListObjectsV2 • ListParts • PutObject • PutObjectTagging • UploadPart • UploadPartCopy

É possível configurar seletores de eventos avançados para filtrar os campos `eventName`, `readOnly` e `resources.ARN` para registrar em log somente os eventos que são importantes para você. Para obter mais informações sobre esses campos, consulte AdvancedFieldSelector na Referência de API do AWS CloudTrail.

Eventos de gerenciamento do Amazon S3 no CloudTrail

O Amazon S3 registra em log todas as operações do ambiente de gerenciamento como eventos de gerenciamento. Consulte mais informações sobre as operações de API do S3 na Referência de API do Amazon S3.

Como o CloudTrail captura solicitações feitas para o Amazon S3

Por padrão, o CloudTrail registra em log chamadas de API no nível de buckets do S3 que foram feitas nos últimos 90 dias, mas não registra em log solicitações feitas a objetos. As chamadas de buckets incluem eventos como `CreateBucket`, `DeleteBucket`, `PutBucketLifecycle`, `PutBucketPolicy` e assim por diante. Você pode ver eventos no nível do bucket no console do CloudTrail. No entanto, não é possível visualizar eventos de dados (chamadas no nível do objeto do Amazon S3). Você deve analisar ou consultar os logs do CloudTrail para eles.

Se você estiver registrando atividades de dados em log com o AWS CloudTrail, o registro de um evento de dados `DeleteObjects` do Amazon S3 inclui o evento `DeleteObjects` e um evento `DeleteObject` para cada objeto excluído como parte dessa operação. Você pode omitir a visibilidade adicional sobre objetos excluídos do registro de eventos. Para ter mais informações, consulte AWS CLI examples for filtering data events no Guia do usuário do AWS CloudTrail.

Ações no nível da conta do Amazon S3 rastreadas pelo registro em log do CloudTrail

O CloudTrail registra ações no nível da conta. Os registros do Amazon S3 são gravados com outros registros de AWS service (Serviço da AWS) em um arquivo de log. O CloudTrail determina quando criar e gravar em um novo arquivo de acordo com o período e o tamanho do arquivo.

As tabelas nesta seção listam as ações no nível da conta do Amazon S3 que são compatíveis com o registro do CloudTrail.

Ações de API no nível da conta do Amazon S3 rastreadas pelo registro em log do CloudTrail aparecem como os seguintes nomes de eventos. Os nomes dos eventos do CloudTrail diferem do nome da ação da API. Por exemplo, DeletePublicAccessBlock é DeleteAccountPublicAccessBlock.

- DeleteAccountPublicAccessBlock
- GetAccountPublicAccessBlock
- PutAccountPublicAccessBlock

Ações de buckets do Amazon S3 rastreadas pelo registro em log do CloudTrail

Por padrão, o CloudTrail registra em log as ações nos buckets de uso geral. Os registros do Amazon S3 são gravados com outros registros de serviço da AWS em um arquivo de log. O CloudTrail determina quando criar e gravar em um novo arquivo de acordo com o período e o tamanho do arquivo.

Esta seção lista as ações no nível do bucket do Amazon S3 que são compatíveis com o registro em log do CloudTrail.

Ações de API no nível do bucket do Amazon S3 rastreadas pelo registro em log do CloudTrail aparecerão como os seguintes nomes de eventos. Em alguns casos, o nome do evento do CloudTrail é diferente do nome da ação da API. Por exemplo, `PutBucketLifecycleConfiguration` é `PutBucketLifecycle`.

- CreateBucket
- CreateBucketMetadataTableConfiguration
- DeleteBucket
- DeleteBucketAnalyticsConfiguration
- DeleteBucketCors
- DeleteBucketEncryption
- DeleteBucketIntelligentTieringConfiguration
- DeleteBucketInventoryConfiguration
- DeleteBucketLifecycle
- DeleteBucketMetadataTableConfiguration
- DeleteBucketMetricsConfiguration
- DeleteBucketOwnershipControls
- DeleteBucketPolicy
- DeleteBucketPublicAccessBlock
- DeleteBucketReplication
- DeleteBucketTagging
- GetAccelerateConfiguration
- GetBucketAcl
- GetBucketAnalyticsConfiguration
- GetBucketCors
- GetBucketEncryption
- GetBucketIntelligentTieringConfiguration
- GetBucketInventoryConfiguration

- GetBucketLifecycle
- GetBucketLocation
- GetBucketLogging
- GetBucketMetadataTableConfiguration
- GetBucketMetricsConfiguration
- GetBucketNotification
- GetBucketObjectLockConfiguration
- GetBucketOwnershipControls
- GetBucketPolicy
- GetBucketPolicyStatus
- GetBucketPublicAccessBlock
- GetBucketReplication
- GetBucketRequestPayment
- GetBucketTagging
- GetBucketVersioning
- GetBucketWebsite
- HeadBucket
- ListBuckets
- PutAccelerateConfiguration
- PutBucketAcl
- PutBucketAnalyticsConfiguration
- PutBucketCors
- PutBucketEncryption
- PutBucketIntelligentTieringConfiguration
- PutBucketInventoryConfiguration
- PutBucketLifecycle
- PutBucketLogging
- PutBucketMetricsConfiguration
- PutBucketNotification

- PutBucketObjectLockConfiguration
- PutBucketOwnershipControls
- PutBucketPolicy
- PutBucketPublicAccessBlock
- PutBucketReplication
- PutBucketRequestPayment
- PutBucketTagging
- PutBucketVersioning
- PutBucketWebsite

Além dessas operações de API, também é possível usar a ação de objetos OPTIONS object. Essa ação é tratada como uma ação do nível do bucket no registro em log do CloudTrail, pois verifica a configuração CORS de um bucket.

Ações em nível de bucket da classe Amazon S3 Express One Zone (endpoint de API regional) monitoradas pelo registro em log do CloudTrail

Por padrão, o CloudTrail registra em log as ações nos buckets de diretório como eventos de gerenciamento. O `eventsource` para os eventos de gerenciamento do CloudTrail para a classe S3 Express One Zone é `s3express.amazonaws.com`.

Veja a seguir as operações de API de endpoint regional que são registradas em log no CloudTrail.

- CreateBucket
- DeleteBucket
- DeleteBucketPolicy
- GetBucketPolicy
- PutBucketPolicy
- ListDirectoryBuckets
- PutBucketEncryption
- GetBucketEncryption
- DeleteBucketEncryption

Para ter mais informações, consulte Logging with AWS CloudTrail for S3 Express One Zone.

Ações em nível de objeto do Amazon S3 em cenários entre contas

Os seguintes são casos de uso especiais que envolvem chamadas de API do nível do objeto em cenários entre contas e como os logs do CloudTrail são relatados. O CloudTrail entrega logs ao solicitante (a conta que fez a chamada de API), exceto em alguns casos de acesso negado em que as entradas de log são editadas ou omitidas. Para estabelecer acesso entre contas, considere os exemplos nesta seção.

> **Note**
>
> Os exemplos supõem que os logs do CloudTrail estejam configurados adequadamente.

Exemplo 1: CloudTrail entrega logs ao proprietário do bucket

O CloudTrail entrega os logs de acesso ao proprietário do bucket mesmo que o proprietário do bucket não tenha permissão para a mesma operação de API do objeto. Considere o seguinte cenário entre contas:

- A conta A é proprietária do bucket.
- A conta B (o solicitante) tenta acessar um objeto nesse bucket.
- A conta C é proprietária do objeto. A conta C pode ou não ser igual à conta A.

> **Note**
>
> O CloudTrail sempre entrega os logs de API de objetos ao solicitante (conta B). Além disso, o CloudTrail também entrega os mesmo logs ao proprietário do bucket (conta A) mesmo quando o proprietário do bucket (conta C) não é proprietário do objeto (conta C) nem tem permissões para as mesmas operações de API sobre esse objeto.

Exemplo 2: CloudTrail não prolifera os endereços de e-mail usados na definição de ACLs de objeto

Considere o seguinte cenário entre contas:

- A conta A é proprietária do bucket.

- A conta B (solicitante) envia uma solicitação para definir uma concessão de ACL de objeto usando um endereço de e-mail. Para obter mais informações sobre ACLs, consulte Visão geral da lista de controle de acesso (ACL).

O solicitante recebe os logs junto com as informações do e-mail. Contudo, o proprietário do bucket - se for qualificado para receber logs como no exemplo 1 - recebe o log do CloudTrail que relata o evento. Contudo, o proprietário do bucket não obtém as informações de configuração da ACL, especificamente o endereço de e-mail do favorecido e a concessão. A única informação que o log dá ao proprietário do bucket é que a chamada da API da ACL foi feita pela conta B.

Entradas de arquivo de log do CloudTrail para Amazon S3 e S3 on Outposts

> **Important**
>
> O Amazon S3 agora aplica criptografia do lado do servidor com chaves gerenciadas do Amazon S3 (SSE-S3) como nível básico de criptografia para cada bucket no Amazon S3. Desde 5 de janeiro de 2023, todos os novos uploads de objetos para o Amazon S3 são automaticamente criptografados sem custo adicional e sem impacto na performance. O status de criptografia automática para a configuração de criptografia padrão do bucket do S3 e para novos uploads de objetos está disponível em logs do AWS CloudTrail, no Inventário do S3, na Lente de Armazenamento do S3, no console do Amazon S3 e como cabeçalho adicional de resposta da API do Amazon S3 na AWS Command Line Interface e em AWS SDKs. Para obter mais informações, consulte Perguntas frequentes sobre criptografia padrão.

Um evento representa uma única solicitação de qualquer origem e inclui informações sobre a operação solicitada, a data e a hora da operação da API, os parâmetros de solicitação etc. Os arquivos de log do CloudTrail não são um rastreamento de pilha ordenada de chamadas de API públicas, portanto não são exibidos em uma ordem específica.

> **Note**
>
> Para ver exemplos de arquivo de log do CloudTrail para Amazon S3 Express One Zone, consulte CloudTrail log file examples for S3 Express One Zone.

Para obter mais informações, veja os exemplos a seguir:

Tópicos

- Exemplo: entrada de arquivo de log do CloudTrail para o Amazon S3

Exemplo: entrada de arquivo de log do CloudTrail para o Amazon S3

O exemplo a seguir mostra uma entrada de log do CloudTrail que demonstra as ações GET Service, PutBucketAcl e GetBucketVersioning.


```
{
    "Records": [
    {
        "eventVersion": "1.03",
        "userIdentity": {
            "type": "IAMUser",
            "principalId": "111122223333",
            "arn": "arn:aws:iam::111122223333:user/myUserName",
            "accountId": "111122223333",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "userName": "myUserName"
        },
        "eventTime": "2019-02-01T03:18:19Z",
        "eventSource": "s3.amazonaws.com",
        "eventName": "ListBuckets",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "127.0.0.1",
        "userAgent": "[]",
        "requestParameters": {
            "host": [
                "s3.us-west-2.amazonaws.com"
            ]
        },
        "responseElements": null,
        "additionalEventData": {
            "SignatureVersion": "SigV2",
            "AuthenticationMethod": "QueryString",
            "aclRequired": "Yes"
    },
        "requestID": "47B8E8D397DCE7A6",
        "eventID": "cdc4b7ed-e171-4cef-975a-ad829d4123e8",
        "eventType": "AwsApiCall",
```

```
        "recipientAccountId": "444455556666",
        "tlsDetails": {
            "tlsVersion": "TLSv1.2",
            "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
            "clientProvidedHostHeader": "s3.amazonaws.com"
    }
    },
    {
       "eventVersion": "1.03",
       "userIdentity": {
            "type": "IAMUser",
            "principalId": "111122223333",
            "arn": "arn:aws:iam::111122223333:user/myUserName",
            "accountId": "111122223333",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "userName": "myUserName"
        },
      "eventTime": "2019-02-01T03:22:33Z",
      "eventSource": "s3.amazonaws.com",
      "eventName": "PutBucketAcl",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "",
      "userAgent": "[]",
      "requestParameters": {
          "bucketName": "",
          "AccessControlPolicy": {
              "AccessControlList": {
                  "Grant": {
                      "Grantee": {
                          "xsi:type": "CanonicalUser",
                          "xmlns:xsi": "http://www.w3.org/2001/XMLSchema-instance",
                          "ID":
"d25639fbe9c19cd30a4c0f43fbf00e2d3f96400a9aa8dabfbbebe1906Example"
                       },
                      "Permission": "FULL_CONTROL"
                   }
              },
              "xmlns": "http://s3.amazonaws.com/doc/2006-03-01/",
              "Owner": {
                  "ID":
"d25639fbe9c19cd30a4c0f43fbf00e2d3f96400a9aa8dabfbbebe1906Example"
              }
          },
          "host": [
```

```
            "s3.us-west-2.amazonaws.com"
        ],
        "acl": [
            ""
        ]
    },
    "responseElements": null,
    "additionalEventData": {
        "SignatureVersion": "SigV4",
        "CipherSuite": "ECDHE-RSA-AES128-SHA",
        "AuthenticationMethod": "AuthHeader"
    },
    "requestID": "BD8798EACDD16751",
    "eventID": "607b9532-1423-41c7-b048-ec2641693c47",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333",
    "tlsDetails": {
          "tlsVersion": "TLSv1.2",
          "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
          "clientProvidedHostHeader": "s3.amazonaws.com"
}
},
{
    "eventVersion": "1.03",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "111122223333",
        "arn": "arn:aws:iam::111122223333:user/myUserName",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "myUserName"
     },
    "eventTime": "2019-02-01T03:26:37Z",
    "eventSource": "s3.amazonaws.com",
    "eventName": "GetBucketVersioning",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "",
    "userAgent": "[]",
    "requestParameters": {
        "host": [
            "s3.us-west-2.amazonaws.com"
        ],
        "bucketName": "amzn-s3-demo-bucket1",
        "versioning": [
```

```
                ""
            ]
        },
        "responseElements": null,
        "additionalEventData": {
            "SignatureVersion": "SigV4",
            "CipherSuite": "ECDHE-RSA-AES128-SHA",
            "AuthenticationMethod": "AuthHeader"
    },
        "requestID": "07D681279BD94AED",
        "eventID": "f2b287f3-0df1-4961-a2f4-c4bdfed47657",
        "eventType": "AwsApiCall",
        "recipientAccountId": "111122223333",
        "tlsDetails": {
              "tlsVersion": "TLSv1.2",
              "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
              "clientProvidedHostHeader": "s3.amazonaws.com"
    }
    }
  ]
}
```


Habilitar o log de eventos do CloudTrail para buckets e objetos do S3

Você pode usar eventos de dados do CloudTrail para obter informações sobre solicitações no nível do bucket e do objeto no Amazon S3. Para habilitar eventos de dados do CloudTrail para todos os seus buckets ou para uma lista de buckets específicos, você deve criar uma trilha manualmente no CloudTrail.

> **Note**
>
> - A configuração padrão para o CloudTrail é encontrar somente eventos de gerenciamento. Verifique se os eventos de dados estão habilitados para sua conta.
> - Com um bucket do S3 que está gerando uma workload elevada, você poderia rapidamente gerar milhares de logs em um curto período. Esteja atento a quanto tempo você escolhe para habilitar eventos de dados do CloudTrail para um bucket ocupado.

O CloudTrail armazena logs de eventos de dados do Amazon S3 em um bucket do S3 de sua escolha. Você deve considerar a possibilidade de usar um bucket em uma Conta da AWS separada

para organizar melhor os eventos de vários buckets que você venha a ter em um local central para facilitar a consulta e a análise. O AWS Organizations ajuda você a criar uma Conta da AWS vinculada à conta que é proprietária do bucket que está sendo monitorado. Para obter mais informações, consulte O que é o AWS Organizations? no Guia do usuário do AWS Organizations.

Ao registrar eventos de dados de uma trilha no CloudTrail, é possível optar por usar seletores de eventos avançados ou básicos para registrar eventos de dados para objetos armazenados em buckets de uso geral. Para registrar eventos de dados de objetos armazenados em buckets de diretório, é necessário usar seletores de eventos avançados. Para ter mais informações, consulte Logging with AWS CloudTrail for S3 Express One Zone.

Ao criar uma trilha no console do CloudTrail usando seletores de eventos avançados, na seção de eventos de dados, é possível selecionar Registrar todos os eventos no Modelo de seletor de log para registrar em log todos os eventos no nível de objeto. Ao criar uma trilha no console do CloudTrail usando seletores de eventos básicos, na seção de eventos de dados, marque a caixa de seleção Selecionar todos os buckets do S3 em sua conta para registrar em log todos os eventos no nível de objeto.

> **Note**
>
> - É uma prática recomendada criar uma configuração de ciclo de vida para o bucket de evento de dados do AWS CloudTrail. Configure a configuração de ciclo de vida para remover periodicamente arquivos de log após o período que você acredita ser necessário auditá-los. Fazer isso reduz a quantidade de dados que o Athena analisa para cada consulta. Para obter mais informações, consulte Definir uma configuração do Ciclo de Vida do S3 em um bucket.
> - Para obter mais informações sobre o formato do registro em log, consulte Registrar chamadas de API do Amazon S3 em log usando AWS CloudTrail.
> - Para obter exemplos de como consultar logs do CloudTrail, consulte a publicação do Blog sobre big data da AWS Análise da segurança, compatibilidade e atividade operacional usando o AWS CloudTrail e o Amazon Athena.

Habilitar o registro em log de objetos em um bucket usando o console

Você pode usar o console do Amazon S3 para configurar uma trilha do AWS CloudTrail e registrar em log eventos de dados de objetos em um bucket do S3. O CloudTrail oferece suporte ao registro

em log de operações de API no nível do objeto do Amazon S3, como `GetObject`, `DeleteObject` e `PutObject`. Esses eventos são chamados de eventos de dados.

Por padrão, as trilhas do CloudTrail não registram em log eventos de dados, mas é possível configurar as trilhas para registrar eventos de dados para buckets do S3 que você especificar, ou para registrar eventos de dados para todos os buckets do Amazon S3 em sua Conta da AWS. Para obter mais informações, consulte Registrar chamadas de API do Amazon S3 em log usando AWS CloudTrail.

O CloudTrail não preenche eventos de dados no histórico de eventos do CloudTrail. Além disso, nem todas as ações no nível do bucket são preenchidas no histórico de eventos do CloudTrail. Para obter mais informações sobre ações de API no nível do bucket do Amazon S3 monitoradas pelo registro em log do CloudTrail, consulte Ações de buckets do Amazon S3 rastreadas pelo registro em log do CloudTrail. Para obter mais informações sobre como consultar os logs do CloudTrail, consulte o artigo da Central de Conhecimento da AWS que fala sobre o uso de padrões de filtro do Amazon CloudWatch Logs e o Amazon Athena para consultar logs do CloudTrail.

> **Note**
>
> Se você estiver registrando atividades de dados em log com o AWS CloudTrail, o registro de um evento de dados `DeleteObjects` do Amazon S3 inclui o evento `DeleteObjects` e um evento `DeleteObject` para cada objeto excluído como parte dessa operação. Você pode omitir a visibilidade adicional sobre objetos excluídos do registro de eventos. Para ter mais informações, consulte AWS CLI examples for filtering data events no Guia do usuário do AWS CloudTrail.

Para configurar uma trilha para registrar em log eventos de dados para um bucket do S3, você pode usar o console do AWS CloudTrail ou o console do Amazon S3. Se você estiver configurando uma trilha para registrar em log eventos de dados para todos os buckets do Amazon S3 na sua Conta da AWS, será mais fácil usar o console do CloudTrail. Para obter informações sobre como usar o console do CloudTrail para configurar uma trilha para registrar em log eventos de dados do S3, consulte Eventos de dados no Guia do usuário do AWS CloudTrail.

> **Important**
>
> Há cobranças adicionais para eventos de dados. Para obter mais informações, consulte Definição de preço do AWS CloudTrail.

O procedimento a seguir mostra como usar o console do Amazon S3 para configurar uma trilha do CloudTrail para registrar em log eventos de dados para um bucket do S3.

Como habilitar o registro em log de eventos de dados do CloudTrail para objetos em um bucket de uso geral do S3 ou em um bucket de diretório do S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Na lista Buckets, escolha o nome do bucket.
3. Escolha Properties (Propriedades).
4. Em Eventos de dados do AWS CloudTrail, selecione Configurar no CloudTrail.

   Você pode criar uma nova trilha do CloudTrail ou reutilizar uma trilha existente e configurar eventos de dados do Amazon S3 para serem registrados em sua trilha. Para obter informações sobre como criar trilhas no console do CloudTrail, consulte Criação e atualização de uma trilha com o console no Guia do usuário do AWS CloudTrail. Para obter informações sobre como configurar o registro em log de eventos de dados do Amazon S3 no console do CloudTrail, consulte Registro em log de eventos de dados para objetos do Amazon S3 no Guia do usuário do AWS CloudTrail.

   > **Note**
   >
   > Se você usar o console do CloudTrail ou o console do Amazon S3 para configurar uma trilha para registro em log de eventos de dados para um bucket do S3, o console do Amazon S3 mostra que o registro está habilitado no nível do objeto para o bucket.

Para desabilitar o registro de eventos de dados do CloudTrail para objetos em um bucket do S3

1. Faça login no AWS Management Console e abra o console do CloudTrail em https://console.aws.amazon.com/cloudtrail/.
2. No painel de navegação à esquerda, selecione Trilhas.
3. Escolha o nome da trilha que você criou para registrar eventos para o bucket.
4. Na página de detalhes da trilha, escolha Parar o registro no canto superior direito.
5. Na caixa de diálogo exibida, selecione Parar o registro.

Para obter informações sobre como habilitar o registro no nível do objeto ao criar um bucket do S3, consulte Criar um bucket de uso geral.

Para obter mais informações sobre o registro em log do CloudTrail com buckets do S3, consulte os seguintes tópicos:

- Visualizar das propriedades de um bucket de uso geral do S3
- Registrar chamadas de API do Amazon S3 em log usando AWS CloudTrail
- Como trabalhar com arquivos de log do CloudTrail no Guia do usuário do AWS CloudTrail

Identificar solicitações do Amazon S3 usando o CloudTrail

No Amazon S3, você pode identificar solicitações usando um log de eventos do AWS CloudTrail. O AWS CloudTrail é a maneira preferida de identificar solicitações do Amazon S3, mas se você estiver usando logs de acesso ao servidor do Amazon S3, consulte the section called “Identificar solicitações do S3”.

Tópicos

- Identificar solicitações feitas ao Amazon S3 em um log do CloudTrail
- Identificar solicitações de Signature Version 2 do Amazon S3 usando o CloudTrail
- Identificar o acesso a objetos do S3 usando o CloudTrail

Identificar solicitações feitas ao Amazon S3 em um log do CloudTrail

Após configurar o CloudTrail para entregar eventos a um bucket, você deve começar a ver objetos irem para seu bucket de destino no console do Amazon S3. Eles são formatados da seguinte maneira:

```
s3://amzn-s3-demo-bucket1/AWSLogs/111122223333/CloudTrail/Region/yyyy/mm/dd
```

Eventos registrados pelo CloudTrail são armazenados como objetos JSON compactados no formato gzipped no bucket do S3. Para encontrar solicitações com eficiência, você deve usar um serviço como o Amazon Athena para indexar e consultar os logs do CloudTrail.

Para obter mais informações sobre o CloudTrail e o Athena, consulte Criar a tabela de logs do AWS CloudTrail no Athena usando projeção de partições no Guia do usuário do Amazon Athena.

Identificar solicitações de Signature Version 2 do Amazon S3 usando o CloudTrail

Você pode usar um log de eventos do CloudTrail para identificar qual versão de assinatura de API foi usada para assinar uma solicitação no Amazon S3. Esse recurso é importante, pois o suporte ao Signature versão 2 será desativado (suspenso). Depois disso, o Amazon S3 não aceitará mais solicitações que usam o Signature versão 2 e todas as solicitações deverão usar assinaturas do Signature versão 4.

É altamente recomendável que você use o CloudTrail para ajudar a determinar se algum dos seus fluxos de trabalho está usando o Signature versão 2. Corrija-os atualizando suas bibliotecas e o código para usar o Signature versão 4 para evitar qualquer impacto em seus negócios.

Para obter mais informações, consulte Anúncio: AWS CloudTrail para Amazon S3 adiciona novos campos para auditoria de segurança aprimorada no AWS re:Post.

> **Note**
>
> Os eventos do CloudTrail para o Amazon S3 incluem a versão da assinatura nos detalhes da solicitação sob o nome de chave de `additionalEventData`. Para encontrar a versão da assinatura em solicitações feitas para objetos no Amazon S3, como `GET`, `PUT` e `DELETE`, você deve habilitar os eventos de dados do CloudTrail. (Esse recurso está desativado por padrão.)

O AWS CloudTrail é o método preferencial para identificar solicitações do Signature versão 2. Se você estiver usando logs de acesso ao servidor do Amazon S3, consulte Identificar solicitações do Signature Version 2 usando logs de acesso do Amazon S3.

Tópicos

- Exemplos de consulta do Athena para identificar solicitações do Amazon S3 Signature versão 2
- Particionar dados do Signature versão 2

Exemplos de consulta do Athena para identificar solicitações do Amazon S3 Signature versão 2

Example : Selecione todos os eventos do Signature Version 2 e imprima somente **`EventTime`**, **`S3_Action`**, **`Request_Parameters`**, **`Region`**, **`SourceIP`** e **`UserAgent`**

Na consulta do Athena a seguir, substitua *`s3_cloudtrail_events_db.cloudtrail_table`* pelos seus detalhes do Athena e aumente ou remova o limite, conforme necessário.

```
SELECT EventTime, EventName as S3_Action, requestParameters as Request_Parameters,
 awsregion as AWS_Region, sourceipaddress as Source_IP, useragent as User_Agent
FROM s3_cloudtrail_events_db.cloudtrail_table
WHERE eventsource='s3.amazonaws.com'
AND json_extract_scalar(additionalEventData, '$.SignatureVersion')='SigV2'
LIMIT 10;
```

Example : Selecione todos os solicitantes que estão enviando tráfego do Signature versão 2

```
SELECT useridentity.arn, Count(requestid) as RequestCount
FROM s3_cloudtrail_events_db.cloudtrail_table
WHERE eventsource='s3.amazonaws.com'
    and json_extract_scalar(additionalEventData, '$.SignatureVersion')='SigV2'
Group by useridentity.arn
```

Particionar dados do Signature versão 2

Se você tiver uma grande quantidade de dados para consultar, poderá reduzir os custos e o tempo de execução do Athena criando uma tabela particionada.

Para fazer isso, crie uma tabela com partições conforme indicado a seguir.

```
  CREATE EXTERNAL TABLE s3_cloudtrail_events_db.cloudtrail_table_partitioned(
       eventversion STRING,
       userIdentity STRUCT<
           type:STRING,
           principalid:STRING,
           arn:STRING,
           accountid:STRING,
           invokedby:STRING,
           accesskeyid:STRING,
           userName:STRING,
        sessioncontext:STRUCT<
                   attributes:STRUCT<
                   mfaauthenticated:STRING,
                   creationdate:STRING>,
                   sessionIssuer:STRUCT<
```

```
                    type:STRING,
                    principalId:STRING,
                    arn:STRING,
                    accountId:STRING,
                    userName:STRING>
                >
            >,
        eventTime STRING,
        eventSource STRING,
        eventName STRING,
        awsRegion STRING,
        sourceIpAddress STRING,
        userAgent STRING,
        errorCode STRING,
        errorMessage STRING,
        requestParameters STRING,
        responseElements STRING,
        additionalEventData STRING,
        requestId STRING,
        eventId STRING,
        resources ARRAY<STRUCT<ARN:STRING,accountId: STRING,type:STRING>>,
        eventType STRING,
        apiVersion STRING,
        readOnly STRING,
        recipientAccountId STRING,
        serviceEventDetails STRING,
        sharedEventID STRING,
        vpcEndpointId STRING
    )
    PARTITIONED BY (region string, year string, month string, day string)
    ROW FORMAT SERDE 'org.apache.hadoop.hive.ql.io.orc.OrcSerde'
    STORED AS INPUTFORMAT 'org.apache.hadoop.hive.ql.io.SymlinkTextInputFormat'
    OUTPUTFORMAT 'org.apache.hadoop.hive.ql.io.HiveIgnoreKeyTextOutputFormat'
    LOCATION 's3://amzn-s3-demo-bucket1/AWSLogs/111122223333/';
```

Em seguida, crie as partições individualmente. Não é possível obter resultados de datas que não foram criadas.

```
ALTER TABLE s3_cloudtrail_events_db.cloudtrail_table_partitioned ADD
    PARTITION (region= 'us-east-1', year= '2019', month= '02', day= '19') LOCATION
 's3://amzn-s3-demo-bucket1/AWSLogs/111122223333/CloudTrail/us-east-1/2019/02/19/'
```

```
    PARTITION (region= 'us-west-1', year= '2019', month= '02', day= '19') LOCATION
 's3://amzn-s3-demo-bucket1/AWSLogs/111122223333/CloudTrail/us-west-1/2019/02/19/'
    PARTITION (region= 'us-west-2', year= '2019', month= '02', day= '19') LOCATION
 's3://amzn-s3-demo-bucket1/AWSLogs/111122223333/CloudTrail/us-west-2/2019/02/19/'
    PARTITION (region= 'ap-southeast-1', year= '2019', month= '02', day= '19') LOCATION
 's3://amzn-s3-demo-bucket1/AWSLogs/111122223333/CloudTrail/ap-southeast-1/2019/02/19/'
    PARTITION (region= 'ap-southeast-2', year= '2019', month= '02', day= '19') LOCATION
 's3://amzn-s3-demo-bucket1/AWSLogs/111122223333/CloudTrail/ap-southeast-2/2019/02/19/'
    PARTITION (region= 'ap-northeast-1', year= '2019', month= '02', day= '19') LOCATION
 's3://amzn-s3-demo-bucket1/AWSLogs/111122223333/CloudTrail/ap-northeast-1/2019/02/19/'
    PARTITION (region= 'eu-west-1', year= '2019', month= '02', day= '19') LOCATION
 's3://amzn-s3-demo-bucket1/AWSLogs/111122223333/CloudTrail/eu-west-1/2019/02/19/'
    PARTITION (region= 'sa-east-1', year= '2019', month= '02', day= '19') LOCATION
 's3://amzn-s3-demo-bucket1/AWSLogs/111122223333/CloudTrail/sa-east-1/2019/02/19/';
```

Você pode, então, fazer a solicitação com base nessas partições e não é preciso carregar todo o bucket.

```
SELECT useridentity.arn,
Count(requestid) AS RequestCount
FROM s3_cloudtrail_events_db.cloudtrail_table_partitioned
WHERE eventsource='s3.amazonaws.com'
AND json_extract_scalar(additionalEventData, '$.SignatureVersion')='SigV2'
AND region='us-east-1'
AND year='2019'
AND month='02'
AND day='19'
Group by useridentity.arn
```

Identificar o acesso a objetos do S3 usando o CloudTrail

Você pode usar seus logs de eventos do AWS CloudTrail para identificar solicitações de acesso a objetos do Amazon S3 para eventos de dados como `GetObject`, `DeleteObject` e `PutObject` e descobrir informações adicionais sobre essas solicitações.

> **Note**
>
> Se você estiver registrando atividades de dados em log com o AWS CloudTrail, o registro de um evento de dados `DeleteObjects` do Amazon S3 inclui o evento `DeleteObjects`

e um evento `DeleteObject` para cada objeto excluído como parte dessa operação. Você pode omitir a visibilidade adicional sobre objetos excluídos do registro de eventos. Para ter mais informações, consulte AWS CLI examples for filtering data events no Guia do usuário do AWS CloudTrail.

O exemplo a seguir mostra como obter todas as solicitações PUT de objetos para o Amazon S3 de um log de eventos do AWS CloudTrail.

Tópicos

- Exemplos de consulta do Athena para identificar solicitações de acesso a objetos do Amazon S3

Exemplos de consulta do Athena para identificar solicitações de acesso a objetos do Amazon S3

Nos exemplos de consultas do Athena a seguir, substitua *s3_cloudtrail_events_db.cloudtrail_table* pelos seus detalhes do Athena e modifique o intervalo de datas, conforme necessário.

Example : Selecione todos os eventos que tenham solicitações **PUT** de acesso a objetos e imprima somente **EventTime**, **EventSource**, **SourceIP**, **UserAgent**, **BucketName**, **object** e **UserARN**

```
SELECT
  eventTime,
  eventName,
  eventSource,
  sourceIpAddress,
  userAgent,
  json_extract_scalar(requestParameters, '$.bucketName') as bucketName,
  json_extract_scalar(requestParameters, '$.key') as object,
  userIdentity.arn as userArn
FROM
  s3_cloudtrail_events_db.cloudtrail_table
WHERE
  eventName = 'PutObject'
  AND eventTime BETWEEN '2019-07-05T00:00:00Z' and '2019-07-06T00:00:00Z'
```

Example : Selecione todos os eventos que tenham solicitações **GET** de acesso a objetos e imprima somente **EventTime**, **EventSource**, **SourceIP**, **UserAgent**, **BucketName**, **object** e **UserARN**

```
SELECT
  eventTime,
  eventName,
  eventSource,
  sourceIpAddress,
  userAgent,
  json_extract_scalar(requestParameters, '$.bucketName') as bucketName,
  json_extract_scalar(requestParameters, '$.key') as object,
  userIdentity.arn as userArn
FROM
  s3_cloudtrail_events_db.cloudtrail_table
WHERE
  eventName = 'GetObject'
  AND eventTime BETWEEN '2019-07-05T00:00:00Z' and '2019-07-06T00:00:00Z'
```

Example : Selecione todos os eventos de solicitante anônimo em um bucket em determinado período e imprima somente **EventTime**, **EventName**, **EventSource**, **SourceIP**, **UserAgent**, **BucketName**, **UserARN** e **AccountID**

```
SELECT
  eventTime,
  eventName,
  eventSource,
  sourceIpAddress,
  userAgent,
  json_extract_scalar(requestParameters, '$.bucketName') as bucketName,
  userIdentity.arn as userArn,
  userIdentity.accountId
FROM
  s3_cloudtrail_events_db.cloudtrail_table
WHERE
  userIdentity.accountId = 'anonymous'
  AND eventTime BETWEEN '2019-07-05T00:00:00Z' and '2019-07-06T00:00:00Z'
```

Example : Identifique todas as solicitações que exigiram uma ACL para autorização

O exemplo de consulta do Amazon Athena a seguir mostra como identificar todas as solicitações feitas aos seus buckets do S3 que exigiram uma lista de controle de acesso (ACL) para autorização. Se a solicitação exigiu uma ACL para autorização, o valor de `aclRequired` em

`additionalEventData` é `Yes`. Se nenhuma ACL foi necessária, `aclRequired` não está presente. Você pode usar essas informações para migrar essas permissões de ACL para as políticas de bucket apropriadas. Depois de criar essas políticas de bucket, você pode desativar as ACLs para esses buckets. Para obter mais informações sobre como desativar as ACLs, consulte Pré-requisitos para desabilitar ACLs.

```
SELECT
  eventTime,
  eventName,
  eventSource,
  sourceIpAddress,
  userAgent,
  userIdentity.arn as userArn,
  json_extract_scalar(requestParameters, '$.bucketName') as bucketName,
  json_extract_scalar(requestParameters, '$.key') as object,
  json_extract_scalar(additionalEventData, '$.aclRequired') as aclRequired
FROM
  s3_cloudtrail_events_db.cloudtrail_table
WHERE
  json_extract_scalar(additionalEventData, '$.aclRequired') = 'Yes'
  AND eventTime BETWEEN '2022-05-10T00:00:00Z' and '2022-08-10T00:00:00Z'
```

Note

- Esses exemplos de consulta também podem ser úteis para o monitoramento de segurança. Você pode ver os resultados de chamadas `PutObject` ou `GetObject` de solicitantes ou endereços IP inesperados ou não autorizados e identificar solicitações anônimas aos seus buckets.
- Essa consulta recupera somente informações do momento no qual o registro estava habilitado.

Se você estiver usando logs de acesso ao servidor do Amazon S3, consulte Identificar solicitações de acesso a objetos usando logs de acesso do Amazon S3.

Registrar em log as solicitações com registro em log de acesso ao servidor

O registro em log de acesso ao servidor fornece detalhes sobre as solicitações que são feitas a um bucket. Os logs de acesso ao servidor são úteis para muitos aplicativos. Por exemplo, as informações do log de acesso podem ser úteis em auditorias de segurança e acesso. Essas informações também podem ajudar você a conhecer sua base de clientes e entender a cobrança do Amazon S3.

> **Note**
>
> Os logs de acesso ao servidor não registram informações sobre erros de redirecionamento a regiões erradas para regiões lançadas após 20 de março de 2019. Erros de redirecionamento para regiões erradas ocorrem quando uma solicitação para um objeto ou bucket é feita fora da região em que o bucket existe.

Como faço para habilitar a entrega de logs?

Para habilitar a entrega de logs, execute as seguintes etapas básicas. Para obter detalhes, consulte Habilitar o log de acesso ao servidor do Amazon S3.

1. Forneça o nome do bucket de destino (também conhecido como bucket de destino). Esse bucket é onde você deseja que o Amazon S3 salve os logs de acesso como objetos. Os buckets de origem e de destino devem estar na mesma Região da AWS e pertencer à mesma conta. O bucket de destino não pode ter uma configuração de período de retenção padrão da funcionalidade Bloqueio de Objetos do S3. O bucket de destino também não pode ter a opção Pagamento pelo solicitante habilitada.

   Os logs podem ser entregues a qualquer bucket que você possui e que esteja na mesma região que o bucket de origem, incluindo o próprio bucket de origem. No entanto, para um gerenciamento de logs mais simples, recomendamos que você salve logs de acesso em um bucket diferente.

   Quando o bucket de origem e o bucket de destino são os mesmos, logs adicionais serão criados para os logs que forem gravados no bucket, o que criará um ciclo infinito de logs. Não recomendamos fazer isso, pois pode gerar um pequeno aumento na cobrança do armazenamento. Além disso, com os logs adicionais sobre logs, pode ser mais difícil encontrar o log que você está procurando.

Se você optar por salvar os logs de acesso no bucket de origem, recomendamos que especifique um prefixo de destino (também conhecido como prefixo-alvo) para todas as chaves de objeto de log. Quando você especifica um prefixo, todos os nomes de objeto de log começam com uma string comum, o que facilita a identificação dos objetos de log.

2. (Opcional) Atribua um prefixo de destino a todas as chaves de objeto de log do Amazon S3. O prefixo de destino (também conhecido como prefixo-alvo) facilita a localização de objetos de log. Por exemplo, se você especificar o valor do prefixo `logs/`, cada objeto de log criado pelo Amazon S3 começará com o prefixo `logs/` na sua chave, por exemplo:

   ```
   logs/2013-11-01-21-32-16-E568B2907131C0C0
   ```

   Se você especificar o valor de prefixo `logs`, o objeto de log será exibido da seguinte forma:

   ```
   logs2013-11-01-21-32-16-E568B2907131C0C0
   ```

   Os prefixos também são úteis para distinguir entre buckets de origem quando vários buckets são registrados em log no mesmo bucket de destino.

   Esse prefixo também ajuda ao excluir os logs. Por exemplo, você pode definir uma regra de configuração do ciclo de vida para que o Amazon S3 exclua objetos com um prefixo específico. Para obter mais informações, consulte Exclusão de arquivos de log do Amazon S3.

3. (Opcional) Defina permissões para que outros possam acessar os logs gerados. Por padrão, somente o proprietário do bucket sempre tem acesso completo aos objetos de log. Se o bucket de destino usam a configuração Imposto pelo proprietário do bucket para a Propriedade de Objetos do S3 a fim de desabilitar as listas de controle de acesso (ACLs), você não pode conceder permissões nas concessões de destino (também chamadas de concessões-alvo) que usam ACLs. Porém, você pode atualizar a política do bucket de destino para conceder acesso a outros. Para obter mais informações, consulte Gerenciamento de identidade e acesso para o Amazon S3 e Permissões para entrega de logs.

4. (Opcional) Defina um formato de chave de objeto de log para os arquivos de log. Você tem duas opções para o formato da chave de objeto de log (também conhecido como formato da chave de objeto-alvo):

   - Particionamento não baseado em data: esse é o formato original da chave de objeto de log. Se você escolher esse formato, o formato da chave de arquivo de log será exibido da seguinte forma:

```
[DestinationPrefix][YYYY]-[MM]-[DD]-[hh]-[mm]-[ss]-[UniqueString]
```

Por exemplo, se você especificar `logs/` como prefixo, os objetos de log serão nomeados assim:

```
logs/2013-11-01-21-32-16-E568B2907131C0C0
```

- Particionamento baseado em data: se você escolher o particionamento baseado em data, poderá escolher a hora do evento ou a hora de entrega do arquivo de log como a fonte de data usada no formato do log. Esse formato facilita a consulta dos logs.

  Se você escolher o particionamento baseado em data, o formato da chave de arquivo de log será exibido da seguinte forma:

  ```
  [DestinationPrefix][SourceAccountId]/[SourceRegion]/[SourceBucket]/[YYYY]/[MM]/
  [DD]/[YYYY]-[MM]-[DD]-[hh]-[mm]-[ss]-[UniqueString]
  ```

  Por exemplo, se você especificar `logs/` como prefixo-alvo, os objetos de log serão nomeados assim:

  ```
  logs/123456789012/us-west-2/amzn-s3-demo-source-
  bucket/2023/03/01/2023-03-01-21-32-16-E568B2907131C0C0
  ```

  Para a entrega na hora de entrega, a hora nos nomes de arquivo de log corresponde à hora de entrega dos arquivos de log.

  Para a entrega na hora do evento, o ano, o mês e o dia correspondem ao dia em que o evento ocorreu, e a hora, os minutos e os segundos são definidos como `00` na chave. Os logs entregues nesses arquivos de log são somente para um dia específico.

Se você estiver configurando os logs por meio da AWS Command Line Interface (AWS CLI), AWS SDKs ou API REST do Amazon S3, use `TargetObjectKeyFormat` para especificar o formato da chave de objeto de log. Para especificar o particionamento não baseado em data, use `SimplePrefix`. Para especificar o particionamento baseado em data, use `PartitionedPrefix`. Se você usar `PartitionedPrefix`, use `PartitionDateSource` para especificar `EventTime` ou `DeliveryTime`.

Para `SimplePrefix`, o formato da chave de arquivo de log aparece da seguinte forma:

```
[TargetPrefix][YYYY]-[MM]-[DD]-[hh]-[mm]-[ss]-[UniqueString]
```

Para `PartitionedPrefix` com hora do evento ou hora da entrega, o formato da chave de arquivo de log aparece da seguinte forma:

```
[TargetPrefix][SourceAccountId]/[SourceRegion]/[SourceBucket]/[YYYY]/[MM]/[DD]/
[YYYY]-[MM]-[DD]-[hh]-[mm]-[ss]-[UniqueString]
```

Formato da chave de objeto de log

O Amazon S3 usa os seguintes formatos de chave de objeto para os objetos de log carregados no bucket de destino:

- Particionamento não baseado em data: esse é o formato original da chave de objeto de log. Se você escolher esse formato, o formato da chave de arquivo de log será exibido da seguinte forma:

  ```
  [DestinationPrefix][YYYY]-[MM]-[DD]-[hh]-[mm]-[ss]-[UniqueString]
  ```

- Particionamento baseado em data: se você escolher o particionamento baseado em data, poderá escolher a hora do evento ou a hora de entrega do arquivo de log como a fonte de data usada no formato do log. Esse formato facilita a consulta dos logs.

  Se você escolher o particionamento baseado em data, o formato da chave de arquivo de log será exibido da seguinte forma:

  ```
  [DestinationPrefix][SourceAccountId]/[SourceRegion]/[SourceBucket]/[YYYY]/[MM]/[DD]/
  [YYYY]-[MM]-[DD]-[hh]-[mm]-[ss]-[UniqueString]
  ```

Na chave de objeto de log, `YYYY`, `MM`, `DD`, `hh`, `mm` e `ss` são os dígitos do ano, mês, dia, hora, minutos e segundos (respectivamente). Essas datas e horas estão em Tempo Universal Coordenado (UTC).

Um arquivo de log entregue em um horário específico pode conter registros gravados a qualquer momento até aquele horário. Não há como saber se todos os logs de um certo intervalo de tempo foram entregues ou não.

O componente `UniqueString` da chave existe para impedir que arquivos sejam substituídos por outros. Ele não tem significado, e o software de processamento de logs deve ignorá-lo.

Como os logs são entregues?

O Amazon S3 coleta periodicamente os registros de log de acesso, consolida-os em arquivos de log e faz upload desses arquivos no bucket de destino como objetos de log. Caso o registro em log esteja habilitado em diversos buckets de origem que identifiquem o mesmo bucket de destino, esse bucket de destino terá os logs de acesso de todos os buckets de origem. No entanto, cada objeto de log relata registros de log para um bucket de origem específico.

O Amazon S3 usa uma conta especial de entrega de logs para gravar logs de acesso ao servidor. Essas gravações estão sujeitas a restrições usuais de controle de acesso. Recomendamos atualizar a política do bucket de destino para conceder acesso à entidade principal de serviço do registro em log (`logging.s3.amazonaws.com`) para entrega de logs de acesso. Você também pode conceder acesso para a entrega de logs de acesso ao grupo de entrega de logs do S3 por meio da lista de controle de acesso (ACL) do bucket. No entanto, não é recomendável conceder acesso ao grupo de entrega de logs do S3 usando a ACL do bucket.

Ao habilitar o registro em log de acesso ao servidor e conceder acesso para a entrega de logs de acesso por meio da política do bucket de destino, atualize a política para permitir acesso `s3:PutObject` para a entidade principal de serviço do registro em log. Se você usar o console do Amazon S3 para habilitar o registro em log de acesso ao servidor, o console atualizará automaticamente a política do bucket de destino para conceder essas permissões à entidade principal de serviço do registro em log. Para obter mais informações sobre como conceder permissões para logs de acesso ao servidor, consulte Permissões para entrega de logs.

> **Note**
>
> O S3 não é compatível com a entrega de logs do CloudTrail ou logs de acesso ao servidor ao solicitante ou ao proprietário do bucket para solicitações de endpoint da VPC quando a política de endpoint da VPC as nega ou para solicitações que falham antes da política da VPC ser avaliada.

Configuração aplicada pelo proprietário do bucket em S3 Object Ownership

Se o bucket de destino usar a configuração Imposto pelo proprietário do bucket para a Propriedade de Objetos, as ACLs serão desabilitadas e não afetarão mais as permissões. É necessário atualizar

a política do bucket de destino para conceder acesso à entidade principal de serviço do registro em log. Para obter informações sobre o Object Ownership, consulte Conceder acesso ao grupo de entrega de logs do S3 para registro em log de acesso ao servidor.

Entrega de logs do servidor de melhor esforço

Os registros de log de acesso ao servidor são entregues com base no melhor esforço. A maioria das solicitações para um bucket configurado corretamente para registro em log tem como resultado um registro do log entregue. A maioria dos registros de log é entregue dentro de algumas horas após o tempo em que forem registrados, mas eles podem ser entregues com mais frequência.

A integralidade e a pontualidade do registro em log do servidor não são garantidas. O registro de log de uma solicitação específica pode ser entregue muito depois de a solicitação ter sido realmente processada ou pode nem ser entregue. É possível que você até veja uma duplicação de um registro de log. A finalidade dos logs do servidor é proporcionar uma ideia da natureza do tráfego no bucket. Embora a perda ou a duplicação de registros de log sejam acontecimentos raros, esteja ciente de que o registro em log do servidor não tem como objetivo ser uma contabilidade completa de todas as solicitações.

Devido à natureza de melhor esforço do registro em log do servidor, os relatórios de uso podem incluir uma ou mais solicitações de acesso que não aparecem em um log do servidor entregue. Você pode encontrar esses relatórios de uso em Cost & usage reports no console do Gerenciamento de Faturamento e Custos da AWS.

As alterações do status do registro de bucket em logs entram em vigor ao longo do tempo

As alterações no status do log de um bucket levam tempo para realmente afetar a entrega de arquivos de log. Por exemplo, se você habilitar o registro em log para um bucket, algumas solicitações feitas na hora seguinte poderão ser registradas, enquanto outras não. Suponha que você altere o bucket de destino para registro em log do bucket A para o bucket B. Durante a hora seguinte, alguns logs poderão continuar sendo entregues ao bucket A, enquanto outros serão entregues ao novo bucket de destino B. Em todo caso, as novas configurações entrarão em vigor posteriormente, sem a necessidade de ações adicionais.

Para obter mais informações sobre registro em log e arquivos de log, consulte as seguintes seções:

Tópicos

- Habilitar o log de acesso ao servidor do Amazon S3
- Formato dos logs de acesso ao servidor do Amazon S3
- Exclusão de arquivos de log do Amazon S3
- Usar logs de acesso ao servidor do Amazon S3 para identificar solicitações
- Solução de problemas do registro em log de acessos ao servidor

Habilitar o log de acesso ao servidor do Amazon S3

O registro em log de acesso ao servidor fornece detalhes sobre as solicitações que são feitas a um bucket do Amazon S3. Os logs de acesso ao servidor são úteis para muitos aplicativos. Por exemplo, as informações do log de acesso podem ser úteis em auditorias de segurança e acesso. Essas informações também podem ajudar você a conhecer sua base de clientes e entender a cobrança do Amazon S3.

Por padrão, o Amazon S3 não coleta logs de acesso ao servidor. Quando você habilita o registro em log, o Amazon S3 entrega os logs de acesso de um bucket de origem a um bucket de destino (também conhecido como bucket-alvo) de sua escolha. O bucket de destino deve estar nas mesmas Região da AWS e Conta da AWS que o bucket de origem.

Um registro do log de acesso contém detalhes sobre as solicitações feitas a um bucket. Essa informação pode incluir o tipo de solicitação, os recursos que foram especificados na solicitação e a hora e data em que a solicitação foi processada. Para obter mais informações sobre noções básicas de registro em log, consulte Registrar em log as solicitações com registro em log de acesso ao servidor.

⚠ Important

- Não há custo adicional para a ativação de registro de acesso ao servidor em um bucket do Amazon S3. No entanto, todos os arquivos de log que o sistema fornece acumularão as cobranças normais de armazenamento. Você pode excluir os arquivos de registro em log a qualquer momento. Não estimamos as cobranças pela transferência de dados por entrega de arquivo de log, mas cobramos a taxa normal de transferência de dados pelo acesso aos arquivos de log.
- O bucket de destino não deve ter registro em log de acesso ao servidor habilitado. Os logs podem ser entregues a qualquer bucket que você possui e que esteja na mesma região que o bucket de origem, incluindo o próprio bucket de origem. No entanto, a entrega de

logs para o bucket de origem causará um loop infinito de logs e não é recomendada. Para um gerenciamento de logs mais simples, recomendamos que você salve logs de acesso em um bucket diferente. Para obter mais informações, consulte Como faço para habilitar a entrega de logs?.

- Os buckets do S3 com a funcionalidade Bloqueio de Objetos do S3 habilitada não podem ser usados como buckets de destino para logs de acesso ao servidor. O bucket de destino não pode ter uma configuração de período de retenção padrão.
- O bucket de destino não pode ter a opção Pagamento pelo solicitante habilitada.
- Você poderá usar a criptografia de bucket padrão no bucket de destino somente se usar a criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3), que usa o Advanced Encryption Standard de 256 bits (AES-256). A criptografia do lado do servidor padrão com chaves do AWS Key Management Service (AWS KMS) (SSE-KMS) não é compatível.

Você pode habilitar ou desabilitar o registro em log de acesso ao servidor usando o console do Amazon S3, a API do Amazon S3, a AWS Command Line Interface (AWS CLI) ou os AWS SDKs.

Permissões para entrega de logs

O Amazon S3 usa uma conta especial de entrega de logs para gravar logs de acesso ao servidor. Essas gravações estão sujeitas a restrições usuais de controle de acesso. Para a entrega dos logs de acesso, você deve conceder à entidade principal de serviço do registro em log (`logging.s3.amazonaws.com`) acesso ao bucket de destino.

Para conceder permissões ao Amazon S3 para a entrega de logs, você pode usar uma política de bucket ou listas de controle de acesso (ACLs) de bucket, dependendo das configurações da Propriedade de Objetos do S3 do bucket de destino. No entanto, recomendamos usar uma política de bucket em vez de ACLs.

Configuração aplicada pelo proprietário do bucket em S3 Object Ownership

Se o bucket de destino usar a configuração Imposto pelo proprietário do bucket para a Propriedade de Objetos, as ACLs serão desabilitadas e não afetarão mais as permissões. Nesse caso, é necessário atualizar a política do bucket de destino para conceder acesso à entidade principal de serviço do registro em log. Não é possível atualizar sua ACL de bucket para conceder acesso ao grupo de entrega de logs do S3. Você também não pode incluir concessões de destino (também conhecidas como concessões-alvo) na configuração PutBucketLogging.

Para obter informações sobre como migrar ACLs de bucket existentes para entrega de logs de acesso para uma política de bucket, consulte Conceder acesso ao grupo de entrega de logs do S3 para registro em log de acesso ao servidor. Para obter informações sobre o Object Ownership, consulte Controlar a propriedade de objetos e desabilitar ACLs para seu bucket. Quando você cria um bucket, as ACLs são desabilitadas por padrão.

Conceder acesso usando uma política de bucket

Para conceder acesso usando uma política de bucket no bucket de destino, atualize a política de bucket para conceder a permissão `s3:PutObject` à entidade principal de serviço do registro em log. Se você usar o console do Amazon S3 para habilitar o registro em log de acesso ao servidor, o console atualizará automaticamente a política do bucket de destino para conceder essa permissão à entidade principal de serviço do registro em log. Se você habilitar o registro em log de acesso ao servidor de maneira programática, poderá atualizar manualmente a política do bucket de destino para conceder acesso à entidade principal de serviço do registro em log.

Para ver um exemplo de política de bucket que concede acesso à entidade principal de serviço do registro em log, consulte the section called “Conceder permissões à entidade principal do serviço de log usando uma política de bucket”.

Conceder acesso usando ACLs de bucket

Você pode alternar com ACLs de bucket para conceder acesso à entrega de logs de acesso. Adicione uma entrada de concessão à ACL de bucket que concede as permissões `WRITE` e `READ_ACP` para o grupo de entrega de logs do S3. No entanto, não é recomendável conceder acesso ao grupo de entrega de logs do S3 usando ACLs de bucket. Para obter mais informações, consulte Controlar a propriedade de objetos e desabilitar ACLs para seu bucket. Para obter informações sobre como migrar ACLs de bucket existentes para entrega de logs de acesso para uma política de bucket, consulte Conceder acesso ao grupo de entrega de logs do S3 para registro em log de acesso ao servidor. Para ver um exemplo de ACL que concede acesso à entidade principal de serviço do registro em log, consulte the section called “Conceder permissões ao grupo de entrega de logs usando a ACL de bucket”.

Conceder permissões à entidade principal do serviço de log usando uma política de bucket

Este exemplo de política de bucket concede a permissão `s3:PutObject` à entidade principal de serviço do registro em log (`logging.s3.amazonaws.com`). Para usar essa política de bucket, substitua os *`user input placeholders`* por suas próprias informações. Na política a seguir, *`amzn-s3-demo-destination-bucket`* é o bucket de destino em que os logs de acesso ao

servidor serão entregues e *amzn-s3-demo-source-bucket* é o bucket de origem. *EXAMPLE-LOGGING-PREFIX* é o prefixo de destino opcional (também conhecido como prefixo-alvo) que você deseja usar para os objetos de log. *SOURCE-ACCOUNT-ID* é a Conta da AWS à qual o bucket de origem pertence.

> **Note**
>
> Se houver declarações `Deny` na política de bucket, verifique se elas não estão impedindo que o Amazon S3 entregue logs de acesso.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "S3ServerAccessLogsPolicy",
            "Effect": "Allow",
            "Principal": {
                "Service": "logging.s3.amazonaws.com"
            },
            "Action": [
                "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/EXAMPLE-LOGGING-PREFIX*",
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:s3:::amzn-s3-demo-source-bucket"
                },
                "StringEquals": {
                    "aws:SourceAccount": "SOURCE-ACCOUNT-ID"
                }
            }
        }
    ]
}
```

Conceder permissões ao grupo de entrega de logs usando a ACL de bucket

> **Note**
>
> Com base em uma prática recomendada de segurança, o Amazon S3 desabilita as listas de controle de acesso (ACLs) por padrão em todos os novos buckets. Para obter mais informações sobre permissões de ACL no console do Amazon S3, consulte Configurar ACLs.

Embora esse método não seja recomendado, é possível conceder permissões ao grupo de entrega de logs usando uma ACL de bucket. Porém, se o bucket de destino usar a configuração Imposto pelo proprietário do bucket para a Propriedade de Objetos, você não poderá definir ACLs de bucket ou de objeto. Você também não pode incluir concessões de destino (também conhecidas como concessões-alvo) na configuração PutBucketLogging. Em vez disso, é necessário usar uma política de bucket para conceder acesso à entidade principal do serviço de log (`logging.s3.amazonaws.com`). Para obter mais informações, consulte Permissões para entrega de logs.

Na ACL de bucket, o grupo de entrega de logs é representado pelo seguinte URL:

```
http://acs.amazonaws.com/groups/s3/LogDelivery
```

Para conceder as permissões `WRITE` e `READ_ACP` (leitura de ACL), adicione as seguintes concessões à ACL do bucket de destino:

```
<Grant>
    <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"  xsi:type="Group">
        <URI>http://acs.amazonaws.com/groups/s3/LogDelivery</URI>
    </Grantee>
    <Permission>WRITE</Permission>
</Grant>
<Grant>
    <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"  xsi:type="Group">
        <URI>http://acs.amazonaws.com/groups/s3/LogDelivery</URI>
    </Grantee>
    <Permission>READ_ACP</Permission>
</Grant>
```

Para obter exemplos de adição de concessões de ACL de forma programada, consulte Configurar ACLs.

Important

Ao habilitar o log de acesso ao servidor do Amazon S3 usando o AWS CloudFormation em um bucket e usar ACLs para conceder acesso ao grupo de entrega de logs do S3, você também deverá adicionar "`AccessControl": "LogDeliveryWrite`"" ao modelo do CloudFormation. Fazer isso é importante porque só é possível conceder essas permissões criando uma ACL para o bucket, mas não é possível criar ACLs personalizadas para buckets no CloudFormation. Você só pode usar ACLs predefinidas com o CloudFormation.

Para habilitar o log de acesso ao servidor

Para habilitar o registro em log de acesso ao servidor usando o console do Amazon S3, a API REST do Amazon S3, os AWS SDKs e a AWS CLI, use os procedimentos a seguir.

Usar o console do S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets de uso geral.
3. Na lista de buckets, escolha o nome do bucket para o qual você deseja habilitar o registro em log do acesso ao servidor.
4. Escolha Properties (Propriedades).
5. Na seção Server access logging (Registro de acesso ao servidor) escolha Edit (Editar).
6. Em Registro em log de acesso ao servidor, selecione Habilitar.
7. Em Bucket de destino, especifique um bucket e um prefixo opcional. Se você especificar um prefixo, recomendamos incluir uma barra (/) depois dele para facilitar a localização dos logs.

Note

Especificar um prefixo com uma barra (/) simplifica a localização de objetos de log. Por exemplo, se você especificar o valor do prefixo `logs/`, cada objeto de log criado pelo Amazon S3 começará com o prefixo `logs/` na sua chave, da seguinte forma:

```
logs/2013-11-01-21-32-16-E568B2907131C0C0
```

Se você especificar o valor de prefixo `logs`, o objeto de log será exibido da seguinte forma:

```
logs2013-11-01-21-32-16-E568B2907131C0C0
```

8. Em Formato da chave do objeto de log, execute uma das seguintes ações:

   - Para escolher o particionamento não baseado em data, escolha [DestinationPrefix][AAAA]-[MM]-[DD]-[hh]-[mm]-[ss]-[UniqueString].
   - Para escolher o particionamento baseado em data, escolha [DestinationPrefix][SourceAccountId]/[SourceRegion]/[SourceBucket]/[AAAA]/[MM]/[DD]/[AAAA]-[MM]-[DD]-[hh]-[mm]-[ss]-[UniqueString], depois escolha Hora do evento do S3 ou Hora de entrega do arquivo de log.

9. Escolha Salvar alterações.

   Quando você habilita o registro em log de acesso ao servidor em um bucket, o console habilita o registro em log no bucket de origem e atualiza a política do bucket de destino para conceder a permissão `s3:PutObject` à entidade principal de serviço do registro em log (`logging.s3.amazonaws.com`). Para obter mais informações sobre esta política de bucket, consulte Conceder permissões à entidade principal do serviço de log usando uma política de bucket.

   Você pode visualizar os logs no bucket de destino. Depois de habilitar o registro em log de acesso ao servidor, pode demorar algumas horas antes que os logs sejam entregues no bucket de destino. Para obter mais informações sobre como e quando os logs são entregues, consulte Como os logs são entregues?.

Para obter mais informações, consulte Visualizar das propriedades de um bucket de uso geral do S3.

Uso da API REST

Para habilitar o registro em log, envie uma solicitação PutBucketLogging para adicionar a configuração de registro em log no bucket de origem. A solicitação especifica o bucket de destino (também conhecido como bucket-alvo) e, opcionalmente, o prefixo a ser usado com todas as chaves de objeto de log.

O exemplo a seguir identifica *amzn-s3-demo-destination-bucket* como o bucket de destino e *logs/* como o prefixo.

```
<BucketLoggingStatus xmlns="http://doc.s3.amazonaws.com/2006-03-01">
  <LoggingEnabled>
    <TargetBucket>amzn-s3-demo-destination-bucket</TargetBucket>
    <TargetPrefix>logs/</TargetPrefix>
  </LoggingEnabled>
</BucketLoggingStatus>
```

O exemplo a seguir identifica *amzn-s3-demo-destination-bucket* como o bucket de destino, *logs/* como o prefixo e `EventTime` como o formato da chave de objeto de log.

```
<BucketLoggingStatus xmlns="http://doc.s3.amazonaws.com/2006-03-01">
  <LoggingEnabled>
    <TargetBucket>amzn-s3-demo-destination-bucket</TargetBucket>
    <TargetPrefix>logs/</TargetPrefix>
    <TargetObjectKeyFormat>
      <PartitionedPrefix>
         <PartitionDateSource>EventTime</PartitionDateSource>
      </PartitionedPrefix>
  </TargetObjectKeyFormat>
  </LoggingEnabled>
</BucketLoggingStatus>
```

Os objetos de log são gravados e pertencem à conta de entrega de logs do S3, e o proprietário do bucket tem permissões totais sobre os objetos de log. Você tem a opção de usar concessões de destino (também conhecidas como concessões-alvo) para conceder permissões a outros usuários para que eles possam acessar os logs. Para obter mais informações, consulte PutBucketLogging.

> **Note**
>
> Se o bucket de destino usar a configuração Imposto pelo proprietário do bucket para a Propriedade de Objetos, você não poderá usar concessões de destino para conceder permissões a outros usuários. Para conceder permissões a outros, é possível atualizar a política de bucket no bucket de destino. Para obter mais informações, consulte Permissões para entrega de logs.

Para recuperar a configuração de registro em log de um bucket, use a operação de API GetBucketLogging.

Para excluir a configuração de registro em log, envie uma solicitação `PutBucketLogging` com um `BucketLoggingStatus` vazio:

```
<BucketLoggingStatus xmlns="http://doc.s3.amazonaws.com/2006-03-01">
</BucketLoggingStatus>
```

Para habilitar o registro em log em um bucket, é possível usar a API do Amazon S3 ou as bibliotecas wrapper do AWS SDK.

Uso dos SDKs da AWS

O exemplo a seguir habilita o registro em log em um bucket. Você deve criar dois buckets, um de origem e um de destino (alvo). Os exemplos atualizam primeiro a ACL do bucket de destino. Depois, eles concedem ao grupo de entrega de logs as permissões necessárias para gravar logs no bucket de destino e habilitam o registro em log no bucket de origem.

Este exemplo não funcionará em buckets de destino que usam a configuração Imposto pelo proprietário do bucket para a Propriedade de Objetos.

Se o bucket de destino (alvo) usar a configuração Imposto pelo proprietário do bucket para a Propriedade de Objetos, você não poderá definir ACLs de bucket ou de objeto. Também não é possível incluir concessões de destino (alvo) na configuração PutBucketLogging. É necessário usar uma política de bucket para conceder acesso à entidade principal do serviço de log (`logging.s3.amazonaws.com`). Para obter mais informações, consulte Permissões para entrega de logs.

.NET

SDK para .NET

> **Note**
>
> Há mais no GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWSCode Examples Repository.

```
using System;
```

```
    using System.IO;
    using System.Threading.Tasks;
    using Amazon.S3;
    using Amazon.S3.Model;
    using Microsoft.Extensions.Configuration;

    /// <summary>
    /// This example shows how to enable logging on an Amazon Simple Storage
    /// Service (Amazon S3) bucket. You need to have two Amazon S3 buckets for
    /// this example. The first is the bucket for which you wish to enable
    /// logging, and the second is the location where you want to store the
    /// logs.
    /// </summary>
    public class ServerAccessLogging
    {
        private static IConfiguration _configuration = null!;

        public static async Task Main()
        {
            LoadConfig();

            string bucketName = _configuration["BucketName"];
            string logBucketName = _configuration["LogBucketName"];
            string logObjectKeyPrefix = _configuration["LogObjectKeyPrefix"];
            string accountId = _configuration["AccountId"];

            // If the AWS Region defined for your default user is different
            // from the Region where your Amazon S3 bucket is located,
            // pass the Region name to the Amazon S3 client object's constructor.
            // For example: RegionEndpoint.USWest2 or RegionEndpoint.USEast2.
            IAmazonS3 client = new AmazonS3Client();

            try
            {
                // Update bucket policy for target bucket to allow delivery of
logs to it.
                await SetBucketPolicyToAllowLogDelivery(
                    client,
                    bucketName,
                    logBucketName,
                    logObjectKeyPrefix,
                    accountId);

                // Enable logging on the source bucket.
```

```
                await EnableLoggingAsync(
                    client,
                    bucketName,
                    logBucketName,
                    logObjectKeyPrefix);
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine($"Error: {e.Message}");
            }
        }

        /// <summary>
        /// This method grants appropriate permissions for logging to the
        /// Amazon S3 bucket where the logs will be stored.
        /// </summary>
        /// <param name="client">The initialized Amazon S3 client which will be
used
        /// to apply the bucket policy.</param>
        /// <param name="sourceBucketName">The name of the source bucket.</param>
        /// <param name="logBucketName">The name of the bucket where logging
        /// information will be stored.</param>
        /// <param name="logPrefix">The logging prefix where the logs should be
delivered.</param>
        /// <param name="accountId">The account id of the account where the
source bucket exists.</param>
        /// <returns>Async task.</returns>
        public static async Task SetBucketPolicyToAllowLogDelivery(
            IAmazonS3 client,
            string sourceBucketName,
            string logBucketName,
            string logPrefix,
            string accountId)
        {
            var resourceArn = @"""arn:aws:s3:::" + logBucketName + "/" +
logPrefix + @"*""";

            var newPolicy = @"{
                                ""Statement"":[{
                                ""Sid"": ""S3ServerAccessLogsPolicy"",
                                ""Effect"": ""Allow"",
                                ""Principal"": { ""Service"":
""logging.s3.amazonaws.com"" },
                                ""Action"": [""s3:PutObject""],
```

```
                                ""Resource"": [" + resourceArn + @"],
                                ""Condition"": {
                                ""ArnLike"": { ""aws:SourceArn"":
 ""arn:aws:s3:::" + sourceBucketName + @""" },
                                ""StringEquals"": { ""aws:SourceAccount"": """ +
 accountId + @""" }
                                        }
                                    }]
                                }";
            Console.WriteLine($"The policy to apply to bucket {logBucketName} to
 enable logging:");
            Console.WriteLine(newPolicy);

            PutBucketPolicyRequest putRequest = new PutBucketPolicyRequest
            {
                BucketName = logBucketName,
                Policy = newPolicy,
            };
            await client.PutBucketPolicyAsync(putRequest);
            Console.WriteLine("Policy applied.");
        }

        /// <summary>
        /// This method enables logging for an Amazon S3 bucket. Logs will be
 stored
        /// in the bucket you selected for logging. Selected prefix
        /// will be prepended to each log object.
        /// </summary>
        /// <param name="client">The initialized Amazon S3 client which will be
 used
        /// to configure and apply logging to the selected Amazon S3 bucket.</
param>
        /// <param name="bucketName">The name of the Amazon S3 bucket for which
 you
        /// wish to enable logging.</param>
        /// <param name="logBucketName">The name of the Amazon S3 bucket where
 logging
        /// information will be stored.</param>
        /// <param name="logObjectKeyPrefix">The prefix to prepend to each
        /// object key.</param>
        /// <returns>Async task.</returns>
        public static async Task EnableLoggingAsync(
            IAmazonS3 client,
            string bucketName,
```

```
            string logBucketName,
            string logObjectKeyPrefix)
        {
            Console.WriteLine($"Enabling logging for bucket {bucketName}.");
            var loggingConfig = new S3BucketLoggingConfig
            {
                TargetBucketName = logBucketName,
                TargetPrefix = logObjectKeyPrefix,
            };

            var putBucketLoggingRequest = new PutBucketLoggingRequest
            {
                BucketName = bucketName,
                LoggingConfig = loggingConfig,
            };
            await client.PutBucketLoggingAsync(putBucketLoggingRequest);
            Console.WriteLine($"Logging enabled.");
        }

        /// <summary>
        /// Loads configuration from settings files.
        /// </summary>
        public static void LoadConfig()
        {
            _configuration = new ConfigurationBuilder()
                .SetBasePath(Directory.GetCurrentDirectory())
                .AddJsonFile("settings.json") // Load settings from .json file.
                .AddJsonFile("settings.local.json", true) // Optionally, load
local settings.
                .Build();
        }
    }
```

- Para obter detalhes da API, consulte PutBucketLogging na Referência da API do AWS SDK para .NET.

Java

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3.S3Client;
```

```
import software.amazon.awssdk.services.s3.model.BucketLoggingStatus;
import software.amazon.awssdk.services.s3.model.LoggingEnabled;
import software.amazon.awssdk.services.s3.model.PartitionedPrefix;
import software.amazon.awssdk.services.s3.model.PutBucketLoggingRequest;
import software.amazon.awssdk.services.s3.model.TargetObjectKeyFormat;

// Class to set a bucket policy on a target S3 bucket and enable server access
 logging on a source S3 bucket.
public class ServerAccessLogging {
    private static S3Client s3Client;

    public static void main(String[] args) {
        String sourceBucketName = "SOURCE-BUCKET";
        String targetBucketName = "TARGET-BUCKET";
        String sourceAccountId = "123456789012";
        String targetPrefix = "logs/";

        // Create S3 Client.
        s3Client = S3Client.builder().
                region(Region.US_EAST_2)
                .build();

        // Set a bucket policy on the target S3 bucket to enable server access
 logging by granting the
        // logging.s3.amazonaws.com principal permission to use the PutObject
 operation.
        ServerAccessLogging serverAccessLogging = new ServerAccessLogging();
        serverAccessLogging.setTargetBucketPolicy(sourceAccountId, sourceBucketName,
 targetBucketName);

        // Enable server access logging on the source S3 bucket.
        serverAccessLogging.enableServerAccessLogging(sourceBucketName,
 targetBucketName,
                targetPrefix);

    }

    // Function to set a bucket policy on the target S3 bucket to enable server
 access logging by granting the
    // logging.s3.amazonaws.com principal permission to use the PutObject operation.
    public void setTargetBucketPolicy(String sourceAccountId, String
 sourceBucketName, String targetBucketName) {
        String policy = "{\n" +
                "    \"Version\": \"2012-10-17\",\n" +
```

```
                "    \"Statement\": [\n" +
                "        {\n" +
                "            \"Sid\": \"S3ServerAccessLogsPolicy\",\n" +
                "            \"Effect\": \"Allow\",\n" +
                "            \"Principal\": {\"Service\": \"logging.s3.amazonaws.com
\"},\n" +
                "            \"Action\": [\n" +
                "                \"s3:PutObject\"\n" +
                "            ],\n" +
                "            \"Resource\": \"arn:aws:s3:::" + targetBucketName + "/*
\",\n" +
                "            \"Condition\": {\n" +
                "                \"ArnLike\": {\n" +
                "                    \"aws:SourceArn\": \"arn:aws:s3:::" +
 sourceBucketName + "\"\n" +
                "                },\n" +
                "                \"StringEquals\": {\n" +
                "                    \"aws:SourceAccount\": \"" + sourceAccountId +
 "\"\n" +
                "                }\n" +
                "            }\n" +
                "        }\n" +
                "    ]\n" +
                "}";
        s3Client.putBucketPolicy(b -> b.bucket(targetBucketName).policy(policy));
    }

    // Function to enable server access logging on the source S3 bucket.
    public void enableServerAccessLogging(String sourceBucketName, String
 targetBucketName,
            String targetPrefix) {
        TargetObjectKeyFormat targetObjectKeyFormat =
 TargetObjectKeyFormat.builder()

 .partitionedPrefix(PartitionedPrefix.builder().partitionDateSource("EventTime").build())
                .build();
        LoggingEnabled loggingEnabled = LoggingEnabled.builder()
                .targetBucket(targetBucketName)
                .targetPrefix(targetPrefix)
                .targetObjectKeyFormat(targetObjectKeyFormat)
                .build();
        BucketLoggingStatus bucketLoggingStatus = BucketLoggingStatus.builder()
                .loggingEnabled(loggingEnabled)
                .build();
```

```
        s3Client.putBucketLogging(PutBucketLoggingRequest.builder()
                .bucket(sourceBucketName)
                .bucketLoggingStatus(bucketLoggingStatus)
                .build());
    }

}
```

Como usar o AWS CLI

Recomendamos que você crie um bucket de registro dedicado em cada Região da AWS em que tenha buckets do S3. Depois, faça com que os logs de acesso do Amazon S3 sejam entregues a esse bucket do S3. Para obter mais informações e exemplos, consulte put-bucket-logging na Referência da AWS CLI.

Se o bucket de destino (alvo) usar a configuração Imposto pelo proprietário do bucket para a Propriedade de Objetos, você não poderá definir ACLs de bucket ou de objeto. Também não é possível incluir concessões de destino (alvo) na configuração PutBucketLogging. É necessário usar uma política de bucket para conceder acesso à entidade principal do serviço de log (`logging.s3.amazonaws.com`). Para obter mais informações, consulte Permissões para entrega de logs.

Example : Habilite logs de acesso com cinco buckets em duas regiões

Neste exemplo, você tem estes cinco buckets:

- *amzn-s3-demo-source-bucket*-us-east-1
- *amzn-s3-demo-source-bucket1*-us-east-1
- *amzn-s3-demo-source-bucket2*-us-east-1
- *amzn-s3-demo-bucket1*-us-west-2
- *amzn-s3-demo-bucket2*-us-west-2

> **Note**
>
> A etapa final do procedimento a seguir fornece exemplos de scripts bash que você pode usar para criar buckets de registro em log e habilitar o registro em log de acesso ao servidor

nesses buckets. Para usar esses scripts, você deve criar os arquivos `policy.json` e `logging.json`, conforme descrito no procedimento a seguir.

1. Crie dois buckets de destino do registro em log nas regiões Oeste dos EUA (Oregon) e Leste dos EUA (N. da Virgínia) e dê a eles os seguintes nomes:
   - *amzn-s3-demo-destination-bucket*-logs-us-east-1
   - *amzn-s3-demo-destination-bucket1*-logs-us-west-2
2. Posteriormente nessas etapas, você habilitará o registro em log de acesso ao servidor da seguinte forma:
   - Logs de *amzn-s3-demo-source-bucket*-us-east-1 no bucket do S3 *amzn-s3-demo-destination-bucket*-logs-us-east-1 com o prefixo *amzn-s3-demo-source-bucket*-us-east-1
   - Logs de *amzn-s3-demo-source-bucket1*-us-east-1 no bucket do S3 *amzn-s3-demo-destination-bucket*-logs-us-east-1 com o prefixo *amzn-s3-demo-source-bucket1*-us-east-1
   - Logs de *amzn-s3-demo-source-bucket2*-us-east-1 no bucket do S3 *amzn-s3-demo-destination-bucket*-logs-us-east-1 com o prefixo *amzn-s3-demo-source-bucket2*-us-east-1
   - Logs de *amzn-s3-demo-bucket1*-us-west-2 no bucket do S3 *amzn-s3-demo-destination-bucket1*-logs-us-west-2 com o prefixo *amzn-s3-demo-bucket1*-us-west-2
   - Logs de *amzn-s3-demo-bucket2*-us-west-2 no bucket do S3 *amzn-s3-demo-destination-bucket1*-logs-us-west-2 com o prefixo *amzn-s3-demo-bucket2*-us-west-2
3. Para cada bucket de registro em log de destino, conceda permissões para a entrega de logs de acesso ao servidor usando uma ACL de bucket ou uma política de bucket:
   - Atualizar a política de bucket (recomendado): para conceder permissões à entidade principal do serviço de log, use o comando `put-bucket-policy` a seguir. Substitua *amzn-s3-demo-destination-bucket*-logs pelo nome de seu bucket de destino.

     ```
     aws s3api put-bucket-policy --bucket amzn-s3-demo-destination-bucket-logs --
     policy file://policy.json
     ```

`Policy.json` é um documento JSON na pasta atual que contém a política de bucket a seguir. Para usar essa política de bucket, substitua os *`user input placeholders`* por suas próprias informações. Na política a seguir, *`amzn-s3-demo-destination-bucket-logs`* é o bucket de destino em que os logs de acesso ao servidor serão entregues e *`amzn-s3-demo-source-bucket`* é o bucket de origem. *`SOURCE-ACCOUNT-ID`* é a Conta da AWS à qual o bucket de origem pertence.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "S3ServerAccessLogsPolicy",
            "Effect": "Allow",
            "Principal": {
                "Service": "logging.s3.amazonaws.com"
            },
            "Action": [
                "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket-logs/*",
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:s3:::amzn-s3-demo-source-bucket"
                },
                "StringEquals": {
                    "aws:SourceAccount": "SOURCE-ACCOUNT-ID"
                }
            }
        }
    ]
}
```

- Atualizar a ACL de bucket: para conceder permissões ao grupo de entrega de logs do S3, use o comando `put-bucket-acl` a seguir. Substitua *`amzn-s3-demo-destination-bucket-logs`* pelo nome do bucket de destino (alvo).

```
aws s3api put-bucket-acl --bucket amzn-s3-demo-destination-bucket-logs  --
grant-write URI=http://acs.amazonaws.com/groups/s3/LogDelivery --grant-read-acp
 URI=http://acs.amazonaws.com/groups/s3/LogDelivery
```

4. Depois, crie um arquivo `logging.json` que contenha a configuração de registro em log (com base em um dos três exemplos a seguir). Depois de criar o arquivo `logging.json`, você pode aplicar a configuração de registro em log usando o comando `put-bucket-logging` a seguir. Substitua *amzn-s3-demo-destination-bucket-logs* pelo nome do bucket de destino (alvo).

```
aws s3api put-bucket-logging --bucket amzn-s3-demo-destination-bucket-logs --
bucket-logging-status file://logging.json
```

> **Note**
>
> Em vez de usar esse comando `put-bucket-logging` para aplicar a configuração de registro em log em cada bucket de destino, você pode usar um dos scripts bash fornecidos na próxima etapa. Para usar esses scripts, você deve criar os arquivos `policy.json` e `logging.json`, conforme descrito nesse procedimento.

O arquivo `logging.json` é um documento JSON na pasta atual que contém a configuração do registro em log. Se um bucket de destino usar a configuração Imposto pelo proprietário do bucket para a Propriedade de Objetos, a configuração de registro em log não poderá conter concessões de destino (alvo). Para obter mais informações, consulte Permissões para entrega de logs.

Example : **`logging.json`** sem concessões de destino (alvo)

O exemplo de arquivo `logging.json` a seguir não contém concessões de destino (alvo). Portanto, você pode aplicar essa configuração a um bucket de destino (alvo) que usa a configuração Imposto pelo proprietário do bucket para a Propriedade de Objetos.

```
{
    "LoggingEnabled": {
```

```
        "TargetBucket": "amzn-s3-demo-destination-bucket-logs",
        "TargetPrefix": "amzn-s3-demo-destination-bucket/"
    }
}
```

Example : **`logging.json`** com concessões de destino (alvo)

O exemplo de arquivo `logging.json` a seguir contém concessões de destino (alvo).

Se o bucket de destino usar a configuração Imposto pelo proprietário do bucket para a Propriedade de Objetos, você não poderá incluir concessões de destino (alvo) na configuração PutBucketLogging. Para obter mais informações, consulte Permissões para entrega de logs.

```
{
    "LoggingEnabled": {
        "TargetBucket": "amzn-s3-demo-destination-bucket-logs",
        "TargetPrefix": "amzn-s3-demo-destination-bucket/",
        "TargetGrants": [
             {
                "Grantee": {
                    "Type": "AmazonCustomerByEmail",
                    "EmailAddress": "user@example.com"
                 },
                "Permission": "FULL_CONTROL"
             }
         ]
    }
}
```

Valores referentes ao beneficiário

Você pode especificar a pessoa (beneficiária) a quem você está atribuindo direitos de acesso (usando elementos de solicitação) das seguintes formas:

- Pelo ID da pessoa:

```
{
  "Grantee": {
    "Type": "CanonicalUser",
```

```
    "ID": "ID",
    "DisplayName": "GranteesEmail"
  }
}
```

`DisplayName` é opcional e é ignorado na solicitação.

- Por endereço de e-mail:

```
{
  "Grantee": {
    "Type": "AmazonCustomerByEmail",
    "EmailAddress": "username@example.com"
  }
}
```

O beneficiário é resolvido para o `CanonicalUser` e, em resposta a uma solicitação `GetObjectAcl`, aparece como o `CanonicalUser`.

> **Note**
>
> É possível usar endereços de e-mail para especificar um beneficiário somente nas seguintes Regiões da AWS: Para obter mais informações, consulte Grantee na Referência da API do Amazon S3.

- Por URI:

```
{
  "Grantee": {
    "Type": "Group",
    "URI": "http://acs.amazonaws.com/groups/global/AuthenticatedUsers"
  }
}
```

Example : **`logging.json`** com o formato da chave de objeto de log definido como a hora do evento do S3

O arquivo `logging.json` a seguir altera o formato da chave de objeto de log para a hora do evento do S3. Para obter mais informações sobre como definir o formato da chave de objeto de log, consulte the section called “Como faço para habilitar a entrega de logs?”.

```
  {
    "LoggingEnabled": {
        "TargetBucket": "amzn-s3-demo-destination-bucket-logs",
        "TargetPrefix": "amzn-s3-demo-destination-bucket/",
        "TargetObjectKeyFormat": {
            "PartitionedPrefix": {
                "PartitionDateSource": "EventTime"
            }
         }
    }
}
```

5. Use um script bash a seguir para adicionar o registro em log de acesso a todos os buckets em sua conta. Substitua *amzn-s3-demo-destination-bucket-logs* pelo nome do bucket de destino (alvo) e substitua *us-west-2* pelo nome da região em que os buckets estão localizados.

> **Note**
>
> Esse script só funcionará se todos os buckets estiverem na mesma região. Se você tiver buckets em várias regiões, deverá ajustar o script.

Example – Conceda acesso com políticas de bucket e adicione log para os buckets de sua conta

```
loggingBucket='amzn-s3-demo-destination-bucket-logs'
region='us-west-2'


# Create the logging bucket.
aws s3 mb s3://$loggingBucket --region $region

aws s3api put-bucket-policy --bucket $loggingBucket --policy file://policy.json

# List the buckets in this account.
buckets="$(aws s3 ls | awk '{print $3}')"

# Put a bucket logging configuration on each bucket.
```

```
  for bucket in $buckets
      do
        # This if statement excludes the logging bucket.
        if [ "$bucket" == "$loggingBucket" ] ; then
            continue;
        fi
        printf '{
          "LoggingEnabled": {
            "TargetBucket": "%s",
            "TargetPrefix": "%s/"
        }
      }' "$loggingBucket" "$bucket"  > logging.json
      aws s3api put-bucket-logging --bucket $bucket --bucket-logging-status file://
logging.json
      echo "$bucket done"
  done

  rm logging.json

  echo "Complete"
```

Example – Conceda acesso com ACLs de bucket e adicione log para os buckets de sua conta

```
  loggingBucket='amzn-s3-demo-destination-bucket-logs'
  region='us-west-2'


  # Create the logging bucket.
  aws s3 mb s3://$loggingBucket --region $region

  aws s3api put-bucket-acl --bucket $loggingBucket --grant-write URI=http://
acs.amazonaws.com/groups/s3/LogDelivery --grant-read-acp URI=http://
acs.amazonaws.com/groups/s3/LogDelivery

  # List the buckets in this account.
  buckets="$(aws s3 ls | awk '{print $3}')"

  # Put a bucket logging configuration on each bucket.
  for bucket in $buckets
      do
        # This if statement excludes the logging bucket.
        if [ "$bucket" == "$loggingBucket" ] ; then
```

```
            continue;
        fi
        printf '{
          "LoggingEnabled": {
            "TargetBucket": "%s",
            "TargetPrefix": "%s/"
        }
      }' "$loggingBucket" "$bucket"  > logging.json
      aws s3api put-bucket-logging --bucket $bucket --bucket-logging-status file://
logging.json
      echo "$bucket done"
  done

  rm logging.json

  echo "Complete"
```

Verificar a configuração dos logs de acesso ao servidor

Depois de habilitar o registro em log de acesso ao servidor, execute as seguintes etapas:

- Acesse o bucket de destino e verifique se os arquivos de log estão sendo entregues. Depois que os logs de acesso são configurados, o Amazon S3 começa imediatamente a capturar as solicitações e registrá-las em log. No entanto, pode demorar algumas horas para que os logs sejam entregues ao bucket de destino. Para obter mais informações, consulte the section called “As alterações do status do registro de bucket em logs entram em vigor ao longo do tempo” e the section called “Entrega de logs do servidor de melhor esforço”.

  Também é possível verificar automaticamente a entrega de logs usando métricas de solicitação do Amazon S3 e configurando alarmes do Amazon CloudWatch para essas métricas. Para obter mais informações, consulte Monitoramento de métricas com o Amazon CloudWatch.
- Verifique se você consegue abrir e ler o conteúdo dos arquivos de log.

Para obter informações sobre solução de problemas do registro de acesso ao servidor, consulte Solução de problemas do registro em log de acessos ao servidor.

Formato dos logs de acesso ao servidor do Amazon S3

O registro em log de acesso ao servidor fornece detalhes sobre as solicitações que são feitas a um bucket do Amazon S3. Você pode usar logs de acesso ao servidor para as seguintes finalidades:

- Realizar auditorias de segurança e acesso
- Aprender sobre sua base de clientes
- Entender sua fatura do Amazon S3

Esta seção descreve o formato e outros detalhes sobre os arquivos de log de acesso ao servidor do Amazon S3.

Os arquivos de log de acesso ao servidor consistem em uma sequência de registros de log delimitados por novas linhas. Cada registro do log representa uma solicitação e consiste em campos delimitados por espaço.

Veja a seguir o exemplo de um log que consiste em cinco registros de log.

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
 amzn-s3-demo-bucket1 [06/Feb/2019:00:00:38 +0000] 192.0.2.3
 79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be 3E57427F3EXAMPLE
 REST.GET.VERSIONING - "GET /amzn-s3-demo-bucket1?versioning HTTP/1.1" 200 - 113 - 7 -
 "-" "S3Console/0.4" - s9lzHYrFp76ZVxRcpX9+5cjAnEH2ROuNkd2BHfIa6UkFVdtjf5mKR3/eTPFvsiP/
XV/VLi31234= SigV4 ECDHE-RSA-AES128-GCM-SHA256 AuthHeader amzn-s3-demo-bucket1.s3.us-
west-1.amazonaws.com TLSV1.2 arn:aws:s3:us-west-1:123456789012:accesspoint/example-AP
 Yes
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
 amzn-s3-demo-bucket1 [06/Feb/2019:00:00:38 +0000] 192.0.2.3
 79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be 891CE47D2EXAMPLE
 REST.GET.LOGGING_STATUS - "GET /amzn-s3-demo-bucket1?logging HTTP/1.1" 200 -
 242 - 11 - "-" "S3Console/0.4" - 9vKBE6vMhrNiWHZmb2L0mXOcqPGzQOI5XLnCtZNPxev+Hf
+7tpT6sxDwDty4LHBUOZJG96N1234= SigV4 ECDHE-RSA-AES128-GCM-SHA256 AuthHeader amzn-s3-
demo-bucket1.s3.us-west-1.amazonaws.com TLSV1.2 - -
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
 amzn-s3-demo-bucket1 [06/Feb/2019:00:00:38 +0000] 192.0.2.3
 79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be A1206F460EXAMPLE
 REST.GET.BUCKETPOLICY - "GET /amzn-s3-demo-bucket1?policy HTTP/1.1" 404
 NoSuchBucketPolicy 297 - 38 - "-" "S3Console/0.4" - BNaBsXZQQDbssi6xMBdBU2sLt
+Yf5kZDmeBUP35sFoKa3sLLeMC78iwEIWxs99CRUrbS4n11234= SigV4 ECDHE-RSA-AES128-GCM-SHA256
 AuthHeader amzn-s3-demo-bucket1.s3.us-west-1.amazonaws.com TLSV1.2 - Yes
```

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
 amzn-s3-demo-bucket1 [06/Feb/2019:00:01:00 +0000] 192.0.2.3
 79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be 7B4A0FABBEXAMPLE
 REST.GET.VERSIONING - "GET /amzn-s3-demo-bucket1?versioning HTTP/1.1" 200 -
 113 - 33 - "-" "S3Console/0.4" - Ke1bUcazaN1jWuUlPJaxF64cQVpUEhoZKEG/hmy/gijN/
I1DeWqDfFvnpybfEseEME/u7ME1234= SigV4 ECDHE-RSA-AES128-GCM-SHA256 AuthHeader amzn-s3-
demo-bucket1.s3.us-west-1.amazonaws.com TLSV1.2 - -
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
 amzn-s3-demo-bucket1 [06/Feb/2019:00:01:57 +0000] 192.0.2.3
 79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
 DD6CC733AEXAMPLE REST.PUT.OBJECT s3-dg.pdf "PUT /amzn-s3-demo-bucket1/
s3-dg.pdf HTTP/1.1" 200 - - 4406583 41754 28 "-" "S3Console/0.4" -
 10S62Zv81kBW7BB6SX4XJ48o6kpcl6LPwEoizZQQxJd5qDSCTLX0TgS37kYUBKQW3+bPdrg1234= SigV4
 ECDHE-RSA-AES128-SHA AuthHeader amzn-s3-demo-bucket1.s3.us-west-1.amazonaws.com
 TLSV1.2 - Yes
```

> **Note**
>
> Qualquer campo pode ser definido como - para indicar que os dados eram desconhecidos ou estavam indisponíveis ou que o campo não era aplicável para essa solicitação.

Tópicos

- Campos de registro de log
- Registro em log adicional para operações de cópia
- Informações personalizadas do log de acesso
- Considerações de programação para o formato do log de acesso ao servidor extensível

Campos de registro de log

A lista a seguir descreve os campos dos registros em log.

Proprietário do bucket

O ID canônico do usuário do proprietário do bucket de origem. O ID de usuário canônico é outra forma de ID da Conta da AWS. Para obter mais informações sobre IDs de usuário canônico, consulte Identificadores de Conta da AWS na Referência geral da AWS. Para obter informações sobre como encontrar o ID de usuário canônico da conta, consulte Como localizar o ID de usuário canônico de sua Conta da AWS.

Exemplo de registro

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
```

Bucket

O nome do bucket no qual a solicitação foi processada. Se o sistema receber uma solicitação malformada e não puder determinar o bucket, a solicitação não aparecerá em nenhum log de acesso ao servidor.

Exemplo de registro

```
amzn-s3-demo-bucket1
```

Tempo

O horário em que a solicitação foi recebida. As datas e horas estão em Tempo Universal Coordenado (UTC). O formato que usa a terminologia `strftime()` é o seguinte: `[%d/%b/%Y:%H:%M:%S %z]`

Exemplo de registro

```
[06/Feb/2019:00:00:38 +0000]
```

IP remoto

O endereço IP aparente do solicitante. Os proxies e os firewalls intermediários podem obscurecer o endereço IP real da máquina que faz a solicitação.

Exemplo de registro

```
192.0.2.3
```

Solicitante

O ID canônico do usuário do solicitante ou um `-` para solicitações não autenticadas. Se o solicitante for um usuário do IAM, esse campo retornará o nome do usuário do IAM do solicitante com o Conta da AWS ao qual o usuário do IAM pertence. Esse identificador é o mesmo usado para fins de controle de acesso.

Exemplo de registro

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
```

Se o solicitante estiver usando um perfil assumido, esse campo retornará o perfil do IAM assumido.

Exemplo de registro

```
arn:aws:sts::123456789012:assumed-role/roleName/test-role
```

ID da solicitação

Uma string gerada pelo Amazon S3 para identificar exclusivamente cada solicitação.

Exemplo de registro

```
3E57427F33A59F07
```

Operação

A operação listada aqui é declarada como `SOAP.operation`, `REST.HTTP_method.resource_type`, `WEBSITE.HTTP_method.resource_type` ou `BATCH.DELETE.OBJECT`, ou `S3.action.resource_type` para Ciclo de Vida do S3 e registro em log.

Exemplo de registro

```
REST.PUT.OBJECT
```

Chave

A parte da chave (nome do objeto) da solicitação.

Exemplo de registro

```
/photos/2019/08/puppy.jpg
```

Request-URI

A parte `Request-URI` da mensagem de solicitação HTTP.

Entrada de exemplo

```
"GET /amzn-s3-demo-bucket1/photos/2019/08/puppy.jpg?x-foo=bar HTTP/1.1"
```

Status HTTP

O código numérico do status do HTTP da resposta.

Exemplo de registro

```
200
```

Código de erro

As respostas de erro do Amazon S3, ou - se não houver erros.

Exemplo de registro

```
NoSuchBucket
```

Bytes enviados

O número de bytes de resposta enviados, excluindo a sobrecarga do protocolo HTTP, ou - se zero.

Exemplo de registro

```
2662992
```

Tamanho do objeto

O tamanho total do objeto em questão.

Exemplo de registro

```
3462992
```

Tempo total

O número de milissegundos (ms) em que a solicitação esteve em trânsito da perspectiva do servidor. Esse valor é medido do momento do recebimento da solicitação até o momento em que o último byte da resposta é enviado. As medidas feitas da perspectiva do cliente podem ser mais longas devido à latência da rede.

Exemplo de registro

```
70
```

Tempo de retorno

O número de milissegundos que o Amazon S3 gastou processando a solicitação. Esse valor é medido do momento do recebimento do último byte da solicitação até o momento em que o primeiro byte da resposta foi enviado.

Exemplo de registro

```
10
```

Referer

O valor do cabeçalho do `Referer` HTTP, se presente. Os agentes do usuário HTTP (por exemplo, navegadores) normalmente definem esse cabeçalho como o URL da página de vinculação ou incorporação ao fazer uma solicitação.

Exemplo de registro

```
"http://www.example.com/webservices"
```

User-Agent

O valor do cabeçalho do `User-Agent` HTTP.

Exemplo de registro

```
"curl/7.15.1"
```

ID da versão

O ID da versão na solicitação ou `-` se a operação não usar um parâmetro `versionId`.

Exemplo de registro

```
3HL4kqtJvjVBH40Nrjfkd
```

ID do host

O `x-amz-id-2` ou o ID de solicitação estendida do Amazon S3.

Exemplo de registro

```
s9lzHYrFp76ZVxRcpX9+5cjAnEH2ROuNkd2BHfIa6UkFVdtjf5mKR3/eTPFvsiP/XV/VLi31234=
```

Versão do Signature

A versão do Signature, `SigV2` ou `SigV4`, que foi usada para autenticar a solicitação ou `-` para solicitações não autenticadas.

Exemplo de registro

```
SigV2
```

Pacote de criptografia

A cifra de Transport Layer Security (TLS) que foi negociada para uma solicitação HTTPS, ou um `-` para HTTP.

Exemplo de registro

```
ECDHE-RSA-AES128-GCM-SHA256
```

Tipo de autenticação

O tipo de autenticação de solicitação usada: `AuthHeader` para cabeçalhos de autenticação, `QueryString` para string de consulta (URL pré-assinado) ou um `-` para solicitações não autenticadas.

Exemplo de registro

```
AuthHeader
```

Cabeçalho de host

O endpoint usado para conectar-se ao Amazon S3.

Exemplo de registro

```
s3.us-west-2.amazonaws.com
```

Algumas regiões mais antigas oferecem suporte a endpoints herdados. Você poderá ver esses endpoints nos logs de acesso ao servidor ou nos logs do AWS CloudTrail. Para obter mais informações, consulte Endpoints herdados. Para obter uma lista completa de regiões e endpoints do Amazon S3, consulte Endpoints e cotas do Amazon S3 na Referência geral da Amazon Web Services.

Versão do TLS

A versão do Transport Layer Security (TLS) negociada pelo cliente. O valor é um dos seguintes: `TLSv1.1`, `TLSv1.2`, `TLSv1.3` ou `-` se o TLS não foi usado.

Exemplo de registro

```
TLSv1.2
```

ARN do ponto de acesso

O nome de recurso da Amazon (ARN) do ponto de acesso da solicitação. Se o ARN do ponto de acesso estiver malformado ou se não for usado, o campo apresentará um `-`. Para obter mais informações sobre pontos de acesso, consulte Usar o recurso Pontos de Acesso Amazon S3 para buckets de uso geral. Para obter mais informações sobre ARNs, consulte Nome do recurso da Amazon (ARN) no Guia de referência da AWS.

Exemplo de registro

```
arn:aws:s3:us-east-1:123456789012:accesspoint/example-AP
```

aclRequired

Uma string que indica se a solicitação exigiu uma lista de controle de acesso (ACL) para autorização. Se a solicitação exigiu uma ACL para autorização, a string é `Yes`. Se nenhuma ACL foi necessária, a string é `-`. Para obter mais informações sobre ACLs, consulte Visão geral da lista de controle de acesso (ACL). Para obter mais informações sobre como usar o campo `aclRequired` para desativar ACLs, consulte Controlar a propriedade de objetos e desabilitar ACLs para seu bucket.

Exemplo de registro

```
Yes
```

Registro em log adicional para operações de cópia

Uma operação de cópia envolve um `GET` e um `PUT`. Por esse motivo, registramos dois registros em log ao executar uma operação de cópia. A seção anterior descreve os campos relacionados à parte `PUT` da operação. A lista a seguir descreve os campos no registro que se relacionam à parte `GET` da operação de cópia.

Proprietário do bucket

O ID canônico do usuário do bucket que armazena o objeto que está sendo copiado. O ID de usuário canônico é outra forma de ID da Conta da AWS. Para obter mais informações sobre IDs de usuário canônico, consulte Identificadores de Conta da AWS na Referência geral da AWS. Para obter informações sobre como encontrar o ID de usuário canônico da conta, consulte Como localizar o ID de usuário canônico de sua Conta da AWS.

Exemplo de registro

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
```

Bucket

O nome do bucket que armazena o objeto que está sendo copiado.

Exemplo de registro

```
amzn-s3-demo-bucket1
```

Tempo

O horário em que a solicitação foi recebida. As datas e horas estão em Tempo Universal Coordenado (UTC). O formato que usa a terminologia `strftime()` é o seguinte: `[%d/%B/%Y:%H:%M:%S %z]`

Exemplo de registro

```
[06/Feb/2019:00:00:38 +0000]
```

IP remoto

O endereço IP aparente do solicitante. Os proxies e os firewalls intermediários podem obscurecer o endereço IP real da máquina que faz a solicitação.

Exemplo de registro

```
192.0.2.3
```

Solicitante

O ID canônico do usuário do solicitante ou um - para solicitações não autenticadas. Se o solicitante for um usuário do IAM, esse campo retornará o nome do usuário do IAM do solicitante junto com o Usuário raiz da conta da AWS ao qual o usuário do IAM pertence. Esse identificador é o mesmo usado para fins de controle de acesso.

Exemplo de registro

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
```

Se o solicitante estiver usando um perfil assumido, esse campo retornará o perfil do IAM assumido.

Exemplo de registro

```
arn:aws:sts::123456789012:assumed-role/roleName/test-role
```

ID da solicitação

Uma string gerada pelo Amazon S3 para identificar exclusivamente cada solicitação.

Exemplo de registro

```
3E57427F33A59F07
```

Operação

A operação listada aqui é declarada como `SOAP.`*`operation`*, `REST.`*`HTTP_method`*`.`*`resource_type`*, `WEBSITE.`*`HTTP_method`*`.`*`resource_type`* ou `BATCH.DELETE.OBJECT`.

Exemplo de registro

```
REST.COPY.OBJECT_GET
```

Chave

A chave (nome do objeto) do objeto que está sendo copiado, ou `-` se a operação não usar um parâmetro de chave.

Exemplo de registro

```
/photos/2019/08/puppy.jpg
```

Request-URI

A parte `Request-URI` da mensagem de solicitação HTTP.

Exemplo de registro

```
"GET /amzn-s3-demo-bucket1/photos/2019/08/puppy.jpg?x-foo=bar"
```

Status HTTP

O código numérico do status do HTTP da parte `GET` da operação de cópia.

Exemplo de registro

```
200
```

Código de erro

As respostas de erro do Amazon S3, ou a parte `GET` da operação de cópia, ou `-` se não houver erros.

Exemplo de registro

```
NoSuchBucket
```

Bytes enviados

O número de bytes de resposta enviados, excluindo a sobrecarga do protocolo HTTP, ou `-` se zero.

Exemplo de registro

```
2662992
```

Tamanho do objeto

O tamanho total do objeto em questão.

Exemplo de registro

```
3462992
```

Tempo total

O número de milissegundos (ms) em que a solicitação esteve em trânsito da perspectiva do servidor. Esse valor é medido do momento do recebimento da solicitação até o momento em que o último byte da resposta é enviado. As medidas feitas da perspectiva do cliente podem ser mais longas devido à latência da rede.

Exemplo de registro

```
70
```

Tempo de retorno

O número de milissegundos que o Amazon S3 gastou processando a solicitação. Esse valor é medido do momento do recebimento do último byte da solicitação até o momento em que o primeiro byte da resposta foi enviado.

Exemplo de registro

```
10
```

Referer

O valor do cabeçalho do `Referer` HTTP, se presente. Os agentes do usuário HTTP (por exemplo, navegadores) normalmente definem esse cabeçalho como o URL da página de vinculação ou incorporação ao fazer uma solicitação.

Exemplo de registro

```
"http://www.example.com/webservices"
```

User-Agent

O valor do cabeçalho do `User-Agent` HTTP.

Exemplo de registro

```
"curl/7.15.1"
```

ID da versão

O ID da versão do objeto que está sendo copiado, ou `-` se o cabeçalho `x-amz-copy-source` não tiver especificado um parâmetro `versionId` como parte da fonte da cópia.

Entrada de exemplo

```
3HL4kqtJvjVBH40Nrjfkd
```

ID do host

O `x-amz-id-2` ou o ID de solicitação estendida do Amazon S3.

Exemplo de registro

```
s9lzHYrFp76ZVxRcpX9+5cjAnEH2ROuNkd2BHfIa6UkFVdtjf5mKR3/eTPFvsiP/XV/VLi31234=
```

Versão do Signature

A versão de assinatura, `SigV2` ou `SigV4`, que foi usada para autenticar a solicitação, ou um `-` para solicitações não autenticadas.

Exemplo de registro

```
SigV4
```

Pacote de criptografia

A cifra de Transport Layer Security (TLS) que foi negociada para uma solicitação HTTPS ou um `-` para HTTP.

Exemplo de registro

```
ECDHE-RSA-AES128-GCM-SHA256
```

Tipo de autenticação

O tipo de autenticação de solicitação usada: `AuthHeader` para cabeçalhos de autenticação, `QueryString` para strings de consulta (URL pré-assinados) ou um `-` para solicitações não autenticadas.

Exemplo de registro

```
AuthHeader
```

Cabeçalho de host

O endpoint que foi usado para conectar ao Amazon S3.

Exemplo de registro

```
s3.us-west-2.amazonaws.com
```

Algumas regiões mais antigas oferecem suporte a endpoints herdados. Você poderá ver esses endpoints nos logs de acesso ao servidor ou nos logs do AWS CloudTrail. Para obter mais informações, consulte Endpoints herdados. Para obter uma lista completa de regiões e endpoints do Amazon S3, consulte Endpoints e cotas do Amazon S3 na Referência geral da Amazon Web Services.

Versão do TLS

A versão do Transport Layer Security (TLS) negociada pelo cliente. O valor é um dos seguintes: `TLSv1.1`, `TLSv1.2`, `TLSv1.3` ou `-` se o TLS não foi usado.

Exemplo de registro

```
TLSv1.2
```

ARN do ponto de acesso

O nome de recurso da Amazon (ARN) do ponto de acesso da solicitação. Se o ARN do ponto de acesso estiver malformado ou se não for usado, o campo apresentará um `-`. Para obter mais informações sobre pontos de acesso, consulte Usar o recurso Pontos de Acesso Amazon S3 para buckets de uso geral. Para obter mais informações sobre ARNs, consulte Nome do recurso da Amazon (ARN) no Guia de referência da AWS.

Exemplo de registro

```
arn:aws:s3:us-east-1:123456789012:accesspoint/example-AP
```

aclRequired

Uma string que indica se a solicitação exigiu uma lista de controle de acesso (ACL) para autorização. Se a solicitação exigiu uma ACL para autorização, a string é `Yes`. Se nenhuma ACL foi necessária, a string é `-`. Para obter mais informações sobre ACLs, consulte Visão geral da lista de controle de acesso (ACL). Para obter mais informações sobre como usar o campo `aclRequired` para desativar ACLs, consulte Controlar a propriedade de objetos e desabilitar ACLs para seu bucket.

Exemplo de registro

```
Yes
```

Informações personalizadas do log de acesso

Você pode incluir informações personalizadas a serem armazenadas no registro de log de acesso de uma solicitação. Para fazer isso, adicione um parâmetro de string de consulta personalizado à URL da solicitação. O Amazon S3 ignora os parâmetros query-string que começam com `x-`, mas inclui esses parâmetros no registro do log de acesso da solicitação, como parte do campo `Request-URI` do registro do log.

Por exemplo, uma solicitação `GET` para `"s3.amazonaws.com/amzn-s3-demo-bucket1/photos/2019/08/puppy.jpg?x-user=johndoe"` funciona da mesma forma que a solicitação para `"s3.amazonaws.com/amzn-s3-demo-bucket1/photos/2019/08/puppy.jpg"`, exceto pelo fato de que a string `"x-user=johndoe"` está incluída no campo `Request-URI` do registro de log associado. Essa funcionalidade está disponível apenas na interface REST.

Considerações de programação para o formato do log de acesso ao servidor extensível

Ocasionalmente, podemos estender o formato de registro de log de acesso adicionando novos campos ao final de cada linha. Portanto, certifique-se de que qualquer código que analise logs de acesso ao servidor consiga lidar com os campos finais que talvez não entenda.

Exclusão de arquivos de log do Amazon S3

Um bucket do Amazon S3 com registro em log de acesso ao servidor habilitado pode acumular muitos objetos de log do servidor ao longo do tempo. Seu aplicativo pode precisar desses logs de acesso por um período específico após sua criação e, depois disso, você poderá excluí-los. Use a configuração da funcionalidade Ciclo de Vida do Amazon S3 para definir regras de modo que o Amazon S3 organize esses objetos automaticamente para exclusão ao final de suas vidas.

É possível definir uma configuração de ciclo de vida para um subconjunto de objetos no bucket do S3 usando um prefixo compartilhado. Se você especificou um prefixo na sua configuração do registro em log de acesso ao servidor, defina uma regra de configuração do ciclo de vida para excluir objetos de log com esse prefixo.

Por exemplo, suponha que os objetos de log tenham o prefixo `logs/`. Você pode definir uma regra de configuração do ciclo de vida para excluir todos os objetos no bucket com o prefixo `logs/` após um período especificado.

Para obter mais informações sobre a configuração do ciclo de vida, consulte Gerenciar o ciclo de vida dos objetos.

Para obter mais informações sobre o registro em log de acesso ao servidor, consulte Registrar em log as solicitações com registro em log de acesso ao servidor.

Usar logs de acesso ao servidor do Amazon S3 para identificar solicitações

Você pode identificar solicitações do Amazon S3 usando os logs de acesso ao servidor do Amazon S3.

> **Note**
>
> - Para identificar as solicitações do Amazon S3, recomendamos que você use eventos de dados do AWS CloudTrail em vez de logs de acesso ao servidor do Amazon S3. Os eventos de dados do CloudTrail são mais fáceis de configurar e contêm mais informações. Para obter mais informações, consulte Identificar solicitações do Amazon S3 usando o CloudTrail.
> - Dependendo de quantas solicitações de acesso você receber, a análise dos logs poderá exigir mais recursos ou tempo do que o uso dos eventos de dados do CloudTrail.

Tópicos

- Consultar logs de acesso para solicitações usando o Amazon Athena
- Identificar solicitações do Signature Version 2 usando logs de acesso do Amazon S3
- Identificar solicitações de acesso a objetos usando logs de acesso do Amazon S3

Consultar logs de acesso para solicitações usando o Amazon Athena

Você pode identificar solicitações do Amazon S3 com logs de acesso do Amazon S3 usando o Amazon Athena.

O Amazon S3 armazena logs de acesso ao servidor como objetos em um bucket do S3. Muitas vezes, é mais fácil usar uma ferramenta que possa analisar os logs no Amazon S3. O Athena oferece suporte à análise de objetos do S3 e pode ser usado para consultar logs de acesso do Amazon S3.

Example

O exemplo a seguir mostra como você pode consultar os logs de acesso ao servidor do Amazon S3 no Amazon Athena. Substitua os *`user input placeholders`* utilizados nos exemplos a seguir por suas próprias informações.

> **Note**
>
> Para especificar um local do Amazon S3 em uma consulta do Athena, é necessário fornecer um URI do S3 para o bucket ao qual os logs são entregues. Esse URI deve incluir o nome e o prefixo do bucket no seguinte formato: `s3://`*`amzn-s3-demo-bucket1-logs/prefix`*`/`

1. Abra o console do Athena em https://console.aws.amazon.com/athena/.
2. No Editor de consultas, execute um comando semelhante ao seguinte. Substitua *`s3_access_logs_db`* pelo nome que você deseja atribuir ao banco de dados.

```
CREATE DATABASE s3_access_logs_db
```

> **Note**
>
> É uma prática recomendada criar o banco de dados na mesma Região da AWS em que o bucket do S3 está.

3. No Query Editor, execute um comando semelhante ao seguinte para criar um esquema de tabela no banco de dados criado na etapa 2. Substitua *s3_access_logs_db.mybucket_logs* pelo nome que você deseja atribuir à tabela. Os valores dos tipo de dados `STRING` e `BIGINT` são propriedades do log de acesso. É possível consultar essas propriedades no Athena. Para `LOCATION`, insira o bucket do S3 e o caminho do prefixo conforme indicado anteriormente.

   Date-based partitioning

```
CREATE EXTERNAL TABLE s3_access_logs_db.mybucket_logs(
 `bucketowner` STRING,
 `bucket_name` STRING,
 `requestdatetime` STRING,
 `remoteip` STRING,
 `requester` STRING,
 `requestid` STRING,
 `operation` STRING,
 `key` STRING,
 `request_uri` STRING,
 `httpstatus` STRING,
 `errorcode` STRING,
 `bytessent` BIGINT,
 `objectsize` BIGINT,
 `totaltime` STRING,
 `turnaroundtime` STRING,
 `referrer` STRING,
 `useragent` STRING,
 `versionid` STRING,
 `hostid` STRING,
 `sigv` STRING,
 `ciphersuite` STRING,
 `authtype` STRING,
 `endpoint` STRING,
 `tlsversion` STRING,
 `accesspointarn` STRING,
 `aclrequired` STRING)
```

```
 PARTITIONED BY (
   `timestamp` string)
ROW FORMAT SERDE
 'org.apache.hadoop.hive.serde2.RegexSerDe'
WITH SERDEPROPERTIES (
 'input.regex'='([^ ]*) ([^ ]*) \\[(.*?)\\] ([^ ]*) ([^ ]*) ([^ ]*) ([^ ]*)
 ([^ ]*) (\"[^\"]*\"|-) (-|[0-9]*) ([^ ]*) ([^ ]*) ([^ ]*) ([^ ]*) ([^ ]*)
 ([^ ]*) (\"[^\"]*\"|-) ([^ ]*)(?: ([^ ]*) ([^ ]*) ([^ ]*) ([^ ]*) ([^ ]*)
 ([^ ]*) ([^ ]*) ([^ ]*))?.*$')
STORED AS INPUTFORMAT
 'org.apache.hadoop.mapred.TextInputFormat'
OUTPUTFORMAT
 'org.apache.hadoop.hive.ql.io.HiveIgnoreKeyTextOutputFormat'
LOCATION
 's3://bucket-name/prefix-name/account-id/region/source-bucket-name/'
 TBLPROPERTIES (
  'projection.enabled'='true',
  'projection.timestamp.format'='yyyy/MM/dd',
  'projection.timestamp.interval'='1',
  'projection.timestamp.interval.unit'='DAYS',
  'projection.timestamp.range'='2024/01/01,NOW',
  'projection.timestamp.type'='date',
  'storage.location.template'='s3://bucket-name/prefix-name/account-id/region/
source-bucket-name/${timestamp}')
```

Non-date-based partitioning

```
CREATE EXTERNAL TABLE `s3_access_logs_db.mybucket_logs`(
  `bucketowner` STRING,
  `bucket_name` STRING,
  `requestdatetime` STRING,
  `remoteip` STRING,
  `requester` STRING,
  `requestid` STRING,
  `operation` STRING,
  `key` STRING,
  `request_uri` STRING,
  `httpstatus` STRING,
  `errorcode` STRING,
  `bytessent` BIGINT,
  `objectsize` BIGINT,
  `totaltime` STRING,
```

```
  `turnaroundtime` STRING,
  `referrer` STRING,
  `useragent` STRING,
  `versionid` STRING,
  `hostid` STRING,
  `sigv` STRING,
  `ciphersuite` STRING,
  `authtype` STRING,
  `endpoint` STRING,
  `tlsversion` STRING,
  `accesspointarn` STRING,
  `aclrequired` STRING)
ROW FORMAT SERDE
  'org.apache.hadoop.hive.serde2.RegexSerDe'
WITH SERDEPROPERTIES (
  'input.regex'='([^ ]*) ([^ ]*) \\[(.*?)\\] ([^ ]*) ([^ ]*) ([^ ]*) ([^ ]*)
 ([^ ]*) (\"[^\"]*\"|-) (-|[0-9]*) ([^ ]*) ([^ ]*) ([^ ]*) ([^ ]*) ([^ ]*)
 ([^ ]*) (\"[^\"]*\"|-) ([^ ]*)(?: ([^ ]*) ([^ ]*) ([^ ]*) ([^ ]*) ([^ ]*)
 ([^ ]*) ([^ ]*) ([^ ]*))?.*$')
STORED AS INPUTFORMAT
  'org.apache.hadoop.mapred.TextInputFormat'
OUTPUTFORMAT
  'org.apache.hadoop.hive.ql.io.HiveIgnoreKeyTextOutputFormat'
LOCATION
  's3://amzn-s3-demo-bucket1-logs/prefix/'
```

4. No painel de navegação, em Database (Banco de dados), escolha o banco de dados.
5. Em Tables (Tabelas), selecione Preview table (Visualizar tabela) ao lado do nome da tabela.

   No painel Results (Resultados), você deve ver dados dos logs de acesso ao servidor, como `bucketowner`, `bucket`, `requestdatetime` e assim por diante. Isso significa que você criou a tabela do Athena com êxito. Agora você pode consultar os logs de acesso ao servidor do Amazon S3.

Example : Mostre quem excluiu um objeto e quando (timestamp, endereço IP e usuário IAM)

```
SELECT requestdatetime, remoteip, requester, key
FROM s3_access_logs_db.mybucket_logs
WHERE key = 'images/picture.jpg' AND operation like '%DELETE%';
```

Example : Mostre todas as operações que foram realizadas por um usuário do IAM

```
SELECT *
FROM s3_access_logs_db.mybucket_logs
WHERE requester='arn:aws:iam::123456789123:user/user_name';
```

Example : mostrar todas as operações que foram realizadas em um objeto em um determinado período

```
SELECT *
FROM s3_access_logs_db.mybucket_logs
WHERE Key='prefix/images/picture.jpg'
    AND parse_datetime(requestdatetime,'dd/MMM/yyyy:HH:mm:ss Z')
    BETWEEN parse_datetime('2017-02-18:07:00:00','yyyy-MM-dd:HH:mm:ss')
    AND parse_datetime('2017-02-18:08:00:00','yyyy-MM-dd:HH:mm:ss');
```

Example : Mostrar a quantidade de dados transferidos por um endereço IP específico em determinado período

```
SELECT coalesce(SUM(bytessent), 0) AS bytessenttotal
FROM s3_access_logs_db.mybucket_logs
WHERE remoteip='192.0.2.1'
AND parse_datetime(requestdatetime,'dd/MMM/yyyy:HH:mm:ss Z')
BETWEEN parse_datetime('2022-06-01','yyyy-MM-dd')
AND parse_datetime('2022-07-01','yyyy-MM-dd');
```

Example – Encontre IDs de solicitação para erros HTTP 5xx em um período específico

```
SELECT requestdatetime, key, httpstatus, errorcode, requestid, hostid
FROM s3_access_logs_db.mybucket_logs
WHERE httpstatus like '5%' AND timestamp
BETWEEN '2024/01/29'
AND '2024/01/30'
```

> **Note**
>
> Para reduzir o tempo de retenção dos logs, você pode criar uma configuração da funcionalidade Ciclo de Vida do S3 para o bucket de logs de acesso ao servidor. Crie regras de configuração de ciclo de vida para remover os arquivos de log periodicamente. Fazer isso reduz a quantidade de dados que o Athena analisa para cada consulta. Para obter mais informações, consulte Definir uma configuração do Ciclo de Vida do S3 em um bucket.

Identificar solicitações do Signature Version 2 usando logs de acesso do Amazon S3

O suporte do Amazon S3 para o Signature versão 2 será desativado (defasado). Depois disso, o Amazon S3 não aceitará mais solicitações que usam o Signature versão 2 e todas as solicitações deverão usar assinaturas do Signature versão 4. É possível identificar solicitações de acesso do Signature Version 2 usando os logs de acesso do Amazon S3.

> **Note**
>
> Para identificar as solicitações do Signature Version 2, recomendamos que você use eventos de dados do AWS CloudTrail em vez de logs de acesso ao servidor do Amazon S3. Os eventos de dados do CloudTrail são mais fáceis de configurar e contêm mais informações do que os logs de acesso ao servidor. Para obter mais informações, consulte Identificar solicitações de Signature Version 2 do Amazon S3 usando o CloudTrail.

Example : mostrar todos os solicitantes que estão enviando tráfego do Signature versão 2

```
SELECT requester, sigv, Count(sigv) as sigcount
FROM s3_access_logs_db.mybucket_logs
GROUP BY requester, sigv;
```

Identificar solicitações de acesso a objetos usando logs de acesso do Amazon S3

É possível usar consultas em logs de acesso ao servidor do Amazon S3 para identificar solicitações de acesso a objetos do Amazon S3, para operações como `GET`, `PUT` e `DELETE`, e descobrir mais informações sobre essas solicitações.

O exemplo de consulta do Amazon Athena a seguir mostra como obter todas as solicitações PUT de objetos para o Amazon S3 de um log de acesso ao servidor.

Example : Mostrar todos os solicitantes que estão enviando solicitações **PUT** de objetos em determinado período

```
SELECT bucket_name, requester, remoteip, key, httpstatus, errorcode, requestdatetime
FROM s3_access_logs_db
WHERE operation='REST.PUT.OBJECT' AND
parse_datetime(requestdatetime,'dd/MMM/yyyy:HH:mm:ss Z')
BETWEEN parse_datetime('2019-07-01:00:42:42','yyyy-MM-dd:HH:mm:ss')
AND
parse_datetime('2019-07-02:00:42:42','yyyy-MM-dd:HH:mm:ss')
```

O exemplo de consulta do Amazon Athena a seguir mostra como obter todas as solicitações GET de objetos para o Amazon S3 do log de acesso ao servidor.

Example : Mostrar todos os solicitantes que estão enviando solicitações **GET** de objetos em determinado período

```
SELECT bucket_name, requester, remoteip, key, httpstatus, errorcode, requestdatetime
FROM s3_access_logs_db
WHERE operation='REST.GET.OBJECT' AND
parse_datetime(requestdatetime,'dd/MMM/yyyy:HH:mm:ss Z')
BETWEEN parse_datetime('2019-07-01:00:42:42','yyyy-MM-dd:HH:mm:ss')
AND
parse_datetime('2019-07-02:00:42:42','yyyy-MM-dd:HH:mm:ss')
```

O exemplo de consulta do Amazon Athena a seguir mostra como obter todas as solicitações anônimas ao seu bucket do S3 do log de acesso ao servidor.

Example : Mostrar todos os solicitantes anônimos que estão fazendo solicitações a um bucket em determinado período

```
SELECT bucket_name, requester, remoteip, key, httpstatus, errorcode, requestdatetime
FROM s3_access_logs_db.mybucket_logs
WHERE requester IS NULL AND
parse_datetime(requestdatetime,'dd/MMM/yyyy:HH:mm:ss Z')
BETWEEN parse_datetime('2019-07-01:00:42:42','yyyy-MM-dd:HH:mm:ss')
AND
```

```
parse_datetime('2019-07-02:00:42:42','yyyy-MM-dd:HH:mm:ss')
```

A consulta do Amazon Athena a seguir mostra como identificar todas as solicitações feitas aos seus buckets do S3 que exigiram uma lista de controle de acesso (ACL) para autorização. Você pode usar essas informações para migrar essas permissões de ACL para as políticas de bucket apropriadas e desativar as ACLs. Depois de criar essas políticas de bucket, você pode desativar as ACLs para esses buckets. Para obter mais informações sobre como desativar as ACLs, consulte Pré-requisitos para desabilitar ACLs.

Example : Identifique todas as solicitações que exigiram uma ACL para autorização

```
SELECT bucket_name, requester, key, operation, aclrequired, requestdatetime
FROM s3_access_logs_db
WHERE aclrequired = 'Yes' AND
parse_datetime(requestdatetime,'dd/MMM/yyyy:HH:mm:ss Z')
BETWEEN parse_datetime('2022-05-10:00:00:00','yyyy-MM-dd:HH:mm:ss')
AND parse_datetime('2022-08-10:00:00:00','yyyy-MM-dd:HH:mm:ss')
```

Note

- É possível modificar o intervalo de datas conforme necessário para atender às suas necessidades.
- Esses exemplos de consulta também podem ser úteis para o monitoramento de segurança. Você pode ver os resultados de chamadas `PutObject` ou `GetObject` de solicitantes ou endereços IP inesperados ou não autorizados e identificar solicitações anônimas aos seus buckets.
- Essa consulta recupera somente informações do momento no qual o registro estava habilitado.
- Se você estiver usando logs do AWS CloudTrail, consulte Identificar o acesso a objetos do S3 usando o CloudTrail.

Solução de problemas do registro em log de acessos ao servidor

Os tópicos a seguir podem ajudar a solucionar problemas que você pode encontrar ao configurar o registro em log com o Amazon S3.

Tópicos

- Mensagens de erro comuns ao configurar o registro em log
- Solução de problemas de falha de entrega

Mensagens de erro comuns ao configurar o registro em log

As seguintes mensagens de erro comuns podem aparecer quando você ativa o registro em log por meio da AWS Command Line Interface (AWS CLI) e dos AWS SDKs:

Erro: registro em log de localização cruzada do S3 não é permitido

Se o bucket de destino (também conhecido como bucket-alvo) estiver em uma região diferente do bucket de origem, ocorrerá um erro Não é permitido o registro em log entre locais do S3. Para resolver esse erro, verifique se o bucket de destino configurado para receber os logs de acesso está na mesma Região da AWS e Conta da AWS que o bucket de origem.

Erro: o proprietário do bucket a ser registrado e o bucket de destino devem ser os mesmos

Quando você habilitar o registro em log de acesso ao servidor, esse erro ocorrerá se o bucket de destino especificado pertencer a uma conta diferente. Para resolver esse erro, verifique se o bucket de destino está na mesma Conta da AWS que o bucket de origem.

> **Note**
>
> Recomendamos que você escolha um bucket de destino diferente do bucket de origem. Quando o bucket de origem e o bucket de destino são os mesmos, logs adicionais são criados para os logs que são gravados no bucket, o que pode aumentar a fatura de armazenamento. Esses logs extras sobre logs também podem dificultar a localização dos logs específicos que você está procurando. Para um gerenciamento de logs mais simples, recomendamos salvar logs de acesso em um bucket diferente. Para obter mais informações, consulte the section called “Como faço para habilitar a entrega de logs?”.

Erro: o bucket de destino para registro em log não existe

O bucket de destino precisa existir antes de definir a configuração. Esse erro indica que o bucket de destino não existe ou não pôde ser encontrado. Verifique se o nome do bucket está escrito corretamente e tente novamente.

Erro: concessões de destino não são permitidas para buckets com proprietário de bucket aplicado

Esse erro indica que o bucket de destino usa a configuração Imposto pelo proprietário do bucket para a funcionalidade Propriedade de Objetos do S3. A configuração Imposto pelo proprietário do bucket não é compatível com concessões de destino (alvo). Para obter mais informações, consulte Permissões para entrega de logs.

Solução de problemas de falha de entrega

Para evitar problemas de registro em log de acesso ao servidor, siga estas práticas recomendadas:

- O grupo de entrega de logs do S3 tem acesso de gravação ao bucket de destino: o grupo de entrega de logs do S3 entrega logs de acesso ao servidor para o bucket de destino. Uma política de bucket ou uma lista de controle de acesso (ACL) do bucket para conceder acesso de gravação ao bucket de destino. No entanto, recomendamos usar uma política de bucket em vez de uma ACL. Para obter mais informações sobre como conceder acesso de gravação ao bucket de destino, consulte Permissões para entrega de logs.

  > **Note**
  >
  > Se o bucket de destino usar a configuração Imposto pelo proprietário do bucket para a funcionalidade Propriedade de Objetos, esteja ciente do seguinte:
  >
  > - As ACLs estão desativadas e não afetam mais as permissões. Isso significa que não é possível atualizar a ACL do bucket para conceder acesso ao grupo de entrega de log do S3. Em vez disso, para conceder acesso à entidade principal de serviço do registro em log, é necessário atualizar a política de bucket para o bucket de destino.
  > - Não é possível incluir concessões de destino na configuração de `PutBucketLogging`.

- A política de bucket para o bucket de destino permite o acesso aos logs: verifique a política do bucket de destino. Pesquise na política de bucket declarações que contenham `"Effect": "Deny"`. Depois, verifique se a declaração `Deny` não está impedindo que os logs de acesso sejam gravados no bucket.
- A funcionalidade Bloqueio de Objetos do S3 não está habilitada no bucket de destino: verifique se o bucket de destino está com a funcionalidade Bloqueio de Objetos habilitada. O bloqueio de objetos bloqueia a entrega do log de acesso ao servidor. Você deve escolher um bucket de destino que não esteja com funcionalidade Bloqueio de Objetos habilitada.
- As chaves gerenciadas pelo Amazon S3 (SSE-S3) são selecionadas se a criptografia padrão está habilitada no bucket de destino: é possível usar a criptografia de bucket padrão no bucket

de destino somente se você usa a criptografia do lado do servidor com as chaves gerenciadas pelo Amazon S3 (SSE-S3). A criptografia padrão do lado do servidor com chaves do AWS Key Management Service (AWS KMS) (SSE-KMS) não é compatível com os buckets de destino do registro em log de acesso ao servidor. Para obter mais informações sobre como ativar a criptografia padrão, consulte Configurar a criptografia padrão.

- O bucket de destino não tem a opção Pagamento pelo solicitante habilitada: o uso de um bucket de Pagamento pelo solicitante como bucket de destino para o registro em log de acesso ao servidor não é compatível. Para permitir a entrega de logs de acesso ao servidor, desabilite a opção Pagamento pelo solicitante no bucket de destino.
- Revise as políticas de controle de serviços (SCPs) e as políticas de controle de recursos (RCPs) do AWS Organizations: ao usar o AWS Organizations, verifique as políticas de controle de serviços e as políticas de controle de recursos para garantir que o acesso ao Amazon S3 seja permitido. Essas políticas especificam o número máximo de permissões para entidades principais e recursos nas contas afetadas. Pesquise nas políticas as instruções que contenham `"Effect": "Deny"` e verifique se as instruções `Deny` não estão impedindo que os logs de acesso sejam gravados no bucket. Consulte mais informações em Authorization policies in AWS Organizations no Guia do usuário do AWS Organizations.
- Aguarde um tempo para que as alterações recentes na configuração do registro em log entrem em vigor: as ações de habilitar o registro em log de acesso ao servidor pela primeira vez ou alterar o bucket de destino para os logs levam tempo para entrar em vigor totalmente. Pode levar mais de uma hora para que todas as solicitações sejam registradas e entregues adequadamente.

  Para verificar se há falha de entrega de log, ative as métricas de solicitação do Amazon CloudWatch. Se os logs não forem entregues em algumas horas, procure a métrica `4xxErrors`, que pode indicar falhas na entrega dos logs. Para obter mais informações sobre como ativar as métricas de solicitação, consulte the section called “Criar uma configuração de métricas para todos os objetos”.

Monitoramento de métricas com o Amazon CloudWatch

As métricas do Amazon CloudWatch para Amazon S3 podem ajudar você a entender e melhorar a performance das aplicações que usam o Amazon S3. Existem várias maneiras de usar o CloudWatch com o Amazon S3.

Métricas de armazenamento diárias para buckets

Monitore o armazenamento do bucket usando o CloudWatch, que coleta e processa dados de armazenamento do Amazon S3 para gerar métricas legíveis diárias. Essas métricas de armazenamento para o Amazon S3 são relatadas uma vez por dia e fornecidas a todos os clientes sem qualquer custo adicional.

Métricas de solicitação

Monitore as solicitações do Amazon S3 para identificar e atuar rapidamente em problemas operacionais. As métricas estão disponíveis em intervalos de um minuto após alguma latência para processamento. Essas métricas do CloudWatch são cobradas na mesma taxa que as métricas personalizadas do Amazon CloudWatch. Para obter mais informações sobre a definição de preço do CloudWatch, consulte Definição de preço do Amazon CloudWatch. Para saber como optar por obter essas métricas, consulte Configurações de métricas do CloudWatch.

Quando ativadas, as métricas de solicitações são relatadas para todas as operações de objeto. Por padrão, essas métricas de 1 minuto estão disponíveis no nível do bucket do Amazon S3. Também é possível definir um filtro para as métricas usando um prefixo compartilhado, etiqueta de objeto ou ponto de acesso.

- Ponto de acesso: os pontos de acesso são endpoints de rede nomeados que estão conectados a buckets e simplificam o gerenciamento do acesso a dados em escala para conjuntos de dados compartilhados no S3. Com o filtro de ponto de acesso, você pode obter informações sobre o uso do ponto de acesso. Para obter mais informações sobre pontos de acesso, consulte Monitorar e registrar de pontos de acesso.
- Prefixo: embora o modelo de dados do Amazon S3 seja uma estrutura plana, você pode inferir a hierarquia usando um prefixo. Um prefixo é semelhante a um nome de diretório que permite agrupar objetos semelhantes em um bucket. O console do S3 oferece suporte a esses prefixos com o conceito de pastas. Se você filtrar por prefixo, os objetos com mesmo prefixo serão incluídos na configuração de métricas. Para obter mais informações sobre prefixos, consulte Organizar objetos usando prefixos.
- Etitquetas: etiquetas são pares de nomes de chave-valor que você pode adicionar aos objetos. As etiquetas ajudam a encontrar e organizar objetos com facilidade. Você também pode usar etiquetas como um filtro para configurações de métricas para que somente objetos com essas etiquetas sejam incluídos na configuração de métricas. Para obter mais informações sobre etiquetas de objeto, consulte Categorizar seu armazenamento usando tags.

Para alinhar essas métricas a aplicações de negócios, fluxos de trabalho ou organizações internas específicas, você pode filtrar por um prefixo compartilhado, marca de objeto ou ponto de acesso.

Métricas de replicação

Monitore o número total de operações de API do S3 que estão pendentes de replicação, o tamanho total de objetos com replicação pendente e o tempo máximo de replicação para a Região da AWS de destino e o número total de operações com replicação falhada. As regras de replicação com Controle de Tempo de Replicação do S3 (S3 RTC) ou métricas de replicação do S3 habilitadas publicarão as métricas de replicação.

Para ter mais informações, consulte Monitorar a replicação com métricas, notificações de eventos e status ou Atender aos requisitos de conformidade com o Controle do Tempo de Replicação do S3.

Métricas do Amazon S3 Storage Lens

É possível publicar métricas de uso e atividade do S3 Storage Lens no Amazon CloudWatch para criar uma visão unificada de sua integridade operacional nos painéis do CloudWatch. As métricas do S3 Storage Lens estão disponíveis no namespace `AWS/S3/Storage-Lens`. A opção de publicação do CloudWatch está disponível para painéis do S3 Storage Lens atualizados para métricas e recomendações avançadas. É possível habilitar a opção de publicação do CloudWatch para uma configuração de painel nova ou existente no S3 Storage Lens.

Para obter mais informações, consulte Monitorar métricas do S3 Storage Lens no CloudWatch.

Todas as estatísticas do CloudWatch ficam retidas por um período de 15 meses, para que você possa acessar informações históricas e obter uma perspectiva melhor sobre como o serviço ou o aplicação Web estão se saindo. Para obter mais informações sobre o CloudWatch, consulte O que é o Amazon CloudWatch? no Guia do usuário do Amazon CloudWatch. Você pode precisar de algumas configurações adicionais para os alarmes do CloudWatch, dependendo dos seus casos de uso. Por exemplo, você pode usar a expressão matemática de métricas para criar um alarme. Para obter mais informações, consulte Usar métricas do CloudWatch, Usar matemática de métricas, Usar de alarmes do Amazon CloudWatch e Criar um alarme do CloudWatch com base em uma expressão matemática de métricas no Guia do usuário do Amazon CloudWatch.

Entrega de métricas do CloudWatch com o melhor esforço

As métricas do CloudWatch são entregues com base em melhor esforço. A maioria de solicitações para um objeto do Amazon S3 que tenha métricas de solicitações resulta no envio de um ponto de dados ao CloudWatch.

A integridade e pontualidade das métricas não são garantidas. O ponto de dados para uma solicitação específica pode ser retornado com um timestamp posterior à solicitação processada. O ponto de dados de um minuto pode ser atrasado antes de ser disponibilizado pelo CloudWatch ou pode nem ser entregue. As métricas de solicitação do CloudWatch lhe dão uma ideia da natureza do tráfego em seu bucket em tempo quase real. Não se trata de uma contabilidade completa de todas as solicitações.

Devido à natureza de melhor esforço deste recurso, os relatórios disponíveis no Painel de faturamento e de gerenciamento de custo podem incluir uma ou mais solicitações de acesso que não aparecem nas métricas do bucket.

Para obter mais informações, consulte os tópicos a seguir.

Tópicos

- Métricas e dimensões
- Acessar métricas do CloudWatch
- Configurações de métricas do CloudWatch

Métricas e dimensões

As métricas e dimensões que o Amazon S3 envia para o Amazon CloudWatch estão listadas nas tabelas a seguir.

Entrega de métricas do CloudWatch com o melhor esforço

As métricas do CloudWatch são entregues com base em melhor esforço. A maioria de solicitações para um objeto do Amazon S3 que tenha métricas de solicitações resulta no envio de um ponto de dados ao CloudWatch.

A integridade e pontualidade das métricas não são garantidas. O ponto de dados para uma solicitação específica pode ser retornado com um timestamp posterior à solicitação processada. O ponto de dados de um minuto pode ser atrasado antes de ser disponibilizado pelo CloudWatch ou pode nem ser entregue. As métricas de solicitação do CloudWatch lhe dão uma ideia da natureza do tráfego em seu bucket em tempo quase real. Não se trata de uma contabilidade completa de todas as solicitações.

Devido à natureza de melhor esforço deste recurso, os relatórios disponíveis no Painel de faturamento e de gerenciamento de custo podem incluir uma ou mais solicitações de acesso que não aparecem nas métricas do bucket.

Tópicos

- Métricas de armazenamento diárias do Amazon S3 para buckets no CloudWatch
- Métricas de solicitação do Amazon S3 no CloudWatch
- Métricas de replicação do S3 no CloudWatch
- Métricas do S3 Storage Lens no CloudWatch
- Métricas de solicitação do S3 Object Lambda no CloudWatch
- Dimensões do Amazon S3 no CloudWatch
- Dimensões da funcionalidade Replicação do S3 no CloudWatch
- Dimensões do S3 Storage Lens no CloudWatch
- Dimensões de solicitação do S3 Object Lambda no CloudWatch
- Métricas de uso do Amazon S3

Métricas de armazenamento diárias do Amazon S3 para buckets no CloudWatch

O namespace `AWS/S3` inclui as métricas de armazenamento diário a seguir para buckets.

Métrica	Descrição
`BucketSizeBytes`	A quantidade de dados, em bytes, armazenados em um bucket nas seguintes classes de armazenamento: • Reduced Redundancy Storage (RRS) (`REDUCED_REDUNDANCY`) • S3 Express One Zone (`EXPRESS_ONEZONE`) • S3 Glacier Deep Archive (`DEEP_ARCHIVE`) • S3 Glacier Flexible Retrieval (`GLACIER`) • S3 Glacier Instant Retrieval (`GLACIER_IR`) • S3 Intelligent-Tiering (`INTELLIGENT_TIERING`) • S3 One Zone-Infrequent Access (`ONEZONE_IA`) • S3 Standard (`STANDARD`)

Métrica	Descrição
	• S3 Standard-Infrequent Access (`STANDARD_IA`) O valor é calculado somando o tamanho de todos os objetos e metadados (como nomes de buckets) no bucket (objetos atuais e não atuais), incluindo o tamanho de todas as partes de todos os carregamentos fracionados incompletos do bucket. **Note** A classe de armazenamento S3 Express One Zone está disponível somente para buckets de diretório. Filtros de tipo de armazenamento válidos (consulte a dimensão `StorageType`): • Reduced Redundancy Storage (RRS): `ReducedRedundancyStorage` • S3 Express One Zone: `ExpressOneZoneStorage` • S3 Glacier Deep Archive: `DeepArchiveObjectOverhead`, `DeepArchiveS3ObjectOverhead`, `DeepArchiveStagingStorage`, `DeepArchiveStorage` • S3 Glacier Flexible Retrieval: `GlacierObjectOverhead`, `GlacierS3ObjectOverhead`, `GlacierStagingStorage`, `GlacierStorage` • S3 Glacier Instant Retrieval: `GlacierInstantRetrievalStorage`, `GlacierIRSizeOverhead` • S3 Intelligent-Tiering: `IntelligentTieringAAStorage`, `IntelligentTieringAIAStorage`, `IntelligentTieringDAAStorage`, `IntelligentTieringFAStorage`, `IntelligentTieringIAStorage` • S3 One Zone-Infrequent Access: `OneZoneIASizeOverhead`, `OneZoneIAStorage` • S3 Standard: `StandardStorage`

Métrica	Descrição
	• S3 Standard-Infrequent Access: `StandardIAObjectOverhead` , `StandardIASizeOverhead` , `StandardIAStorage` Unidades: bytes Estatística válida: média Para ter mais informações sobre as dimensões `StorageType` , consulte the section called “Dimensões do Amazon S3 no CloudWatch”.
`NumberOfObjects`	O número total de objetos armazenados em um bucket de uso geral para todas as classes de armazenamento. Esse valor é calculado contando todos os objetos do bucket, que incluem objetos atuais e não atuais, marcadores de exclusão e o número total de partes de todos os carregamentos fracionados incompletos do bucket. Para buckets de diretório com objetos na classe de armazenamento S3 Express One Zone, esse valor é calculado contando todos os objetos do bucket, mas não inclui uploads múltiplos incompletos no bucket. Filtros de tipo de armazenamento válidos: `AllStorageTypes` (consulte a dimensão `StorageType`) Unidade: contagem Estatística válida: média

Métricas de solicitação do Amazon S3 no CloudWatch

O namespace `AWS/S3` inclui as métricas de solicitação a seguir. Essas métricas incluem solicitações não faturáveis (no caso de solicitações `GET` de `CopyObject` e Replication).

> **Note**
>
> As métricas de solicitação do Amazon S3 no CloudWatch não são compatíveis com buckets de diretório.

Métrica	Descrição
`AllRequests`	O número total de solicitações HTTP feitas em um bucket do Amazon S3, independentemente do tipo. Se você estiver usando uma configura ção de métricas com um filtro, então essa métrica só retornará as solicitações HTTP que atendam aos requisitos do filtro. Unidades: contagem Estatística válida: soma
`GetRequests`	O número de solicitações HTTP `GET` feitas para objetos em um bucket do Amazon S3. Isso não inclui operações de lista. Essa métrica é incrementada para a origem de cada solicitação `CopyObject` . Unidades: contagem Estatística válida: soma **Note** Solicitações paginadas orientadas a listas, como ListMulti partUploads, ListParts e ListObjectVersions, não estão incluídas nessa métrica.
`PutRequests`	O número de solicitações HTTP `PUT` feitas para objetos em um bucket do Amazon S3. Essa métrica é incrementada para o destino de cada solicitação `CopyObject` . Unidades: contagem Estatística válida: soma
`DeleteRequests`	O número de solicitações HTTP `DELETE` feitas para objetos em um bucket do Amazon S3. Essa métrica também inclui as solicitações DeleteObjects. Essa métrica exibe o número de solicitações feitas, não o número de objetos excluídos. Unidades: contagem

Métrica	Descrição
	Estatística válida: soma
`HeadRequests`	O número de solicitações HTTP `HEAD` feitas para um bucket do Amazon S3. Unidades: contagem Estatística válida: soma
`PostRequests`	O número de solicitações HTTP `POST` feitas para um bucket do Amazon S3. Unidades: contagem Estatística válida: soma **Note** As solicitações DeleteObjects e SelectObjectContent não estão incluídas nessa métrica.
`SelectRequests`	O número de solicitações SelectObjectContent do Amazon S3 feitas para objetos em um bucket do Amazon S3. Unidades: contagem Estatística válida: soma
`SelectBytesScanned`	O número de bytes de dados verificados com solicitações SelectObjectContent do Amazon S3 em um bucket do Amazon S3. Unidades: bytes Estatísticas válidas: média (bytes por solicitação), soma (bytes por período), contagem de amostras, mín., máx. (o mesmo que p100), qualquer percentil entre p0,0 e p99,9

Métrica	Descrição
`SelectBytesReturned`	O número de bytes de dados retornados com solicitações SelectObjectContent do Amazon S3 em um bucket do Amazon S3. Unidades: bytes Estatísticas válidas: média (bytes por solicitação), soma (bytes por período), contagem de amostras, mín., máx. (o mesmo que p100), qualquer percentil entre p0,0 e p99,9
`ListRequests`	O número de solicitações HTTP que listam o conteúdo de um bucket. Unidade: contagem Estatística válida: soma
`BytesDownloaded`	O número de bytes baixados para solicitações feitas para um bucket do Amazon S3, em que a resposta inclui um corpo. Unidade: bytes Estatísticas válidas: média (bytes por solicitação), soma (bytes por período), contagem de amostras, mín., máx. (o mesmo que p100), qualquer percentil entre p0,0 e p99,9
`BytesUploaded`	O número de bytes carregados para solicitações feitas a um bucket do Amazon S3, em que a solicitação inclui um corpo. Unidades: bytes Estatísticas válidas: média (bytes por solicitação), soma (bytes por período), contagem de amostras, mín., máx. (o mesmo que p100), qualquer percentil entre p0,0 e p99,9

Métrica	Descrição
`4xxErrors`	O número de solicitações com código de status de erro do cliente HTTP 4xx feitas para um bucket do Amazon S3 com um valor de 0 ou 1. A estatística Average (Média) mostra a taxa de erros, e a estatística Sum (Soma) mostra a contagem desse tipo de erro, durante cada período. Unidades: contagem Estatísticas válidas: média (relatórios por solicitação), soma (relatórios por período), mín., máx., contagem de amostras
`5xxErrors`	O número de solicitações com código de status de erro do servidor HTTP 5xx feitas para um bucket do Amazon S3 com um valor de 0 ou 1. A estatística Average (Média) mostra a taxa de erros, e a estatística Sum (Soma) mostra a contagem desse tipo de erro, durante cada período. Unidades: contagem Estatísticas válidas: média (relatórios por solicitação), soma (relatórios por período), mín., máx., contagem de amostras
`FirstByte Latency`	O tempo por solicitação desde o recebimento da solicitação completa por um bucket do Amazon S3 até o momento em que a resposta começa a ser retornada. Unidade: milissegundos Estatísticas válidas: Average (Média), Sum (Soma), Min (Mínimo), Max (Máximo) (o mesmo que p100), Sample Count (Contagem de amostras), qualquer percentil entre p0,0 e p100

Métrica	Descrição
`TotalRequestLatency`	O tempo por solicitação decorrido do primeiro byte recebido até o último byte enviado para um bucket do Amazon S3. Essa métrica inclui o tempo necessário para receber o corpo da solicitação e enviar o corpo da resposta, que não está incluído em `FirstByteLatency` . Unidade: milissegundos Estatísticas válidas: Average (Média), Sum (Soma), Min (Mínimo), Max (Máximo) (o mesmo que p100), Sample Count (Contagem de amostras), qualquer percentil entre p0,0 e p100

Métricas de replicação do S3 no CloudWatch

Você pode monitorar o progresso da replicação com métricas de replicação do S3 rastreando bytes pendentes, operações pendentes e latência de replicação. Para obter mais informações, consulte Monitoramento do progresso com métricas de replicação.

> **Note**
>
> Você pode habilitar alarmes para suas métricas de replicação no Amazon CloudWatch. Quando você configurar alarmes para as métricas de replicação, defina o campo Missing data treatment (Tratamento de dados ausentes) como Treat missing data as ignore (maintain the alarm state) (Ignorar dados ausentes [manter o estado de alarme]).

Métrica	Descrição
`ReplicationLatency`	O número máximo de segundos em que a Região da AWS de destino da replicação está atrás da Região da AWS de origem de uma determinada regra de replicação. Unidade: segundos Estatísticas válidas: Max

Métrica	Descrição
`BytesPendingReplication`	O número total de bytes de objetos com replicação pendente para uma determinada regra de replicação. Unidade: bytes Estatísticas válidas: Max
`OperationsPendingReplication`	O número de operações com replicação pendente para uma determinada regra de replicação. Unidades: contagem Estatísticas válidas: Max
`OperationsFailedReplication`	O número de operações com falha na replicação para determinada regra de replicação. Unidades: contagem Estatísticas válidas: soma (número total de operações com falha), média (taxa de falha), contagem de amostras (número total de operações de replicação)

Métricas do S3 Storage Lens no CloudWatch

É possível publicar métricas de uso e atividade do S3 Storage Lens no Amazon CloudWatch para criar uma visão unificada de sua integridade operacional nos painéis do CloudWatch. As métricas da lente de armazenamento do S3 são publicadas no namespace `AWS/S3/Storage-Lens` no CloudWatch. A opção de publicação do CloudWatch está disponível para painéis do S3 Storage Lens que foram atualizados para métricas e recomendações avançadas.

Para obter uma lista das métricas do S3 Storage Lens publicadas no CloudWatch, consulte Glossário de métricas de lente de armazenamento do Amazon S3. Para obter uma lista completa de dimensões, consulte Dimensões.

Métricas de solicitação do S3 Object Lambda no CloudWatch

O S3 Object Lambda inclui as métricas de solicitação a seguir.

Métrica	Descrição
`AllRequests`	O número total de solicitações HTTP feitas para um bucket do Amazon S3 usando um ponto de acesso do Object Lambda. Unidades: contagem Estatística válida: soma
`GetRequests`	O número de solicitações HTTP `GET` feitas para objetos usando um ponto de acesso do Object Lambda. Essa métrica não inclui operações de lista. Unidades: contagem Estatística válida: soma
`BytesUploaded`	O número de bytes carregados para um bucket do Amazon S3 usando um ponto de acesso do Object Lambda, para solicitações que incluem um corpo. Unidades: bytes Estatísticas válidas: média (bytes por solicitação), soma (bytes por período), contagem de amostras, mín., máx. (o mesmo que p100), qualquer percentil entre p0,0 e p99,9
`PostRequests`	O número de solicitações HTTP `POST` feitas para um bucket do Amazon S3 usando um ponto de acesso do Object Lambda. Unidades: contagem Estatística válida: soma
`PutRequests`	O número de solicitações HTTP `PUT` feitas para objetos em um bucket do Amazon S3 usando um ponto de acesso do Object Lambda. Unidades: contagem Estatística válida: soma

Métrica	Descrição
`DeleteRequests`	O número de solicitações HTTP `DELETE` feitas para objetos em um bucket do Amazon S3 usando um ponto de acesso do Object Lambda. Essa métrica inclui as solicitações DeleteObjects. Essa métrica exibe o número de solicitações feitas, não o número de objetos excluídos. Unidades: contagem Estatística válida: soma
`BytesDownloaded`	O número de bytes baixados para solicitações feitas a um bucket do Amazon S3 usando um ponto de acesso do Object Lambda, em que a resposta inclui um corpo. Unidades: bytes Estatísticas válidas: média (bytes por solicitação), soma (bytes por período), contagem de amostras, mín., máx. (o mesmo que p100), qualquer percentil entre p0,0 e p99,9
`FirstByte Latency`	O tempo por solicitação desde o recebimento da solicitação completa por um bucket do Amazon S3 por meio de um ponto de acesso do Object Lambda até o momento em que a resposta começa a ser retornada. Essa métrica depende do tempo de execução da função do AWS Lambda para transformar o objeto antes que a função retorne os bytes para o ponto de acesso do Object Lambda. Unidade: milissegundos Estatísticas válidas: Average (Média), Sum (Soma), Min (Mínimo), Max (Máximo) (o mesmo que p100), Sample Count (Contagem de amostras), qualquer percentil entre p0,0 e p100

Métrica	Descrição
`TotalRequestLatency`	O tempo por solicitação decorrido do primeiro byte recebido até o último byte enviado para um ponto de acesso do Object Lambda. Essa métrica inclui o tempo necessário para receber o corpo da solicitação e enviar o corpo da resposta, que não está incluído em `FirstByteLatency` . Unidade: milissegundos Estatísticas válidas: Average (Média), Sum (Soma), Min (Mínimo), Max (Máximo) (o mesmo que p100), Sample Count (Contagem de amostras), qualquer percentil entre p0,0 e p100
`HeadRequests`	O número de solicitações HTTP `HEAD` feitas para um bucket do Amazon S3 usando um ponto de acesso do Object Lambda. Unidades: contagem Estatística válida: soma
`ListRequests`	O número de solicitações HTTP `GET` que listam o conteúdo de um bucket do Amazon S3. Essa métrica inclui as operações `ListObjects` e `ListObjectsV2` . Unidades: contagem Estatística válida: soma
`4xxErrors`	O número de solicitações com código de status de erro do servidor HTTP 4xx feitas para um bucket do Amazon S3 usando um ponto de acesso do Object Lambda com um valor de 0 ou 1. A estatística Average (Média) mostra a taxa de erros, e a estatística Sum (Soma) mostra a contagem desse tipo de erro, durante cada período. Unidades: contagem Estatísticas válidas: média (relatórios por solicitação), soma (relatórios por período), mín., máx., contagem de amostras

Métrica	Descrição
`5xxErrors`	O número de solicitações com código de status de erro do servidor HTTP 5xx feitas para um bucket do Amazon S3 usando um ponto de acesso do Object Lambda com um valor de 0 ou 1. A estatística Average (Média) mostra a taxa de erros, e a estatística Sum (Soma) mostra a contagem desse tipo de erro, durante cada período. Unidades: contagem Estatísticas válidas: média (relatórios por solicitação), soma (relatórios por período), mín., máx., contagem de amostras
`ProxiedRequests`	O número de solicitações HTTP para um ponto de acesso do Object Lambda que retornam a resposta padrão de API do Amazon S3. (Essas solicitações não têm uma função do Lambda configurada.) Unidades: contagem Estatística válida: soma
`InvokedLambda`	O número de solicitações HTTP para um objeto do S3 em que uma função do Lambda foi invocada. Unidades: contagem Estatística válida: soma
`LambdaResponseRequests`	O número de solicitações `WriteGetObjectResponse` feitas pela função do Lambda. Esta métrica aplica-se apenas às solicitações `GetObject` .
`LambdaResponse4xx`	O número de erros de cliente HTTP 4xx que ocorrem ao chamar `WriteGetObjectResponse` de uma função do Lambda. Essa métrica fornece as mesmas informações que `4xxErrors` , mas somente para chamadas de `WriteGetObjectResponse` .

Métrica	Descrição
`LambdaResponse5xx`	O número de erros de servidor HTTP 5xx que ocorrem ao chamar `WriteGetObjectResponse` de uma função do Lambda. Essa métrica fornece as mesmas informações que `5xxErrors` , mas somente para chamadas de `WriteGetObjectResponse` .

Dimensões do Amazon S3 no CloudWatch

As seguintes dimensões são usadas para filtrar as métricas do Amazon S3.

Dimensão	Descrição
`BucketName`	Essa dimensão filtra os dados que você solicita apenas para o bucket identificado.
`StorageType`	Essa dimensão filtra os dados que você armazenou em um bucket pelos seguintes tipos de armazenamento: • `DeepArchiveObjectOverhead` : para cada objeto arquivado, o S3 Glacier adiciona 32 KB de armazenamento para índice e metadados relacionados. Esses dados adicionais são necessários para identificar e recuperar seu objeto. Você é cobrado pelas taxas do S3 Glacier Deep Archive nesse armazenamento adicional. • `DeepArchiveS3ObjectOverhead` : para cada objeto arquivado no S3 Glacier Deep Archive, o Simple Storage Service (Amazon S3) usa 8 KB de armazenamento para o nome do objeto e outros metadados. Você é cobrado com as tarifas S3 Standard pelo armazenamento adicional. • `DeepArchiveStagingStorage` : o número de bytes usados para partes de objetos de carregamento fracionado antes que a solicitação `CompleteMultipartUpload` seja concluída em objetos na classe de armazenamento S3 Glacier Deep Archive.

Dimensão	Descrição
	• `DeepArchiveStorage` : o número de bytes usados para objetos na classe de armazenamento S3 Glacier Deep Archive. • `ExpressOneZoneStorage` : o número de bytes usados para objetos na classe de armazenamento S3 Express One Zone. • `GlacierInstantRetrievalStorage` : o número de bytes usados para objetos na classe de armazenamento Instant Retrieval do S3 Glacier. • `GlacierIRSizeOverhead` : o número de bytes usados para objetos com menos de 128 KB na classe de armazenamento Instant Retrieval do S3 Glacier. • `GlacierObjectOverhead` : para cada objeto arquivado, o S3 Glacier adiciona 32 KB de armazenamento para índice e metadados relacionados. Esses dados adicionais são necessários para identificar e recuperar seu objeto. Você é cobrado nas tarifas do S3 Glacier Flexible Retrieval por esse armazenamento adicional. • `GlacierS3ObjectOverhead` : para cada objeto arquivado no S3 Glacier Flexible Retrieval, o Simple Storage Service (Amazon S3) usa 8 KB de armazenamento para o nome do objeto e outros metadados. Você é cobrado com as tarifas S3 Standard pelo armazenamento adicional. • `GlacierStagingStorage` : o número de bytes usados para as partes de objetos de carregamento fracionado antes que a solicitação `CompleteMultipartUpload` seja concluída em objetos na classe de armazenamento S3 Glacier Flexible Retrieval. • `GlacierStorage` : o número de bytes usados para objetos na classe de armazenamento S3 Glacier Flexible Retrieval. • `IntAAObjectOverhead` : para cada objeto na classe de armazenamento `INTELLIGENT_TIERING` no nível Archive Access, o S3 Glacier adiciona 32 KB de armazenamento para

Dimensão	Descrição
	índice e metadados relacionados. Esses dados adicionais são necessários para identificar e recuperar seu objeto. Você é cobrado nas tarifas do S3 Glacier Flexible Retrieval por esse armazenamento adicional. • `IntAAS3ObjectOverhead` : para cada objeto na classe de armazenamento `INTELLIGENT_TIERING` no nível Archive Access, o Amazon S3 usa 8 KB de armazenamento para o nome do objeto e outros metadados. Você é cobrado com as tarifas S3 Standard pelo armazenamento adicional. • `IntDAAObjectOverhead` : para cada objeto na classe de armazenamento `INTELLIGENT_TIERING` no nível Deep Archive Access, o S3 Glacier adiciona 32 KB de armazenamento para índice e metadados relacionados. Esses dados adicionais são necessários para identificar e recuperar seu objeto. Você é cobrado pelas taxas do S3 Glacier Deep Archive nesse armazenamento adicional. • `IntDAAS3ObjectOverhead` : para cada objeto na classe de armazenamento `INTELLIGENT_TIERING` no nível Deep Archive Access, o Amazon S3 adiciona 8 KB de armazenamento para índice e metadados relacionados. Esses dados adicionais são necessários para identificar e recuperar seu objeto. Você é cobrado com as tarifas S3 Standard pelo armazenamento adicional. • `IntelligentTieringAAStorage` : o número de bytes usados para objetos no nível Archive Access da classe de armazenamento `INTELLIGENT_TIERING` . • `IntelligentTieringAIAStorage` : o número de bytes usados para objetos no nível Archive Instant Access da classe de armazenamento `INTELLIGENT_TIERING` . • `IntelligentTieringDAAStorage` : o número de bytes usados para objetos no nível Deep Archive Access da classe de armazenamento `INTELLIGENT_TIERING` .

Dimensão	Descrição
	• `IntelligentTieringFAStorage` : o número de bytes usados para objetos no nível Frequent Access da classe de armazenamento `INTELLIGENT_TIERING` . • `IntelligentTieringIAStorage` : o número de bytes usados para objetos no nível Infrequent Access da classe de armazenamento `INTELLIGENT_TIERING` . • `OneZoneIASizeOverhead` : o número de bytes usados para objetos com menos de 128 KB na classe de armazenam ento `ONEZONE_IA` . • `OneZoneIAStorage` : o número de bytes usados para objetos na classe de armazenamento S3 One Zone-Infrequent Access (`ONEZONE_IA`). • `ReducedRedundancyStorage` : o número de bytes usados para objetos na classe de armazenamento de redundância reduzida (RRS - Reduced Redundancy Storage). • `StandardIASizeOverhead` : o número de bytes usados para objetos com menos de 128 KB na classe de armazenam ento `STANDARD_IA` . • `StandardIAStorage` : o número de bytes usados para objetos na classe de armazenamento S3 Standard-Infrequent Access (`STANDARD_IA`). • `StandardStorage` : o número de bytes usados para objetos na classe de armazenamento `STANDARD`.
`FilterId`	Esta dimensão filtra as configurações de métricas que você especifica para métricas de solicitação em um bucket. Ao criar uma configuração de métricas, especifique um ID de filtro (por exemplo, um prefixo, uma etiqueta ou um ponto de acesso). Para obter mais informações, consulte Criar uma configuração de métricas.

Dimensões da funcionalidade Replicação do S3 no CloudWatch

As seguintes dimensões são usadas para filtrar as métricas da funcionalidade Replicação do S3.

Dimensão	Descrição
`SourceBucket`	O nome do bucket do qual os objetos são replicados.
`DestinationBucket`	O nome do bucket para o qual os objetos são replicados.
`RuleId`	Um identificador exclusivo da regra que acionou a atualização da métrica de replicação.

Dimensões do S3 Storage Lens no CloudWatch

Para obter uma lista das dimensões usadas para filtrar métricas do S3 Storage Lens no CloudWatch, consulte Dimensões.

Dimensões de solicitação do S3 Object Lambda no CloudWatch

As dimensões a seguir são usadas para filtrar dados de um ponto de acesso do Object Lambda.

Dimensão	Descrição
`AccessPointName`	O nome do ponto de acesso do qual as solicitações estão sendo feitas.
`DataSourceARN`	A origem da qual o ponto de acesso do Object Lambda está recuperando os dados. Se a solicitação invocar uma função do Lambda, isso se referirá ao nome do recurso da Amazon (ARN) do Lambda. Caso contrário, isso se refere ao ARN do ponto de acesso.

Métricas de uso do Amazon S3

É possível usar métricas de uso do CloudWatch para fornecer visibilidade sobre o uso de recursos de sua conta. Use essas métricas para visualizar o uso do serviço atual nos gráficos e painéis do CloudWatch.

As métricas de uso do Amazon S3 correspondem às cotas de serviço do AWS. Também é possível configurar alarmes que alertem você quando o uso se aproximar de uma cota de serviço. Para obter mais informações sobre a integração do CloudWatch com o Service Quotas, consulte Métricas de uso da AWS no Guia do usuário do Amazon CloudWatch.

O Amazon S3 publica as métricas a seguir no namespace `AWS/Usage`.

Métrica	Descrição
`ResourceCount`	O número dos recursos especificados em execução em sua conta. Os recursos são definidos pelas dimensões associadas à métrica.

As dimensões a seguir são usadas para refinar as métricas de uso publicadas pelo Amazon S3.

Dimensão	Descrição
`Service`	O nome do serviço da AWS que contém o recurso. Para as métricas de uso do Amazon S3, o valor dessa dimensão é `S3`.
`Type`	O tipo de entidade que está sendo relatado. Atualmente, o único valor válido para métricas de uso do Amazon S3 é `Resource`.
`Resource`	O tipo de recurso que está em execução. Atualmente, o único valor válido para métricas de uso do Amazon S3 é `GeneralPurposeBuckets`, que mostra o número de buckets de uso geral em uma Conta da AWS. Os buckets de uso geral permitem que objetos sejam armazenados em todas as classes de armazenamento, exceto na classe S3 Express One Zone.

Acessar métricas do CloudWatch

Você pode usar os procedimentos a seguir para visualizar as métricas de armazenamento para o Amazon S3. Para obter as métricas do Amazon S3 envolvidas, é necessário definir um timestamp de início e de término. Para métricas para qualquer período de 24 horas, configure o período para 86400 segundos, o número de segundos em um dia. Além disso, lembre de configurar as dimensões `BucketName` e `StorageType`.

Como usar o AWS CLI

Por exemplo, se você quiser usar a AWS CLI para obter a média do tamanho de um bucket específico, em bytes, poderá usar o seguinte comando:

```
aws cloudwatch get-metric-statistics --metric-name BucketSizeBytes --namespace AWS/S3
 --start-time 2016-10-19T00:00:00Z --end-time 2016-10-20T00:00:00Z --statistics Average
 --unit Bytes --region us-west-2 --dimensions Name=BucketName,Value=amzn-s3-demo-bucket
 Name=StorageType,Value=StandardStorage --period 86400 --output json
```

Este exemplo gera a saída a seguir.

```
{
    "Datapoints": [
        {
            "Timestamp": "2016-10-19T00:00:00Z",
            "Average": 1025328.0,
            "Unit": "Bytes"
        }
    ],
    "Label": "BucketSizeBytes"
}
```

Usar o console do S3

Como visualizar as métricas usando o console do Amazon CloudWatch

1. Abra o console do CloudWatch, em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação à esquerda, escolha Metrics.
3. Selecione o namespace S3.
4. (Opcional) Para visualizar uma métrica, insira o nome da métrica na caixa de pesquisa.
5. (Opcional) Para filtrar pela dimensão StorageType, insira o nome de classe de armazenamento na caixa de pesquisa.

Como visualizar uma lista de métricas válidas armazenadas para sua Conta da AWS usando a AWS CLI

- Em um prompt de comando, use o seguinte comando.

```
aws cloudwatch list-metrics --namespace "AWS/S3"
```

Para obter mais informações sobre as permissões necessárias para acessar painéis do CloudWatch, consulte Permissões de painéis do CloudWatch no Guia do usuário do Amazon CloudWatch.

Configurações de métricas do CloudWatch

Com as métricas de solicitação do Amazon CloudWatch para o Amazon S3, você pode receber métricas do CloudWatch de 1 minuto, definir alarmes do CloudWatch e acessar painéis do CloudWatch para visualizar operações quase em tempo real e performance do armazenamento do Amazon S3. Para aplicativos que dependem do armazenamento em nuvem, essas métricas permitem que você identifique rapidamente os problemas operacionais e aja em relação a eles. Quando ativadas, essas métricas de 1 minuto estão disponíveis por padrão no nível do bucket do Amazon S3.

Se quiser obter as métricas de solicitações do CloudWatch para objetos em um bucket, será necessário criar uma configuração de métricas para o bucket. Para obter mais informações, consulte Criar uma configuração de métricas do CloudWatch para todos os objetos em seu bucket.

Você também pode usar um prefixo compartilhado, etiquetas do objeto ou um ponto de acesso para definir um filtro para as métricas coletadas. Esse método de definir um filtro permite que você alinhe filtros de métricas para aplicações de negócios, fluxos de trabalho ou organizações internas específicas. Para obter mais informações, consulte Criação de uma configuração de métricas que filtre por prefixo, etiqueta de objeto ou ponto de acesso. Para obter mais informações sobre as métricas do CloudWatch que estão disponíveis e as diferenças entre métricas de armazenamento e métricas de solicitação, consulte Monitoramento de métricas com o Amazon CloudWatch.

Tenha o seguinte em mente ao usar as configurações de métricas:

- Você pode ter um máximo de 1.000 configurações de métricas por bucket.
- Você pode escolher que objetos em um bucket serão incluídos nas configurações de métricas, utilizando filtros. Você pode filtrar em um prefixo compartilhado, etiqueta de objeto ou ponto de acesso para alinhar filtros de métricas para aplicações de negócios, fluxos de trabalho ou organizações internas específicas. Para métricas de solicitação para todo o bucket, crie uma configuração de métricas sem um filtro.
- As configurações de métricas são necessárias apenas para permitir métricas de solicitação. As métricas diárias de armazenamento ao nível do bucket- estão sempre ativadas e são fornecidas

sem nenhum custo adicional. Atualmente, não é possível obter métricas diárias de armazenamento para um subconjunto filtrado de objetos.

- Cada configuração de métricas permite o conjunto completo de métricas de solicitações disponíveis. As métricas específicas de operações (como `PostRequests`) serão relatadas somente se houver solicitações daquele tipo para o bucket ou filtro.
- As métricas de solicitações são relatadas para todas as operações no nível de objeto. Elas também são informadas para operações que listam o conteúdo do bucket, como GET Bucket (List Objects) [Obter Bucket(listar objetos) , GET Bucket Object Versions (Obter versões de objeto do bucket) e List Multipart Uploads (Listar carregamentos fracionados), mas não são informadas para outras operações em buckets.
- As métricas de solicitações oferecem suporte à filtragem por prefixo, etiquetas do objeto ou ponto de acesso, mas as métricas de armazenamento não.

Entrega de métricas do CloudWatch com o melhor esforço

As métricas do CloudWatch são entregues com base em melhor esforço. A maioria de solicitações para um objeto do Amazon S3 que tenha métricas de solicitações resulta no envio de um ponto de dados ao CloudWatch.

A integridade e pontualidade das métricas não são garantidas. O ponto de dados para uma solicitação específica pode ser retornado com um timestamp posterior à solicitação processada. O ponto de dados de um minuto pode ser atrasado antes de ser disponibilizado pelo CloudWatch ou pode nem ser entregue. As métricas de solicitação do CloudWatch lhe dão uma ideia da natureza do tráfego em seu bucket em tempo quase real. Não se trata de uma contabilidade completa de todas as solicitações.

Devido à natureza de melhor esforço deste recurso, os relatórios disponíveis no Painel de faturamento e de gerenciamento de custo podem incluir uma ou mais solicitações de acesso que não aparecem nas métricas do bucket.

Para obter mais informações sobre como trabalhar com métricas do CloudWatch no Amazon S3, consulte os tópicos a seguir.

Tópicos

- Criar uma configuração de métricas do CloudWatch para todos os objetos em seu bucket
- Criação de uma configuração de métricas que filtre por prefixo, etiqueta de objeto ou ponto de acesso

- Excluir um filtro de métricas

Criar uma configuração de métricas do CloudWatch para todos os objetos em seu bucket

Ao configurar métricas de solicitação, você pode criar uma configuração de métricas do CloudWatch para todos os objetos no bucket ou filtrar por prefixo, etiqueta de objeto ou ponto de acesso. Os procedimentos neste tópico mostram como criar uma configuração para todos os objetos em seu bucket. Para criar uma configuração que filtre por etiqueta de objeto ou prefixo ou ponto de acesso, consulte Criação de uma configuração de métricas que filtre por prefixo, etiqueta de objeto ou ponto de acesso.

Existem três tipos de métricas do Amazon CloudWatch para o Amazon S3: métricas de armazenamento, métricas de solicitação e métricas de replicação. As métricas de armazenamento são relatadas uma vez por dia e fornecidas para todos os clientes sem qualquer custo adicional. As métricas de solicitação estão disponíveis em intervalos de um minuto após alguma latência para processamento. As métricas de solicitação são cobradas na taxa padrão do CloudWatch. Você deve aceitar métricas de solicitação configurando-as no console ou usando a API do Amazon S3. As métricas da funcionalidade Replicação do S3 são métricas detalhadas para as regras de replicação na configuração de replicação. Com as métricas de replicação, você pode monitorar o andamento minuto a minuto rastreando bytes pendentes, operações pendentes, operações com falha na replicação e latência de replicação.

Para obter mais informações sobre métricas do CloudWatch para o Amazon S3, consulte Monitoramento de métricas com o Amazon CloudWatch.

Você pode adicionar configurações de métricas a um bucket usando o console do Amazon S3, a AWS Command Line Interface (AWS CLI) ou a API REST do Amazon S3.

Uso do console do S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets de uso geral.
3. Na lista de buckets, selecione o nome do bucket que contém os objetos para os quais você deseja solicitar métricas.
4. Escolha a guia Metrics.

5. Em Bucket metrics (Métricas de bucket), escolha View additional charts (Exibir gráficos adicionais).
6. Escolha a guia Request metrics (Solicitar métricas) .
7. Escolha Create Filter (Criar filtro).
8. Na caixa Filter name (Nome do filtro) insira o nome do filtro.

   Nomes podem conter apenas letras, números, pontos, traços e sublinhados. Recomendamos usar o nome `EntireBucket` para um filtro que se aplica a todos os objetos.
9. Em Filter scope (Escopo do filtro), escolha This filter applies to all objects in the bucket (Este filtro se aplica a todos os objetos no bucket).

   Você também pode definir um filtro para que as métricas sejam coletadas e relatadas apenas em um subconjunto de objetos no bucket. Para obter mais informações, consulte Criação de uma configuração de métricas que filtre por prefixo, etiqueta de objeto ou ponto de acesso.
10. Escolha Salvar alterações.
11. Na guia Request metrics (métricas de solicitação), em Filters (Filtros), escolha o filtro que você acabou de criar.

    Após cerca de 15 minutos, o CloudWatch começa a rastrear essas métricas de solicitação. Você pode vê-las na guia Request metrics (Métricas de solicitação) . Você pode ver gráficos para as métricas no console do Amazon S3 ou do CloudWatch. As métricas de solicitação são cobradas na taxa padrão do CloudWatch. Para obter mais informações, consulte Definição de preços do Amazon CloudWatch.

Uso dos REST API

Você também pode adicionar configurações de métricas de maneira programática com a API REST do Amazon S3. Para obter mais informações sobre como adicionar e trabalhar com configurações de métricas, consulte os tópicos a seguir na Referência da API do Amazon Simple Storage Service:

- Configuração de métrica PUT Bucket
- Configuração de métrica GET Bucket
- Configuração de métrica List Bucket
- Configuração de métrica DELETE Bucket

Como usar o AWS CLI

1. Instalar e configurar a AWS CLI. Para obter instruções, consulte Instalação, atualização e desinstalação da AWS CLI no Guia do usuário da AWS Command Line Interface.
2. Abra um terminal.
3. Execute o comando a seguir para adicionar uma configuração de métricas.

```
aws s3api put-bucket-metrics-configuration --endpoint https://s3.us-
west-2.amazonaws.com --bucket bucket-name --id metrics-config-id --metrics-
configuration '{"Id":"metrics-config-id"}'
```

Criação de uma configuração de métricas que filtre por prefixo, etiqueta de objeto ou ponto de acesso

Existem três tipos de métricas do Amazon CloudWatch para o Amazon S3: métricas de armazenamento, métricas de solicitação e métricas de replicação. As métricas de armazenamento são relatadas uma vez por dia e fornecidas para todos os clientes sem qualquer custo adicional. As métricas de solicitação estão disponíveis em intervalos de um minuto após alguma latência para processamento. As métricas de solicitação são cobradas na taxa padrão do CloudWatch. Você deve aceitar métricas de solicitação configurando-as no console ou usando a API do Amazon S3. As métricas da funcionalidade Replicação do S3 são métricas detalhadas para as regras de replicação na configuração de replicação. Com as métricas de replicação, você pode monitorar o andamento minuto a minuto rastreando bytes pendentes, operações pendentes, operações com falha na replicação e latência de replicação.

Para obter mais informações sobre métricas do CloudWatch para o Amazon S3, consulte Monitoramento de métricas com o Amazon CloudWatch.

Ao configurar métricas do CloudWatch, você pode criar um filtro para todos os objetos em seu bucket ou filtrar a configuração em grupos de objetos relacionados em um único bucket. Você pode filtrar objetos em um bucket para inclusão em uma configuração de métricas baseada em um ou mais dos seguintes tipos de filtros:

- Prefixo de nome de chave de objeto: embora o modelo de dados do Amazon S3 seja uma estrutura plana, você pode inferir a hierarquia usando um prefixo. O console do Amazon S3 oferece suporte a esses prefixos com o conceito de pastas. Se você filtrar por prefixo, os objetos

com mesmo prefixo serão incluídos na configuração de métricas. Para obter mais informações sobre prefixos, consulte Organizar objetos usando prefixos.

- Etiqueta: você pode adicionar etiquetas que são pares de nome chave-valor, aos objetos. As tags ajudam a encontrar e organizar objetos com facilidade. Você também pode usar etiquetas como filtros para configurações de métricas. Para obter mais informações sobre etiquetas de objeto, consulte Categorizar seu armazenamento usando tags.
- Ponto de acesso: os pontos de acesso são nomeados endpoints de rede que estão conectados a buckets e simplificam o gerenciamento do acesso a dados em escala para conjuntos de dados compartilhados no S3. Quando você cria um filtro de ponto de acesso, o Amazon S3 inclui solicitações ao ponto de acesso que você especifica na configuração de métricas. Para obter mais informações, consulte Monitorar e registrar de pontos de acesso.

> **Note**
>
> Ao criar uma configuração de métricas que filtra por ponto de acesso, você deve usar o ponto de acesso Nome de recurso da Amazon (ARN), não o alias do ponto de acesso. Certifique-se de usar o ARN para o próprio ponto de acesso, não o ARN para um objeto específico. Para obter mais informações sobre ARNs de ponto de acesso, consulte Usar o recurso Pontos de Acesso Amazon S3 para buckets de uso geral.

Se você especificar um filtro, somente solicitações que operem em objetos únicos podem corresponder ao filtro e serem incluídas nas métricas relatadas. Algumas solicitações, como DeleteObjects e `ListObjects`, não exibem nenhuma métrica para configurações com filtros.

Para solicitar uma filtragem mais complexa, escolha dois ou mais elementos. Somente os objetos que têm todos esses elementos são incluídos na configuração de métricas. Se você não definir filtros, todos os objetos no bucket estão incluídos na configuração de métricas.

Uso do console do S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets de uso geral.
3. Na lista de buckets, selecione o nome do bucket que contém os objetos para os quais você deseja solicitar métricas.
4. Escolha a guia Metrics.

5. Em Bucket metrics (Métricas de bucket), escolha View additional charts (Exibir gráficos adicionais).
6. Escolha a guia Request metrics (Solicitar métricas) .
7. Escolha Create Filter (Criar filtro).
8. Na caixa Filter name (Nome do filtro), insira o nome do filtro.

   Nomes podem conter apenas letras, números, pontos, traços e sublinhados.
9. Em Filter scope (Escopo do filtro), escolha Limit the scope of this filter using a prefix, object tags, and an S3 Access Point, or a combination of all three (Limitar o escopo desse filtro usando um prefixo, etiquetas de objeto e um ponto de acesso do S3 ou uma combinação de todos os três).
10. Em Filter type (Tipo de filtro), escolha pelo menos um tipo de filtro: Prefix (Prefixo), Object tags (Etiquetas do objeto) ou Access Point (Ponto de acesso).
11. Para definir um filtro de prefixo e limitar o escopo do filtro a um único caminho, na caixa Prefix (Prefixo), insira um prefixo.
12. Para definir um filtro de etiquetas do objeto, em Object tags (Etiquetas do objeto), selecione Add tag (Adicionar etiqueta) e, em seguida, insira uma Key (Chave) e Value (Valor) da etiqueta.
13. Para definir um filtro de ponto de acesso, no campo S3 Access Point (Ponto de acesso do S3), informe o ARN do ponto de acesso ou escolha Browse S3 (Navegar no S3) para navegar até o ponto de acesso.

    > **Important**
    >
    > Não é possível inserir um alias de ponto de acesso. Você deve inserir o ARN para o próprio ponto de acesso, não o ARN de um objeto específico.
14. Escolha Salvar alterações.

    O Amazon S3 cria um filtro que usa o prefixo, as etiquetas ou o ponto de acesso especificado.
15. Na guia Request metrics (métricas de solicitação), em Filters (Filtros), escolha o filtro que você acabou de criar.

    Agora você criou um filtro que limita o escopo de métricas de solicitação por prefixo, etiquetas de objeto ou ponto de acesso. Cerca de 15 minutos após o CloudWatch começar a rastrear essas métricas de solicitação, você pode ver gráficos para as métricas nos consoles do Amazon S3 e do CloudWatch. As métricas de solicitação são cobradas na taxa padrão do CloudWatch. Para obter mais informações, consulte Definição de preços do Amazon CloudWatch.

Você também pode configurar métricas de solicitação no nível de bucket. Para mais informações, consulte Criar uma configuração de métricas do CloudWatch para todos os objetos em seu bucket.

Como usar o AWS CLI

1. Instalar e configurar a AWS CLI. Para obter instruções, consulte Instalação, atualização e desinstalação da AWS CLI no Guia do usuário da AWS Command Line Interface.
2. Abra um terminal.
3. Para adicionar uma configuração de métricas, execute um dos seguintes comandos:

   Example : para filtrar por prefixo

   ```
   aws s3api put-bucket-metrics-configuration --bucket amzn-s3-demo-bucket --
   id metrics-config-id --metrics-configuration '{"Id":"metrics-config-id", "Filter":
   {"Prefix":"prefix1"}} '
   ```

   Example : para filtrar por etiquetas

   ```
   aws s3api put-bucket-metrics-configuration --bucket amzn-s3-demo-bucket --
   id metrics-config-id --metrics-configuration '{"Id":"metrics-config-id", "Filter":
   {"Tag": {"Key": "string", "Value": "string"}} '
   ```

   Example : para filtrar por ponto de acesso

   ```
   aws s3api put-bucket-metrics-configuration --bucket amzn-s3-demo-bucket --
   id metrics-config-id --metrics-configuration '{"Id":"metrics-config-id", "Filter":
   {"AccessPointArn":"arn:aws:s3:Region:account-id:accesspoint/access-point-name"}} '
   ```

   Example : para filtrar por prefixo, etiquetas e ponto de acesso

   ```
   aws s3api put-bucket-metrics-configuration --endpoint https://
   s3.Region.amazonaws.com --bucket amzn-s3-demo-bucket --id metrics-config-id --
   metrics-configuration '
   {
       "Id": "metrics-config-id",
       "Filter": {
           "And": {
   ```

```
            "Prefix": "string",
            "Tags": [
                {
                    "Key": "string",
                    "Value": "string"
                }
            ],
            "AccessPointArn": "arn:aws:s3:Region:account-id:accesspoint/access-
point-name"
        }
    }
}'
```

Uso da API REST

Você também pode adicionar configurações de métricas de maneira programática com a API REST do Amazon S3. Para obter mais informações sobre como adicionar e trabalhar com configurações de métricas, consulte os tópicos a seguir na Referência da API do Amazon Simple Storage Service:

- Configuração de métrica PUT Bucket
- Configuração de métrica GET Bucket
- Configuração de métrica List Bucket
- Configuração de métrica DELETE Bucket

Excluir um filtro de métricas

Você pode excluir um filtro de métricas de solicitação do Amazon CloudWatch se não precisar mais dele. Ao excluir um filtro, você não será mais cobrado pelas métricas de solicitação que usam esse filtro específico. No entanto, você continuará a ser cobrado por qualquer outra configuração de filtro existente.

Ao excluir um filtro, você não poderá mais usar o filtro para métricas de solicitação. A exclusão de um filtro não pode ser desfeita.

Para obter informações sobre como criar um filtro de métricas de solicitação, consulte os seguintes tópicos:

- Criar uma configuração de métricas do CloudWatch para todos os objetos em seu bucket

- Criação de uma configuração de métricas que filtre por prefixo, etiqueta de objeto ou ponto de acesso

Uso do console do S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets de uso geral.
3. Na lista de buckets, selecione o nome do bucket para o qual você deseja excluir um filtro de solicitação de métricas.
4. Escolha a guia Metrics.
5. Em Bucket metrics (Métricas de bucket), escolha View additional charts (Exibir gráficos adicionais).
6. Escolha a guia Request metrics (Solicitar métricas) .
7. Escolha Manage filters (Gerenciar filtros).
8. Escolha o seu filtro.

> **Important**
>
> A exclusão de um filtro não pode ser desfeita.

9. Escolha Delete.

   O Amazon S3 exclui seu filtro.

Uso dos REST API

Você também pode adicionar configurações de métricas de maneira programática com a API REST do Amazon S3. Para obter mais informações sobre como adicionar e trabalhar com configurações de métricas, consulte os tópicos a seguir na Referência da API do Amazon Simple Storage Service:

- Configuração de métrica PUT Bucket
- Configuração de métrica GET Bucket
- Configuração de métrica List Bucket
- Configuração de métrica DELETE Bucket

Notificações de eventos do Amazon S3

Você pode usar o recurso Notificações de eventos do Amazon S3 para receber notificações quando determinados eventos acontecerem no bucket do S3. Para habilitar notificações, adicione uma configuração de notificação que identifique os eventos que deseja que o Amazon S3 publique. Verifique se ele também identifica os destinos para os quais você deseja que o Amazon S3 envie as notificações. Armazene essa configuração no sub-recurso notification associado a um bucket. Para obter mais informações, consulte opções de configuração de bucket de uso geral. O Amazon S3 fornece uma API para gerenciamento desse sub-recurso.

> **Important**
>
> As notificações de eventos do Amazon S3 são projetadas para serem entregues pelo menos uma vez. Em geral, as notificações de eventos são entregues em segundos, mas, às vezes, podem levar um minuto ou mais.

Visão geral das notificações de eventos do Amazon S3

Atualmente, o Amazon S3 pode publicar notificações para os seguintes eventos:

- Eventos de criação de novos objetos
- Eventos de remoção de objetos
- Eventos de restauração de objetos
- Eventos de perda de objeto com Reduced Redundancy Storage (RRS)
- Eventos de replicação
- Eventos de validade do S3 Lifecycle
- Eventos de transição do S3 Lifecycle
- Eventos de arquivamento automático do S3 Intelligent-Tiering
- Eventos de marcação de objetos
- Eventos PUT de ACL de objeto

Para obter descrições completas de todos os tipos de evento compatíveis, consulte Tipos de evento compatíveis com SQS, SNS e Lambda.

O Amazon S3 pode enviar mensagens de notificação de eventos aos seguintes destinos. Você especifica o valor do nome de recurso da Amazon (ARN) desses destinos na configuração de notificação.

- Amazon Simple Notification Service (Amazon SNS) topics
- Filas do Amazon Simple Queue Service (Amazon SQS)
- Função do AWS Lambda
- Amazon EventBridge

Para obter mais informações, consulte Destinos de eventos suportados.

> **Note**
>
> As filas FIFO (primeiro entrar, primeiro a sair) do Amazon Simple Queue Service não são compatíveis como destino de notificação de evento do Amazon S3. Para enviar uma notificação de um evento do Amazon S3 para uma fila FIFO do Amazon SQS, você pode usar o Amazon EventBridge. Para obter mais informações, consulte Habilitar o Amazon EventBridge.

> **Warning**
>
> Se a notificação for gravada no mesmo bucket que aciona a notificação, isso poderá causar um loop de execução. Por exemplo, se o bucket acionar uma função do Lambda toda vez que houver um upload de objeto, e a função fizer upload de um objeto no bucket, a função será acionada indiretamente. Para evitar isso, use dois buckets ou configure o trigger para só se aplicar a um prefixo usado em objetos recebidos.
> Para obter mais informações e um exemplo de uso de notificações do Amazon S3 com AWS Lambda, consulte Uso do AWS Lambda com o Amazon S3 no Guia do desenvolvedor do AWS Lambda.

Para obter mais informações sobre o número de configurações de notificação de eventos que você pode criar por bucket, consulte Cotas de serviço do Amazon S3 na Referência geral da AWS.

Para obter mais informações sobre notificações de eventos do S3, consulte as seções a seguir.

Tópicos

- Tipos e destinos de notificações de evento
- Usar o Amazon SQS, o Amazon SNS e o Lambda
- Usar o EventBridge

Tipos e destinos de notificações de evento

O Amazon S3 oferece suporte a vários tipos de notificação de eventos e destinos nos quais as notificações podem ser publicadas. Você pode especificar o tipo de evento e o destino ao configurar suas notificações de eventos. Somente um destino pode ser especificado para cada notificação de evento. As notificações de eventos do Amazon S3 enviam uma entrada de evento para cada mensagem de notificação.

Tópicos

- Destinos de eventos suportados
- Tipos de evento compatíveis com SQS, SNS e Lambda
- Tipos de evento compatíveis com o Amazon EventBridge
- Ordenação de eventos e eventos duplicados

Destinos de eventos suportados

O Amazon S3 pode enviar mensagens de notificação de eventos aos seguintes destinos.

- Amazon Simple Notification Service (Amazon SNS) topics
- Filas do Amazon Simple Queue Service (Amazon SQS)
- AWS Lambda
- Amazon EventBridge

No entanto, somente um tipo de destino pode ser especificado para cada notificação de evento.

> **Note**
>
> Você deve conceder ao Amazon S3 permissões para postar mensagens em um tópico do Amazon SNS ou em uma fila do Amazon SQS. Você também deve conceder permissão ao Amazon S3 para invocar uma função do AWS Lambda em seu nome. Para obter instruções

sobre como conceder essas permissões, consulte Conceder permissões para publicar mensagens de notificação de vento a um destino.

Tópico do Amazon SNS

O Amazon SNS é um serviço de mensagens por push flexível e totalmente gerenciado. Você pode usar esse serviço para enviar mensagens por push para dispositivos móveis ou serviços distribuídos. Com o SNS, você pode publicar uma mensagem uma vez e entregá-la uma ou mais vezes. Atualmente, o SNS padrão só é permitido como um destino de notificação de eventos do S3, enquanto o SNS FIFO não é permitido.

O Amazon SNS coordena e gerencia o envio e a entrega de mensagens para endpoints ou clientes assinantes. Você pode usar o console do Amazon SNS para criar um tópico do Amazon SNS para o qual suas notificações podem ser enviadas.

O tópico deve estar na mesma Região da AWS que o bucket do Amazon S3. Para obter instruções sobre como criar um tópico do Amazon SNS, consulte Conceitos básicos do Amazon SNS no Guia do desenvolvedor do Amazon Simple Notification Service e as Perguntas frequentes do Amazon SNS.

Antes de poder usar o tópico do Amazon SNS criado como um destino de notificação de evento, você precisará de:

- O Nome de recurso da Amazon (ARN) do tópico do Amazon SNS
- Uma assinatura válida do tópico do Amazon SNS. Com ela, os assinantes do tópico são notificados quando uma mensagem é publicada em seu tópico do Amazon SNS.

Fila do Amazon SQS

O Amazon SQS oferece filas hospedadas confiáveis e escaláveis para o armazenamento de mensagens à medida que transitam entre computadores. Você pode usar o Amazon SQS para transmitir qualquer volume de dados sem exigir que outros serviços estejam sempre disponíveis. Você pode usar o console do Amazon SQS para criar uma fila do Amazon SQS para a qual suas notificações podem ser enviadas.

A fila do Amazon SQS deve estar na mesma Região da AWS que o bucket do Amazon S3. Para obter instruções sobre como criar uma fila do Amazon SQS, consulte O que é o Amazon Simple

Queue Service e Conceitos básicos do Amazon SQS no Guia do desenvolvedor do Amazon Simple Queue Service.

Antes de poder usar a fila do Amazon SQS como um destino de notificação de evento, você precisa do seguinte:

- O nome do recurso da Amazon (ARN) da fila do Amazon SQS

> **Note**
>
> As filas FIFO (primeiro entrar, primeiro a sair) do Amazon Simple Queue Service não são compatíveis como destino de notificação de evento do Amazon S3. Para enviar uma notificação de um evento do Amazon S3 para uma fila FIFO do Amazon SQS, você pode usar o Amazon EventBridge. Para obter mais informações, consulte Habilitar o Amazon EventBridge.

Função Lambda

É possível usar o AWS Lambda para estender outros produtos da AWS com lógica personalizada ou criar seu próprio backend que opere de acordo com a escala, a performance e a segurança da AWS. Com o Lambda, é possível criar aplicações discretas orientadas por eventos que são executadas somente quando necessário. Você também pode usá-lo para escalar essas aplicações automaticamente de poucas solicitações por dia a milhares por segundo.

O Lambda pode executar código personalizado em resposta a eventos do bucket do Amazon S3. Carregue o código personalizado no Lambda e crie o que é chamado de função Lambda. Quando o Amazon S3 detecta um evento de um tipo específico, ele pode publicar o evento no AWS Lambda e invocar sua função no Lambda. Em resposta, o Lambda executa a função. Um tipo de evento que ele pode detectar, por exemplo, é um evento criado por objeto.

Você pode usar o console do AWS Lambda para criar uma função do Lambda que use a infraestrutura da AWS para executar o código em seu nome. A função do Lambda deve estar na mesma região que seu bucket do S3. Você também deve ter o nome ou o ARN de uma função do Lambda para configurar a função do Lambda como um destino de notificação de evento.

> **Warning**
>
> Se a notificação for gravada no mesmo bucket que aciona a notificação, isso poderá causar um loop de execução. Por exemplo, se o bucket acionar uma função do Lambda toda vez que houver um upload de objeto, e a função fizer upload de um objeto no bucket, a função será acionada indiretamente. Para evitar isso, use dois buckets ou configure o trigger para só se aplicar a um prefixo usado em objetos recebidos.
> Para obter mais informações e um exemplo de uso de notificações do Amazon S3 com AWS Lambda, consulte Uso do AWS Lambda com o Amazon S3 no Guia do desenvolvedor do AWS Lambda.

Amazon EventBridge

O Amazon EventBridge é um barramento de eventos sem servidor, que recebe eventos de produtos da AWS. É possível configurar regras para corresponder a eventos e entregá-los a destinos, como um produto da AWS ou um endpoint de HTTP. Para obter mais informações, consulte O que é o EventBridge no Guia do usuário do Amazon EventBridge.

Ao contrário de outros destinos, você pode habilitar ou desabilitar eventos a serem entregues ao EventBridge para um bucket. Se você habilitar a entrega, todos os eventos serão enviados ao EventBridge. Além disso, você pode usar regras do EventBridge para encaminhar eventos para outros destinos.

Tipos de evento compatíveis com SQS, SNS e Lambda

O Amazon S3 pode publicar eventos dos seguintes tipos. Você especifica esses tipos de evento na configuração de notificação.

Tipos de evento	Descrição
`s3:TestEvent`	Quando uma notificação é habilitada, o Amazon S3 publica uma notificação de teste. Isso serve para verificar se o tópico existe e se o proprietário do bucket tem permissão para publicar o tópico especificado. Se a ativação da notificação falhar, você não receberá a notificação de teste.

Tipos de evento	Descrição

`s3:ObjectCreated:*`
 	
`s3:ObjectCreated:Put`
 	
`s3:ObjectCreated:Post`
 	
`s3:ObjectCreated:Copy`
 	
`s3:ObjectCreated:CompleteMultipartUpload`
	As operações de API do Amazon S3, como PUT, POST e COPY, podem criar um objeto. Com esses tipos de evento, você pode habilitar notificações quando um objeto é criado usando uma operação de API específica. Se preferir, você pode usar o tipo de evento `s3:ObjectCreated:*` para solicitar notificação, qualquer que seja a API usada para criar um objeto.
	
	`s3:ObjectCreated:CompleteMultipartUpload` inclui objetos criados usando UploadPartCopy para operações de cópia.

`s3:ObjectRemoved:*`
 	
`s3:ObjectRemoved:Delete`
 	
`s3:ObjectRemoved:DeleteMarkerCreated`
	Usando os tipos de evento `ObjectRemoved`, é possível habilitar a notificação quando um objeto ou um lote de objetos é removido de um bucket.
	
	Você pode solicitar uma notificação quando um objeto for excluído ou quando um objeto com versionamento for excluído permanentemente usando o tipo de evento `s3:ObjectRemoved:Delete`. Se preferir, você pode solicitar uma notificação quando um marcador de exclusão for criado para um objeto com versionamento usando `s3:ObjectRemoved:DeleteMarkerCreated`. Para obter instruções sobre como excluir objetos com versionamento, consulte Excluir versões de objetos de um bucket com versionamento habilitado. Você também pode usar um caractere curinga `s3:ObjectRemoved:*` para solicitar uma notificação sempre que um objeto for excluído.
	
	Essas notificações de eventos não alertam sobre exclusões automáticas de configurações de ciclo de vida ou operações que falharam.

Tipos de evento	Descrição

`s3:ObjectRestore:*`
 	
`s3:ObjectRestore:Post`
 	
`s3:ObjectRestore:Completed`
 	
`s3:ObjectRestore:Delete`
	Com os tipos de evento `ObjectRestore` , é possível receber notificações de iniciação e conclusão de eventos ao restaurar objetos das classes de armazenamento S3 Glacier Flexible Retrieval, S3 Glacier Deep Archive, nível de acesso S3 Intelligent-Tiering Archive e nível de acesso S3 Intelligent-Tiering Deep Archive. Você também pode receber notificações quando a cópia restaurada de um objeto expirar.
	
	O tipo de evento `s3:ObjectRestore:Post` notifica você sobre o início da restauração de objetos. O tipo de evento `s3:ObjectRestore:Completed` notifica você sobre a conclusão da restauração. O tipo de evento `s3:ObjectRestore:Delete` notifica você quando a cópia temporária de um objeto restaurado expira.

`s3:ReducedRedundancyLostObject`	Você recebe esse evento de notificação quando o Amazon S3 detecta que um objeto da classe de armazenamento RRS foi perdido.

Tipos de evento	Descrição

`s3:Replication:*`
 	
`s3:Replication:OperationFailedReplication`
 	
`s3:Replication:OperationMissedThreshold`
 	
`s3:Replication:OperationReplicatedAfterThreshold`
 	
`s3:Replication:OperationNotTracked`
	Com tipos de evento `Replication` , é possível receber notificações de configurações de replicação com métricas de replicação do S3 ou o Controle de Tempo de Replicação do S3 (S3 RTC) habilitados. Você pode monitorar o progresso minuto a minuto de eventos de replicação, rastreando bytes pendentes, operações pendentes e latência de replicação. Para obter informações sobre métricas de replicação, consulte Monitorar a replicação com métricas, notificações de eventos e status.
	
	• O tipo de evento `s3:Replication:OperationFailedReplication` notifica você quando um objeto qualificado para replicação falhou ao replicar.
	• O tipo de evento `s3:Replication:OperationMissedThreshold` notifica você quando um objeto qualificado para replicação e que usa o S3 RTC excede o limite de 15 minutos para replicação.
	• O tipo de evento `s3:Replication:OperationReplicatedAfterThreshold` notifica você quando um objeto qualificado para replicação e que usa o S3 RTC replica após o limite de 15 minutos.
	• O tipo de evento `s3:Replication:OperationNotTracked` notifica você quando um objeto que era elegível para a replicação em tempo real [Replicação na Mesma Região (SRR) ou Replicação Entre Regiões Diferentes (CRR)] não está mais sendo monitorado por métricas de replicação.

Tipos de evento	Descrição

`s3:LifecycleExpiration:*`
 	
`s3:LifecycleExpiration:Delete`
 	
`s3:LifecycleExpiration:DeleteMarkerCreated`
	Ao usar os tipos de evento `LifecycleExpiration`, você poderá receber uma notificação sempre que o Amazon S3 excluir um objeto com base na configuração de ciclo de vida do S3.
	
	O tipo de evento `s3:LifecycleExpiration:Delete` notifica você quando um objeto em um bucket sem versionamento é excluído. Ele também notifica quando uma versão de objeto é excluída permanentemente por uma configuração do S3 Lifecycle. O tipo de evento `s3:LifecycleExpiration:DeleteMarkerCreated` notifica você quando o S3 Lifecycle cria um marcador de exclusão quando uma versão atual de um objeto no bucket com versionamento é excluída.

`s3:LifecycleTransition`	Você recebe esse evento de notificação quando um objeto é transferido para outra classe de armazenamento do Amazon S3 por uma configuração do S3 Lifecycle.
`s3:IntelligentTiering`	Você recebe esse evento de notificação quando um objeto dentro da classe de armazenamento S3 Intelligent-Tiering for movido para o nível de acesso de arquivo ou para o nível de acesso de arquivo profundo.

`s3:ObjectTagging:*`
 	
`s3:ObjectTagging:Put`
 	
`s3:ObjectTagging:Delete`
	Usando os tipos de evento `ObjectTagging`, é possível habilitar a notificação quando uma tag de objeto é adicionada ou excluída de um objeto.
	
	O tipo de evento `s3:ObjectTagging:Put` notifica você quando ocorre PUT de uma etiqueta em um objeto ou quando uma etiqueta existente é atualizada. O tipo de evento `s3:ObjectTagging:Delete` notifica você quando uma etiqueta é removida de um objeto.

Tipos de evento	Descrição
`s3:ObjectAcl:Put`	Você recebe esse evento de notificação quando ocorre PUT de uma ACL em um objeto ou quando uma ACL existente é alterada. Não é gerado evento quando uma solicitação não resulta em alteração na ACL de um objeto.

Tipos de evento compatíveis com o Amazon EventBridge

Para obter uma lista de tipos de eventos que o Amazon S3 enviará ao Amazon EventBridge, consulte Usar o EventBridge.

Ordenação de eventos e eventos duplicados

As notificações de eventos do Amazon S3 foram projetadas para entregar notificações pelo menos um dia, mas não há garantia de que cheguem na mesma ordem em que os eventos ocorreram. Em raras ocasiões, o mecanismo de nova tentativa do Amazon S3 pode causar notificações de eventos do S3 duplicadas para o mesmo evento de objeto. Consulte mais informações sobre como lidar com eventos duplicados ou fora de ordem em Manage event ordering and duplicate events with Amazon S3 Event Notifications no Blog de armazenamento do AWS.

Usar o Amazon SQS, o Amazon SNS e o Lambda

A habilitação de notificações é uma operação no nível do bucket. Você armazena informações de configuração de notificação no sub-recurso de notificação que está associado a um bucket. Depois que você cria ou altera a configuração de notificação de bucket, normalmente é necessário aguardar cinco minutos para que as alterações entrem em vigor. Ocorre um `s3:TestEvent` quando a notificação é habilitada pela primeira vez. Você pode usar qualquer um dos métodos a seguir para gerenciar a configuração de notificação:

- Usar o console do Amazon S3: você pode usar a interface de usuário do console para definir uma configuração de notificação em um bucket sem ter que escrever nenhum código. Para obter mais informações, consulte Habilitar e configurar notificações de eventos usando o console do Amazon S3.
- Uso dos AWS SDKs de forma programática: internamente, tanto o console como os SDKs chamam a API REST do Amazon S3 para gerenciar sub-recursos de notificação que estão associados ao bucket. Para obter exemplos de configurações de notificação usando exemplos do

AWS SDK, consulte Demonstração: configurar um bucket para notificações (tópico do SNS ou fila do SQS).

> **Note**
>
> Você também pode fazer chamadas de API REST do Amazon S3 diretamente do seu código. Porém, isso pode ser complicado, porque é necessário gravar o código para autenticar suas solicitações.

Independentemente do método usado, o Amazon S3 armazena a configuração de notificação como XML no sub-recurso notification (notificação) que está associado a um bucket. Para obter informações sobre sub-recursos de bucket, consulte opções de configuração de bucket de uso geral.

> **Note**
>
> Se você tiver várias notificações de eventos de falha devido a destinos excluídos, poderá receber a mensagem Não é possível validar as seguintes configurações de destino ao tentar excluí-las. É possível resolver isso no console do S3 excluindo todas as notificações de falha ao mesmo tempo.

Tópicos

- Conceder permissões para publicar mensagens de notificação de vento a um destino
- Habilitar e configurar notificações de eventos usando o console do Amazon S3
- Configuração de notificações de eventos de forma programática
- Demonstração: configurar um bucket para notificações (tópico do SNS ou fila do SQS)
- Configurar notificações de eventos usando filtragem de nomes de chave de objeto
- Estrutura de mensagens de evento

Conceder permissões para publicar mensagens de notificação de vento a um destino

É necessário garantir à entidade principal do Amazon S3 as permissões necessárias para chamar a API relevante para publicar mensagens em um tópico do SNS, uma fila do SQS ou uma função Lambda. Isso serve para que o Amazon S3 possa publicar mensagens de notificação de eventos em um destino.

Para solucionar problemas de publicação de mensagens de notificação de eventos em um destino, consulte Solução de problemas para publicar notificações de eventos do Amazon S3 em um tópico do Amazon Simple Notification Service.

Tópicos

- Conceder permissões para invocar uma função do AWS Lambda
- Conceder permissões para publicar mensagens em um tópico do SNS ou em uma fila do SQS

Conceder permissões para invocar uma função do AWS Lambda

O Amazon S3 publica mensagens de eventos no AWS Lambda invocando uma função do Lambda e fornecendo a mensagem de evento como um argumento.

Ao usar o console do Amazon S3 para configurar notificações de eventos em um bucket do Amazon S3 para uma função do Lambda, o console configurará as permissões necessárias na função Lambda. Isso ocorre para que o Amazon S3 tenha permissões para invocar a função do bucket. Para obter mais informações, consulte Habilitar e configurar notificações de eventos usando o console do Amazon S3.

Você também pode conceder permissões do Amazon S3 do AWS Lambda para invocar a função do Lambda. Para obter mais informações, consulte Tutorial: uso do AWS Lambda com o Amazon S3 no Guia do desenvolvedor do AWS Lambda.

Conceder permissões para publicar mensagens em um tópico do SNS ou em uma fila do SQS

Para conceder ao Amazon S3 permissões para publicar mensagens em um tópico do SNS ou uma fila do SQS, anexe uma política do AWS Identity and Access Management (IAM) ao tópico do SNS ou à fila do SQS de destino.

Para obter um exemplo de como anexar uma política a um tópico do SNS ou a uma fila do SQS, consulte Demonstração: configurar um bucket para notificações (tópico do SNS ou fila do SQS). Para obter mais informações sobre permissões, consulte os tópicos a seguir:

- Exemplos de casos de controle de acesso do Amazon SNS no Guia do desenvolvedor do Amazon Simple Notification Service
- Gerenciamento de identidade e acesso no Amazon SQS no Guia do desenvolvedor do Amazon Simple Queue Service

Política do IAM para um tópico do SNS de destino

Veja a seguir um exemplo de uma política do AWS Identity and Access Management (IAM) anexada ao tópico do SNS de destino. Para obter mais instruções sobre como usar essa política para configurar um tópico do Amazon SNS de destino para notificações de eventos, consulte Demonstração: configurar um bucket para notificações (tópico do SNS ou fila do SQS).

```
{
    "Version": "2012-10-17",
    "Id": "example-ID",
    "Statement": [
        {
            "Sid": "Example SNS topic policy",
            "Effect": "Allow",
            "Principal": {
                "Service": "s3.amazonaws.com"
            },
            "Action": [
                "SNS:Publish"
            ],
            "Resource": "SNS-topic-ARN",
            "Condition": {
                "ArnEquals": {
                    "aws:SourceArn": "arn:aws:s3:::amzn-s3-demo-bucket"
                },
                "StringEquals": {
                    "aws:SourceAccount": "bucket-owner-account-id"
                }
            }
        }
    ]
}
```

Política do IAM para uma fila do SQS de destino

Veja a seguir um exemplo de uma política do IAM anexada à fila do SQS de destino. Para obter mais instruções sobre como usar essa política para configurar uma fila do Amazon SQS de destino para notificações de eventos, consulte Demonstração: configurar um bucket para notificações (tópico do SNS ou fila do SQS).

Para usar essa política, você deve atualizar o ARN da fila do Amazon SQS, o nome do bucket e o ID da Conta da AWS do proprietário do bucket.

```
{
    "Version": "2012-10-17",
    "Id": "example-ID",
    "Statement": [
        {
            "Sid": "example-statement-ID",
            "Effect": "Allow",
            "Principal": {
                "Service": "s3.amazonaws.com"
            },
            "Action": [
                "SQS:SendMessage"
            ],
            "Resource": "arn:aws:sqs:Region:account-id:queue-name",
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:s3:*:*:awsexamplebucket1"
                },
                "StringEquals": {
                    "aws:SourceAccount": "bucket-owner-account-id"
                }
            }
        }
    ]
}
```

Tanto para as políticas do IAM do Amazon SNS e do Amazon SQS, você pode especificar a condição `StringLike` na política, em vez da condição `ArnLike`.

Quando o `ArnLike` é usado, as partes partição, serviço, ID da conta, tipo de recurso e ID parcial do recurso do ARN devem ter a correspondência exata com o ARN no contexto da solicitação. Somente a região e o caminho do recurso permitem a correspondência parcial.

Quando `StringLike` é usado em vez de `ArnLike`, a correspondência ignora a estrutura do ARN e permite a correspondência parcial, independentemente da parte que foi marcada como curinga. Para obter mais informações, consulte Elementos de política JSON do IAM no Guia do usuário do IAM.

```
"Condition": {
  "StringLike": { "aws:SourceArn": "arn:aws:s3:*:*:amzn-s3-demo-bucket" }
  }
```

Política de chave do AWS KMS

Se a fila do SQS ou os tópicos do SNS estiverem criptografados com uma chave gerenciada pelo cliente do AWS Key Management Service (AWS KMS), será necessário conceder permissão para que a entidade de serviço do Amazon S3 trabalhe com a fila ou os tópicos criptografados. Para conceder a permissão à entidade de serviço do Amazon S3, adicione a instrução a seguir à política de chave para a chave gerenciada pelo cliente.

```
{
    "Version": "2012-10-17",
    "Id": "example-ID",
    "Statement": [
        {
            "Sid": "example-statement-ID",
            "Effect": "Allow",
            "Principal": {
                "Service": "s3.amazonaws.com"
            },
            "Action": [
                "kms:GenerateDataKey",
                "kms:Decrypt"
            ],
            "Resource": "*"
        }
    ]
}
```

Para obter mais informações sobre políticas de chave do AWS KMS, consulte Uso de políticas de chave no AWS KMS no Guia do desenvolvedor do AWS Key Management Service.

Para obter mais informações sobre como usar a criptografia no lado do servidor com o AWS KMS para o Amazon SQS e o Amazon SNS, consulte:

- Gerenciamento de chaves no Guia do desenvolvedor do Amazon Simple Notification Service.
- Gerenciamento de chaves no Guia do desenvolvedor do Amazon Simple Queue Service.
- Criptografia de mensagens publicadas no Amazon SNS com o AWS KMS no Blog de computação da AWS.

Habilitar e configurar notificações de eventos usando o console do Amazon S3

Você pode habilitar certos eventos de bucket de uso geral do Amazon S3 para enviar uma mensagem de notificação a um destino sempre que ocorrer um desses eventos. Esta seção explica como usar o console do Amazon S3 para habilitar notificações de evento. Para obter informações sobre como usar notificações de eventos com os AWS SDKs e as APIs REST do Amazon S3, consulte Configuração de notificações de eventos de forma programática.

Pré-requisitos: antes de habilitar as notificações de eventos para seu bucket, você deve configurar um dos tipos de destino e, em seguida, configurar permissões. Para obter mais informações, consulte Destinos de eventos suportados e Conceder permissões para publicar mensagens de notificação de vento a um destino.

> **Note**
>
> As filas FIFO (primeiro entrar, primeiro a sair) do Amazon Simple Queue Service não são compatíveis como destino de notificação de evento do Amazon S3. Para enviar uma notificação de um evento do Amazon S3 para uma fila FIFO do Amazon SQS, você pode usar o Amazon EventBridge. Para obter mais informações, consulte Habilitar o Amazon EventBridge.

Tópicos

- Habilitar notificações do Amazon SNS, Amazon SQS ou Lambda usando o console do Amazon S3

Habilitar notificações do Amazon SNS, Amazon SQS ou Lambda usando o console do Amazon S3

Para habilitar e configurar notificações de evento para um bucket do S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets de uso geral.
3. Na lista de buckets, escolha o nome do bucket para o qual você deseja habilitar eventos.
4. Escolha Properties (Propriedades).
5. Navegue até a seção Event Notifications (Notificações de eventos) e escolha Create event notification (Criar notificação de evento).

6. Na seção General configuration (Configuração geral), especifique o nome do evento descritivo para sua notificação de evento. Opcionalmente, você também pode especificar um prefixo e um sufixo para limitar as notificações a objetos com chaves terminando nos caracteres especificados.

   a. Insira uma descrição para o Event name (Nome do evento).

      Se você não inserir um nome, um identificador exclusivo global (GUID) será gerado e usado para o nome.

   b. (Opcional) Para filtrar notificações de eventos por prefixo, insira um Prefix (Prefixo).

      Por exemplo, é possível configurar um filtro de prefixo para receber notificações somente quando os arquivos são adicionados a uma pasta específica (por exemplo, `images/`).

   c. (Opcional) Para filtrar notificações de eventos por sufixo, insira um Suffix (Sufixo).

      Para obter mais informações, consulte Configurar notificações de eventos usando filtragem de nomes de chave de objeto.

7. Na seção Event types (Tipos de evento), selecione um ou mais tipos de eventos para os quais você deseja receber notificações.

   Para obter uma lista dos diferentes tipos de evento, consulte Tipos de evento compatíveis com SQS, SNS e Lambda.

8. Na seção Destination (Destino), escolha o destino da notificação de evento.

   > **Note**
   >
   > Antes de publicar notificações de eventos, você deve conceder à entidade principal do Amazon S3 as permissões necessárias para chamar a API relevante. Desse modo, ela pode publicar notificações em uma função Lambda, tópico do SNS ou fila SQS.

   a. Selecione o tipo de destino: Lambda Function (Função do Lambda), SNS Topic (Tópico do SNS) ou SQS Queue (Fila do SQS).

   b. Depois de escolher o tipo de destino, escolha uma função, um tópico ou uma fila na lista.

   c. Como alternativa, se você preferir especificar um nome de recurso da Amazon (ARN), selecione Enter ARN (Inserir ARN) e insira o ARN.

Para obter mais informações, consulte Destinos de eventos suportados.

9. Escolha Save changes (Salvar alterações) e o Amazon S3 enviará uma mensagem de teste para o destino de notificação de evento.

Configuração de notificações de eventos de forma programática

Por padrão, as notificações não estão habilitadas para nenhum tipo de evento. Portanto, o sub-recurso notification (notificação) armazena inicialmente uma configuração vazia.

```
<NotificationConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
</NotificationConfiguration>
```

Para habilitar notificações para eventos de tipos específicos, você substitui o XML pela configuração apropriada que identifica os tipos de evento que deseja que o Amazon S3 publique e o destino onde deseja que os eventos sejam publicados. Para cada destino, você adiciona uma configuração correspondente de XML.

Para publicar mensagens de eventos em uma fila do SQS

Para definir uma fila do SQS como o destino de notificação para um ou mais tipos de evento, adicione o `QueueConfiguration`.

```
<NotificationConfiguration>
  <QueueConfiguration>
    <Id>optional-id-string</Id>
    <Queue>sqs-queue-arn</Queue>
    <Event>event-type</Event>
    <Event>event-type</Event>
     ...
  </QueueConfiguration>
   ...
</NotificationConfiguration>
```

Para publicar mensagens de eventos em um tópico do SNS

Para definir um tópico do SNS como o destino de notificação para tipos de eventos específicos, adicione o `TopicConfiguration`.

```
<NotificationConfiguration>
  <TopicConfiguration>
     <Id>optional-id-string</Id>
     <Topic>sns-topic-arn</Topic>
     <Event>event-type</Event>
     <Event>event-type</Event>
      ...
  </TopicConfiguration>
   ...
</NotificationConfiguration>
```

Para invocar a função do AWS Lambda e fornecer uma mensagem de evento como um argumento

Para definir uma função do Lambda como o destino de notificação para tipos de evento específicos, adicione o `CloudFunctionConfiguration`.

```
<NotificationConfiguration>
  <CloudFunctionConfiguration>
     <Id>optional-id-string</Id>
     <CloudFunction>cloud-function-arn</CloudFunction>
     <Event>event-type</Event>
     <Event>event-type</Event>
      ...
  </CloudFunctionConfiguration>
   ...
</NotificationConfiguration>
```

Para remover todas as notificações configuradas em um bucket

Para remover todas as notificações configuradas em um bucket, salve um elemento `<NotificationConfiguration/>` vazio no sub-recurso notificação.

Quando o Amazon S3 detecta um evento do tipo específico, ele publica uma mensagem com as informações do evento. Para obter mais informações, consulte Estrutura de mensagens de evento.

Para obter mais informações sobre como configurar notificações de eventos, consulte os seguintes tópicos:

- Demonstração: configurar um bucket para notificações (tópico do SNS ou fila do SQS).
- Configurar notificações de eventos usando filtragem de nomes de chave de objeto

Demonstração: configurar um bucket para notificações (tópico do SNS ou fila do SQS)

Você pode receber notificações do Amazon S3 usando o Amazon Simple Notification Service (Amazon SNS) ou o Amazon Simple Queue Service (Amazon SQS). Nesta demonstração, você adiciona uma configuração de notificação ao seu bucket usando um tópico do Amazon SNS e uma fila do Amazon SQS.

> **Note**
>
> As filas FIFO (primeiro entrar, primeiro a sair) do Amazon Simple Queue Service não são compatíveis como destino de notificação de evento do Amazon S3. Para enviar uma notificação de um evento do Amazon S3 para uma fila FIFO do Amazon SQS, você pode usar o Amazon EventBridge. Para obter mais informações, consulte Habilitar o Amazon EventBridge.

Tópicos

- Resumo da demonstração
- Etapa 1: Criar uma fila do Amazon SQS
- Etapa 2: Criar um tópico do Amazon SNS
- Etapa 3: Adicionar a configuração de notificação para o bucket
- Etapa 4: Testar a configuração

Resumo da demonstração

Esta demonstração ajuda você a fazer o seguinte:

- Publicar eventos do tipo `s3:ObjectCreated:*` em uma fila do Amazon SQS.
- Publicar eventos do tipo `s3:ReducedRedundancyLostObject` em um tópico do Amazon SNS.

Para obter informações sobre configuração de notificação, consulte Usar o Amazon SQS, o Amazon SNS e o Lambda.

Você pode executar todas essas etapas usando o console, sem escrever nenhum código. Além disso, exemplos de código, que usam os AWS SDKs para Java e .NET, também são fornecidos para ajudar a adicionar configurações de notificação de maneira programática.

Este procedimento inclui as seguintes etapas:

1. Crie uma fila do Amazon SQS.

   Usando o console do Amazon SQS, crie uma fila do SQS. É possível acessar todas as mensagens que o Amazon S3 envia à fila de forma programática. Porém, para esta demonstração, verifique as mensagens de notificação no console.

   Anexe uma política de acesso à fila para conceder ao Amazon S3 permissão para postar mensagens.
2. Crie um tópico do Amazon SNS.

   Usando o console do Amazon SNS, crie um tópico do SNS e assine o tópico. Assim, todos os eventos postados nele são entregues a você. Especifique o e-mail como o protocolo de comunicações. Depois de criar um tópico, o Amazon SNS envia um e-mail. Use o link no e-mail para confirmar a assinatura do tópico.

   Anexe uma política de acesso ao tópico para conceder ao Amazon S3 permissão para postar mensagens.
3. Adicione a configuração de notificação a um bucket.

Etapa 1: Criar uma fila do Amazon SQS

Siga as etapas para criar e assinar uma fila do Amazon Simple Queue Service (Amazon SQS).

1. Usando o console do Amazon SQS, crie uma fila. Para obter instruções, consulte Conceitos básicos do Amazon SQS no Guia do desenvolvedor do Amazon Simple Queue Service.
2. Substitua a política de acesso que está anexada à fila pela política a seguir.

   a. No console do Amazon SQS, na lista Queues (Filas), escolha o nome da fila.

   b. Na guia Access policy (Política de acesso), escolha Edit (Editar).

   c. Substitua a política de acesso que está anexada à fila. Nele, forneça o ARN do Amazon SQS, o nome do bucket de origem e o ID da conta do proprietário do bucket.

```
{
    "Version": "2012-10-17",
    "Id": "example-ID",
    "Statement": [
        {
```

```
            "Sid": "example-statement-ID",
            "Effect": "Allow",
            "Principal": {
                "Service": "s3.amazonaws.com"
            },
            "Action": [
                "SQS:SendMessage"
            ],
            "Resource": "SQS-queue-ARN",
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:s3:*:*:awsexamplebucket1"
                },
                "StringEquals": {
                    "aws:SourceAccount": "bucket-owner-account-id"
                }
            }
        }
    ]
}
```

d. Escolha Salvar.

3. (Opcional) Se a fila do Amazon SQS ou o tópico do Amazon SNS for habilitado para criptografia no lado do servidor com o AWS Key Management Service (AWS KMS), adicione a política a seguir à chave de criptografia simétrica correspondente gerenciada pelo cliente.

   Adicione a política a uma chave gerenciada pelo cliente porque você não pode modificar a chave gerenciada pela AWS para o Amazon SQS ou o Amazon SNS.

```
{
    "Version": "2012-10-17",
    "Id": "example-ID",
    "Statement": [
        {
            "Sid": "example-statement-ID",
            "Effect": "Allow",
            "Principal": {
                "Service": "s3.amazonaws.com"
            },
            "Action": [
                "kms:GenerateDataKey",
                "kms:Decrypt"
            ],
```

```
            "Resource": "*"
        }
    ]
}
```

Para obter mais informações sobre como usar o SSE para o Amazon SQS e o Amazon SNS com o AWS KMS, consulte:

- Gerenciamento de chaves no Guia do desenvolvedor do Amazon Simple Notification Service.
- Gerenciamento de chaves no Guia do desenvolvedor do Amazon Simple Queue Service.

4. Anotar o ARN da fila.

   A fila do SQS que você criou é outro recurso em sua Conta da AWS. Ele tem um nome do recurso da Amazon (ARN) exclusivo. Esse ARN será necessário na próxima etapa. O ARN tem este formato:

   ```
   arn:aws:sqs:aws-region:account-id:queue-name
   ```

Etapa 2: Criar um tópico do Amazon SNS

Siga as etapas para criar e assinar um tópico do Amazon SNS.

1. Usando o console do Amazon SNS, crie um tópico. Para obter instruções, consulte Criação de um tópico do Amazon SNS no Guia do desenvolvedor do Amazon Simple Notification Service.
2. Inscreva-se no tópico. Neste exercício, use o e-mail como o protocolo de comunicação. Para obter instruções, consulte Assinatura de um tópico do Amazon SNS no Guia do desenvolvedor do Amazon Simple Notification Service.

   Você receberá um e-mail solicitando a confirmação da assinatura do tópico. Confirme a assinatura.
3. Substitua a política de acesso anexada ao tópico pela seguinte política. Nele, forneça o ARN do tópico SNS, o nome do bucket de origem e o ID da conta do proprietário do bucket.

   ```
   {
       "Version": "2012-10-17",
       "Id": "example-ID",
       "Statement": [
           {
   ```

```
            "Sid": "Example SNS topic policy",
            "Effect": "Allow",
            "Principal": {
                "Service": "s3.amazonaws.com"
            },
            "Action": [
                "SNS:Publish"
            ],
            "Resource": "SNS-topic-ARN",
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:s3:*:*:amzn-s3-demo-bucket"
                },
                "StringEquals": {
                    "aws:SourceAccount": "bucket-owner-account-id"
                }
            }
        }
    ]
}
```

4. Anote o ARN do tópico.

   O tópico do SNS que você criou é outro recurso em sua Conta da AWS e tem um ARN exclusivo. Você precisará desse ARN na próxima etapa. O ARN terá o seguinte formato:

   ```
   arn:aws:sns:aws-region:account-id:topic-name
   ```

Etapa 3: Adicionar a configuração de notificação para o bucket

Você pode habilitar notificações de bucket usando o console do Amazon S3 ou de forma programática usando os AWS SDKs. Escolha qualquer uma das opções para configurar notificações no bucket. Esta seção fornece exemplos de código que usam os AWS SDKs para Java e .NET.

Opção A: habilitar notificações em um bucket usando o console

Usando o console do Amazon S3, adicione uma configuração de notificação solicitando que o Amazon S3 faça o seguinte:

- Publique eventos do tipo Todos os eventos criados por objetos na fila do Amazon SQS.
- Publique eventos do tipo Objeto em RRS perdido no tópico do Amazon SNS.

Depois de salvar a configuração de notificação, o Amazon S3 posta uma mensagem de teste, que você recebe via e-mail.

Para instruções, consulte Habilitar e configurar notificações de eventos usando o console do Amazon S3.

Opção B: habilitar notificações em um bucket usando os AWS SDKs

.NET

O exemplo de código C# a seguir fornece uma lista completa de códigos que adicionam uma configuração de notificação a um bucket. Você deve atualizar o código e fornecer o nome do bucket e o ARN do tópico do SNS. Para obter informações sobre como configurar e executar exemplos de código, consulte Conceitos básicos do AWS SDK for .NET no Guia do desenvolvedor do AWS SDK for .NET.

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Collections.Generic;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class EnableNotificationsTest
    {
        private const string bucketName = "*** bucket name ***";
        private const string snsTopic = "*** SNS topic ARN ***";
        private const string sqsQueue = "*** SQS topic ARN ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 client;

        public static void Main()
        {
            client = new AmazonS3Client(bucketRegion);
            EnableNotificationAsync().Wait();
        }

        static async Task EnableNotificationAsync()
        {
```

```
            try
            {
               PutBucketNotificationRequest request = new
 PutBucketNotificationRequest
                {
                    BucketName = bucketName
                };

                TopicConfiguration c = new TopicConfiguration
                {
                    Events = new List<EventType> { EventType.ObjectCreatedCopy },
                    Topic = snsTopic
                };
                request.TopicConfigurations = new List<TopicConfiguration>();
                request.TopicConfigurations.Add(c);
                request.QueueConfigurations = new List<QueueConfiguration>();
                request.QueueConfigurations.Add(new QueueConfiguration()
                {
                    Events = new List<EventType> { EventType.ObjectCreatedPut },
                    Queue = sqsQueue
                });

                PutBucketNotificationResponse response = await
 client.PutBucketNotificationAsync(request);
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered on server. Message:'{0}' ",
 e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine("Unknown error encountered on server.
 Message:'{0}' ", e.Message);
            }
        }
    }
}
```

Java

O seguinte exemplo mostra como adicionar uma configuração de notificação a um bucket. Consulte instruções sobre como criar e testar uma amostra funcional em Getting Started no Guia do desenvolvedor do AWS SDK para Java.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.*;

import java.io.IOException;
import java.util.EnumSet;

public class EnableNotificationOnABucket {

    public static void main(String[] args) throws IOException {
        String bucketName = "*** Bucket name ***";
        Regions clientRegion = Regions.DEFAULT_REGION;
        String snsTopicARN = "*** SNS Topic ARN ***";
        String sqsQueueARN = "*** SQS Queue ARN ***";

        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(clientRegion)
                    .build();
            BucketNotificationConfiguration notificationConfiguration = new
 BucketNotificationConfiguration();

            // Add an SNS topic notification.
            notificationConfiguration.addConfiguration("snsTopicConfig",
                    new TopicConfiguration(snsTopicARN,
 EnumSet.of(S3Event.ObjectCreated)));

            // Add an SQS queue notification.
            notificationConfiguration.addConfiguration("sqsQueueConfig",
                    new QueueConfiguration(sqsQueueARN,
 EnumSet.of(S3Event.ObjectCreated)));
```

```
            // Create the notification configuration request and set the bucket
 notification
            // configuration.
            SetBucketNotificationConfigurationRequest request = new
 SetBucketNotificationConfigurationRequest(
                    bucketName, notificationConfiguration);
            s3Client.setBucketNotificationConfiguration(request);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Etapa 4: Testar a configuração

Agora você pode testar a configuração carregando um objeto no bucket e verificando a notificação de evento no console do Amazon SQS. Para obter instruções, consulte Receber uma mensagem na seção “Conceitos básicos” do Guia do desenvolvedor do Amazon Simple Queue Service.

Configurar notificações de eventos usando filtragem de nomes de chave de objeto

Ao configurar uma notificação de evento do Amazon S3, você deve especificar quais tipos de evento suportados do Amazon S3 fazem com que o Amazon S3 envie a notificação. Se um tipo de evento que você não especificou ocorrer no bucket do S3, o Amazon S3 não enviará a notificação.

Você pode configurar as notificações para serem filtradas pelo prefixo e pelo sufixo do nome da chave de objetos. Por exemplo, é possível definir uma configuração para que uma notificação seja enviada para você apenas quando arquivos de imagem com uma extensão de nome de arquivo "`.jpg`" forem adicionados a um bucket. Ou ter uma configuração que entregue uma notificação a um tópico do Amazon SNS quando um objeto com o prefixo "`images/`" for adicionado ao bucket, e fazer com que notificações para objetos com um prefixo "`logs/`" no mesmo bucket sejam entregues a uma função do AWS Lambda.

> **Note**
>
> Um caractere curinga (“*”) não pode ser usado em filtros como um prefixo ou sufixo. Se seu prefixo ou sufixo contiver um espaço, você deverá substituí-lo pelo caractere “+”. Se você usar qualquer outro caractere especial no valor do prefixo ou sufixo, deverá inseri-los no formato codificado em URL (codificado em porcentagem). Para obter uma lista completa de caracteres especiais que devem ser convertidos em formato codificado em URL quando usados em um prefixo ou sufixo para notificações de eventos, consulte Caracteres seguros.

É possível definir configurações de notificação que usem filtro de nomes de chaves de objetos no console do Amazon S3. Você pode fazer isso usando as APIs do Amazon S3 por meio dos AWS SDKs ou das APIs REST diretamente. Para obter informações sobre como usar a interface do usuário do console para definir uma configuração de notificação em um bucket, consulte Habilitar e configurar notificações de eventos usando o console do Amazon S3.

O Amazon S3 armazena a configuração de notificação como XML no sub-recurso notificação associado a um bucket, conforme descrito em Usar o Amazon SQS, o Amazon SNS e o Lambda. Use a estrutura XML do `Filter` para definir regras para que as notificações sejam filtradas pelo prefixo ou pelo sufixo do nome da chave de um objeto. Para obter informações sobre a estrutura XML `Filter`, consulte Notificação de PUT Bucket na Referência da API do Amazon Simple Storage Service.

Configurações de notificação que usam o `Filter` não podem definir regras de filtragem com prefixos sobrepostos, sufixos sobrepostos ou prefixos e sufixos sobrepostos. As seções a seguir têm exemplos de configurações de notificação válidas com filtragem de nome de chave de objeto. Elas também contêm exemplos de configurações de notificação que não são válidas devido à sobreposição de prefixo e sufixo.

Tópicos

- Exemplos de configurações válidas de notificação com filtragem de nome de chave de objeto
- Exemplos de configurações de notificação com sobreposição inválida de prefixo e sufixo

Exemplos de configurações válidas de notificação com filtragem de nome de chave de objeto

A configuração de notificação a seguir contém uma configuração de fila que identifica uma fila do Amazon SQS para a qual o Amazon S3 publica eventos do tipo `s3:ObjectCreated:Put`. Os

eventos são publicados sempre que um objeto que tenha um prefixo `images/` e um sufixo `jpg` é PUT em um bucket.

```
<NotificationConfiguration>
  <QueueConfiguration>
      <Id>1</Id>
      <Filter>
          <S3Key>
              <FilterRule>
                  <Name>prefix</Name>
                  <Value>images/</Value>
              </FilterRule>
              <FilterRule>
                  <Name>suffix</Name>
                  <Value>jpg</Value>
              </FilterRule>
          </S3Key>
     </Filter>
     <Queue>arn:aws:sqs:us-west-2:444455556666:s3notificationqueue</Queue>
     <Event>s3:ObjectCreated:Put</Event>
  </QueueConfiguration>
</NotificationConfiguration>
```

A configuração de notificação a seguir tem vários prefixos não sobrepostos. A configuração define que as notificações para solicitações PUT na pasta `images/` vão para a fila A, enquanto as notificações para solicitações PUT na pasta `logs/` vão para a fila B.

```
<NotificationConfiguration>
  <QueueConfiguration>
     <Id>1</Id>
     <Filter>
            <S3Key>
                <FilterRule>
                    <Name>prefix</Name>
                    <Value>images/</Value>
                </FilterRule>
            </S3Key>
     </Filter>
     <Queue>arn:aws:sqs:us-west-2:444455556666:sqs-queue-A</Queue>
     <Event>s3:ObjectCreated:Put</Event>
  </QueueConfiguration>
  <QueueConfiguration>
```

```
     <Id>2</Id>
     <Filter>
            <S3Key>
                <FilterRule>
                    <Name>prefix</Name>
                    <Value>logs/</Value>
                </FilterRule>
            </S3Key>
     </Filter>
     <Queue>arn:aws:sqs:us-west-2:444455556666:sqs-queue-B</Queue>
     <Event>s3:ObjectCreated:Put</Event>
  </QueueConfiguration>
</NotificationConfiguration>
```

A configuração de notificação a seguir tem vários sufixos não sobrepostos. A configuração define que todas as imagens `.jpg` recém-adicionadas ao bucket sejam processadas por cloud-function-A do Lambda e que todas as imagens `.png` recém-adicionadas sejam processadas por cloud-function-B. Os sufixos `.png` e `.jpg` não se sobrepõem, apesar de terminarem com a mesma letra. Dois sufixos são considerados sobrepostos se determinada string puder terminar com ambos os sufixos. Uma string não pode terminar com `.png` e com `.jpg`, então os sufixos na configuração de exemplo não são sufixos sobrepostos.

```
<NotificationConfiguration>
  <CloudFunctionConfiguration>
     <Id>1</Id>
     <Filter>
            <S3Key>
                <FilterRule>
                    <Name>suffix</Name>
                    <Value>.jpg</Value>
                </FilterRule>
            </S3Key>
     </Filter>
     <CloudFunction>arn:aws:lambda:us-west-2:444455556666:cloud-function-A</
CloudFunction>
     <Event>s3:ObjectCreated:Put</Event>
  </CloudFunctionConfiguration>
  <CloudFunctionConfiguration>
     <Id>2</Id>
     <Filter>
            <S3Key>
                <FilterRule>
```

```
                    <Name>suffix</Name>
                    <Value>.png</Value>
                </FilterRule>
            </S3Key>
     </Filter>
     <CloudFunction>arn:aws:lambda:us-west-2:444455556666:cloud-function-B</
CloudFunction>
     <Event>s3:ObjectCreated:Put</Event>
  </CloudFunctionConfiguration>
</NotificationConfiguration>
```

As configurações de notificação que usam o `Filter` não podem definir regras de filtro com prefixos sobrepostos para os mesmos tipos de evento. Eles só podem fazer isso se os prefixos sobrepostos forem usados com sufixos que não são sobrepostos. A configuração de exemplo a seguir mostra como objetos criados com um prefixo comum, mas com sufixos não sobrepostos, podem ser entregues a destinos diferentes.

```
<NotificationConfiguration>
  <CloudFunctionConfiguration>
     <Id>1</Id>
     <Filter>
            <S3Key>
                <FilterRule>
                    <Name>prefix</Name>
                    <Value>images</Value>
                </FilterRule>
                <FilterRule>
                    <Name>suffix</Name>
                    <Value>.jpg</Value>
                </FilterRule>
            </S3Key>
     </Filter>
     <CloudFunction>arn:aws:lambda:us-west-2:444455556666:cloud-function-A</
CloudFunction>
     <Event>s3:ObjectCreated:Put</Event>
  </CloudFunctionConfiguration>
  <CloudFunctionConfiguration>
     <Id>2</Id>
     <Filter>
            <S3Key>
                <FilterRule>
                    <Name>prefix</Name>
                    <Value>images</Value>
```

```
                </FilterRule>
                <FilterRule>
                    <Name>suffix</Name>
                    <Value>.png</Value>
                </FilterRule>
            </S3Key>
     </Filter>
     <CloudFunction>arn:aws:lambda:us-west-2:444455556666:cloud-function-B</
CloudFunction>
     <Event>s3:ObjectCreated:Put</Event>
  </CloudFunctionConfiguration>
</NotificationConfiguration>
```

Exemplos de configurações de notificação com sobreposição inválida de prefixo e sufixo

Na maioria das vezes, as configurações de notificação que usam `Filter` não podem definir regras de filtro com prefixos sobrepostos, sufixos sobrepostos ou combinações sobrepostas de prefixos e sufixos para os mesmos tipos de evento. Você pode ter prefixos sobrepostos, desde que os sufixos não se sobreponham. Para obter um exemplo, consulte Configurar notificações de eventos usando filtragem de nomes de chave de objeto.

Você pode usar filtros de nomes de chave de objetos sobrepostos com diferentes tipos de evento. Por exemplo, você poderia criar uma configuração de notificação que usasse o prefixo `image/` para o tipo de evento `ObjectCreated:Put` e o prefixo `image/` para o tipo de evento `ObjectRemoved:*`.

Você receberá um erro se tentar salvar uma configuração de notificação que tenha filtros de nomes sobrepostos inválidos para os mesmos tipos de evento ao usar o console ou a API do Amazon S3. Esta seção mostra exemplos de configurações de notificação que não são válidas devido aos filtros de nomes sobrepostos.

Presume-se que qualquer regra de configuração de notificação tenha um prefixo e um sufixo padrão que correspondam a qualquer outro prefixo e um sufixo, respectivamente. A configuração de notificação a seguir não é válida porque tem prefixos sobrepostos. Especificamente, o prefixo raiz sobrepõe qualquer outro prefixo. O mesmo se aplica se você usar um sufixo em vez de um prefixo neste exemplo. O sufixo raiz sobrepõe qualquer outro sufixo.

```
<NotificationConfiguration>
     <TopicConfiguration>
         <Topic>arn:aws:sns:us-west-2:444455556666:sns-notification-one</Topic>
         <Event>s3:ObjectCreated:*</Event>
```

```
    </TopicConfiguration>
    <TopicConfiguration>
         <Topic>arn:aws:sns:us-west-2:444455556666:sns-notification-two</Topic>
         <Event>s3:ObjectCreated:*</Event>
         <Filter>
             <S3Key>
                 <FilterRule>
                     <Name>prefix</Name>
                     <Value>images</Value>
                 </FilterRule>
            </S3Key>
        </Filter>
    </TopicConfiguration>
</NotificationConfiguration>
```

A configuração de notificação a seguir não é válida porque tem sufixos sobrepostos. Dois sufixos são considerados sobrepostos se determinada string puder terminar com ambos os sufixos. Uma string pode terminar com `jpg` e `pg`. Portanto, os sufixos se sobrepõem. O mesmo vale para prefixos. Dois prefixos são considerados sobrepostos se determinada string puder começar com ambos os prefixos.

```
 <NotificationConfiguration>
     <TopicConfiguration>
         <Topic>arn:aws:sns:us-west-2:444455556666:sns-topic-one</Topic>
         <Event>s3:ObjectCreated:*</Event>
         <Filter>
             <S3Key>
                 <FilterRule>
                     <Name>suffix</Name>
                     <Value>jpg</Value>
                 </FilterRule>
            </S3Key>
        </Filter>
    </TopicConfiguration>
    <TopicConfiguration>
         <Topic>arn:aws:sns:us-west-2:444455556666:sns-topic-two</Topic>
         <Event>s3:ObjectCreated:Put</Event>
         <Filter>
             <S3Key>
                 <FilterRule>
                     <Name>suffix</Name>
                     <Value>pg</Value>
                 </FilterRule>
            </S3Key>
```

```
        </Filter>
    </TopicConfiguration>
</NotificationConfiguration
```

A configuração de notificação a seguir não é válida porque tem prefixos e sufixos sobrepostos.

```
<NotificationConfiguration>
     <TopicConfiguration>
         <Topic>arn:aws:sns:us-west-2:444455556666:sns-topic-one</Topic>
         <Event>s3:ObjectCreated:*</Event>
         <Filter>
             <S3Key>
                 <FilterRule>
                     <Name>prefix</Name>
                     <Value>images</Value>
                 </FilterRule>
                 <FilterRule>
                     <Name>suffix</Name>
                     <Value>jpg</Value>
                 </FilterRule>
            </S3Key>
        </Filter>
    </TopicConfiguration>
    <TopicConfiguration>
         <Topic>arn:aws:sns:us-west-2:444455556666:sns-topic-two</Topic>
         <Event>s3:ObjectCreated:Put</Event>
         <Filter>
             <S3Key>
                 <FilterRule>
                     <Name>suffix</Name>
                     <Value>jpg</Value>
                 </FilterRule>
            </S3Key>
        </Filter>
    </TopicConfiguration>
</NotificationConfiguration>
```

Estrutura de mensagens de evento

A mensagem de notificação que o Amazon S3 envia para publicar um evento tem o formato JSON.

Para obter uma visão geral e instruções sobre como configurar notificações de eventos, consulte Notificações de eventos do Amazon S3.

Este exemplo mostra a versão 2.2 da estrutura JSON da notificação do evento. O Amazon S3 usa as versões 2.1, 2.2 e 2.3 desta estrutura de evento. O Amazon S3 usa a versão 2.2 para notificações de eventos de replicação entre regiões. Utiliza a versão 2.3 para o S3 Lifecycle, S3 Intelligent-Tiering, ACL de objeto, marcação de objetos e eventos de exclusão de restauração de objetos. Essas versões contêm informações adicionais específicas para essas operações. As versões 2.2 e 2.3 são compatíveis com a versão 2.1, que o Amazon S3 usa atualmente para outros tipos de notificação de eventos.

```
{
   "Records":[
      {
         "eventVersion":"2.2",
         "eventSource":"aws:s3",
         "awsRegion":"us-west-2",
         "eventTime":"The time, in ISO-8601 format, for example,
 1970-01-01T00:00:00.000Z, when Amazon S3 finished processing the request",
         "eventName":"event-type",
         "userIdentity":{
            "principalId":"Amazon-customer-ID-of-the-user-who-caused-the-event"
         },
         "requestParameters":{
            "sourceIPAddress":"ip-address-where-request-came-from"
         },
         "responseElements":{
            "x-amz-request-id":"Amazon S3 generated request ID",
            "x-amz-id-2":"Amazon S3 host that processed the request"
         },
         "s3":{
            "s3SchemaVersion":"1.0",
            "configurationId":"ID found in the bucket notification configuration",
            "bucket":{
               "name":"amzn-s3-demo-bucket",
               "ownerIdentity":{
                  "principalId":"Amazon-customer-ID-of-the-bucket-owner"
               },
               "arn":"bucket-ARN"
            },
            "object":{
               "key":"object-key",
               "size":"object-size in bytes",
               "eTag":"object eTag",
```

```
                "versionId":"object version if bucket is versioning-enabled, otherwise
 null",
                "sequencer": "a string representation of a hexadecimal value used to
 determine event sequence, only used with PUTs and DELETEs"
             }
          },
          "glacierEventData": {
             "restoreEventData": {
                "lifecycleRestorationExpiryTime": "The time, in ISO-8601 format, for
 example, 1970-01-01T00:00:00.000Z, of Restore Expiry",
                "lifecycleRestoreStorageClass": "Source storage class for restore"
             }
          }
       }
    ]
}
```

Sobre a estrutura de mensagens de evento, observe:

- O valor da chave `eventVersion` contém uma versão principal e secundária no formulário `<major>.<minor>`.

  A versão principal será incrementada se o Amazon S3 fizer uma alteração na estrutura do evento que não seja compatível com versões anteriores. Isso inclui remover um campo JSON que já está presente ou alterar como os conteúdos de um campo são representados (por exemplo, um formato de data).

  A versão secundária será incrementada se o Amazon S3 adicionar novos campos à estrutura do evento. Isso pode ocorrer se forem fornecidas novas informações para alguns ou todos os eventos existentes. Isso também pode ocorrer se novas informações forem fornecidas apenas nos tipos de evento recém-apresentados. Os aplicativos devem ignorar novos campos para permanecerem compatíveis com novas versões secundárias da estrutura do evento.

  Se novos tipos de evento forem apresentados, mas a estrutura do evento não for modificada, a versão do evento não será alterada.

  Para garantir que seus aplicativos possam analisar a estrutura do evento corretamente, recomendamos que você faça uma comparação "igual a" no número da versão principal. Para garantir que os campos esperados por sua aplicação estejam presentes, também recomendamos fazer uma comparação “maior que ou igual a” na versão secundária.

- O `eventName` faz referência à lista de tipos de notificação de evento, mas não contém o prefixo `s3:`.
- O valor da chave `responseElements` será útil se você quiser rastrear uma solicitação acompanhando o AWS Support. Tanto o `x-amz-request-id` quanto o `x-amz-id-2` ajudam o Amazon S3 a rastrear uma solicitação individual. Esses valores são os mesmos que os retornados pelo Amazon S3 na resposta à solicitação que inicia os eventos. Isso ocorre para que eles possam ser usados para corresponder o evento à solicitação.
- A chave `s3` fornece informações sobre o bucket e o objeto envolvidos no evento. O valor do nome da chave de objetos é codificado para URL. Por exemplo, "red flower.jpg" se torna "red +flower.jpg" (o Amazon S3 retorna "`application/x-www-form-urlencoded`" como o tipo do conteúdo na resposta).
- A chave `sequencer` fornece uma maneira de determinar a sequência de eventos. Não há garantia de que as notificações de evento cheguem na mesma ordem em que os eventos ocorreram. No entanto, as notificações de eventos que criam objetos (PUTs) e excluem objetos contêm um `sequencer`. Ele pode ser usado para determinar a ordem dos eventos de determinada chave de objeto.

  Se você comparar a sequências do `sequencer` nas duas notificações de evento na mesma chave de objeto, a notificação de evento com o valor hexadecimal `sequencer` maior será o evento que ocorreu depois. Se você estiver usando notificações de evento para manter um banco de dados ou um índice separado dos objetos do Amazon S3, recomendamos comparar e armazenar os valores de `sequencer` ao processar cada notificação de evento.

  Observe o seguinte:

  - Não é possível usar `sequencer` para determinar a ordem de eventos em chaves de objetos diferentes.
  - Os sequenciadores podem ter comprimentos diferentes. Portanto, para comparar esses valores, primeiro preencha zeros à direita do menor valor e faça uma comparação lexicográfica.
- A chave `glacierEventData` só está visível para eventos `s3:ObjectRestore:Completed`.
- A chave `restoreEventData` contém atributos que estão relacionados à solicitação de restauração.
- A chave `replicationEventData` só é visível para eventos de replicação.
- A chave `intelligentTieringEventData` só fica visível para eventos do S3 Intelligent-Tiering.
- A chave `lifecycleEventData` só fica visível para eventos de transição do S3 Lifecycle.

Exemplos de mensagens

Veja a seguir exemplos de mensagens de notificação de eventos do Amazon S3.

Mensagem de teste do Amazon S3

Depois que você configura uma notificação de evento em um bucket, o Amazon S3 envia a mensagem de teste a seguir.

```
{
   "Service":"Amazon S3",
   "Event":"s3:TestEvent",
   "Time":"2014-10-13T15:57:02.089Z",
   "Bucket":"amzn-s3-demo-bucket",
   "RequestId":"5582815E1AEA5ADF",
   "HostId":"8cLeGAmw098X5cv4Zkwcmo8vvZa3eH3eKxsPzbB9wrR+YstdA6Knx4Ip8EXAMPLE"
}
```

> **Note**
>
> A mensagem `s3:TestEvent` usa um formato diferente do formato usado por notificações de eventos regulares do S3. Diferentemente de outras notificações de eventos que usam a estrutura de matriz `Records` mostrada acima, o evento de teste usa um formato simplificado com campos diretos. Ao implementar o tratamento de eventos, seu código deve distinguir e lidar adequadamente com ambos os formatos de mensagem.

Mensagem de exemplo quando um objeto é criado usando uma solicitação PUT

A mensagem a seguir é um exemplo de mensagem que o Amazon S3 envia para publicar um evento `s3:ObjectCreated:Put`.

```
{
   "Records":[
      {
         "eventVersion":"2.1",
         "eventSource":"aws:s3",
         "awsRegion":"us-west-2",
         "eventTime":"1970-01-01T00:00:00.000Z",
         "eventName":"ObjectCreated:Put",
         "userIdentity":{
```

```
            "principalId":"AIDAJDPLRKLG7UEXAMPLE"
         },
         "requestParameters":{
            "sourceIPAddress":"127.0.0.1"
         },
         "responseElements":{
            "x-amz-request-id":"C3D13FE58DE4C810",
            "x-amz-id-2":"FMyUVURIY8/IgAtTv8xRjskZQpcIZ9KG4V5Wp6S7S/
JRWeUWerMUE5JgHvANOjpD"
         },
         "s3":{
            "s3SchemaVersion":"1.0",
            "configurationId":"testConfigRule",
            "bucket":{
               "name":"amzn-s3-demo-bucket",
               "ownerIdentity":{
                  "principalId":"A3NL1KOZZKExample"
               },
               "arn":"arn:aws:s3:::amzn-s3-demo-bucket"
            },
            "object":{
               "key":"HappyFace.jpg",
               "size":1024,
               "eTag":"d41d8cd98f00b204e9800998ecf8427e",
               "versionId":"096fKKXTRTtl3on89fVO.nfljtsv6qko",
               "sequencer":"0055AED6DCD90281E5"
            }
         }
      }
   ]
}
```

Para obter uma definição de cada prefixo de identificação do IAM (por exemplo, AIDA, AROA, AGPA), consulte Identificadores do IAM no Guia do usuário do IAM.

Usar o EventBridge

O Amazon S3 pode enviar eventos ao Amazon EventBridge sempre que certos eventos ocorrerem no bucket. Ao contrário de outros destinos, não é necessário selecionar quais tipos de evento você deseja entregar. Depois que o EventBridge estiver habilitado, todos os eventos abaixo serão enviados ao EventBridge. Você pode usar regras do EventBridge para encaminhar eventos para outros destinos. A seguir, estão listados os eventos que o Amazon S3 envia ao EventBridge.

Tipo de evento	Descrição
Objeto criado	Um objeto foi criado. O campo reason (motivo) na estrutura de mensagens de evento indica qual API do S3 foi usada para criar o objeto:PutObject, POST Object, CopyObject ou CompleteMultipartUpload.
Objeto excluído (DeleteObject) Objeto excluído (validade do ciclo de vida)	Um objeto foi excluído. Quando um objeto é excluído usando uma chamada de API do S3, o campo reason (motivo) é definido como DeleteObject. Quando um objeto é excluído por uma regra de validade do S3 Lifecycle, o campo reason (motivo) é definido como Lifecycle Expiration (Validade do ciclo de vida). Para obter mais informações, consulte Expirando objetos. Quando um objeto sem versionamento é excluído ou um objeto com versionamento é excluído permanentemente, o campo deletion-type (tipo de exclusão) é definido como Permanently Deleted (Excluído permanentemente). Quando um marcador de exclusão é criado para um objeto versionado, o campo do deletion-type (tipo de exclusão) é definido como Delete Marker Created (Marcador de exclusão criado). Para obter mais informações, consulte Excluir versões de objetos de um bucket com versionamento habilitado.
Restauração de objeto iniciada	Uma restauração de objetos foi iniciada da classe de armazenamento S3 Glacier ou S3 Glacier Deep Archive ou do nível de acesso de arquivo ou de acesso de arquivo profundo do S3 Intelligent-Tiering. Para obter mais informações, consulte Trabalhando com objetos arquivados.
Restauração de objeto concluída	Uma restauração de objeto foi concluída.

Tipo de evento	Descrição
Restauração de objeto expirada	A cópia temporária de um objeto restaurado do S3 Glacier ou S3 Glacier Deep Archive expirou e foi excluída.
Classe de armazenamento de objetos alterada	Um objeto foi transferido para uma classe de armazenam ento diferente. Para obter mais informações, consulte Transição de objetos usando o Amazon S3 Lifecycle.
Nível de acesso de objeto alterado	Um objeto foi transferido para o nível de acesso de arquivo ou de acesso de arquivo profundo do S3 Intelligent-Tiering. Para obter mais informações, consulte Gerenciar custos de armazenamento com o Amazon S3 Intelligent-Tiering.
ACL de objeto atualizada	Uma lista de controle de acesso (ACL) de objetos foi definida usando PutObjectACL. Não é gerado evento quando uma solicitação não resulta em alteração na ACL de um objeto. Para obter mais informações, consulte Visão geral da lista de controle de acesso (ACL).
Etiquetas de objeto adicionadas	Um conjunto de etiquetas foi adicionado a um objeto usando PutObjectTagging. Para obter mais informações, consulte Categorizar seu armazenamento usando tags.
Etiquetas de objeto excluídas	Todas as etiquetas foram removidas de um objeto usando DeleteObjectTagging. Para obter mais informações, consulte Categorizar seu armazenamento usando tags.

> **Note**
>
> Para obter mais informações sobre como os tipos de eventos do Amazon S3 são mapeados para os tipos de evento do EventBridge, consulte Mapeamento e solução de problemas do Amazon EventBridge.

Você pode usar o Amazon S3 Event Notifications com o EventBridge para escrever regras que executam ações quando um evento ocorre em seu bucket. Por exemplo, ele pode enviar uma

notificação para você. Para obter mais informações, consulte O que é o EventBridge no Guia do usuário do Amazon EventBridge.

Para obter mais informações sobre as ações e os tipos de dados com os quais você pode interagir usando a API do EventBridge, consulte Amazon EventBridge API Reference na Referência da API do Amazon EventBridge.

Para obter informações sobre preços, consulte Preços do Amazon EventBridge.

Tópicos

- Permissões do Amazon EventBridge
- Habilitar o Amazon EventBridge
- Estrutura de mensagens de eventos do EventBridge
- Mapeamento e solução de problemas do Amazon EventBridge

Permissões do Amazon EventBridge

O Amazon S3 não necessita de outras permissões para entregar eventos ao Amazon EventBridge.

Habilitar o Amazon EventBridge

Você pode habilitar o Amazon EventBridge usando o console do S3, a AWS Command Line Interface (AWS CLI) ou a API REST do Amazon S3.

> **Note**
>
> Depois que você habilitar o EventBridge, leva cerca de cinco minutos para que as alterações sejam implementadas.

Usar o console do S3

Para habilitar a entrega de eventos do EventBridge no console do S3.

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets de uso geral.
3. Na lista de buckets, escolha o nome do bucket para o qual você deseja habilitar eventos.

4. Escolha Properties (Propriedades).
5. Navegue até a seção Event Notifications (Notificações de eventos) e encontre a subsecção Amazon EventBridge. Escolha Editar.
6. Em Send notifications to Amazon EventBridge for all events in this bucket (Enviar notificações para o Amazon EventBridge para todos os eventos deste bucket), escolha No (Não).

Como usar o AWS CLI

O exemplo a seguir cria uma configuração de notificação de bucket para bucket `amzn-s3-demo-bucket1` com o Amazon EventBridge habilitado.

```
aws s3api put-bucket-notification-configuration --bucket amzn-s3-demo-bucket1 --
notification-configuration='{ "EventBridgeConfiguration": {} }'
```

Uso da API REST

Você pode habilitar o Amazon EventBridge de maneira programática em um bucket chamando a API REST do Amazon S3. Para ter mais informações, consulte PutBucketNotificationConfiguration na Referência de API do Amazon Simple Storage Service.

O exemplo a seguir exibe o XML usado para criar uma configuração de notificação de bucket com o Amazon EventBridge habilitado.

```
<NotificationConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <EventBridgeConfiguration>
  </EventBridgeConfiguration>
</NotificationConfiguration>
```

Criar regras do EventBridge

Depois de habilitado, você pode criar regras do Amazon EventBridge para determinadas tarefas. Por exemplo, é possível enviar notificações por e-mail quando um objeto é criado. Para obter um tutorial completo, consulte Tutorial: enviar uma notificação quando um objeto do Amazon S3 for criado no Guia do usuário do Amazon EventBridge.

Estrutura de mensagens de eventos do EventBridge

A mensagem de notificação que o Amazon S3 envia para publicar um evento tem o formato JSON. Quando o Amazon S3 envia um evento ao Amazon EventBridge, os campos a seguir estão presentes.

- version (versão): atualmente 0 (zero) para todos os eventos.
- id: um UUID gerado para cada evento.
- detail-type (detalhe-tipo): o tipo de evento que está sendo enviado. Consulte Usar o EventBridge para obter uma lista dos tipos de evento.
- source (origem): identifica o serviço que originou o evento.
- account (conta): o ID de 12 dígitos da Conta da AWS do proprietário do bucket.
- time (hora): a hora em que o evento ocorreu.
- region (região): identifica a Região da AWS do bucket.
- resources (recursos): uma matriz JSON que contém o nome do recurso da Amazon (ARN) do bucket.
- detail (detalhe): contém um objeto JSON com as informações sobre o evento. Para obter mais informações sobre o que pode ser incluído nesse campo, consulte Campo de detalhes da mensagem de evento.

Exemplos de estrutura de mensagens de evento

Veja a seguir exemplos de algumas das mensagens de notificação de eventos do Amazon S3 que podem ser enviadas ao Amazon EventBridge.

Objeto criado

```
{
  "version": "0",
  "id": "17793124-05d4-b198-2fde-7ededc63b103",
  "detail-type": "Object Created",
  "source": "aws.s3",
  "account": "111122223333",
  "time": "2021-11-12T00:00:00Z",
  "region": "ca-central-1",
  "resources": [
    "arn:aws:s3:::amzn-s3-demo-bucket1"
  ],
  "detail": {
    "version": "0",
    "bucket": {
      "name": "amzn-s3-demo-bucket1"
    },
    "object": {
```

```
      "key": "example-key",
      "size": 5,
      "etag": "b1946ac92492d2347c6235b4d2611184",
      "version-id": "IYV3p45BT0ac8hjHg1houSdS1a.Mro8e",
      "sequencer": "617f08299329d189"
    },
    "request-id": "N4N7GDK58NMKJ12R",
    "requester": "123456789012",
    "source-ip-address": "1.2.3.4",
    "reason": "PutObject"
  }
}
```

Objeto excluído (usando DeleteObject)

```
{
  "version": "0",
  "id": "2ee9cc15-d022-99ea-1fb8-1b1bac4850f9",
  "detail-type": "Object Deleted",
  "source": "aws.s3",
  "account": "111122223333",
  "time": "2021-11-12T00:00:00Z",
  "region": "ca-central-1",
  "resources": [
    "arn:aws:s3:::amzn-s3-demo-bucket1"
  ],
  "detail": {
    "version": "0",
    "bucket": {
      "name": "amzn-s3-demo-bucket1"
    },
    "object": {
      "key": "example-key",
      "etag": "d41d8cd98f00b204e9800998ecf8427e",
      "version-id": "1QW9g1Z99LUNbvaaYVpW9xDlOLU.qxgF",
      "sequencer": "617f0837b476e463"
    },
    "request-id": "0BH729840619AG5K",
    "requester": "123456789012",
    "source-ip-address": "1.2.3.4",
    "reason": "DeleteObject",
    "deletion-type": "Delete Marker Created"
```

```
  }
}
```

Objeto excluído (usando validade do ciclo de vida)

```
{
  "version": "0",
  "id": "ad1de317-e409-eba2-9552-30113f8d88e3",
  "detail-type": "Object Deleted",
  "source": "aws.s3",
  "account": "111122223333",
  "time": "2021-11-12T00:00:00Z",
  "region": "ca-central-1",
  "resources": [
    "arn:aws:s3:::amzn-s3-demo-bucket1"
  ],
  "detail": {
    "version": "0",
    "bucket": {
      "name": "amzn-s3-demo-bucket1"
    },
    "object": {
      "key": "example-key",
      "etag": "d41d8cd98f00b204e9800998ecf8427e",
      "version-id": "mtB0cV.jejK63XkRNceanNMC.qXPWLeK",
      "sequencer": "617b398000000000"
    },
    "request-id": "20EB74C14654DC47",
    "requester": "s3.amazonaws.com",
    "reason": "Lifecycle Expiration",
    "deletion-type": "Delete Marker Created"
  }
}
```

Restauração de objeto concluída

```
{
  "version": "0",
  "id": "6924de0d-13e2-6bbf-c0c1-b903b753565e",
  "detail-type": "Object Restore Completed",
  "source": "aws.s3",
```

```
  "account": "111122223333",
  "time": "2021-11-12T00:00:00Z",
  "region": "ca-central-1",
  "resources": [
    "arn:aws:s3:::amzn-s3-demo-bucket1"
  ],
  "detail": {
    "version": "0",
    "bucket": {
      "name": "amzn-s3-demo-bucket1"
    },
    "object": {
      "key": "example-key",
      "size": 5,
      "etag": "b1946ac92492d2347c6235b4d2611184",
      "version-id": "KKsjUC1.6gIjqtvhfg5AdMI0eCePIiT3"
    },
    "request-id": "189F19CB7FB1B6A4",
    "requester": "s3.amazonaws.com",
    "restore-expiry-time": "2021-11-13T00:00:00Z",
    "source-storage-class": "GLACIER"
  }
}
```

Campo de detalhes da mensagem de evento

O campo detail (detalhe) contém um objeto JSON com informações sobre o evento. Os campos a seguir podem estar presentes no campo detail (detalhe).

- version (versão): atualmente 0 (zero) para todos os eventos.
- bucket: informações sobre o bucket do Amazon S3 envolvido no evento.
- object (objeto): informações sobre o objeto do Amazon S3 envolvido no evento.
- request-id (solicitação-id): ID da solicitação na resposta do S3.
- requester (solicitante): ID da Conta da AWS ou entidade principal do serviço da AWS do solicitante.
- source-ip-address (origem-ip-endereço): endereço IP de origem da solicitação do S3. Presente somente para eventos acionados por uma solicitação do S3.
- reason (motivo): para eventos Object Created (Objeto criado), a API do S3 usada para criar o objeto: PutObject, POST Object, CopyObject ou CompleteMultipartUpload. Em eventos Object

Deleted (Objeto excluído), é definido como DeleteObject quando um objeto é excluído por uma chamada de API do S3 ou Lifecycle Expiration (Validade do ciclo de vida) quando um objeto é excluído por uma regra de validade do S3 Lifecycle. Para obter mais informações, consulte Expirando objetos.

- deletion-type (exclusão-tipo): em eventos Object Deleted (Objeto excluído) quando um objeto sem versionamento é excluído ou um objeto com versionamento é excluído permanentemente, o campo deletion-type é definido como Permanently Deleted (Excluído permanentemente). Quando um marcador de exclusão é criado para um objeto versionado, é definido como Delete Marker Created (Marcador de exclusão criado). Para obter mais informações, consulte Excluir versões de objetos de um bucket com versionamento habilitado.

  > **Note**
  >
  > Alguns atributos do objeto (como `etag` e `size`) estão presentes somente quando um delete marker é criado.

- restore-expiry-time (restaurar-validade-hora): para eventos Object Restore Completed (Restauração de objetos concluída), a hora em que a cópia temporária do objeto será excluída do S3. Para obter mais informações, consulte Trabalhando com objetos arquivados.
- source-storage-class (origem-armazenamento-classe): para eventos Object Restore Initiated (Iniciar a restauração de objetos) e Object Restore Completed (Restauração de objetos concluída), a classe de armazenamento do objeto que está sendo restaurado. Para obter mais informações, consulte Trabalhando com objetos arquivados.
- destination-storage-class (destino-armazenamento-classe): para eventos Object Storage Class Changed (Classe de armazenamento de objetos alterada), a nova classe de armazenamento do objeto. Para obter mais informações, consulte Transição de objetos usando o Amazon S3 Lifecycle.
- destination-access-tier (destino-acesso-nível): para eventos Object Access Tier Changed (Nível de acesso a objetos alterado), o novo nível de acesso do objeto. Para obter mais informações, consulte Gerenciar custos de armazenamento com o Amazon S3 Intelligent-Tiering.

Mapeamento e solução de problemas do Amazon EventBridge

A tabela a seguir descreve como os tipos de eventos do Amazon S3 são mapeados para os tipos de evento do Amazon EventBridge.

Tipo de evento do S3	Tipo de detalhes do Amazon EventBridge
ObjectCreated:Put ObjectCreated:Post ObjectCreated:Copy ObjectCreated:CompleteMultipartUpload	Objeto criado
ObjectRemoved:Delete ObjectRemoved:DeleteMarkerCreated LifecycleExpiration:Delete LifecycleExpiration:DeleteMarkerCreated	Objeto excluído
ObjectRestore:Post	Restauração de objeto iniciada
ObjectRestore:Completed	Restauração de objeto concluída
ObjectRestore:Delete	Restauração de objeto expirada
LifecycleTransition	Classe de armazenamento de objetos alterada
IntelligentTiering	Nível de acesso de objeto alterado
ObjectTagging:Put	Etiquetas de objeto adicionadas
ObjectTagging:Delete	Etiquetas de objeto excluídas
ObjectAcl:Put	ACL de objeto atualizada

Solução de problemas do Amazon EventBridge

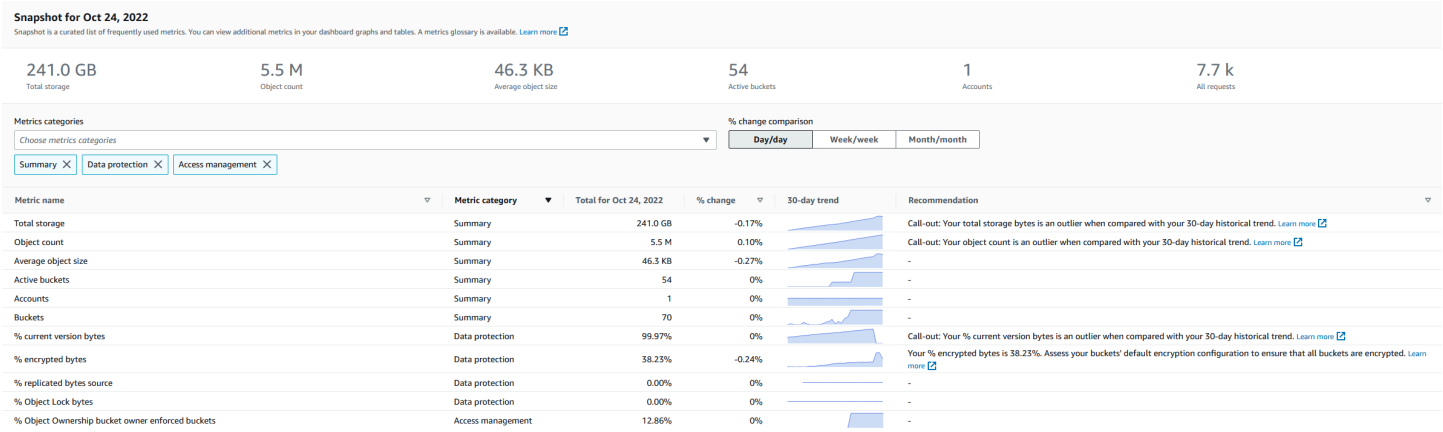
Para obter informações sobre como solucionar problemas do EventBridge, consulte Solucionar problemas no Amazon EventBridge no Guia do usuário do Amazon EventBridge.

Avaliação de sua atividade de armazenamento e uso com a Lente de Armazenamento do Amazon S3

A Lente de Armazenamento do Amazon S3 é um recurso de análise de armazenamento em nuvem que você pode usar para obter visibilidade em toda a organização sobre o uso e a atividade do armazenamento de objetos. A Lente de Armazenamento do S3 também analisa as métricas para fornecer recomendações contextuais que você pode usar para otimizar os custos de armazenamento e aplicar as práticas recomendadas de proteção de dados.

Você pode usar métricas da Lente de Armazenamento do S3 para gerar insights resumidos. Por exemplo, você pode descobrir quanto armazenamento você tem em toda a sua organização ou quais são os buckets e prefixos de crescimento mais rápido. Você também pode usar as métricas da Lente de Armazenamento do S3 para identificar oportunidades de otimização de custos, implementar práticas recomendadas de proteção de dados e gerenciamento de acesso, e melhorar a performance das workloads de aplicações. Por exemplo, você pode identificar buckets que não têm regras de ciclo de vida do S3 para encerrar uploads fracionados incompletos com mais de sete dias. Você também pode identificar buckets que não estão seguindo as práticas recomendadas de proteção de dados, como usar a Replicação do S3 ou o Versionamento do S3.

A Lente de Armazenamento do S3 agrega suas métricas e exibe as informações na seção Snapshot da conta na página Buckets do console do Amazon S3. A Lente de Armazenamento do S3 também oferece um painel interativo para visualizar insights e tendências, sinalizar discrepâncias e receber recomendações para otimizar os custos de armazenamento e aplicar as práticas recomendadas de proteção de dados. O painel tem opções de detalhamento para gerar e visualizar insights no nível da organização, conta, Região da AWS, classe de armazenamento, bucket, prefixo ou grupo de Lente de Armazenamento. Você também pode enviar uma exportação diária de métricas em CSV ou no formato Parquet para um bucket do S3.



Métricas e recursos da Lente de Armazenamento do S3

A Lente de Armazenamento do S3 fornece um painel padrão interativo que é atualizado diariamente. A Lente de Armazenamento do S3 pré-configura esse painel para visualizar um resumo de insights e tendências para toda a sua conta e atualiza esse resumo diariamente no console do S3. As métricas desse painel também são resumidas no snapshot da conta na página Buckets. Para obter mais informações, consulte Painel padrão.

Para criar outros painéis e definir o escopo por Regiões da AWS, buckets do S3 ou contas (para o AWS Organizations), crie uma configuração de painel da Lente de Armazenamento do S3. Você pode criar e gerenciar configurações do painel de Lente de Armazenamento do S3 usando o console do Amazon S3, AWS Command Line Interface (AWS CLI), AWS SDKs ou a API REST do Amazon S3. Ao criar ou editar um painel da Lente de Armazenamento do S3, defina o escopo do painel e a seleção de métricas.

A Lente de Armazenamento do S3 oferece métricas gratuitas, bem como métricas e recomendações avançadas que podem ser adquiridas por um custo adicional. Com métricas e recomendações avançadas, você pode acessar métricas e recursos adicionais para obter informações sobre seu armazenamento. Esses recursos incluem categorias de métricas avançadas, agregação de prefixos, recomendações contextuais e publicação no Amazon CloudWatch. A agregação de prefixos e as recomendações contextuais estão disponíveis somente no console do Amazon S3. Para obter mais informações sobre a definição de preço do S3 Storage Lens, consulte Definição de preço do Amazon S3.

Categorias de métricas

Nos níveis gratuito e avançado, as métricas estão organizadas em categorias que se alinham aos principais casos de uso, como otimização de custos e proteção de dados. As métricas gratuitas incluem métricas de resumo, otimização de custos, proteção de dados, gerenciamento de acesso, performance e eventos. Ao fazer upgrade para métricas e recomendações avançadas, você pode ativar métricas avançadas de otimização de custos e proteção de dados. Você pode usar essas métricas avançadas para reduzir ainda mais os custos de armazenamento do S3 e melhorar sua postura de proteção de dados. Você também pode ativar métricas de atividade e métricas de códigos de status detalhados para melhorar a performance das workloads de aplicações que acessam os buckets do S3. Para obter mais informações sobre as categorias de métricas gratuitas e avançadas, consulte Seleção de métricas.

Você pode avaliar seu armazenamento com base nas práticas recomendadas do S3, como analisar a porcentagem de buckets com criptografia ou que têm o Bloqueio de Objeto do S3 ou o

Versionamento do S3 habilitado. Você também pode identificar possíveis oportunidades de redução de custos. Por exemplo, você pode usar métricas de contagem de regras do Ciclo de Vida do S3 para identificar buckets que não têm regras de ciclo de vida de validade ou transição. Você também pode analisar sua atividade de solicitações por bucket para encontrar buckets onde os objetos podem ser transferidos para uma classe de armazenamento de menor custo. Para obter mais informações, consulte Casos de uso das métricas da Lente de Armazenamento do Amazon S3.

Exportação de métricas

Além de visualizar o painel no console do S3, é possível exportar métricas em formato CSV ou Parquet para um bucket do S3 de sua escolha para análise posterior com ferramentas analíticas. Para obter mais informações, consulte Exibição de métricas de lente de armazenamento do Amazon S3 usando uma exportação de dados.

Publicação no Amazon CloudWatch

É possível publicar métricas de uso e atividade do S3 Storage Lens no Amazon CloudWatch para criar uma visão unificada de sua integridade operacional nos painéis do CloudWatch. Também é possível usar os recursos do CloudWatch, como alarmes e ações acionadas, matemática métrica e detecção de anomalias, para monitorar e realizar ações sobre as métricas da Lente de Armazenamento do S3. Além disso, as operações de API do CloudWatch permitem que aplicações, inclusive provedores de terceiros, acessem as métricas da Lente de Armazenamento do S3. A opção de publicação no CloudWatch está disponível para painéis com upgrade para métricas e recomendações avançadas da Lente de Armazenamento do S3. Para obter mais informações sobre suporte às métricas do S3 Storage Lens no CloudWatch, consulte Monitorar métricas do S3 Storage Lens no CloudWatch.

Para obter mais informações sobre como usar a Lente de Armazenamento do S3, consulte os tópicos a seguir.

Tópicos

- Noções básicas sobre o Amazon S3 Storage Lens
- Glossário de métricas de lente de armazenamento do Amazon S3
- Configurar permissões da Lente de Armazenamento do Amazon S3
- Trabalhar com a Lente de Armazenamento do Amazon S3 usando o console e a API
- Visualizar métricas com a Lente de Armazenamento do Amazon S3
- Usar o Amazon S3 Storage Lens com AWS Organizations

- Trabalhar com grupos da Lente de Armazenamento do S3 para filtrar e agregar métricas

Noções básicas sobre o Amazon S3 Storage Lens

> **Important**
>
> O Amazon S3 agora aplica criptografia do lado do servidor com chaves gerenciadas do Amazon S3 (SSE-S3) como nível básico de criptografia para cada bucket no Amazon S3. Desde 5 de janeiro de 2023, todos os novos uploads de objetos para o Amazon S3 são automaticamente criptografados sem custo adicional e sem impacto na performance. O status de criptografia automática para a configuração de criptografia padrão do bucket do S3 e para novos uploads de objetos está disponível em logs do AWS CloudTrail, no Inventário do S3, na Lente de Armazenamento do S3, no console do Amazon S3 e como cabeçalho adicional de resposta da API do Amazon S3 na AWS Command Line Interface e em AWS SDKs. Para obter mais informações, consulte Perguntas frequentes sobre criptografia padrão.

A Lente de Armazenamento do Amazon S3 é um recurso de análise de armazenamento em nuvem que você pode usar para obter visibilidade em toda a organização sobre o uso e a atividade do armazenamento de objetos. Use as métricas da Lente de Armazenamento do S3 para gerar insights resumidos, como descobrir quanto armazenamento você tem em toda a organização ou quais são os buckets e prefixos que mais crescem. Você também pode usar as métricas da Lente de Armazenamento do S3 para identificar oportunidades de otimização de custos, implementar práticas recomendadas de proteção e segurança de dados, e melhorar a performance das workloads de aplicações. Por exemplo, você pode identificar buckets que não têm regras de Ciclo de Vida do S3 para expirar multipart uploads incompletos com mais de 7 dias. Você também pode identificar buckets que não estão seguindo as práticas recomendadas de proteção de dados, como usar a Replicação do S3 ou o Versionamento do S3. A Lente de Armazenamento do S3 também analisa as métricas para fornecer recomendações contextuais que você pode usar para otimizar os custos de armazenamento e aplicar as práticas recomendadas de proteção de dados.

A Lente de Armazenamento do S3 agrega suas métricas e exibe as informações na seção Account snapshot (Snapshot da conta) na página Buckets do console do Amazon S3. A Lente de Armazenamento do S3 também oferece um painel interativo para visualizar insights e tendências, sinalizar discrepâncias e receber recomendações para otimizar os custos de armazenamento e aplicar as práticas recomendadas de proteção de dados. O painel tem opções de detalhamento

para gerar e visualizar insights no nível da organização, conta, Região da AWS, classe de armazenamento, bucket, prefixo ou grupo de Lente de Armazenamento. Você também pode enviar uma exportação diária de métricas em CSV ou no formato Parquet para um bucket do S3. Você pode criar e gerenciar painéis de Lente de Armazenamento do S3 usando o console do Amazon S3, AWS Command Line Interface (AWS CLI), AWS SDKs ou API REST do Amazon S3.

Conceitos e terminologia da Lente de Armazenamento do S3

Esta seção contém a terminologia e os conceitos essenciais para entender e usar a Lente de Armazenamento do Amazon S3.

Tópicos

- Configuração de painel
- Painel padrão
- Painéis
- Snapshot da conta
- Exportação de métricas
- Região inicial
- Período de retenção
- Categorias de métricas
- Recomendações
- Seleção de métricas
- S3 Storage Lens e AWS Organizations

Configuração de painel

A Lente de Armazenamento do S3 requer uma configuração de painel que contém as propriedades necessárias para agregar métricas em seu nome para um único painel ou exportação. Ao criar uma configuração, escolha o nome do painel e a região inicial, que não poderão ser alterados depois de criar o painel. Opcionalmente, você pode adicionar etiquetas e configurar uma exportação de métricas em formato CSV ou Parquet.

Na configuração do painel, defina também o escopo do painel e a seleção de métricas. O escopo pode incluir todo o armazenamento da conta da sua organização ou seções que são filtradas por

região, bucket e conta. Ao configurar a seleção de métricas, escolha entre métricas gratuitas, ou compre métricas e recomendações avançadas por um custo adicional. Com métricas e recomendações avançadas, você tem acesso a métricas e recursos adicionais. Esses recursos incluem categorias de métricas avançadas, agregação por prefixo, recomendações contextuais e publicação no Amazon CloudWatch. Para obter mais informações sobre a definição de preço do S3 Storage Lens, consulte Definição de preço do Amazon S3.

Painel padrão

O painel padrão do S3 Storage Lens no console é chamado default-account-dashboard. O S3 pré-configura esse painel para visualizar um resumo de insights e tendências para toda a sua conta e atualiza esse resumo diariamente no console do S3. Você não pode modificar o escopo de configuração do painel padrão, mas pode atualizar a seleção de métricas gratuitas para métricas e recomendações avançadas. Você pode configurar a exportação opcional de métricas ou até mesmo desabilitar o painel. No entanto, você não pode excluir o painel padrão.

> **Note**
>
> Se você desabilitar o painel padrão, ele deixará de ser atualizado. Você não receberá mais nenhuma métrica diária nova no painel da Lente de Armazenamento do S3, a exportação de métricas ou o snapshot da conta na página Buckets do S3. Se o painel usar métricas e recomendações avançadas, você não receberá mais cobranças. Você ainda pode ver dados históricos no painel durante o período de validade de 14 dias para consultas de dados. Esse período é de 15 meses com a opção de métricas e recomendações avançadas habilitada. Para acessar dados históricos, reative o painel dentro do período de validade.

Painéis

Você pode criar painéis adicionais da Lente de Armazenamento do S3 e definir o escopo deles por Regiões da AWS, bucket do S3 ou conta (para o AWS Organizations). Ao criar ou editar um painel da Lente de Armazenamento do S3, defina o escopo do painel e a seleção de métricas. A Lente de Armazenamento do S3 oferece métricas gratuitas, bem como métricas e recomendações avançadas que podem ser adquiridas por um custo adicional. Com métricas e recomendações avançadas, você pode acessar métricas e recursos adicionais para obter informações sobre seu armazenamento. Elas incluem categorias de métricas avançadas, agregação por prefixo, recomendações contextuais e publicação no Amazon CloudWatch. Para obter mais informações sobre a definição de preço do S3 Storage Lens, consulte Definição de preço do Amazon S3.

Você também pode desativar ou excluir painéis. Se você desabilitar um painel, ele não será mais atualizado e você não receberá mais nenhuma nova métrica diária. Você ainda pode ver dados históricos durante o período de validade de 14 dias. Esse período é de 15 meses com a opção de métricas e recomendações avançadas habilitada para esse painel. Para acessar dados históricos, reative o painel dentro do período de validade.

Se você excluir seu painel, você perderá todas as configurações do painel. Você não receberá mais nenhuma nova métrica diária e também perderá o acesso aos dados históricos associados a esse painel. Se você quiser acessar os dados históricos de um painel excluído, você deve criar outro painel com o mesmo nome na mesma região inicial.

> **Note**
>
> - Você pode usar o S3 Storage Lens para criar até 50 painéis por região inicial.
> - Os painéis por organização só podem ser limitados a um escopo regional.

Snapshot da conta

O Snapshot da conta da Lente de Armazenamento do S3 resume as métricas do painel padrão e exibe o armazenamento total, a contagem de objetos e o tamanho médio dos objetos na página Buckets do console do S3. Esse snapshot de conta oferece acesso rápido a insights sobre o armazenamento sem ter que sair da página Buckets. O snapshot da conta também fornece acesso com um clique ao painel interativo da Lente de Armazenamento do S3.

Você pode usar o painel para visualizar insights e tendências, sinalizar discrepâncias e receber recomendações para otimizar os custos de armazenamento e aplicar as práticas recomendadas de proteção de dados. O painel tem opções de detalhamento para gerar insights por organização, conta, bucket, objeto ou prefixo. Você também pode enviar um arquivo exportado em formato CSV ou Parquet das métricas uma vez por dia para um bucket do S3.

Não é possível modificar o escopo do default-account dashboard (painel padrão da conta) porque ele está vinculado ao Account snapshot (Snapshot da conta). No entanto, você pode fazer upgrade da seleção de métricas no painel padrão da conta de métricas gratuitas para métricas e recomendações avançadas pagas. Depois de fazer upgrade, você pode exibir todas as solicitações, bytes carregados e bytes baixados no Snapshot da conta da Lente de Armazenamento do S3.

> **Note**
>
> Se você desabilitar o painel padrão, o Snapshot da conta não será mais atualizado. Para continuar exibidos as métricas no Account snapshot (Snapshot da conta), você pode reativar o painel padrão da conta.

Exportação de métricas

Uma exportação de métricas do S3 Storage Lens é um arquivo que contém todas as métricas identificadas na configuração do S3 Storage Lens. Essas informações são geradas diariamente em formato CSV ou Parquet e enviadas para um bucket do S3. Você pode usar a exportação de métricas para realizar análises adicionais usando a ferramenta de métricas de sua escolha. O bucket do S3 para a exportação de métricas deve estar na mesma região da configuração do S3 Storage Lens. Você pode gerar uma exportação de métricas da Lente de Armazenamento do S3 pelo console do S3 editando a configuração do painel. Você também pode configurar uma exportação de métricas usando a AWS CLI e AWS SDKs.

Região inicial

A região inicial é a Região da AWS em que todas as métricas da Lente de Armazenamento do S3 para determinada configuração de painel são armazenadas. Você deve escolher uma região inicial ao criar uma configuração de painel da Lente de Armazenamento do S3. Depois de escolher uma região inicial, não será possível alterá-la. Além disso, se você estiver criando um grupo da Lente de Armazenamento, recomendamos que você escolha a mesma região inicial do painel da Lente de Armazenamento.

> **Note**
>
> Você pode escolher uma das seguintes regiões como região inicial:
>
> - Leste dos EUA (Norte da Virgínia): `us-east-1`
> - US East (Ohio) – `us-east-2`
> - US West (N. California) – `us-west-1`
> - US West (Oregon) – `us-west-2`
> - Asia Pacific (Mumbai) – `ap-south-1`
> - Ásia-Pacífico (Seul) – `ap-northeast-2`

- Asia Pacific (Singapore) – `ap-southeast-1`
- Ásia-Pacífico (Sydney) – `ap-southeast-2`
- Ásia-Pacífico (Tóquio) (`ap-northeast-1`)
- Canada (Central) – `ca-central-1`
- China (Pequim): `cn-north-1`
- China (Ningxia): `cn-northwest-1`
- Europe (Frankfurt) – `eu-central-1`
- Europe (Ireland) – `eu-west-1`
- Europe (London) – `eu-west-2`
- Europe (Paris) – `eu-west-3`
- Europe (Stockholm) – `eu-north-1`
- South America (São Paulo) – `sa-east-1`

Período de retenção

As métricas da Lente de Armazenamento do S3 são mantidas para que você possa ver tendências históricas e comparar diferenças na atividade e no armazenamento ao longo do tempo. Você pode usar as métricas do Amazon S3 Storage Lens para consultar o histórico de tendências e comparar diferenças no uso e na atividade do armazenamento ao longo do tempo.

Todas as métricas do S3 Storage Lens são mantidas durante um período de 15 meses. No entanto, as métricas só estão disponíveis para consultas durante um período específico, que depende da sua seleção de métricas. Essa duração não pode ser modificada. As métricas gratuitas estão disponíveis para consultas por 14 dias, e as métricas avançadas estão disponíveis para consultas por 15 meses.

Categorias de métricas

Nos níveis gratuito e avançado, as métricas da Lente de Armazenamento do S3 estão organizadas em categorias que se alinham aos principais casos de uso, como otimização de custos e proteção de dados. As métricas gratuitas incluem métricas de resumo, otimização de custos, proteção de dados, gerenciamento de acesso, performance e eventos. Ao atualizar para métricas e recomendações avançadas, você pode ativar métricas adicionais de otimização de custos e proteção de dados que podem ser usadas para reduzir ainda mais os custos de armazenamento do S3 e garantir que seus dados estejam protegidos. Você também pode ativar métricas de atividade e métricas de códigos de status detalhados que pode usar para melhorar a performance dos fluxos de trabalho de aplicações.

A lista a seguir mostra todas as categorias de métricas gratuitas e avançadas. Para obter uma lista completa das métricas individuais incluídas em cada categoria, consulte o Glossário de métricas.

Métricas de resumo

As métricas de resumo fornecem informações gerais sobre seu armazenamento do S3, incluindo o total de bytes armazenados e a contagem de objetos.

Métricas de otimização de custos

As métricas de otimização de custos fornecem informações que você pode usar para gerenciar e otimizar seus custos de armazenamento. Por exemplo, você pode identificar buckets com multipart uploads que estão incompletos há mais de 7 dias.

Com as métricas e recomendações avançadas, você tem acesso a métricas avançadas de otimização de custos. Essas métricas incluem métricas de contagem de regras do Ciclo de Vida do S3 que você pode usar para obter contagens de regras do Ciclo de Vida do S3 para validade e transição por bucket.

Métricas de proteção de dados

As métricas de proteção de dados fornecem informações sobre recursos de proteção de dados, como criptografia e Versionamento do S3. Você pode usar essas métricas para identificar buckets que não estão seguindo as práticas recomendadas de proteção de dados. Por exemplo, você pode identificar buckets que não usam criptografia padrão com chaves do AWS Key Management Service (SSE-KMS) ou que não usam o Versionamento do S3.

Com as métricas e recomendações avançadas, você tem acesso a métricas avançadas de proteção de dados. Essas métricas incluem métricas de contagem de regras de replicação por bucket.

Métricas de gerenciamento de acesso

As métricas de gerenciamento de acesso fornecem informações sobre a Propriedade de Objeto do S3. Você pode usar essas métricas para ver as configurações de Propriedade de Objeto de seus buckets.

Métricas de eventos

As métricas de eventos fornecem informações sobre as Notificações de Eventos do S3. Com as métricas de eventos, você pode ver quais buckets têm as Notificações de Eventos do S3 configuradas.

Métricas de performance

As métricas de performance fornecem informações sobre a Aceleração de Transferência do S3. Com as métricas de performance, você pode ver quais buckets têm a Aceleração de Transferência ativada.

Métricas de atividade (avançadas)

Se você atualizar seu painel para métricas e recomendações avançadas, poderá ativar métricas de atividade. As métricas de atividade fornecem detalhes sobre como seu armazenamento é solicitado (por exemplo, Todas as solicitações, Obter solicitações, Colocar solicitações), Bytes carregados ou baixados e erros.

As métricas de atividade em nível de prefixo podem ser usadas para ajudar a determinar quais prefixos estão sendo usados com pouca frequência, a fim de fazer a transição para uma classe de armazenamento mais ideal usando o S3 Lifecycle.

Métricas de códigos de status detalhados (avançadas)

Se você atualizar seu painel para métricas e recomendações avançadas, poderá ativar métricas detalhadas de código de status. Métricas detalhadas de código de status fornecem informações para códigos de status HTTP, como 403 Forbidden e 503 Service Unavailable, que você pode usar para solucionar problemas de acesso ou desempenho. Por exemplo, você pode observar a métrica 403 Forbidden error count (Contagem de erros 403 Proibido) para identificar workloads que estão acessando buckets sem as permissões corretas em vigor.

Métricas de código de status detalhadas em nível de prefixo podem ser usadas para obter uma melhor compreensão das ocorrências de código de status HTTP por prefixo. Por exemplo, as métricas de contagem de erros 503 permitem identificar prefixos que recebem solicitações de controle de utilização durante a ingestão de dados.

Recomendações

O S3 Storage Lens fornece recomendações automatizadas para ajudá-lo a otimizar seu armazenamento. As recomendações são colocadas contextualmente ao lado de métricas relevantes no painel do S3 Storage Lens. Os dados históricos não são elegíveis para recomendações porque as recomendações são relevantes para o que está acontecendo no período mais recente. As recomendações só aparecem quando são relevantes.

As recomendações do S3 Storage Lens vêm nos seguintes formulários:

- Sugestões

As sugestões alertam as tendências no armazenamento e atividades que podem indicar uma oportunidade de otimização de custos de armazenamento ou uma prática recomendada de proteção de dados. Você pode usar os tópicos sugeridos no Guia do usuário do Amazon S3 e no painel de Lente de Armazenamento do S3 para especificar mais detalhes sobre regiões, buckets ou prefixos específicos.

- Chamadas

  Chamadas são recomendações que alertam sobre anomalias interessantes no armazenamento e atividade ao longo de um período, as quais podem requerer mais atenção ou monitoramento.

  - Chamadas discrepantes

    O S3 Storage Lens fornece chamadas para métricas que são discrepantes, com base em sua tendência recente de 30 dias. A discrepância é calculada usando uma pontuação padrão, também conhecida como pontuação z. Nessa pontuação, a métrica do dia atual é subtraída da média dos últimos 30 dias dessa métrica. A métrica do dia atual é então dividida pelo desvio padrão dessa métrica nos últimos 30 dias. A pontuação resultante geralmente é entre -3 e +3. Este número representa o número de desvios padrão entre a métrica do dia atual e a média.

    O S3 Storage Lens considera métricas com uma pontuação >2 ou <-2 como discrepâncias porque são maiores ou inferiores a 95% dos dados normalmente distribuídos.

  - Chamadas de alterações significativas

    A chamada de alteração significativa se aplica a métricas que devem ser alteradas com menos frequência. Portanto, ela é definida para uma sensibilidade maior do que o cálculo de discrepância, que geralmente está na faixa de +/- 20% em relação ao dia, semana ou mês anterior.

    Como lidar com chamadas em seu armazenamento e atividade — se você receber uma chamada de alteração significativa, isso não será necessariamente um problema. A chamada pode ser o resultado de uma mudança prevista no seu armazenamento. Por exemplo, você pode ter adicionado recentemente um grande número de novos objetos, excluído um grande número de objetos ou fez alterações planejadas semelhantes.

    Se você vir uma chamada de alteração significativa no seu painel, tome nota e determine se ela pode ser explicada por circunstâncias recentes. Caso contrário, use o painel do S3 Storage Lens para fazer drill-down a fim de obter mais detalhes para entender as regiões, buckets ou prefixos específicos que estão gerando a flutuação.

- Lembretes

  Os lembretes fornecem insights sobre como o Amazon S3 funciona. Eles podem ajudar você a aprender mais sobre maneiras de usar os recursos do S3 para reduzir os custos de armazenamento ou aplicar as práticas recomendadas de proteção de dados.

Seleção de métricas

O S3 Storage Lens oferece duas seleções de métricas que você pode escolher para seu painel e exportar: métricas gratuitas e métricas e recomendações avançadas.

- Métricas gratuitas

  O S3 Storage Lens oferece métricas gratuitas para todos os painéis e configurações. As métricas gratuitas incluem métricas relevantes para seu armazenamento, como o número de buckets e objetos em sua conta. As métricas gratuitas também incluem métricas baseadas em casos de uso (por exemplo, métricas de otimização de custos e proteção de dados) que você pode usar para investigar se seu armazenamento está configurado de acordo com as práticas recomendadas do S3. Todas as métricas gratuitas são coletadas diariamente. Os dados ficam disponíveis para consultas por 14 dias. Para obter mais informações sobre quais métricas estão disponíveis com métricas gratuitas, consulte o Glossário de métricas de lente de armazenamento do Amazon S3.

- Métricas e recomendações avançadas

  O S3 Storage Lens oferece métricas gratuitas para todos os painéis e configurações, bem como a opção de atualizar para métricas e recomendações avançadas. Aplicam-se cobranças adicionais do . Para obter mais informações, consulte Definição de preço do Amazon S3.

  As métricas e recomendações avançadas incluem todas as métricas gratuitas e métricas adicionais, como métricas avançadas de proteção de dados e otimização de custos, métricas de atividade e métricas de códigos de status detalhados. As métricas e recomendações avançadas também fornecem recomendações para ajudar a otimizar o armazenamento. As recomendações são colocadas contextualmente ao lado de métricas relevantes no painel.

  As métricas e recomendações avançadas incluem os seguintes recursos:

  - Métricas avançadas: gere métricas adicionais. Para obter uma lista completa das categorias de métricas avançadas, consulte Categorias de métricas. Para obter uma lista completa das métricas, consulte Glossário de métricas de lente de armazenamento do Amazon S3.

- Publicação do Amazon CloudWatch — publica métricas de Lente de Armazenamento do S3 no CloudWatch para criar uma visão unificada da sua integridade operacional nos painéis do CloudWatch. Também é possível usar operações de API e recursos do CloudWatch, como alarmes e ações acionadas, matemática métrica e detecção de anomalias, para monitorar e realizar ações sobre as métricas da Lente de Armazenamento do S3. Para obter mais informações, consulte Monitorar métricas do S3 Storage Lens no CloudWatch.
- Agregação de prefixo — coleta métricas no nível do prefixo. A ativação da agregação de prefixo estende todas as métricas incluídas na configuração do painel no nível do prefixo. As métricas são geradas apenas para prefixos que atendem ao limite configurado. Observe que as métricas aplicáveis no nível do prefixo estão disponíveis com agregação de prefixo, exceto para configurações no nível do bucket e métricas de contagem de regras. As métricas por prefixo não são publicadas no CloudWatch.
- Agregação do grupo da Lente de Armazenamento: coleta métricas no nível do grupo da Lente de Armazenamento. Depois de ativar Métricas e recomendações avançadas e Agregação de grupos da Lente de Armazenamento, você poderá especificar quais grupos da Lente de Armazenamento incluir ou excluir do painel da Lente de Armazenamento. Pelo menos um grupo da Lente de Armazenamento deve ser especificado. Os grupos da Lente de Armazenamento especificados também devem residir na região inicial designada na conta do painel. As métricas em nível de grupo de Lente de Armazenamento não são publicadas no CloudWatch.

Todas as métricas avançadas são coletadas diariamente. Os dados ficam disponíveis para consulta por até 15 meses. Para obter mais informações sobre as métricas de armazenamento agregadas pela Lente de Armazenamento do S3, consulte Glossário de métricas de lente de armazenamento do Amazon S3.

> **Note**
>
> As recomendações só estão disponíveis quando você usa o painel da Lente de Armazenamento do S3 no console do Amazon S3.

S3 Storage Lens e AWS Organizations

O AWS Organizations é um AWS service (Serviço da AWS) que ajuda você a agregar todas as suas Contas da AWS em uma hierarquia da organização. A Lente de Armazenamento do Amazon S3 funciona com o AWS Organizations para fornecer uma visão única do armazenamento de objetos e da atividade em todo o armazenamento do Amazon S3.

Para obter mais informações, consulte Usar o Amazon S3 Storage Lens com AWS Organizations.

- Acesso confiável

  Usando a conta de gerenciamento da sua organização, você deve habilitar o acesso confiável para a Lente de Armazenamento do S3 a fim de agregar métricas de armazenamento e dados de uso para todas as contas membros da sua organização. Depois, você pode criar painéis ou exportações para sua organização usando sua conta de gerenciamento ou dando acesso de administrador delegado a outras contas da organização.

  Você pode desativar o acesso confiável para o S3 Storage Lens a qualquer momento, o que impede o S3 Storage Lens de agregar métricas para sua organização.

- Administrador delegado

  Você pode criar painéis e métricas para a Lente de Armazenamento do S3 para sua organização usando sua conta de gerenciamento do AWS Organizations ou concedendo acesso de administrador delegado a outras contas em sua organização. Você pode cancelar o registro de administradores delegados a qualquer momento. O cancelamento do registro de um administrador delegado também impede automaticamente que todos os painéis da organização criados por esse administrador delegado agreguem novas métricas de armazenamento.

Para obter mais informações, consulte Amazon S3 Storage Lens e AWS Organizations no Guia do usuário do AWS Organizations.

Funções vinculadas ao serviço do Amazon S3 Storage Lens

Juntamente com o acesso confiável do AWS Organizations, o Amazon S3 Storage Lens usa funções vinculadas ao serviço do AWS Identity and Access Management (IAM). Uma função vinculada a serviço é um tipo exclusivo de função do IAM vinculada diretamente ao S3 Storage Lens. As funções vinculadas ao serviço são predefinidas pela Lente de Armazenamento do S3 e incluem todas as permissões necessárias para coletar métricas diárias de armazenamento e atividades de contas de membros na sua organização.

Para obter mais informações, consulte Usar funções vinculadas de serviço ao Amazon S3 Storage Lens.

Glossário de métricas de lente de armazenamento do Amazon S3

O glossário de métricas da Lente de Armazenamento do Amazon S3 oferece uma lista completa de métricas gratuitas e avançadas para a Lente de Armazenamento do S3.

A Lente de Armazenamento do S3 oferece métricas gratuitas para todos os painéis e configurações, com a opção de upgrade para métricas avançadas.

- Métricas gratuitas contêm métricas relevantes para o uso do armazenamento, como o número de buckets e objetos na sua conta. As métricas gratuitas também incluem métricas baseadas em casos de uso, como otimização de custos e métricas de proteção de dados. Todas as métricas gratuitas são coletadas diariamente, e os dados ficam disponíveis para consultas por até 14 dias.
- Métricas e recomendações avançadas incluem todas as métricas gratuitas e métricas adicionais, como métricas avançadas de proteção de dados e otimização de custos. As métricas avançadas também incluem categorias de métricas adicionais, como métricas de atividade e métricas detalhadas de código de status. Os dados de métricas avançadas ficam disponíveis para consultas por 15 meses.

  Há cobranças adicionais quando você usa o S3 Storage Lens com métricas e recomendações avançadas. Para obter mais informações, consulte Definição de preço do Amazon S3. Para obter mais informações sobre os recursos de métricas e recomendações avançadas, consulte Seleção de métricas.

  > **Note**
  >
  > Para grupos da Lente de Armazenamento, apenas métricas de armazenamento de nível gratuito estão disponíveis. As métricas de nível avançado não estão disponíveis no nível do grupo da Lente de Armazenamento.

Nomes de métricas

A coluna Nome da métrica na tabela a seguir fornece o nome de cada métrica da Lente de Armazenamento do S3 no console S3. A coluna CloudWatch e exportação fornece o nome de cada métrica no Amazon CloudWatch e o arquivo de exportação de métricas que você pode configurar no painel da Lente de Armazenamento do S3.

Fórmulas de métricas derivadas

As métricas derivadas não estão disponíveis para a exportação de métricas e a opção de publicação do CloudWatch. No entanto, você pode usar as fórmulas de métricas mostradas na coluna Fórmula de métricas derivadas para computá-las.

Interpretar os símbolos de prefixo da Lente de Armazenamento do Amazon S3 para os múltiplos de unidades métricas (K, M, G etc.)

Os múltiplos de unidades de métricas da Lente de Armazenamento do S3 são escritos com símbolos de prefixo. Esses símbolos de prefixo correspondem aos símbolos do SI (Sistema Internacional de Unidades) que são padronizados pelo BIPM (Bureau Internacional de Pesos e Medidas). Eles também são usados no UCUM (Unified Code for Units of Measure). Para obter mais informações, consulte a Lista de símbolos de prefixos do SI.

> **Note**
>
> - A unidade de medida para bytes de armazenamento do S3 está em gigabytes binários (GB), em que 1 GB é 2^{30} bytes, 1 TB é 2^{40} bytes e 1 PB é 2^{50} bytes. Essa unidade de medida também é conhecida como gibibyte (GiB), conforme definido pela Comissão Eletrotécnica Internacional (IEC).
> - Quando um objeto atinge o fim de seu ciclo de vida, com base em sua configuração de ciclo de vida, o Amazon S3 o coloca em uma fila para remoção e o remove assincronamente. Assim, pode haver um atraso entre a data de expiração e a data em que o Amazon S3 remove um objeto. A Lente de Armazenamento do S3 não inclui métricas para objetos que expiraram, mas não foram removidos. Para obter mais informações sobre as ações de expiração no ciclo de vida do S3, consulte Expirando objetos.

A tabela a seguir mostra o glossário de métricas da Lente de Armazenamento do S3.

Nome da métrica	CloudWatch e exportação	Descrição	Níve	Cate[2]	D	Fórm da métr deriv
Armazenam ento total	StorageBytes	O armazenamento total, incluindo uploads incomplet	Grat	Resu	N	-

Nome da métrica	CloudWatch e exportação	Descrição	Níve	Cate[2]	D	Fórm da métri deriv
		os de várias partes, metadados de objetos e marcadores de exclusão				
Contagem de objetos	ObjectCount	A contagem total de objetos	Gratu	Resu	N	-
Tamanho médio do objeto	-	O tamanho médio do objeto	Gratu	Resu	S	sum(StorageBytes)/ sum(ObjectCount)
Buckets ativos	-	O número total de buckets com armazenamento > 0 byte	Gratu	Resu	S	-
Buckets	-	O número total de buckets	Gratu	Resu	S	-
Contas	-	O número de contas cujo armazenamento está no escopo	Gratu	Resu	S	-
Bytes da versão atual	CurrentVersionStorageBytes	O número de bytes da versão atual de um objeto	Gratu	Otimo de custo	N	-

Nome da métrica	CloudWatch e exportação	Descrição	Níve	Cate[2]	D	Fórm da métri deriv
% de bytes da versão atual	-	A porcentagem de bytes no escopo de versões atuais de objetos	Gratu	Otim o de cust	S	sum(Curre ntVersion StorageBy tes)/ sum(StorageBy tes)
Contagem de objetos de versões atuais	CurrentVe rsionObje ctCount	A contagem dos objetos de versão atual	Gratu	Prot de dadc	N	-
% de objetos em versão atual	-	A porcentagem de objetos no escopo que são de uma versão atual	Gratu	Otim o de cust	S	sum(Curre ntVersion ObjectCou nt)/ sum(O bjectCoun t)
Bytes de versões desatualizadas	NonCurren tVersionS torageBytes	O número de bytes de versões desatualizadas	Gratu	Otim o de cust	N	-
% de bytes de versões desatualizadas	-	A porcentag em de bytes no escopo de versões desatuali zadas	Gratu	Otim o de cust	S	sum(NonCu rrentVers ionStorag eBytes)/ s um(Storag eBytes)

Nome da métrica	CloudWatch e exportação	Descrição	Níve	Cate[2]	D	Fórm da métri deriv
Contagem de objetos de versões desatualizadas	NonCurrentVersionObjectCount	A contagem de versões de objetos desatualizadas	Gratu	Otim o de cust	N	-
% de objetos de versões desatualizadas	-	A porcentagem de objetos no escopo que são uma versão não atual	Gratu	Otim o de cust	S	sum(NonCurrentVersionObjectCount)/ sum(ObjectCount)
Bytes de marcadores de exclusão	DeleteMarkerStorageBytes	O número de bytes no escopo que são marcadores de exclusão	Gratu	Otim o de cust	N	-
% de bytes de marcadores de exclusão	-	A porcentagem de bytes no escopo que são marcadores de exclusão	Gratu	Otim o de cust	S	sum(DeleteMarkerStorageBytes)/ sum(StorageBytes)
Contagem de objetos de marcadores de exclusão	DeleteMarkerObjectCount	O número total de objetos com um marcador de exclusão	Gratu	Otim o de cust	N	-

Nome da métrica	CloudWatch e exportação	Descrição	Níve	Cate[2]	D	Fórm da métri deriv
% de objetos de marcadores de exclusão	-	A porcentagem de objetos no escopo com um marcador de exclusão	Grat	Otim o de cust	S	sum(Delet eMarkerOb jectCount)/ sum(Obj ectCount)
Bytes de multipart uploads incompletos	IncompleteMultipartUploadStorageBytes	O total de bytes no escopo para multipart uploads incompletos	Grat	Otim o de cust	N	-
% de bytes de multipart uploads incompletos	-	A porcentagem de bytes no escopo que são o resultado de multipart uploads incompletos	Grat	Otim o de cust	S	sum(Incom pleteMult ipartUplo adStorage Bytes)/ su m(Storage Bytes)
Contagem de objetos de multipart uploads incompletos	IncompleteMultipartUploadObjectCount	O número de objetos no escopo com multipart uploads incomplet os	Grat	Otim o de cust	N	-

Nome da métrica	CloudWatch e exportação	Descrição	Níve	Cate[2]	D	Fórm da métri deriv
% de objetos de multipart uploads incompletos	-	A porcentagem de objetos no escopo com multipart uploads incomplet os	Gratu	Otim o de cust	S	sum(Incom pleteMult ipartUplo adObjectC ount)/ sum (ObjectCo unt)
Bytes de armazenam ento de multipart uploads incompletos há mais de 7 dias	IncompletMPUStora geBytesOl derThan7Days	O total de bytes no escopo para multipart uploads incompletos há mais de 7 dias	Gratu	Otim o de cust	N	-
% de bytes de armazenam ento de multipart uploads incompletos há mais de 7 dias	-	A porcentagem de bytes para multipart uploads incompletos há mais de 7 dias	Gratu	Otim o de cust	S	sum(Incom pleteMPUS torageByt esOlderTh an7Days)/ sum(Stora geBytes)
Contagem de objetos de multipart uploads incompletos há mais de 7 dias	IncompletMPUObjec tCountOld erThan7Days	O número de objetos que são o resultado de multipart uploads incompletos há mais de 7 dias	Gratu	Otim o de cust	N	-

Nome da métrica	CloudWatch e exportação	Descrição	Níve	Cate[2]	D	Fórm da métri deriv
% da contagem de objetos de multipart uploads incompletos há mais de 7 dias	-	A porcentagem de objetos que são o resultado de multipart uploads incompletos há mais de 7 dias	Grat	Otim o de cust	S	sum(IncompleteMPUObjectCountOlderThan7Days)/ s um(ObjectCount)
Contagem de regras de ciclo de vida para transição	TransitionLifecycleRuleCount	A contagem de regras de ciclo de vida para transição de objetos para outra classe de armazenamento	Adva (Ava)	Otim o de cust	N	-
Média de regras de ciclo de vida para transição por bucket	-	O número médio de regras de ciclo de vida para transição de objetos para outra classe de armazenamento	Adva (Ava)	Otim o de cust	S	sum(TransitionLifecycleRuleCount)/ su m(DistinctNumberOfBuckets)
Contagem de regras de ciclo de vida para validade	ExpirationLifecycleRuleCount	A contagem de regras de ciclo de vida para expirar objetos	Adva (Ava)	Otim o de cust	N	-

Nome da métrica	CloudWatch e exportação	Descrição	Níve	Cate[2]	D	Fórm da métri deriv
Média de regras de ciclo de vida para validade por bucket	-	O número médio de regras de ciclo de vida para expirar objetos	Adva (Ava)	Otim o de cust	S	sum(Expir ationLife cycleRule Count)/ su m(Distinc tNumberOf Buckets)
Contagem de regras de ciclo de vida para transição de versões desatualizadas	NoncurrentVersionTransitionLifecycleRuleCount	A contagem de regras de ciclo de vida para transição de versões objetos desatualizadas para outra classe de armazenamento	Adva (Ava)	Otim o de cust	N	
Média de regras de ciclo de vida para transição de versões desatualizadas por bucket	-	O número médio de regras de ciclo de vida para transição de versões objetos desatualizadas para outra classe de armazenamento	Adva (Ava)	Otim o de cust	S	sum(Noncu rrentVers ionTransi tionLifec ycleRuleC ount)/ sum (Distinct NumberOfB uckets)

Nome da métrica	CloudWatch e exportação	Descrição	Níve	Cate[2]	D	Fórm da métri deriv
Contagem de regras de ciclo de vida para validade de versões desatualizadas	NoncurrentVersionExpirationLifecycleRuleCount	A contagem de regras de ciclo de vida para expirar versões de objetos desatualizadas	Adva (Ava)	Otim o de cust	N	-
Média de regras de ciclo de vida para validade de versões desatualizadas por bucket	-	O número médio de regras de ciclo de vida para expirar versões de objetos desatualizadas	Adva (Ava)	Otim o de cust	S	sum(NoncurrentVersionExpirationLifecycleRuleCount)/sum(DistinctNumberOfBuckets)
Contagem de regras de ciclo de vida para anulação de multipart uploads incompletos	AbortIncompleteMPULifecycleRuleCount	A contagem de regras de ciclo de vida para excluir multipart uploads incompletos	Adva (Ava)	Otim o de cust	N	-

Nome da métrica	CloudWatch e exportação	Descrição	Nível	Categoria[2]	Dimensão	Fórmula da métrica derivada
Média de regras de ciclo de vida para anular multipart uploads incompletos por bucket	-	O número médio de regras de ciclo de vida para excluir multipart uploads incompletos	Avançado (Avançado)	Otimização de custo	Sem dimensão	sum(AbortIncompleteMPULifecycleRuleCount)/sum(DistinctNumberOfBuckets)
Contagem de regras de ciclo de vida para marcadores de exclusão de objetos expirados	ExpiredObjectDeleteMarkerLifecycleRuleCount	A contagem de regras de ciclo de vida para remover os marcadores de exclusão de objetos expirados	Avançado (Avançado)	Otimização de custo	Número	-
Média de regras de ciclo de vida de marcadores de exclusão de objetos expirados por bucket	-	O número médio de regras de ciclo de vida para remover os marcadores de exclusão de objetos expirados	Avançado (Avançado)	Otimização de custo	Sem dimensão	sum(ExpiredObjectDeleteMarkerLifecycleRuleCount)/sum(DistinctNumberOfBuckets)

Nome da métrica	CloudWatch e exportação	Descrição	Níve	Cate[2]	D	Fórm da métri deriv
Contagem total de regras de ciclo de vida	TotalLife cycleRuleCount	A contagem total de regras de ciclo de vida	Adva (Ava)	Otim o de cust	N	-
Contagem média de regras de ciclo de vida por bucket	-	O número médio de regras de ciclo de vida	Adva (Ava)	Otim o de cust	S	sum(Total Lifecycle RuleCount)/ sum(Dis tinctNumb erOfBucke ts)
Bytes criptogra fados	Encrypted StorageBytes	O número total de bytes criptogra fados	Gratu	Prot de dadc	N	-
% de bytes criptografados	-	A porcentagem do total de bytes criptografados	Gratu	Prot de dadc	S	sum(Encry ptedObjec tCount)/ s um(Storag eBytes)
Contagem de objetos criptografados	Encrypted ObjectCount	A contagem total de objetos criptografados	Gratu	Prot de dadc	N	-

Nome da métrica	CloudWatch e exportação	Descrição	Níve	Cate[2]	D	Fórm da métri deriv
% de objetos criptografados	-	A porcentagem de objetos criptografados	Gratu	Prot de dadc	S	sum(EncryptedStorageBytes)/sum(ObjectCount)
Bytes não criptografados	UnencryptedStorageBytes	O número de bytes não criptografados	Gratu	Prot de dadc	S	sum(StorageBytes) - sum(EncryptedStorageBytes)
% de bytes não criptografados	-	A porcentagem de bytes não criptografados	Gratu	Prot de dadc	S	sum(UnencryptedStorageBytes)/sum(StorageBytes)
Contagem de objetos não criptografados	UnencryptedObjectCount	A contagem total de objetos não criptografados	Gratu	Prot de dadc	S	sum(ObjectCount) - sum(EncryptedObjectCount)

Nome da métrica	CloudWatch e exportação	Descrição	Níve	Cate[2]	D	Fórm da métri deriv
% de objetos não criptografados	-	A porcentagem de objetos não criptografados	Gratu	Prot de dadc	S	sum(UnencryptedStorageBytes)/ sum(ObjectCount)
Bytes de armazenamento replicados da origem	ReplicatedStorageBytesSource	O número total de bytes replicados do bucket de origem	Gratu	Prot de dadc	N	-
% de bytes replicados da origem	-	A porcentagem do total de bytes replicados do bucket de origem	Gratu	Prot de dadc	S	sum(ReplicatedStorageBytesSource)/ sum(StorageBytes)
Contagem de objetos replicados da origem	ReplicatedObjectCountSource	A contagem de objetos replicados do bucket de origem	Gratu	Prot de dadc	N	-
% de objetos replicados da origem	-	A porcentagem do total de objetos replicados do bucket de origem	Gratu	Prot de dadc	S	sum(ReplicatedStorageObjectCount)/ sum(ObjectCount)

Nome da métrica	CloudWatch e exportação	Descrição	Níve	Cate[2]	D	Fórm da métri deriv
Destino dos bytes de armazenam ento replicados	ReplicatedStorageBytes	O número total de bytes replicados para o bucket de destino	Gratu	Prot de dadc	N	-
% de bytes replicados para o destino	-	A porcentagem do total de bytes replicados para o bucket de destino	Gratu	Prot de dadc	S	sum(ReplicatedStorageBytes) / sum(StorageBytes)
Contagem de objetos replicados para o destino	ReplicatedObjectCount	A contagem de objetos replicados para o bucket de destino	Gratu	Prot de dadc	N	-
% de objetos replicados para o destino	-	A porcentagem do total de objetos replicados para o bucket de destino	Gratu	Prot de dadc	S	sum(ReplicatedObjectCount)/ sum(ObjectCount)

Nome da métrica	CloudWatch e exportação	Descrição	Níve	Cate[2]	D	Fórm da métri deriv
Bytes do Bloqueio de Objeto	ObjectLockEnabledStorageBytes	A contagem total de bytes de armazenamento com Bloqueio de Objeto ativado	Gratu	Prot de dadc	N	sum(UnencryptedStorageBytes)/ sum(ObjectLockEnabledStorageCount) - sum(ObjectLockEnabledStorageBytes)
% de bytes do Bloqueio de Objeto	-	A porcentagem de bytes de armazenamento com Bloqueio de Objeto ativado	Gratu	Prot de dadc	S	sum(ObjectLockEnabledStorageBytes)/ sum(StorageBytes)
Contagem de objetos com Bloqueio de Objeto	ObjectLockEnabledObjectCount	A contagem total de objetos com Bloqueio de Objeto	Gratu	Prot de dadc	N	-

Nome da métrica	CloudWatch e exportação	Descrição	Níve	Cate[2]	D	Fórm da métri deriv
% de objetos com Bloqueio de Objeto	-	A porcentagem do total de objetos com Bloqueio de Objeto ativado	Gratu	Prot de dadc	S	sum(ObjectLockEnabledObjectCount)/ su m(ObjectCount)
Contagem de buckets com Versionamento ativado	VersioningEnabledBucketCount	A contagem de buckets com o Versionamento do S3 ativado	Gratu	Prot de dadc	N	-
% de bucket com Versionamento ativado	-	A porcentagem de buckets com o Versionamento do S3 ativado	Gratu	Prot de dadc	S	sum(VersioningEnabledBucketCount)/ su m(DistinctNumberOfBuckets)
Contagem de buckets com exclusão de MFA ativada	MFADeleteEnabledBucketCount	A contagem de buckets com exclusão de MFA (autenticação multifator) ativada	Gratu	Prot de dadc	N	-

Nome da métrica	CloudWatch e exportação	Descrição	Níve	Cate[2]	D	Fórm da métri deriv
% de buckets com exclusão de MFA ativada	-	A porcentagem de buckets com exclusão de MFA (autenticação multifator) ativada	Gratu	Prot de dadc	S	sum(MFADeleteEnabledBucketCount)/ sum (Distinct NumberOfBuckets)
Contagem de buckets com SSE-KMS ativada	SSEKMSEnabledBucketCount	A contagem de buckets que usam criptografia do lado do servidor com chaves do AWS Key Management Service (SSE-KMS) para criptografia padrão	Gratu	Prot de dadc	N	-
% de buckets com SSE-KMS ativada	-	A porcentagem de buckets que usam SSE-KMS para criptografia padrão	Gratu	Prot de dadc	S	sum(SSEKMSEnabledBucketCount)/ sum(DistinctNumberOfBuckets)

Nome da métrica	CloudWatch e exportação	Descrição	Nível	Categoria[2]	Dimensões	Fórmula da métrica derivada
Todas as solicitações de assinatura incompatíveis	AllUnsupportedSignatureRequests	O número total de solicitações que usam versões de assinatura da AWS incompatíveis	Advanced (Avançado)	Proteção de dados	Não	-
% de todas as solicitações de assinatura incompatíveis	-	A porcentagem de solicitações que usam versões de assinatura da AWS incompatíveis	Advanced (Avançado)	Proteção de dados	Sim	sum(AllUnsupportedSignatureRequests) / sum(AllRequests)
Todas as solicitações TLS incompatíveis	AllUnsupportedTLSRequests	O número de solicitações que usam versões de Transport Layer Security (TLS) incompatíveis	Advanced (Avançado)	Proteção de dados	Não	-
% de todas as solicitações TLS incompatíveis	-	A porcentagem de solicitações que usam versões de TLS incompatíveis	Advanced (Avançado)	Proteção de dados	Sim	sum(AllUnsupportedTLSRequests)/ sum(AllRequests)

Nome da métrica	CloudWatch e exportação	Descrição	Nível	Categoria[2]	Dimensões	Fórmula da métrica derivada
Todas as solicitações de SSE-KMS	AllSSEKMSRequests	O número total de solicitações que especificam SSE-KMS	Avançado (Avançado)	Proteção de dados	Não	-
% de todas as solicitações de SSE-KMS	-	A porcentagem de solicitações que especificam SSE-KMS	Avançado (Avançado)	Proteção de dados	Sim	sum(AllSSEKMSRequests)/sum(AllRequests)
Contagem de regras de replicação na mesma região	SameRegionReplicationRuleCount	A contagem de regras para replicação na mesma região (SRR)	Avançado (Avançado)	Proteção de dados	Não	-
Média de regras para replicação na mesma região por bucket	-	O número médio de regras de replicação para SRR	Avançado (Avançado)	Proteção de dados	Sim	sum(SameRegionReplicationRuleCount)/sum(DistinctNumberOfBuckets)
Contagem de regras de replicação entre regiões	CrossRegionReplicationRuleCount	A contagem de regras para replicação entre regiões diferentes (CRR)	Avançado (Avançado)	Proteção de dados	Não	-

Nome da métrica	CloudWatch e exportação	Descrição	Nível	Categoria[2]	Dimensões	Fórmula da métrica derivada
Média de regras para replicação entre regiões diferentes por bucket	-	O número médio de regras de replicação para CRR	Avançado (Avançado)	Proteção de dados	Sim	sum(CrossRegionReplicationRuleCount) / sum(DistinctNumberOfBuckets)
Contagem de regras de replicação na mesma conta	SameAccountReplicationRuleCount	A contagem de regras para replicação na mesma conta	Avançado (Avançado)	Proteção de dados	Não	-
Média de regras para replicação da mesma conta por bucket	-	O número médio de regras para replicação na mesma conta	Avançado (Avançado)	Proteção de dados	Sim	sum(SameAccountReplicationRuleCount) / sum(DistinctNumberOfBuckets)
Contagem de regras de replicação entre contas	CrossAccountReplicationRuleCount	A contagem de regras para replicação entre contas diferentes	Avançado (Avançado)	Proteção de dados	Não	-

Nome da métrica	CloudWatch e exportação	Descrição	Nível	Cate 2	De	Fórm da métri deriv
Média de regras para replicação entre contas diferentes por bucket	-	O número médio de regras para replicação entre contas diferentes	Adva (Ava)	Prot de dado	S	sum(Cross AccountRe plication RuleCount)/ sum(Dis tinctNumb erOfBucke ts)
Contagem de regras de replicação de destino inválido	InvalidDe stination Replicati onRuleCount	A contagem de regras de replicação com um destino de replicação que não é válido	Adva (Ava)	Prot de dado	N	-
Média de regras de replicação de destino inválido por bucket	-	O número médio de regras de replicação com um destino de replicação que não é válido	Adva (Ava)	Prot de dado	S	sum(Inval idReplica tionRuleC ount)/ sum (Distinct NumberOfB uckets)
Contagem total de regras de replicação	-	A contagem total de regras de replicação	Adva (Ava)	Prot de dado	S	-

Nome da métrica	CloudWatch e exportação	Descrição	Nível	Cate[2]	D	Fórm da métri deriv
Média de contagem de regras de replicação por bucket	-	A média de contagem total de regras de replicação	Adva (Ava)	Prot de dadc	S	sum(all replicati on rule count metrics)/ sum(Disti nctNumber OfBuckets)
Contagem de buckets com Imposto pelo proprietário do bucket em Propriedade de Objeto	ObjectOwn ershipBuc ketOwnerE nforcedBu cketCount	A contagem total de buckets com listas de controle de acesso (ACLs) desabilitadas pela configura ção Imposto pelo proprietário do bucket para Propriedade de Objeto	Gratu	Gere ento de aces	N	-

Nome da métrica	CloudWatch e exportação	Descrição	Níve	Cate[2]	D	Fórm da métri deriv
% de buckets com Imposto pelo proprietário do bucket para Propriedade de Objeto	-	A porcentagem de buckets com ACLs desabilitadas pela configuração Imposto pelo proprietário do bucket para Propriedade de Objeto	Gratu	Gere ento de aces	S	sum(ObjectOwnershipBucketOwnerEnforcedBucketCount)/ sum (DistinctNumberOfBuckets)
Contagem de buckets com Proprietário do bucket preferido para Propriedade de Objeto	ObjectOwnershipBucketOwnerPreferredBucketCount	A contagem total de buckets que usam a configuração Proprietário do bucket preferido para Propriedade de Objeto	Gratu	Gere ento de aces	N	-
% de buckets com Proprietário do bucket preferido para Propriedade de Objeto	-	A porcentagem de buckets que usam a configuração Proprietário do bucket preferido para Propriedade de Objeto	Gratu	Gere ento de aces	S	sum(ObjectOwnershipBucketOwnerPreferredBucketCount)/ sum(DistinctNumberOfBuckets)

Nome da métrica	CloudWatch e exportação	Descrição	Níve	Cate[2]	D	Fórm da métri deriv
Contagem de buckets com Autor do objeto para Proprieda de de Objeto	ObjectOwn ershipObj ectWriter BucketCount	A contagem total de buckets que usam a configura ção Autor do objeto para Propriedade de Objeto	Gratu	Gere ento de aces	N	-
% de buckets com Autor do objeto para Propriedade de Objeto	-	A porcentagem de buckets que usam a configuração Autor do objeto para Propriedade de Objeto	Gratu	Gere ento de aces	S	sum(Objec tOwnershi pObjectWr iterBucke tCount)/ s um(Distin ctNumberO fBuckets)
Contagem de buckets com Aceleração de Transferência ativada	TransferA ccelerati onEnabled BucketCount	A contagem total de buckets com Aceleração de Transferência ativada	Gratu	Perfo ce	N	-

Nome da métrica	CloudWatch e exportação	Descrição	Nível	Categoria[2]	Dimensão	Fórmula da métrica derivada
% de buckets com Aceleração de Transferência ativada	-	A porcentagem de buckets com Aceleração de Transferência ativada	Gratuito	Performance	Sem	sum(TransferAccelerationEnabledBucketCount)/sum(DistinctNumberOfBuckets)
Contagem de buckets com Notificações de Eventos ativadas	EventNotificationEnabledBucketCount	A contagem total de buckets com Notificações de Eventos ativadas	Gratuito	Eventos	Nenhum	
% de buckets com Notificações de Eventos ativadas	-	A porcentagem de buckets com Notificações de Eventos ativadas	Gratuito	Eventos	Sem	sum(EventNotificationEnabledBucketCount)/sum(DistinctNumberOfBuckets)
Todas as solicitações	AllRequests	O número total de solicitações feitas	Advanced (Avançado)	Atividade	Nenhum	-

Nome da métrica	CloudWatch e exportação	Descrição	Níve	Cate[2]	D	Fórm da métri deriv
Solicitações GET	GetRequests	O número total de solicitações `GET` feitas	Adva (Ava)	Ativi	N	-
Solicitações PUT	PutRequests	O número total de solicitações `PUT` feitas	Adva (Ava)	Ativi	N	-
Solicitações HEAD	HeadRequests	O número total de solicitações `HEAD` feitas	Adva (Ava)	Ativi	N	-
Solicitações DELETE	DeleteReq uests	O número total de solicitações `DELETE` feitas	Adva (Ava)	Ativi	N	-
Solicitações LIST	ListRequests	O número total de solicitações `LIST` feitas	Adva (Ava)	Ativi	N	-
Solicitações POST	PostRequests	O número total de solicitações `POST` feitas	Adva (Ava)	Ativi	N	-
Solicitações SELECT	SelectRequests	O número total de solicitações do S3 Select	Adva (Ava)	Ativi	N	-
Bytes verificad os do Select	SelectSca nnedBytes	O número de bytes verificados do S3 Select	Adva (Ava)	Ativi	N	-

Nome da métrica	CloudWatch e exportação	Descrição	Níve	Cate[2]	D	Fórm da métri deriv
Bytes devolvidos do Select	SelectReturnedBytes	O número de bytes devolvidos do S3 Select	Adva (Ava)	Ativi	N	-
Bytes baixados	BytesDownloaded	O número de bytes baixados	Adva (Ava)	Ativi	N	-
% de taxa de recuperação	-	A porcentagem de bytes baixados	Adva (Ava)	Ativi	S	sum(BytesDownloaded)/ sum(StorageBytes)
Bytes carregados	BytesUploaded	O número de bytes enviados por upload	Adva (Ava)	Ativi	N	-
% de relação de consumo	-	A porcentagem de bytes carregados	Adva (Ava)	Ativi	S	sum(BytesUploaded) / sum(StorageBytes)
Erros 4xx	4xxErrors	O número total de códigos de status HTTP 4xx	Adva (Ava)	Ativi	N	-
Erros 5xx	5xxErrors	O número total de códigos de status HTTP 5xx	Adva (Ava)	Ativi	N	-

Nome da métrica	CloudWatch e exportação	Descrição	Nível	Categoria[2]	Dimensões	Fórmula da métrica derivada
Total de erros	-	A soma de todos os erros 4xx e 5xx	Avançado (Avançado)	Atividade	Sim	sum(4xxErrors) + sum(5xxErrors)
% de taxa de erros	-	O número total de erros 4xx e 5xx como uma porcentagem do total de solicitações	Avançado (Avançado)	Atividade	Sim	sum(TotalErrors)/sum(TotalRequests)
Contagem de status 200 OK	200OKStatusCount	A contagem total de códigos de status 200 OK	Avançado (Avançado)	Código de status detalhado	Não	-
% de status 200 OK	-	O número total de códigos de status 200 OK como uma porcentagem do total de solicitações	Avançado (Avançado)	Código de status detalhado	Sim	sum(200OKStatusCount)/sum(AllRequests)
Contagem de status 206 Conteúdo Parcial	206PartialContentStatusCount	A contagem total de códigos de status 206 Conteúdo Parcial	Avançado (Avançado)	Código de status detalhado	Não	-

Nome da métrica	CloudWatch e exportação	Descrição	Nível	Categ[2]	D	Fórm da métri deriv
% de status 206 Conteúdo Parcial	-	O número total de códigos de status 206 Conteúdo Parcial como uma porcentagem do total de solicitações	Adva (Ava)	Códi de statu deta	S	sum(206PartialContentStatusCount)/sum(AllRequests)
Contagem de erros 400 Solicitação Inválida	400BadRequestErrorCount	A contagem total de códigos de status 400 Solicitação Inválida	Adva (Ava)	Códi de statu deta	N	-
% de erros 400 Solicitação Inválida	-	O número total de códigos de status 400 Solicitação Inválida como uma porcentagem do total de solicitações	Adva (Ava)	Códi de statu deta	S	sum(400BadRequestErrorCount)/sum(AllRequests)
Contagem de erros 403 Proibido	403ForbiddenErrorCount	A contagem total de códigos de status 403 Proibido	Adva (Ava)	Códi de statu deta	N	-

Nome da métrica	CloudWatch e exportação	Descrição	Nível	Categoria[2]	Dimensões	Fórmula da métrica derivada
% de erros 403 Proibido	-	O número total de códigos de status 403 Proibido como uma porcentagem do total de solicitações	Avançado (Avançado)	Código de status detalhado	Sim	sum(403ForbiddenErrorCount) / sum(AllRequests)
Contagem de erros 404 Não Encontrado	404NotFoundErrorCount	A contagem total de códigos de status 404 Não Encontrado	Avançado (Avançado)	Código de status detalhado	Não	-
% de erros 404 Não Encontrado	-	O número total de códigos de status 404 Não Encontrado como uma porcentagem do total de solicitações	Avançado (Avançado)	Código de status detalhado	Sim	sum(404NotFoundErrorCount)/ sum(AllRequests)
Contagem de erros 500 Erro Interno do Servidor	500InternalServerErrorCount	A contagem total de códigos de status 500 Erro Interno do Servidor	Avançado (Avançado)	Código de status detalhado	Não	-

Nome da métrica	CloudWatch e exportação	Descrição	Nível	Cate[2]	De	Fórm da métri deriv
% de erros 500 Erro Interno do Servidor	-	O número total de códigos de status 500 Erro Interno do Servidor como uma porcentag em do total de solicitações	Adva (Ava)	Códi de statu deta	S	sum(500In ternalSer verErrorC ount)/ sum (AllReque sts)
Contagem de erros 503 Serviço Indisponível	503Servic eUnavaila bleErrorCount	A contagem total de códigos de status 503 Serviço Indisponível	Adva (Ava)	Códi de statu deta	N	-
% de erros 503 Serviço Indisponível	-	O número total de códigos de status 503 Serviço Indisponível como uma porcentag em do total de solicitações	Adva (Ava)	Códi de statu deta	S	sum(503Se rviceUnav ailableEr rorCount) / sum(AllR equests)

[1] Todas as métricas de armazenamento gratuito estão disponíveis no nível do grupo da Lente de Armazenamento. As métricas de nível avançado não estão disponíveis no nível do grupo da Lente de Armazenamento.

[2] As métricas de contagem de regras e de configurações de bucket não estão disponíveis no nível do prefixo.

Configurar permissões da Lente de Armazenamento do Amazon S3

O Amazon S3 Storage Lens requer novas permissões no AWS Identity and Access Management (IAM) para autorizar o acesso às ações do S3 Storage Lens. Para conceder essas permissões, você

pode usar uma política do IAM baseada em identidade. Você pode vincular essa política a usuários, grupos ou funções do IAM para conceder permissões. Essas permissões podem incluir a capacidade de ativar ou desativar a Lente de Armazenamento do S3 ou acessar qualquer painel ou configuração da Lente de Armazenamento do S3.

O usuário ou a função do IAM deve pertencer à conta que criou ou tem o painel ou a configuração, a menos que as duas condições a seguir sejam verdadeiras:

- Sua conta é membro do AWS Organizations.
- Você recebeu acesso para criar painéis no nível da organização por sua conta de gerenciamento como administrador delegado.

> **Note**
>
> - Você não pode usar as credenciais de usuário raiz da sua conta para visualizar os painéis da Lente de Armazenamento do Amazon S3. Para acessar os painéis da Lente de Armazenamento do S3, você deve conceder as permissões do IAM necessárias a um usuário do IAM novo ou existente. Em seguida, faça login com essas credenciais de usuário para acessar os painéis do S3 Storage Lens. Para obter mais informações, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.
> - O uso do S3 Storage Lens no console do Amazon S3 pode exigir várias permissões. Por exemplo; para editar um painel no console, você precisa das seguintes permissões:
>   - `s3:ListStorageLensConfigurations`
>   - `s3:GetStorageLensConfiguration`
>   - `s3:PutStorageLensConfiguration`

Tópicos

- Definição de permissões de conta para usar o S3 Storage Lens
- Definição de permissões de conta para usar a Lente de Armazenamento do S3
- Configuração de permissões para usar o Amazon S3 Storage Lens com AWS Organizations

Definição de permissões de conta para usar o S3 Storage Lens

Para criar e gerenciar painéis da Lente de Armazenamento do S3 e configurações de painel da Lente de Armazenamento, você deve ter as seguintes permissões, dependendo de quais ações deseja executar:

A tabela a seguir mostra o recurso Lente de Armazenamento do Amazon S3 relacionado a permissões do IAM.

Ação	Permissões do IAM

Criar ou atualizar um painel do S3 Storage Lens no console do Amazon S3.	`s3:ListStorageLensConfigurations`
	`s3:GetStorageLensConfiguration`
	`s3:GetStorageLensConfigurationTagging`
	`s3:PutStorageLensConfiguration`
	`s3:PutStorageLensConfigurationTagging`

Obter as etiquetas de um painel da Lente de Armazenamento do S3 no console do Amazon S3.	`s3:ListStorageLensConfigurations` `s3:GetStorageLensConfigurationTagging`

Veja um painel do S3 Storage Lens no console do Amazon S3.	`s3:ListStorageLensConfigurations`
	`s3:GetStorageLensConfiguration`
	`s3:GetStorageLensDashboard`

Exclua um painel do S3 Storage Lens no console do Amazon S3.	`s3:ListStorageLensConfigurations`
	`s3:GetStorageLensConfiguration`
	`s3:DeleteStorageLensConfiguration`

Ação	Permissões do IAM
Criar ou atualizar uma configuração da Lente de Armazenamento do S3 usando a AWS CLI ou um AWS SDK.	`s3:PutStorageLensConfiguration` `s3:PutStorageLensConfigurationTagging`
Obter as etiquetas de uma configuração da Lente de Armazenamento do S3 usando a AWS CLI ou um AWS SDK.	`s3:GetStorageLensConfigurationTagging`
Visualizar uma configuração da Lente de Armazenamento do S3 usando a AWS CLI ou um AWS SDK.	`s3:GetStorageLensConfiguration`
Excluir uma configuração da Lente de Armazenamento do S3 usando a AWS CLI ou um AWS SDK.	`s3:DeleteStorageLensConfiguration`

Note

- Você pode usar tags de recurso em uma política do IAM para gerenciar permissões.
- Um usuário ou perfil do IAM com essas permissões pode ver métricas de buckets e prefixos dos quais pode não ter permissão direta para ler ou listar objetos.
- No caso de painéis da Lente de Armazenamento do S3 com métricas em nível de prefixo habilitadas, se um caminho de prefixo selecionado corresponder a uma chave de objeto, o painel poderá exibir a chave de objeto como outro prefixo.
- Para as exportações de métricas, que são armazenadas em um bucket em sua conta, as permissões são concedidas usando a permissão `s3:GetObject` existente na política do IAM. Da mesma forma, para uma entidade do AWS Organizations, a conta de gerenciamento da organização ou as contas de administrador delegado podem usar políticas do IAM para gerenciar as permissões de acesso para configurações e painéis no nível da organização.

Definição de permissões de conta para usar a Lente de Armazenamento do S3

Você pode usar grupos da Lente de Armazenamento do S3 para entender a distribuição do seu armazenamento dentro de buckets com base no prefixo, sufixo, tag do objeto, tamanho do objeto ou idade do objeto. Você pode anexar grupos da Lente de Armazenamento aos seus painéis para ver suas métricas agregadas.

Para trabalhar com grupos da Lente de Armazenamento, você precisa de determinadas permissões. Para obter mais informações, consulte the section called “Permissões de grupos de Lente de Armazenamento”.

Configuração de permissões para usar o Amazon S3 Storage Lens com AWS Organizations

Você pode usar o Amazon S3 Storage Lens para coletar métricas de armazenamento e dados de uso de todas as contas que fazem parte da hierarquia do AWS Organizations. As tabelas a seguir mostram as ações e permissões relacionadas ao uso do recurso Lente de Armazenamento do S3 com o Organizations.

Ação	Permissões do IAM
Habilite o acesso confiável para o S3 Storage Lens para sua organização.	`organizations:EnableAWSServiceAccess`
Desative o acesso confiável para a Lente de Armazenamento do S3 em sua organização.	`organizations:DisableAWSServiceAccess`
Registre um administrador delegado para criar painéis ou configurações do S3 Storage Lens para sua organização.	`organizations:RegisterDelegatedAdministrator`
Cancele o registro de um administrador delegado para que ele não possa mais criar painéis ou configurações da Lente de Armazenamento do S3 em sua organização.	`organizations:DeregisterDelegatedAdministrator`
Permissões adicionais para criar configurações para toda a organização da Lente de Armazenamento do S3.	`organizations:DescribeOrganization`

Ação	Permissões do IAM

	`organizations:ListAccounts`
	
	`organizations:ListAWSServiceAccessForOrganization`
	
	`organizations:ListDelegatedAdministrators`
	
	`iam:CreateServiceLinkedRole`

Trabalhar com a Lente de Armazenamento do Amazon S3 usando o console e a API

A Lente de Armazenamento do Amazon S3 é um recurso de análise de armazenamento em nuvem que você pode usar para obter visibilidade em toda a organização sobre o uso e a atividade do armazenamento de objetos. Use as métricas da Lente de Armazenamento do S3 para gerar insights resumidos, como descobrir quanto armazenamento você tem em toda a organização ou quais são os buckets e prefixos que mais crescem. Você também pode usar as métricas da Lente de Armazenamento do S3 para identificar oportunidades de otimização de custos, implementar práticas recomendadas de proteção e segurança de dados, e melhorar a performance das workloads de aplicações. Por exemplo, você pode identificar buckets que não têm regras de Ciclo de Vida do S3 para expirar multipart uploads incompletos com mais de 7 dias. Você também pode identificar buckets que não estão seguindo as práticas recomendadas de proteção de dados, como usar a Replicação do S3 ou o Versionamento do S3. A Lente de Armazenamento do S3 também analisa as métricas para fornecer recomendações contextuais que você pode usar para otimizar os custos de armazenamento e aplicar as práticas recomendadas de proteção de dados.

A Lente de Armazenamento do S3 agrega suas métricas e exibe as informações na seção Account snapshot (Snapshot da conta) na página Buckets do console do Amazon S3. A Lente de Armazenamento do S3 também oferece um painel interativo para visualizar insights e tendências, sinalizar discrepâncias e receber recomendações para otimizar os custos de armazenamento e aplicar as práticas recomendadas de proteção de dados. O painel tem opções de detalhamento para gerar e visualizar insights no nível da organização, conta, Região da AWS, classe de armazenamento, bucket, prefixo ou grupo de Lente de Armazenamento. Você também pode enviar uma exportação diária de métricas em CSV ou no formato Parquet para um bucket do S3.

Esta seção contém exemplos de criação, atualização e exibição de configurações do S3 Storage Lens e execução de operações relacionadas ao recurso. Se você estiver usando o S3 Storage Lens com o AWS Organizations, esses exemplos também abordam esses casos de uso. Nos exemplos, substitua todos os valores de variável por valores adequados às suas necessidades.

Tópicos

- Criar um painel da Lente de Armazenamento do Amazon S3
- Atualizar um painel da Lente de Armazenamento do Amazon S3
- Desabilitar um painel da Lente de Armazenamento do Amazon S3
- Excluir um painel da Lente de Armazenamento do Amazon S3
- Listar painéis da Lente de Armazenamento do Amazon S3
- Visualizar detalhes de configuração do painel da Lente de Armazenamento do Amazon S3
- Gerenciamento de tags de recursos da AWS com a Lente de Armazenamento do S3
- Arquivos auxiliares para usar o Amazon S3 Storage Lens

Criar um painel da Lente de Armazenamento do Amazon S3

Você pode criar painéis personalizados adicionais da Lente de Armazenamento do S3 que podem ser colocados no escopo de sua organização no AWS Organizations ou em Regiões da AWS específicas ou buckets específicos em uma conta.

> **Note**
>
> As atualizações na configuração do painel podem levar até 48 horas para serem exibidas ou visualizadas com precisão.

Usar o console do S3

Use as etapas a seguir para criar um painel do Amazon S3 Storage Lens no console do Amazon S3.

Etapa 1: Definir o escopo do painel

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Na barra de navegação na parte superior da página, escolha o nome da região da AWS exibida no momento. Em seguida, escolha a região para a qual você deseja mudar.

3. No painel de navegação esquerdo, em Lente de Armazenamento do S3, selecione Painéis.
4. Escolha Create dashboard (Criar painel).
5. Na página Dashboard (Painel), na seção General (Geral), faça o seguinte:

   a. Visualize a Região de origem para seu painel. A região de origem é a Região da AWS em que a configuração e as métricas referentes a esse painel do Lente de Armazenamento estão armazenadas.

   b. Insira um nome de painel.

      Os nomes do painel devem ter menos de 65 caracteres e não devem conter caracteres ou espaços especiais.

      > **Note**
      >
      > Não é possível alterar o nome do painel depois que o painel for criado.

   c. Opcionalmente, você pode optar por adicionar Tags ao seu painel. Você pode usar tags para gerenciar permissões para seu painel e rastrear os custos para o S3 Storage Lens.

      Para obter mais informações, consulte Controle do acesso usando tags de recurso no Guia do usuário do IAM e Tags de alocação de custos geradas pela AWS no Guia do usuário do AWS Billing.

      > **Note**
      >
      > Você pode adicionar até 50 tags à configuração do painel.

6. Na seção Dashboard scope (Escopo do painel), faça o seguinte:

   a. Escolha as regiões e os buckets que deseja que o S3 Storage Lens inclua ou exclua no painel.

   b. Escolha os buckets nas regiões selecionadas que deseja que o S3 Storage Lens inclua ou exclua. Você pode incluir ou excluir buckets, mas não ambos. Essa opção não está disponível quando você cria painéis no nível da organização.

> **Note**
>
> - Você pode incluir ou excluir regiões e buckets. Essa opção é limitada a regiões somente ao criar painéis no nível da organização em contas de membro na sua organização.
> - Você pode escolher até 50 buckets para incluir ou excluir.

Etapa 2: Configurar a seleção de métricas

1. Na seção Metrics selection (Seleção de métricas), escolha o tipo de métricas que você deseja agregar para este painel.

   - Para incluir métricas gratuitas agregadas por bucket e disponíveis para consultas por 14 dias, escolha Free metrics (Métricas gratuitas).
   - Para ativar métricas avançadas e outras opções avançadas, escolha Advanced metrics and recommendations (Métricas e recomendações avançadas). Essas opções incluem agregação avançada de prefixos, publicação do Amazon CloudWatch e recomendações contextuais. Os dados ficam disponíveis para consultas por 15 meses. As métricas e recomendações avançadas têm um custo adicional. Para obter mais informações, consulte Definição de preço do Amazon S3.

     Para obter mais informações sobre métricas avançadas e métricas gratuitas, consulte Seleção de métricas.
2. Em Advanced metrics and recommendations features (Recursos de métricas e recomendações avançadas), selecione as opções que deseja habilitar:

   - Advanced metrics (Métricas avançadas)
   - Publicação no CloudWatch
   - Agregação de prefixo

> **Important**
>
> Se você habilitar a agregação de prefixos na configuração do S3 Storage Lens, as métricas de nível de prefixo não serão publicadas no CloudWatch. Somente métricas

em nível de organização, conta e bucket do S3 Storage Lens são publicadas no CloudWatch.

3. Se você ativou Advanced metrics (Métricas avançadas), selecione as Advanced metrics categories (Categorias de métricas avançadas) que deseja exibir no painel da Lente de Armazenamento do S3:

   - Métricas de atividade
   - Detailed status code metrics (Métricas detalhadas do código de status)
   - Advanced cost optimization metrics (Métricas avançadas de otimização de custos)
   - Advanced data protection metrics (Métricas avançadas de proteção de dados)

   Para obter mais informações sobre categorias de métricas, consulte Categorias de métricas. Para obter uma lista completa de métricas, consulte Glossário de métricas de lente de armazenamento do Amazon S3.

4. Caso tenha optado por habilitar a agregação de prefixos, configure o seguinte:

   a. Escolha o tamanho mínimo de limite de prefixo para este painel.

      Por exemplo, um limite de prefixo de 5% indica que serão agregados os prefixos que compõem 5% ou mais do tamanho total do armazenamento do bucket.

   b. Escolha o nome do prefixo.

      Essa configuração indica o número máximo de níveis até os quais os prefixos são avaliados. A profundidade do prefixo deve ser inferior a 10.

   c. Insira um caractere delimitador de prefixo.

      Este valor é usado para identificar cada nível de prefixo. O valor padrão no Amazon S3 é o caractere `/`, mas sua estrutura de armazenamento pode usar outros caracteres delimitadores.

(Opcional) Etapa 3: Exportar métricas para o painel

1. Na seção Metrics export (Exportação de métricas), escolha Enable (Ativar) para criar uma exportação de métricas que será colocada diariamente em um bucket de destino de sua escolha.

A exportação de métricas acontece no formato CSV ou Apache Parquet. Ele representa o mesmo escopo de dados que os dados do painel do S3 Storage Lens sem as recomendações.

2. Se a exportação de métricas foi ativada, escolha o formato de saída da exportação diária: CSV ou Apache Parquet.

   Parquet é um formato de arquivo de código aberto para Hadoop que armazena dados aninhados em um formato colunar plano.

3. Escolha o bucket do S3 de destino para sua exportação de métricas.

   Você pode escolher um bucket na conta atual do painel do S3 Storage Lens. Ou você poderá escolher outra Conta da AWS se tiver as permissões do bucket de destino e o ID da conta do proprietário do bucket de destino.

4. Escolha o bucket do S3 de destino (formato: `s3://bucket-name/prefix`).

   O bucket deve estar na região inicial do seu painel da Lente de Armazenamento do S3. O console do S3 mostra a Destination bucket permission (Permissão do bucket de destino) que será adicionada pelo Amazon S3 à política do bucket de destino. O Amazon S3 atualiza a política no bucket de destino para permitir que o S3 coloque dados nesse bucket.

5. (Opcional) Para habilitar a criptografia do lado do servidor para a exportação de métricas, escolha Specify an encryption key (Especificar uma chave de criptografia). Depois, escolha Tipo de criptografia: Chaves gerenciadas do Amazon S3 (SSE-S3) ou Chave do AWS Key Management Service (SSE-KMS).

   Você pode escolher entre uma chave gerenciada pelo Amazon S3 (SSE-S3) e uma chave do AWS Key Management Service (AWS KMS) (SSE-KMS).

6. (Opcional) Para especificar uma chave do AWS KMS, você deve escolher uma chave do KMS ou inserir o nome do recurso da Amazon (ARN) de uma chave.

   Se escolher uma chave gerenciada pelo cliente, você deverá conceder permissão de criptografia à Lente de Armazenamento do S3 na política de chaves do AWS KMS. Para obter mais informações, consulte Usar uma AWS KMS key para criptografar suas exportações de métricas.

7. Escolha Create dashboard (Criar painel).

Como usar o AWS CLI

Example

O comando de exemplo a seguir cria uma configuração da Lente de Armazenamento do Amazon S3 com tags. Para usar esses exemplos, substitua os *user input placeholders* por suas próprias informações.

```
aws s3control put-storage-lens-configuration --account-id=111122223333 --
config-id=example-dashboard-configuration-id --region=us-east-1 --storage-lens-
configuration=file://./config.json --tags=file://./tags.json
```

Example

O comando de exemplo a seguir cria uma configuração da Lente de Armazenamento do Amazon S3 sem tags. Para usar esses exemplos, substitua os *user input placeholders* por suas próprias informações.

```
aws s3control put-storage-lens-configuration --account-id=222222222222 --config-
id=your-configuration-id --region=us-east-1 --storage-lens-configuration=file://./
config.json
```

Usar o AWS SDK para Java

Example – Criar e atualizar uma configuração da Lente de Armazenamento do Amazon S3

O exemplo a seguir cria e atualiza uma configuração da Lente de Armazenamento do Amazon S3 no SDK para Java:

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import com.amazonaws.services.s3control.model.AccountLevel;
import com.amazonaws.services.s3control.model.ActivityMetrics;
import com.amazonaws.services.s3control.model.BucketLevel;
import com.amazonaws.services.s3control.model.CloudWatchMetrics;
import com.amazonaws.services.s3control.model.Format;
import com.amazonaws.services.s3control.model.Include;
```

```
import com.amazonaws.services.s3control.model.OutputSchemaVersion;
import com.amazonaws.services.s3control.model.PrefixLevel;
import com.amazonaws.services.s3control.model.PrefixLevelStorageMetrics;
import com.amazonaws.services.s3control.model.PutStorageLensConfigurationRequest;
import com.amazonaws.services.s3control.model.S3BucketDestination;
import com.amazonaws.services.s3control.model.SSES3;
import com.amazonaws.services.s3control.model.SelectionCriteria;
import com.amazonaws.services.s3control.model.StorageLensAwsOrg;
import com.amazonaws.services.s3control.model.StorageLensConfiguration;
import com.amazonaws.services.s3control.model.StorageLensDataExport;
import com.amazonaws.services.s3control.model.StorageLensDataExportEncryption;
import com.amazonaws.services.s3control.model.StorageLensTag;

import java.util.Arrays;
import java.util.List;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class CreateAndUpdateDashboard {

    public static void main(String[] args) {
        String configurationId = "ConfigurationId";
        String sourceAccountId = "111122223333";
        String exportAccountId = "Destination Account ID";
        String exportBucketArn = "arn:aws:s3:::destBucketName"; // The destination
 bucket for your metrics export must be in the same Region as your S3 Storage Lens
 configuration.
        String awsOrgARN = "arn:aws:organizations::123456789012:organization/o-
abcdefgh";
        Format exportFormat = Format.CSV;

        try {
            SelectionCriteria selectionCriteria = new SelectionCriteria()
                    .withDelimiter("/")
                    .withMaxDepth(5)
                    .withMinStorageBytesPercentage(10.0);
            PrefixLevelStorageMetrics prefixStorageMetrics = new
 PrefixLevelStorageMetrics()
                    .withIsEnabled(true)
                    .withSelectionCriteria(selectionCriteria);
            BucketLevel bucketLevel = new BucketLevel()
                    .withActivityMetrics(new ActivityMetrics().withIsEnabled(true))
                    .withAdvancedCostOptimizationMetrics(new
 AdvancedCostOptimizationMetrics().withIsEnabled(true))
```

```
                    .withAdvancedDataProtectionMetrics(new
AdvancedDataProtectionMetrics().withIsEnabled(true))
                    .withDetailedStatusCodesMetrics(new
DetailedStatusCodesMetrics().withIsEnabled(true))
                    .withPrefixLevel(new
PrefixLevel().withStorageMetrics(prefixStorageMetrics));
            AccountLevel accountLevel = new AccountLevel()
                    .withActivityMetrics(new ActivityMetrics().withIsEnabled(true))
                    .withAdvancedCostOptimizationMetrics(new
AdvancedCostOptimizationMetrics().withIsEnabled(true))
                    .withAdvancedDataProtectionMetrics(new
AdvancedDataProtectionMetrics().withIsEnabled(true))
                    .withDetailedStatusCodesMetrics(new
DetailedStatusCodesMetrics().withIsEnabled(true))
                    .withBucketLevel(bucketLevel);

            Include include = new Include()
                    .withBuckets(Arrays.asList("arn:aws:s3:::bucketName"))
                    .withRegions(Arrays.asList("us-west-2"));

            StorageLensDataExportEncryption exportEncryption = new
StorageLensDataExportEncryption()
                    .withSSES3(new SSES3());
            S3BucketDestination s3BucketDestination = new S3BucketDestination()
                    .withAccountId(exportAccountId)
                    .withArn(exportBucketArn)
                    .withEncryption(exportEncryption)
                    .withFormat(exportFormat)
                    .withOutputSchemaVersion(OutputSchemaVersion.V_1)
                    .withPrefix("Prefix");
            CloudWatchMetrics cloudWatchMetrics = new CloudWatchMetrics()
                    .withIsEnabled(true);
            StorageLensDataExport dataExport = new StorageLensDataExport()
                    .withCloudWatchMetrics(cloudWatchMetrics)
                    .withS3BucketDestination(s3BucketDestination);

            StorageLensAwsOrg awsOrg = new StorageLensAwsOrg()
                    .withArn(awsOrgARN);

            StorageLensConfiguration configuration = new StorageLensConfiguration()
                    .withId(configurationId)
                    .withAccountLevel(accountLevel)
                    .withInclude(include)
                    .withDataExport(dataExport)
```

```
                    .withAwsOrg(awsOrg)
                    .withIsEnabled(true);

            List<StorageLensTag> tags = Arrays.asList(
                    new StorageLensTag().withKey("key-1").withValue("value-1"),
                    new StorageLensTag().withKey("key-2").withValue("value-2")
            );

            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(US_WEST_2)
                    .build();

            s3ControlClient.putStorageLensConfiguration(new
 PutStorageLensConfigurationRequest()
                    .withAccountId(sourceAccountId)
                    .withConfigId(configurationId)
                    .withStorageLensConfiguration(configuration)
                    .withTags(tags)
            );
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Para obter mais visibilidade do seu armazenamento, você pode criar um ou mais grupos da Lente de Armazenamento do S3 e anexá-los ao seu painel. Um grupo da Lente de Armazenamento do S3 é um filtro personalizado definido para objetos com base em prefixos, sufixos, tags de objeto, tamanho do objeto, idade do objeto ou uma combinação desses filtros.

Você pode usar grupos da Lente de Armazenamento do S3 para obter visibilidade granular de grandes buckets compartilhados, como data lakes, para tomar decisões de negócios mais bem informadas. Por exemplo, você pode simplificar a alocação de armazenamento e otimizar os

relatórios de custos dividindo o uso do armazenamento em grupos específicos de objetos para projetos individuais e centros de custo dentro de um bucket ou em vários buckets.

Para usar grupos da Lente de Armazenamento do S3, você deve atualizar o painel para usar métricas e recomendações avançadas. Para obter mais informações sobre grupos de Lente de Armazenamento do S3, consulte the section called “Trabalhar com grupos da Lente de Armazenamento”.

Atualizar um painel da Lente de Armazenamento do Amazon S3

O painel padrão da Lente de Armazenamento do Amazon S3 é `default-account-dashboard`. Esse painel é pré-configurado pelo Amazon S3 para ajudar você a visualizar tendências e insights resumidos para as métricas gratuitas e avançadas agregadas de toda a sua conta no console. Você não pode modificar o escopo de configuração padrão do painel, mas pode atualizar a seleção de métricas das métricas gratuitas para as métricas e recomendações avançadas pagas, configurar a exportação opcional de métricas ou até mesmo desativar o painel padrão. O painel padrão não pode ser excluído, só pode ser desabilitado. Para obter mais informações, consulte Usar o console do S3.

Usar o console do S3

Use as etapas a seguir para atualizar um painel do Amazon S3 Storage Lens no console do Amazon S3.

Etapa 1: Atualizar o escopo do painel

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação esquerdo, escolha Storage Lens, Dashboards (Lente de Armazenamento, Painéis).
3. Escolha o painel que você deseja editar e escolha Edit (Editar).

   A página Edit dashboard (Editar painel) é aberta.

> **Note**
>
> Você não pode alterar o seguinte:
>
> - O nome do painel
> - A região inicial

- O escopo do painel padrão, que tem escopo para o armazenamento de toda a sua conta

4. (Opcional) Na página de configuração do painel, na seção General (Geral), atualize e adicione etiquetas ao seu painel.

   Você pode usar tags para gerenciar permissões para seu painel e rastrear os custos para o S3 Storage Lens. Para obter mais informações, consulte Controle do acesso usando tags de recurso no Guia do usuário do IAM e Tags de alocação de custos geradas pela AWS no Guia do usuário do AWS Billing.

   > **Note**
   >
   > Você pode adicionar até 50 tags à configuração do painel.

5. Na seção Dashboard scope (Escopo do painel), faça o seguinte:

   a. Atualize as regiões e os buckets que deseja que o S3 Storage Lens inclua ou exclua no painel.

      > **Note**
      >
      > - Você pode incluir ou excluir regiões e buckets. Essa opção é limitada a regiões somente ao criar painéis no nível da organização em contas de membro na sua organização.
      > - Você pode escolher até 50 buckets para incluir ou excluir.

   b. Atualize os buckets nas regiões selecionadas que deseja que o S3 Storage Lens inclua ou exclua. Você pode incluir ou excluir buckets, mas não ambos. Esta opção não está presente ao criar painéis no nível da organização.

Etapa 2: Atualizar a seleção de métricas

1. Na seção Metrics selection (Seleção de métricas), escolha o tipo de métricas que você deseja agregar para este painel.

   - Para incluir métricas gratuitas agregadas por bucket e disponíveis para consultas por 14 dias, escolha Free metrics (Métricas gratuitas).

- Para ativar métricas avançadas e outras opções avançadas, escolha Advanced metrics and recommendations (Métricas e recomendações avançadas). Essas opções incluem agregação avançada de prefixos, publicação do Amazon CloudWatch e recomendações contextuais. Os dados ficam disponíveis para consultas por 15 meses. As métricas e recomendações avançadas têm um custo adicional. Para obter mais informações, consulte Definição de preço do Amazon S3.

  Para obter mais informações sobre métricas avançadas e métricas gratuitas, consulte Seleção de métricas.

2. Em Advanced metrics and recommendations features (Recursos de métricas e recomendações avançadas), selecione as opções que deseja habilitar:

   - Advanced metrics (Métricas avançadas)
   - Publicação no CloudWatch
   - Agregação de prefixo

   > **Important**
   >
   > Se você habilitar a agregação de prefixos na configuração do S3 Storage Lens, as métricas de nível de prefixo não serão publicadas no CloudWatch. Somente métricas em nível de organização, conta e bucket do S3 Storage Lens são publicadas no CloudWatch.

3. Se você ativou Advanced metrics (Métricas avançadas), selecione as Advanced metrics categories (Categorias de métricas avançadas) que deseja exibir no painel da Lente de Armazenamento do S3:

   - Métricas de atividade
   - Detailed status code metrics (Métricas detalhadas do código de status)
   - Advanced cost optimization metrics (Métricas avançadas de otimização de custos)
   - Advanced data protection metrics (Métricas avançadas de proteção de dados)

   Para obter mais informações sobre categorias de métricas, consulte Categorias de métricas. Para obter uma lista completa de métricas, consulte Glossário de métricas de lente de armazenamento do Amazon S3.

4. Caso tenha optado por habilitar a agregação de prefixos, configure o seguinte:

   a. Escolha o tamanho mínimo de limite de prefixo para este painel.

      Por exemplo, um limite de prefixo de 5% indica que serão agregados os prefixos que compõem 5% ou mais do tamanho total do armazenamento do bucket.

   b. Escolha o nome do prefixo.

      Essa configuração indica o número máximo de níveis até os quais os prefixos são avaliados. A profundidade do prefixo deve ser inferior a 10.

   c. Insira um caractere delimitador de prefixo.

      Este é o valor usado para identificar cada nível de prefixo. O valor padrão no Amazon S3 é o caractere `/`, mas sua estrutura de armazenamento pode usar outros caracteres delimitadores.

(Opcional) Etapa 3: Exportar métricas para o painel

1. Na seção Metrics export (Exportação de métricas), escolha Enable (Ativar) para criar uma exportação de métricas que será colocada diariamente em um bucket de destino de sua escolha. Para desativar a exportação de métricas, escolha Disable (Desativar).

   A exportação de métricas acontece no formato CSV ou Apache Parquet. Ele representa o mesmo escopo de dados que os dados do painel do S3 Storage Lens sem as recomendações.

2. Se ativada, escolha o formato de saída da exportação de métricas diária: CSV ou Apache Parquet.

   Parquet é um formato de arquivo de código aberto para Hadoop que armazena dados aninhados em um formato colunar plano.

3. Escolha o bucket do S3 de destino para sua exportação de métricas.

   Você pode escolher um bucket na conta atual do painel do S3 Storage Lens. Ou você poderá escolher outra Conta da AWS se tiver as permissões do bucket de destino e o ID da conta do proprietário do bucket de destino.

4. Escolha o bucket do S3 de destino (formato: `s3://`*`bucket-name`*`/`*`prefix`*).

   O bucket deve estar na região inicial do seu painel da Lente de Armazenamento do S3. O console do S3 mostra a Destination bucket permission (Permissão do bucket de destino) que

será adicionada pelo Amazon S3 à política do bucket de destino. O Amazon S3 atualiza a política no bucket de destino para permitir que o S3 coloque dados nesse bucket.

5. (Opcional) Para habilitar a criptografia do lado do servidor para a exportação de métricas, escolha Specify an encryption key (Especificar uma chave de criptografia). Depois, escolha Tipo de criptografia: Chaves gerenciadas do Amazon S3 (SSE-S3) ou Chave do AWS Key Management Service (SSE-KMS).

   Você pode escolher entre uma chave gerenciada pelo Amazon S3 (SSE-S3) e uma chave do AWS Key Management Service (AWS KMS) (SSE-KMS).

6. (Opcional) Para especificar uma chave do AWS KMS, você deve escolher uma chave do KMS ou inserir o nome do recurso da Amazon (ARN) de uma chave. Em Chave do AWS KMS, especifique sua chave do KMS de uma das seguintes maneiras:

   - Para escolher entre uma lista de chaves do KMS disponíveis, selecione Escolher entre suas AWS KMS keys e escolha sua chave do KMS na lista de chaves disponíveis.

     As chaves Chave gerenciada pela AWS (`aws/s3`) e as chaves gerenciadas pelo cliente são exibidas nessa lista. Para ter mais informações sobre chaves gerenciadas pelo cliente, consulte Chaves de clientes e chaves da AWS no Guia do desenvolvedor do AWS Key Management Service.

     > **Note**
     >
     > A Chave gerenciada pela AWS (`aws/S3`) não é compatível com a criptografia SSE-KMS com a Lente de Armazenamento do S3.

   - Para inserir o ARN da chave do KMS, escolha Inserir ARN da AWS KMS key e insira o ARN da chave do KMS no campo exibido.
   - Para criar uma chave gerenciada pelo cliente no console do AWS KMS, selecione Criar uma chave do KMS.

     Se escolher uma chave gerenciada pelo cliente, você deverá conceder permissão de criptografia à Lente de Armazenamento do S3 na política de chaves do AWS KMS. Para obter mais informações, consulte Usar uma AWS KMS key para criptografar suas exportações de métricas.

     Para obter mais informações sobre como criar uma AWS KMS key, consulte Criação de chaves no Guia do desenvolvedor do AWS Key Management Service.

7. Escolha Salvar alterações.

Para obter mais visibilidade do seu armazenamento, você pode criar um ou mais grupos da Lente de Armazenamento do S3 e anexá-los ao seu painel. Um grupo da Lente de Armazenamento do S3 é um filtro personalizado definido para objetos com base em prefixos, sufixos, tags de objeto, tamanho do objeto, idade do objeto ou uma combinação desses filtros.

Você pode usar grupos da Lente de Armazenamento do S3 para obter visibilidade granular de grandes buckets compartilhados, como data lakes, para tomar decisões de negócios mais bem informadas. Por exemplo, você pode simplificar a alocação de armazenamento e otimizar os relatórios de custos dividindo o uso do armazenamento em grupos específicos de objetos para projetos individuais e centros de custo dentro de um bucket ou em vários buckets.

Para usar grupos da Lente de Armazenamento do S3, você deve atualizar o painel para usar métricas e recomendações avançadas. Para obter mais informações sobre grupos de Lente de Armazenamento do S3, consulte the section called “Trabalhar com grupos da Lente de Armazenamento”.

Como usar o AWS CLI

Example

O exemplo de comando a seguir atualiza uma configuração de painel da Lente de Armazenamento do Amazon S3. Para usar esses exemplos, substitua os *`user input placeholders`* por suas próprias informações.

```
aws s3control put-storage-lens-configuration --account-id=111122223333 --
config-id=example-dashboard-configuration-id --region=us-east-1 --storage-lens-
configuration=file://./config.json --tags=file://./tags.json
```

Usar o AWS SDK para Java

Example – Atualizar uma configuração da Lente de Armazenamento do Amazon S3 com métricas e recomendações avançadas

Os exemplos a seguir mostram como atualizar a configuração padrão da Lente de Armazenamento do S3 com métricas e recomendações avançadas no SDK para Java:

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
```

```
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import com.amazonaws.services.s3control.model.AccountLevel;
import com.amazonaws.services.s3control.model.ActivityMetrics;
import com.amazonaws.services.s3control.model.BucketLevel;
import com.amazonaws.services.s3control.model.Format;
import com.amazonaws.services.s3control.model.Include;
import com.amazonaws.services.s3control.model.OutputSchemaVersion;
import com.amazonaws.services.s3control.model.PrefixLevel;
import com.amazonaws.services.s3control.model.PrefixLevelStorageMetrics;
import com.amazonaws.services.s3control.model.PutStorageLensConfigurationRequest;
import com.amazonaws.services.s3control.model.S3BucketDestination;
import com.amazonaws.services.s3control.model.SSES3;
import com.amazonaws.services.s3control.model.SelectionCriteria;
import com.amazonaws.services.s3control.model.StorageLensAwsOrg;
import com.amazonaws.services.s3control.model.StorageLensConfiguration;
import com.amazonaws.services.s3control.model.StorageLensDataExport;
import com.amazonaws.services.s3control.model.StorageLensDataExportEncryption;
import com.amazonaws.services.s3control.model.StorageLensTag;

import java.util.Arrays;
import java.util.List;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class UpdateDefaultConfigWithPaidFeatures {

    public static void main(String[] args) {
        String configurationId = "default-account-dashboard"; // This configuration ID
 cannot be modified.
        String sourceAccountId = "111122223333";

        try {
            SelectionCriteria selectionCriteria = new SelectionCriteria()
                    .withDelimiter("/")
                    .withMaxDepth(5)
                    .withMinStorageBytesPercentage(10.0);
            PrefixLevelStorageMetrics prefixStorageMetrics = new
 PrefixLevelStorageMetrics()
                    .withIsEnabled(true)
                    .withSelectionCriteria(selectionCriteria);
            BucketLevel bucketLevel = new BucketLevel()
```

```
                    .withActivityMetrics(new ActivityMetrics().withIsEnabled(true))
                    .withPrefixLevel(new
 PrefixLevel().withStorageMetrics(prefixStorageMetrics));
            AccountLevel accountLevel = new AccountLevel()
                    .withActivityMetrics(new ActivityMetrics().withIsEnabled(true))
                    .withBucketLevel(bucketLevel);

            StorageLensConfiguration configuration = new StorageLensConfiguration()
                    .withId(configurationId)
                    .withAccountLevel(accountLevel)
                    .withIsEnabled(true);

            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(US_WEST_2)
                    .build();

            s3ControlClient.putStorageLensConfiguration(new
 PutStorageLensConfigurationRequest()
                    .withAccountId(sourceAccountId)
                    .withConfigId(configurationId)
                    .withStorageLensConfiguration(configuration)
            );

        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

> **Note**
>
> Aplicam-se cobranças adicionais para métricas e recomendações avançadas. Para obter mais informações, consulte Métricas e recomendações avançadas.

Desabilitar um painel da Lente de Armazenamento do Amazon S3

É possível desabilitar um painel da Lente de Armazenamento do Amazon S3 pelo console do Amazon S3. Desabilitar um painel impede que ele gere métricas no futuro. Um painel desativado ainda mantém suas informações de configuração, para que possa ser facilmente retomado quando reativado. Um painel desabilitado retém seus dados históricos até que não estejam mais disponíveis para consultas.

Usar o console do S3

Use as etapas a seguir para desabilitar um painel da Lente de Armazenamento do Amazon S3 no console do Amazon S3.

Como desabilitar um painel da Lente de Armazenamento do Amazon S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação esquerdo, escolha Storage Lens (Lente de Armazenamento) e Dashboards (Painéis).
3. Na lista Dashboards (Painéis), escolha o painel que deseja desativar e, em seguida, escolha Disable (Desativar) na parte superior da lista.
4. Na página de confirmação, confirme se deseja desativar o painel inserindo o nome do painel no campo de texto e escolha Confirmar.

Excluir um painel da Lente de Armazenamento do Amazon S3

Você não pode excluir o painel padrão. No entanto, você poderá desabilitá-lo. Antes de excluir um painel que você criou, considere o seguinte:

- Como alternativa à exclusão de um painel, você pode desativar o painel para que ele esteja disponível para ser reativado no futuro. Para obter mais informações, consulte Usar o console do S3.
- A exclusão do painel excluirá todas as configurações associadas a ele.
- A exclusão de um painel torna todos os dados de métricas históricas indisponíveis. Esses dados históricos ainda são mantidos por 15 meses. Se você quiser acessar esses dados novamente, crie um painel com o mesmo nome na mesma região inicial daquele que foi excluído.

Usar o console do S3

É possível excluir um painel da Lente de Armazenamento do Amazon S3 do console do Amazon S3. No entanto, excluir um painel impede que ele gere métricas no futuro.

Exclusão de um painel do Amazon S3 Storage Lens

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação esquerdo, escolha Storage Lens (Lente de Armazenamento) e Dashboards (Painéis).
3. Na lista Dashboards (Painéis), escolha o painel que deseja excluir e escolha Delete (Excluir) na parte superior da lista.
4. Na página Excluir painéis, confirme se deseja excluir o painel inserindo o nome do painel no campo de texto. Depois, selecione Confirm (Confirmar).

Como usar o AWS CLI

Example

O exemplo a seguir exclui uma configuração da Lente de Armazenamento do S3. Para usar esses exemplos, substitua os *user input placeholders* por suas próprias informações.

```
aws s3control delete-storage-lens-configuration --account-id=222222222222 --region=us-east-1 --config-id=your-configuration-id
```

Usar o AWS SDK para Java

Example – Excluir uma configuração de painel da Lente de Armazenamento do Amazon S3

O exemplo a seguir mostra como excluir uma configuração da Lente de Armazenamento do S3 usando o SDK para Java:

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;
```

```
import com.amazonaws.services.s3control.AWSS3ControlClient;
import com.amazonaws.services.s3control.model.DeleteStorageLensConfigurationRequest;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class DeleteDashboard {

    public static void main(String[] args) {
        String configurationId = "ConfigurationId";
        String sourceAccountId = "111122223333";
        try {
            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(US_WEST_2)
                    .build();

            s3ControlClient.deleteStorageLensConfiguration(new
 DeleteStorageLensConfigurationRequest()
                    .withAccountId(sourceAccountId)
                    .withConfigId(configurationId)
            );
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Listar painéis da Lente de Armazenamento do Amazon S3

Usar o console do S3

Como listar painéis da Lente de Armazenamento do S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, acesse Lente de Armazenamento.

3. Escolha Painéis. Agora você pode visualizar os painéis em sua Conta da AWS.

Como usar o AWS CLI

Example

O exemplo de comando a seguir lista os painéis da Lente de Armazenamento do S3 em sua Conta da AWS. Para usar esses exemplos, substitua os *user input placeholders* por suas próprias informações.

```
aws s3control list-storage-lens-configurations --account-id=222222222222 --region=us-east-1 --next-token=abcdefghij1234
```

Example

O exemplo a seguir lista configurações da Lente de Armazenamento do S3 sem um próximo token. Para usar esses exemplos, substitua os *user input placeholders* por suas próprias informações.

```
aws s3control list-storage-lens-configurations --account-id=222222222222 --region=us-east-1
```

Usar o AWS SDK para Java

Example – Listar configurações do painel da Lente de Armazenamento do S3

Os exemplos a seguir mostram como listar as configurações da Lente de Armazenamento do S3 no SDK para Java. Para usar esse exemplo, substitua os *user input placeholders* por suas próprias informações. para cada descrição de exemplo.

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import com.amazonaws.services.s3control.model.ListStorageLensConfigurationEntry;
import com.amazonaws.services.s3control.model.ListStorageLensConfigurationsRequest;
```

```
import java.util.List;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class ListDashboard {

    public static void main(String[] args) {
        String sourceAccountId = "111122223333";
        String nextToken = "nextToken";

        try {
            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(US_WEST_2)
                    .build();

            final List<ListStorageLensConfigurationEntry> configurations =
                    s3ControlClient.listStorageLensConfigurations(new
 ListStorageLensConfigurationsRequest()
                            .withAccountId(sourceAccountId)
                            .withNextToken(nextToken)
                    ).getStorageLensConfigurationList();

            System.out.println(configurations.toString());
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Visualizar detalhes de configuração do painel da Lente de Armazenamento do Amazon S3

É possível visualizar um painel da Lente de Armazenamento do Amazon S3 do console do Amazon S3, da AWS CLI e do SDK para Java.

Usar o console do S3

Como visualizar detalhes da configuração do painel da Lente de Armazenamento do S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, acesse Lente de Armazenamento.
3. Escolha Painéis.
4. Na lista Painéis, clique no painel que você deseja visualizar. Agora, você pode visualizar os detalhes do painel da Lente de Armazenamento.

Como usar o AWS CLI

Example

O exemplo a seguir recupera uma configuração da Lente de Armazenamento do S3 para que você possa visualizar os detalhes da configuração. Para usar esses exemplos, substitua os *user input placeholders* por suas próprias informações.

```
aws s3control get-storage-lens-configuration --account-id=222222222222 --config-
id=your-configuration-id --region=us-east-1
```

Usar o AWS SDK para Java

Example – Recuperar e visualizar uma configuração da Lente de Armazenamento do S3

O exemplo a seguir mostra como recuperar uma configuração da Lente de Armazenamento do S3 no SDK para Java para que você possa visualizar os detalhes da configuração. Para usar esse exemplo, substitua os *user input placeholders* por suas próprias informações.

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import com.amazonaws.services.s3control.model.GetStorageLensConfigurationRequest;
import com.amazonaws.services.s3control.model.GetStorageLensConfigurationResult;
```

```
import com.amazonaws.services.s3control.model.StorageLensConfiguration;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class GetDashboard {

    public static void main(String[] args) {
        String configurationId = "ConfigurationId";
        String sourceAccountId = "111122223333";

        try {
            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(US_WEST_2)
                    .build();

            final StorageLensConfiguration configuration =
                    s3ControlClient.getStorageLensConfiguration(new
 GetStorageLensConfigurationRequest()
                            .withAccountId(sourceAccountId)
                            .withConfigId(configurationId)
                    ).getStorageLensConfiguration();

            System.out.println(configuration.toString());
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Gerenciamento de tags de recursos da AWS com a Lente de Armazenamento do S3

Cada painel da Lente de Armazenamento do Amazon S3 é contado como um recurso da AWS com o próprio nome do recurso da Amazon (ARN). Portanto, ao configurar o painel da Lente de Armazenamento, você tem a opção de adicionar tags de recursos da AWS ao painel. Você pode adicionar até 50 tags para cada painel da Lente de Armazenamento. Para criar um painel da Lente

de Armazenamento com tags, você deve ter as seguintes permissões da Lente de Armazenamento do S3:

- `s3:ListStorageLensConfigurations`
- `s3:GetStorageLensConfiguration`
- `s3:GetStorageLensConfigurationTagging`
- `s3:PutStorageLensConfiguration`
- `s3:PutStorageLensConfigurationTagging`

Use tags de recursos AWS para categorizar os recursos de acordo com o departamento, a linha de negócios ou o projeto. Isso é útil quando você tem muitos recursos do mesmo tipo. Ao aplicar tags, é possível identificar rapidamente um painel específico da Lente de Armazenamento do S3 com base nas tags atribuídas a ele. Você também pode usar tags para rastrear e alocar custos.

Além disso, ao adicionar uma tag de recurso da AWS ao painel da Lente de Armazenamento, você ativa o controle de acesso por atributo (ABAC). ABAC é uma estratégia de autorização que define permissões com base em atributos, como tags. É possível usar condições que especificam tags de recursos nas políticas do IAM para controlar o acesso aos recursos AWS.

É possível editar chaves de tags e valores e é possível remover as tags de um recurso a qualquer momento. Além disso, esteja ciente das seguintes limitações:

- As chaves e os valores das tags diferenciam maiúsculas de minúsculas.
- Ao adicionar uma tag que tenha a mesma chave de uma tag existente nesse recurso, o novo valor substituirá o antigo.
- Se você excluir um recurso, todas as tags do recurso também serão excluídas.
- Não inclua dados privados ou confidenciais nas tags de recursos AWS.
- As tags do sistema (com chaves de tags que começam com `aws:`) não são compatíveis.
- O comprimento de cada chave de tag não pode exceder 128 caracteres. O comprimento de cada valor de tag não pode exceder 256 caracteres.

Os exemplos a seguir demonstram como usar tags de recursos da AWS com o painel da Lente de Armazenamento.

Tópicos

- Adicionar tags de recursos da AWS a um painel da Lente de Armazenamento
- Recuperar tags de recursos da AWS para um painel da Lente de Armazenamento
- Atualizar tags do painel da Lente de Armazenamento
- Excluir tags de recursos da AWS de um painel da Lente de Armazenamento do S3

Adicionar tags de recursos da AWS a um painel da Lente de Armazenamento

Os exemplos a seguir demonstram como adicionar tags de recursos da AWS a um painel da Lente de Armazenamento do S3. Adicione tags de recurso usando o console do Amazon S3, AWS Command Line Interface (AWS CLI) e AWS SDK para Java.

Usar o console do S3

Como adicionar tags de recursos da AWS a um painel da Lente de Armazenamento

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, acesse Lente de Armazenamento.
3. Escolha Painéis.
4. Selecione botão de opção do painel da Lente de Armazenamento que você deseja atualizar. Em seguida, escolha Edit (Editar).
5. Em Geral, escolha Adicionar tag.
6. Na página Adicionar tag, adicione o novo par de chave-valor.

   > **Note**
   >
   > Adicionar uma nova tag com a mesma chave de tag existente substitui o valor da tag anterior.

7. (Opcional) Para adicionar mais de uma tag nova, selecione Adicionar tag novamente para continuar adicionando novas entradas. Você pode adicionar até 50 tags de recursos da AWS ao painel da Lente de Armazenamento.
8. (Opcional) Para remover uma entrada recém-adicionada, selecione Remover ao lado da tag que você deseja remover.
9. Escolha Salvar alterações.

Como usar o AWS CLI

Example

O exemplo de comando a seguir adiciona tags a uma configuração de painel da Lente de Armazenamento do S3. Para usar esses exemplos, substitua os *user input placeholders* por suas próprias informações.

```
aws s3control put-storage-lens-configuration-tagging --account-id=222222222222 --
region=us-east-1 --config-id=your-configuration-id --tags=file://./tags.json
```

Usar o AWS SDK para Java

O exemplo a seguir adiciona tags a uma configuração da Lente de Armazenamento do Amazon S3 com SDK para Java. Para usar esse exemplo, substitua os *user input placeholders* por suas próprias informações.

Example – Adicionar tags a uma configuração da Lente de Armazenamento do S3

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import
 com.amazonaws.services.s3control.model.PutStorageLensConfigurationTaggingRequest;
import com.amazonaws.services.s3control.model.StorageLensTag;

import java.util.Arrays;
import java.util.List;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class PutDashboardTagging {

    public static void main(String[] args) {
        String configurationId = "ConfigurationId";
        String sourceAccountId = "111122223333";

        try {
```

```
            List<StorageLensTag> tags = Arrays.asList(
                    new StorageLensTag().withKey("key-1").withValue("value-1"),
                    new StorageLensTag().withKey("key-2").withValue("value-2")
            );

            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(US_WEST_2)
                    .build();

            s3ControlClient.putStorageLensConfigurationTagging(new
 PutStorageLensConfigurationTaggingRequest()
                    .withAccountId(sourceAccountId)
                    .withConfigId(configurationId)
                    .withTags(tags)
            );
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Recuperar tags de recursos da AWS para um painel da Lente de Armazenamento

Os exemplos a seguir demonstram como adicionar tags de recursos da AWS a um painel da Lente de Armazenamento do S3. É possível adicionar tags de recursos usando o console do Amazon S3, a AWS Command Line Interface (AWS CLI) e o AWS SDK para Java.

Usar o console do S3

Como recuperar as tags de recursos da AWS para um painel da Lente de Armazenamento

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, acesse Lente de Armazenamento.
3. Escolha Painéis.

4. Selecione botão de opção da configuração do painel da Lente de Armazenamento que você deseja visualizar. Depois, selecione Visualizar configuração do painel.
5. Em Tags, revise as tags associadas ao painel.
6. (Opcional) Se quiser adicionar uma nova tag, escolha Editar. Selecione Adicionar tag. Na página Adicionar tag, adicione o novo par de chave-valor.

   > **Note**
   >
   > Adicionar uma nova tag com a mesma chave de tag existente substitui o valor da tag anterior.

7. (Opcional) Para remover uma entrada recém-adicionada, selecione Remover ao lado da tag que você deseja remover.
8. Escolha Salvar alterações.

Como usar o AWS CLI

Example

O exemplo de comando a seguir recupera tags para uma configuração de painel da Lente de Armazenamento do S3. Para usar esses exemplos, substitua os *`user input placeholders`* por suas próprias informações.

```
aws s3control get-storage-lens-configuration-tagging --account-id=222222222222 --
region=us-east-1 --config-id=your-configuration-id --tags=file://./tags.json
```

Usar o AWS SDK para Java

Example – Obter tags para uma configuração de painel da Lente de Armazenamento do S3

O exemplo a seguir mostra como recuperar tags para uma configuração de painel da Lente de Armazenamento do S3 no SDK para Java. Para usar esse exemplo, substitua os *`user input placeholders`* por suas próprias informações.

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
```

```
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import com.amazonaws.services.s3control.model.DeleteStorageLensConfigurationRequest;
import
 com.amazonaws.services.s3control.model.GetStorageLensConfigurationTaggingRequest;
import com.amazonaws.services.s3control.model.StorageLensTag;

import java.util.List;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class GetDashboardTagging {

    public static void main(String[] args) {
        String configurationId = "ConfigurationId";
        String sourceAccountId = "111122223333";
        try {
            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(US_WEST_2)
                    .build();

            final List<StorageLensTag> s3Tags = s3ControlClient
                    .getStorageLensConfigurationTagging(new
 GetStorageLensConfigurationTaggingRequest()
                            .withAccountId(sourceAccountId)
                            .withConfigId(configurationId)
                    ).getTags();

            System.out.println(s3Tags.toString());
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Atualizar tags do painel da Lente de Armazenamento

Os exemplos a seguir demonstram como atualizar as tags de painel da Lente de Armazenamento usando o console do Amazon S3, a AWS Command Line Interface (AWS CLI) e o AWS SDK para Java.

Usar o console do S3

Como atualizar uma tag de recursos da AWS de um painel da Lente de Armazenamento

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, acesse Lente de Armazenamento.
3. Escolha Painéis.
4. Selecione botão de opção da configuração do painel da Lente de Armazenamento que você deseja visualizar. Depois, selecione Visualizar configuração do painel.
5. Em Tags, revise as tags associadas ao painel.
6. (Opcional) Se quiser adicionar uma nova tag, escolha Editar. Selecione Adicionar tag. Na página Adicionar tag, adicione o novo par de chave-valor.

   > **Note**
   >
   > Adicionar uma nova tag com a mesma chave de tag existente substitui o valor da tag anterior.

7. (Opcional) Para remover uma entrada recém-adicionada, selecione Remover ao lado da tag que você deseja remover.
8. Escolha Salvar alterações.

Como usar o AWS CLI

Example

O exemplo de comando a seguir adiciona ou substitui tags em uma configuração existente do painel da Lente de Armazenamento do Amazon S3. Para usar esses exemplos, substitua os *`user input placeholders`* por suas próprias informações.

```
aws s3control put-storage-lens-configuration-tagging --account-id=111122223333 --
config-id=example-dashboard-configuration-id --region=us-east-1 --config-id=your-
configuration-id
```

Usar o AWS SDK para Java

O exemplo do AWS SDK para Java a seguir atualiza as tags de recursos da AWS em um painel existente da Lente de Armazenamento. Para usar esse exemplo, substitua os *user input placeholders* por suas próprias informações.

Example – Atualizar tags em uma configuração existente do painel da Lente de Armazenamento

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import
 com.amazonaws.services.s3control.model.PutStorageLensConfigurationTaggingRequest;
import com.amazonaws.services.s3control.model.StorageLensTag;

import java.util.Arrays;
import java.util.List;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class PutDashboardTagging {

    public static void main(String[] args) {
        String configurationId = "ConfigurationId";
        String sourceAccountId = "111122223333";

        try {
            List<StorageLensTag> tags = Arrays.asList(
                    new StorageLensTag().withKey("key-1").withValue("value-1"),
                    new StorageLensTag().withKey("key-2").withValue("value-2")
            );

            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(US_WEST_2)
```

```
                    .build();

            s3ControlClient.putStorageLensConfigurationTagging(new
 PutStorageLensConfigurationTaggingRequest()
                    .withAccountId(sourceAccountId)
                    .withConfigId(configurationId)
                    .withTags(tags)
            );
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Excluir tags de recursos da AWS de um painel da Lente de Armazenamento do S3

Os exemplos a seguir demonstram como excluir tags de recursos da AWS de um painel existente da Lente de Armazenamento. Exclua tags usando o console do Amazon S3, AWS Command Line Interface (AWS CLI) e AWS SDK para Java.

Usar o console do S3

Como excluir tags de recursos da AWS de um painel existente da Lente de Armazenamento

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, acesse Lente de Armazenamento.
3. Escolha Painéis.
4. Selecione botão de opção da configuração do painel da Lente de Armazenamento que você deseja visualizar. Depois, selecione Visualizar configuração do painel.
5. Em Tags, revise as tags associadas ao painel.
6. Escolha Remover ao lado da tag que você deseja remover.
7. Escolha Salvar alterações.

Como usar o AWS CLI

O comando AWS CLI a seguir exclui tags de recursos da AWS de um painel existente da Lente de Armazenamento. Para usar esse exemplo de comando, substitua os *user input placeholders* por suas próprias informações.

Example

```
aws s3control delete-storage-lens-configuration-tagging --account-id=222222222222 --
config-id=your-configuration-id --region=us-east-1
```

Usar o AWS SDK para Java

O exemplo do AWS SDK para Java a seguir exclui uma tag de recurso da AWS do painel da Lente de Armazenamento usando o nome do recurso da Amazon (ARN) especificado na conta *111122223333*. Para usar esse exemplo, substitua os *user input placeholders* por suas próprias informações.

Example – Excluir tags de uma configuração de painel da Lente de Armazenamento do S3

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import
 com.amazonaws.services.s3control.model.DeleteStorageLensConfigurationTaggingRequest;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class DeleteDashboardTagging {

    public static void main(String[] args) {
        String configurationId = "ConfigurationId";
        String sourceAccountId = "111122223333";
        try {
            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(US_WEST_2)
                    .build();
```

```
            s3ControlClient.deleteStorageLensConfigurationTagging(new
 DeleteStorageLensConfigurationTaggingRequest()
                    .withAccountId(sourceAccountId)
                    .withConfigId(configurationId)
            );
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Arquivos auxiliares para usar o Amazon S3 Storage Lens

Use os seguintes arquivos JSON e suas principais entradas para seus exemplos.

Exemplo de configuração da Lente de Armazenamento do S3 em JSON

Example **`config.json`**

O arquivo `config.json` contém os detalhes de uma configuração de métricas e recomendações avançadas para organizações da Lente de Armazenamento do S3. Para usar o exemplo a seguir, substitua *`user input placeholders`* por suas próprias informações.

> **Note**
>
> Aplicam-se cobranças adicionais para métricas e recomendações avançadas. Para obter mais informações, consulte Métricas e recomendações avançadas.

```
{
  "Id": "SampleS3StorageLensConfiguration", //Use this property to identify your S3
 Storage Lens configuration.
  "AwsOrg": { //Use this property when enabling S3 Storage Lens for AWS Organizations.
    "Arn": "arn:aws:organizations::123456789012:organization/o-abcdefgh"
  },
  "AccountLevel": {
```

```
    "ActivityMetrics": {
      "IsEnabled":true
    },
    "AdvancedCostOptimizationMetrics": {
      "IsEnabled":true
    },
    "AdvancedDataProtectionMetrics": {
      "IsEnabled":true
    },
    "DetailedStatusCodesMetrics": {
      "IsEnabled":true
    },
    "BucketLevel": {
      "ActivityMetrics": {
        "IsEnabled":true
      },
      "AdvancedDataProtectionMetrics": {
      "IsEnabled":true
      },
      "AdvancedCostOptimizationMetrics": {
        "IsEnabled":true
      },
      "DetailedStatusCodesMetrics": {
        "IsEnabled":true
      },
      "PrefixLevel":{
        "StorageMetrics":{
          "IsEnabled":true,
          "SelectionCriteria":{
            "MaxDepth":5,
            "MinStorageBytesPercentage":1.25,
            "Delimiter":"/"
          }
        }
      }
    }
  },
  "Exclude": { //Replace with "Include" if you prefer to include Regions.
    "Regions": [
      "eu-west-1"
    ],
    "Buckets": [ //This attribute is not supported for AWS Organizations-level
configurations.
      "arn:aws:s3:::amzn-s3-demo-source-bucket"
```

```
    ]
  },
  "IsEnabled": true, //Whether the configuration is enabled
  "DataExport": { //Details about the metrics export
    "S3BucketDestination": {
      "OutputSchemaVersion": "V_1",
      "Format": "CSV", //You can add "Parquet" if you prefer.
      "AccountId": "111122223333",
      "Arn": "arn:aws:s3:::
amzn-s3-demo-destination-bucket", // The destination bucket for your metrics export
 must be in the same Region as your S3 Storage Lens configuration.
      "Prefix": "prefix-for-your-export-destination",
      "Encryption": {
        "SSES3": {}
      }
    },
    "CloudWatchMetrics": {
      "IsEnabled": true
    }
  }
}
```

Exemplo de configuração da Lente de Armazenamento do S3 com grupos da Lente de Armazenamento em JSON

Example **`config.json`**

O arquivo `config.json` contém os detalhes para aplicar à configuração de Lente de Armazenamento ao usar grupos de Lente de Armazenamento. Para usar o exemplo, substitua *`user input placeholders`* pelas suas próprias informações.

Para anexar todos os grupos da Lente de Armazenamento ao seu painel, atualize a configuração da Lente de Armazenamento com a seguinte sintaxe:

```
{
  "Id": "ExampleS3StorageLensConfiguration",
  "AccountLevel": {
    "ActivityMetrics": {
      "IsEnabled":true
    },
    "AdvancedCostOptimizationMetrics": {
      "IsEnabled":true
```

```
    },
    "AdvancedDataProtectionMetrics": {
      "IsEnabled":true
    },
    "BucketLevel": {
      "ActivityMetrics": {
      "IsEnabled":true
      },
    "StorageLensGroupLevel": {},
  "IsEnabled": true
}
```

Para incluir apenas dois grupos da Lente de Armazenamento na configuração do painel da Lente de Armazenamento (*slg-1* and *slg-2*), use a seguinte sintaxe:

```
{
  "Id": "ExampleS3StorageLensConfiguration",
  "AccountLevel": {
    "ActivityMetrics": {
      "IsEnabled":true
    },
    "AdvancedCostOptimizationMetrics": {
      "IsEnabled":true
    },
    "AdvancedDataProtectionMetrics": {
      "IsEnabled":true
    },
    "BucketLevel": {
      "ActivityMetrics": {
      "IsEnabled":true
      },
   "StorageLensGroupLevel": {
        "SelectionCriteria": {
            "Include": [
                "arn:aws:s3:us-east-1:111122223333:storage-lens-group/slg-1",
                "arn:aws:s3:us-east-1:444455556666:storage-lens-group/slg-2"
            ]
    },
  "IsEnabled": true
}
```

Para impedir que apenas determinados grupos da Lente de Armazenamento sejam anexados à configuração do seu painel, use a seguinte sintaxe:

```
{
  "Id": "ExampleS3StorageLensConfiguration",
  "AccountLevel": {
    "ActivityMetrics": {
      "IsEnabled":true
    },
    "AdvancedCostOptimizationMetrics": {
      "IsEnabled":true
    },
    "AdvancedDataProtectionMetrics": {
      "IsEnabled":true
    },
    "BucketLevel": {
      "ActivityMetrics": {
      "IsEnabled":true
      },
   "StorageLensGroupLevel": {
        "SelectionCriteria": {
            "Exclude": [
                "arn:aws:s3:us-east-1:111122223333:storage-lens-group/slg-1",
                "arn:aws:s3:us-east-1:444455556666:storage-lens-group/slg-2"
            ]
    },
  "IsEnabled": true
}
```

Configuração de tags de exemplo da Lente de Armazenamento do S3 em JSON

Example **`tags.json`**

O arquivo `tags.json` contém as etiquetas que você deseja aplicar à configuração da Lente de Armazenamento do S3. Para usar esse exemplo, substitua os *`user input placeholders`* por suas próprias informações.

```
[
    {
        "Key": "key1",
        "Value": "value1"
    },
    {
        "Key": "key2",
        "Value": "value2"
    }
```

```
]
```

Exemplo de configuração da Lente de Armazenamento do S3 Permissões IAM

Example **`permissions.json`**: nome de painel específico

Este exemplo de política mostra um arquivo `permissions.json` do IAM da Lente de Armazenamento do S3 com um nome de painel especificado. Substitua *`value1`*, *`us-east-1`*, *`your-dashboard-name`* e *`example-account-id`* pelos seus próprios valores.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetStorageLensConfiguration",
                "s3:DeleteStorageLensConfiguration",
                "s3:PutStorageLensConfiguration"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/key1": "value1"
                }
            },
            "Resource": "arn:aws:s3:us-east-1:example-account-id:storage-lens/your-
dashboard-name"
        }
    ]
}
```

Example **`permissions.json`**: sem um nome de painel específico

Este exemplo de política mostra um arquivo `permissions.json` do IAM da Lente de Armazenamento do S3 sem um nome de painel especificado. Substitua *`value1`*, *`us-east-1`* e *`example-account-id`* pelos seus próprios valores.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Effect": "Allow",
            "Action": [
                "s3:GetStorageLensConfiguration",
                "s3:DeleteStorageLensConfiguration",
                "s3:PutStorageLensConfiguration"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/key1": "value1"
                }
            },
            "Resource": "arn:aws:s3:us-east-1:example-account-id:storage-lens/*"
        }
    ]
}
```

Visualizar métricas com a Lente de Armazenamento do Amazon S3

A Lente de Armazenamento do S3 agrega suas métricas e exibe as informações na seção Account snapshot (Snapshot da conta) na página Buckets do console do Amazon S3. A Lente de Armazenamento do S3 também oferece um painel interativo para visualizar insights e tendências, sinalizar discrepâncias e receber recomendações para otimizar os custos de armazenamento e aplicar as práticas recomendadas de proteção de dados. O painel tem opções de detalhamento para gerar e visualizar insights no nível da organização, conta, Região da AWS, classe de armazenamento, bucket, prefixo ou grupo de Lente de Armazenamento. Você também pode enviar uma exportação diária de métricas em CSV ou no formato Parquet para um bucket do S3.

Por padrão, todos os painéis são configurados com métricas gratuitas, que incluem métricas que você pode usar para entender o uso e a atividade em seu armazenamento do S3, otimizar seus custos de armazenamento e implementar as práticas recomendadas de proteção de dados e gerenciamento de acesso. As métricas gratuitas são agregadas até o nível de bucket. Com métricas gratuitas, os dados ficam disponíveis para consultas por até 14 dias.

As métricas e recomendações avançadas incluem os recursos adicionais a seguir, que você pode usar para obter mais informações sobre o uso e a atividade em seu armazenamento e práticas recomendadas para otimizar o armazenamento:

- Recomendações contextuais (disponíveis apenas no painel)
- Métricas avançadas (incluindo métricas de atividade agregadas por bucket)
- Agregação de prefixo

- Agregação de grupos de Armazenamento de Lente
- Agregação de grupos de Armazenamento de Lente
- Publicação no Amazon CloudWatch

Os dados de métricas avançadas ficam disponíveis para consultas por 15 meses. Há cobranças adicionais pelo uso do S3 Storage Lens com métricas avançadas. Para obter mais informações, consulte Definição de preço do Amazon S3. Para obter mais informações sobre métricas gratuitas e avançadas, consulte Seleção de métricas.

Tópicos

- Exibição das métricas da lente de armazenamento do S3 nos painéis
- Exibição de métricas de lente de armazenamento do Amazon S3 usando uma exportação de dados
- Monitorar métricas do S3 Storage Lens no CloudWatch
- Casos de uso das métricas da Lente de Armazenamento do Amazon S3

Exibição das métricas da lente de armazenamento do S3 nos painéis

No console do Amazon S3, a Lente de Armazenamento do S3 fornece um painel interativo padrão que você pode usar para ver insights e tendências em seus dados. Você também pode usar esse painel para sinalizar valores discrepantes e receber recomendações para otimizar custos de armazenamento e aplicar práticas recomendadas de proteção de dados. Seu painel tem opções de detalhamento para gerar insights em nível de conta, bucket, Região da AWS, prefixo ou grupo de Lente de Armazenamento. Se você tiver habilitado a Lente de Armazenamento do S3 para funcionar com o AWS Organizations, também poderá gerar insights no nível da organização (como dados de todas as contas que fazem parte da hierarquia AWS Organizations). O painel sempre carrega a data mais recente para a qual há métricas disponíveis.

O painel padrão do S3 Storage Lens no console é chamado default-account-dashboard. O Amazon S3 pré-configura esse painel para visualizar insights e tendências resumidos de toda a sua conta e os atualiza diariamente no console do S3. Você não pode modificar o escopo de configuração do painel padrão, mas pode atualizar a seleção de métricas gratuitas para métricas e recomendações avançadas pagas. Com métricas e recomendações avançadas, você tem acesso a métricas e recursos adicionais. Esses recursos incluem categorias de métricas avançadas, agregação por prefixo, recomendações contextuais e publicação no Amazon CloudWatch.

É possível desabilitar o painel padrão, mas não é possível excluí-lo. Se você desabilitar o painel padrão, ele deixará de ser atualizado. Você também não receberá mais novas métricas diárias na Lente de Armazenamento do S3 ou na seção Instantâneo da conta na página Buckets. Você ainda pode ver dados históricos no painel padrão até o fim do período de 14 dias para consultas de dados. Esse período é de 15 meses com a opção de métricas e recomendações avançadas habilitada. Para acessar esses dados, você pode reativar o painel padrão antes do fim do período de validade.

Você pode criar painéis adicionais da Lente de Armazenamento do S3 e definir seu escopo por Regiões da AWS, buckets do S3 ou contas. Você também poderá definir o escopo dos seus painéis por organização se tiver habilitado a Lente de Armazenamento para funcionar com o AWS Organizations. Ao criar ou editar um painel da Lente de Armazenamento do S3, defina o escopo do painel e a seleção de métricas.

Você pode desativar ou excluir qualquer painel adicional criado por você.

- Se você desabilitar um painel, ele não será mais atualizado e você não receberá mais nenhuma nova métrica diária. Você ainda pode ver dados históricos para métricas gratuitas durante o período de validade de 14 dias. Esse período é de 15 meses com a opção de métricas e recomendações avançadas habilitada para esse painel. Para acessar esses dados, você pode reativar o painel antes do fim do período de validade.
- Se você excluir seu painel, você perderá todas as configurações do painel. Você não receberá mais nenhuma nova métrica diária e também perderá o acesso aos dados históricos associados a esse painel. Se você quiser acessar os dados históricos de um painel excluído, você deve criar outro painel com o mesmo nome na mesma região inicial.

Tópicos

- Exibição de um painel do Amazon S3 Storage Lens
- Noções básicas sobre seu painel do S3 Storage Lens

Exibição de um painel do Amazon S3 Storage Lens

O procedimento a seguir mostra como visualizar um painel da Lente de Armazenamento do S3 no console do S3. Para obter orientações baseadas em casos de uso que mostram como usar o painel para otimizar custos, implementar práticas recomendadas e melhorar o desempenho de aplicativos que acessam seus buckets S3, consulte Casos de uso das métricas da Lente de Armazenamento do Amazon S3.

> **Note**
>
> Você não pode usar as credenciais de usuário raiz da sua conta para visualizar os painéis da Lente de Armazenamento do Amazon S3. Para acessar os painéis da Lente de Armazenamento do S3, você deve conceder as permissões do AWS Identity and Access Management (IAM) necessárias a um usuário do IAM novo ou existente. Em seguida, faça login com essas credenciais de usuário para acessar os painéis do S3 Storage Lens. Para obter mais informações, consulte Configurar permissões da Lente de Armazenamento do Amazon S3 e Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação esquerdo, escolha Storage Lens (Lente de Armazenamento) e Dashboards (Painéis).
3. Na lista Dashboards (Painéis), escolha o painel que deseja visualizar.

   Seu painel é aberto na Lente de Armazenamento do S3. A seção Snapshot for date (Snapshot para data) mostra a data mais recente para a qual a Lente de Armazenamento do S3 coletou métricas. Seu painel sempre carrega a data mais recente para a qual há métricas disponíveis.
4. (Opcional) Para alterar a data do painel da Lente de Armazenamento do S3, no seletor de datas que fica no canto superior direito, escolha uma nova data.
5. (Opcional) Para aplicar filtros temporários com o intuito de limitar ainda mais o escopo dos dados do painel, faça o seguinte:

   a. Expanda a seção Filtros.

   b. Para filtrar por contas específicas, Regiões da AWS, classes de armazenamento, buckets, prefixos ou grupos de Lente de Armazenamento, escolha as opções pelas quais filtrar.

      > **Note**
      >
      > Os filtros Prefixos e Grupos da Lente de Armazenamento não podem ser aplicados ao mesmo tempo.

   c. Para atualizar um filtro, escolha Apply (Aplicar).

   d. Para remover um filtro, clique no X ao lado dele.

6. Em qualquer seção do painel da Lente de Armazenamento do S3, para ver os dados de uma métrica específica, escolha o nome da métrica em Metric (Métrica).
7. Em qualquer gráfico ou visualização no painel de Lente de Armazenamento do S3, você pode detalhar níveis mais aprofundados de agregação usando as guias Contas, Regiões da AWS, Classes de armazenamento, Buckets, Prefixos ou Grupos de Lente de Armazenamento. Para obter um exemplo, consulte Descubra buckets inativos do Amazon S3.

Noções básicas sobre seu painel do S3 Storage Lens

O painel da Lente de Armazenamento do S3 tem uma guia Overview (Visão geral) primária e até cinco guias adicionais que representam cada nível de agregação:

- Contas
- Regiões da AWS
- Classes de armazenamento
- Buckets
- Prefixos
- Grupos da Lente de Armazenamento

Na guia Overview (Visão geral), os dados do painel são agregados em três seções diferentes: Snapshot for date (Snapshot for data), Trends and distributions (Tendências e distribuições) e Top N overview (Visão geral dos N principais).

Para obter mais informações sobre a Lente de Armazenamento do S3, consulte as seções a seguir.

Snapshot

A seção Snapshot for date (Snapshot para data) mostra o resumo das métricas que a Lente de Armazenamento do S3 agregou para a data selecionada. Esse resumo inclui as seguintes métricas:

- Armazenamento total: a quantidade total de armazenamento usado em bytes.
- Contagem de objetos: o número total de objetos no seu Conta da AWS.
- Tamanho médio do objeto — O tamanho médio do objeto.
- Buckets ativos — O número total de buckets ativos em uso ativo com armazenamento acima de 0 bytes em sua conta.

- Contas — O número de contas cujo armazenamento está no escopo. Esse valor é 1, a menos que você esteja usando o AWS Organizations, e a Lente de Armazenamento do S3 tenha acesso confiável com uma função vinculada a serviço válida. Para obter mais informações, consulte Usar funções vinculadas a serviços para o Amazon S3 Storage Lens.
- Buckets: o número total de buckets em sua conta.

Dados de métricas

Para cada métrica que aparece no snapshot, você pode ver os seguintes dados:

- Nome da métrica — O nome da métrica.
- Categoria de métrica — A categoria em que a métrica está organizada.
- Total por data — A contagem total para a data selecionada.
- % de alteração — A alteração percentual desde a data do último instantâneo.
- Tendência de 30 dias — Uma linha de tendência que mostra as alterações da métrica durante um período de 30 dias.
- Recomendação — Uma recomendação contextual baseada nos dados fornecidos no instantâneo. As recomendações estão disponíveis com as métricas e recomendações avançadas. Para obter mais informações, consulte Recomendações.

Categorias de métricas

Opcionalmente, você pode atualizar a seção Snapshot for date (Snapshot para data) do painel para exibir métricas para outras categorias. Se você quiser ver dados de snapshot para métricas adicionais, poderá escolher entre as seguintes Metrics categories (Categorias de métricas):

- Otimização de custo
- Proteção de dados
- Atividade (disponível com métricas avançadas)
- Gerenciamento de acesso
- Desempenho
- Eventos

A seção Snapshot for date (Snapshot para data) exibe somente uma seleção de métricas para cada categoria. Para ver todas as métricas de uma categoria específica, escolha a métrica nas

seções Trends and distributions (Tendências e distribuições) ou Top N overview (Visão geral dos N principais). Para obter mais informações sobre as categorias de métricas, consulte Categorias de métricas. Para obter uma lista completa de métricas da Lente de Armazenamento do S3, consulte Glossário de métricas de lente de armazenamento do Amazon S3.

Tendências e distribuições

A segunda seção da guia Overview (Visão geral) é Trends and distributions (Tendências e distribuições). Na seção Trends and distributions (Tendências e distribuições), você pode escolher duas métricas para comparar em um intervalo de datas definido por você. A seção Trends and distributions (Tendências e distribuições) mostra a relação entre duas métricas ao longo do tempo. Essa seção exibe gráficos que podem ser usados para ver a distribuição de Storage classe (Classe de armazenamento) e Region (Região) entre as duas tendências que você está monitorando. Opcionalmente, você pode detalhar um ponto de dados em um dos gráficos para realizar uma análise mais profunda.

Para acessar uma demonstração que usa a seção Trends and distributions (Tendências e distribuições), consulte Identificar buckets que não usam a criptografia do lado do servidor com AWS KMS como criptografia padrão (SSE-KMS).

Visão geral da top N

A terceira seção do painel S3 Storage Lens é a Top N overview (visão geral do Top N) (classificada em ordem crescente ou decrescente). Esta seção mostra as métricas selecionadas no número principal de contas, Regiões da AWS, buckets, prefixos ou grupos de Lente de Armazenamento. Se você tiver ativado a Lente de Armazenamento do S3 para funcionar com o AWS Organizations, também poderá ver as métricas selecionadas em toda a sua organização.

Para acessar uma demonstração que usa a seção Top N overview (Visão geral dos N principais), consulte Identifique os seus maiores buckets do S3.

Opções de detalhamento e análise

Para fornecer uma experiência de análise fluida, o painel de Lente de Armazenamento do S3 fornece um menu de ação, que aparece quando você escolhe qualquer valor do gráfico. Para usar esse menu, escolha qualquer valor de gráfico para ver os valores das métricas associadas e escolha entre duas opções na caixa exibida:

- A ação Drill down (Busca detalhada) aplica o valor selecionado como um filtro em todas as guias do painel. Você pode então detalhar esse valor para uma análise mais profunda.

- A ação Analisar por leva você à guia Dimensão selecionada e aplica esse valor da guia como um filtro. Essas guias incluem Contas, Regiões da AWS, Classes de armazenamento, Buckets, Prefixos (para painéis com Métricas avançadas e Agregação de prefixo habilitadas), e Grupos da Lente de Armazenamento (para painéis com Métricas avançadas e Agregação de grupos da Lente de Armazenamento habilitadas). Com Analisar por, você pode ver os dados no contexto da nova dimensão para uma análise mais aprofundada.

As ações Busca detalhada e Analisar por poderão ser desativadas se o resultado produzir resultados ilógicos ou não tiver valor. As ações Busca detalhada e Analisar por aplicam filtros sobre quaisquer filtros existentes em todas as guias do painel. Você também pode remover os filtros conforme necessário.

Guias

As guias no âmbito de dimensão fornecem uma exibição detalhada de todos os valores dentro de determinada dimensão. Por exemplo, a guia Regiões da AWS mostra métricas para todas as Regiões da AWS, e a guia Buckets mostra métricas para todos os buckets. Cada guia de dimensão contém um layout idêntico composto por quatro seções:

- Um gráfico de tendências que exibe os N itens principais da dimensão nos últimos 30 dias para a métrica selecionada. Por padrão, este gráfico exibe os 10 principais itens, mas você pode diminuí-lo para pelo menos 3 itens ou aumentá-lo para até 50 itens.
- Um gráfico de histograma que mostra um gráfico de barras verticais para a data e métrica selecionadas. Talvez seja necessário rolar horizontalmente se tiver um número grande de itens a serem exibidos neste gráfico.
- Um gráfico de análise de bolhas que representa todos os itens dentro da dimensão. Esse gráfico representa a primeira métrica no eixo x e a segunda métrica no eixo y. A terceira métrica é representada pelo tamanho da bolha.
- Uma exibição de grade métrica que contém cada item da dimensão listado em linhas. As colunas representam cada métrica disponível, organizadas em guias de categoria de métricas para facilitar a navegação.

Exibição de métricas de lente de armazenamento do Amazon S3 usando uma exportação de dados

As métricas da Lente de Armazenamento do Amazon S3 são geradas diariamente em arquivos de exportação de métricas em formato CSV ou Apache Parquet e colocadas em um bucket do S3 em

sua conta. A partir daí, você pode ingerir as métricas exportadas para as ferramentas de análise de sua escolha, como o Amazon QuickSight e o Amazon Athena, onde você pode analisar o uso do armazenamento e as tendências de atividades.

Tópicos

- Usar uma AWS KMS key para criptografar suas exportações de métricas
- O que é um manifesto de exportação do S3 Storage Lens?
- Compreendendo o esquema de exportação do Amazon S3 Storage Lens

Usar uma AWS KMS key para criptografar suas exportações de métricas

Para conceder permissão à Lente de Armazenamento do Amazon S3 para criptografar as exportações de métricas usando uma chave gerenciada pelo cliente, é necessário usar uma política de chaves. Para atualizar a política de chaves a fim de poder usar uma chave do KMS para criptografar as exportações de métricas da Lente de Armazenamento do S3, siga estas etapas.

Como conceder permissões à Lente de Armazenamento do S3 para criptografia usando a chave do KMS

1. Faça login no AWS Management Console usando a Conta da AWS que é proprietária da chave gerenciada pelo cliente.
2. Abra o console do AWS KMS em https://console.aws.amazon.com/kms.
3. Para alterar a Região da AWS, use o Region selector (Seletor de regiões) no canto superior direito da página.
4. No painel de navegação esquerdo, escolha Customer managed keys (Chaves gerenciadas pelo cliente).
5. Em Customer managed keys (Chaves gerenciadas pelo cliente), escolha a chave que você deseja usar para criptografar as exportações de métricas. As AWS KMS keys são específicas da região e devem estar na mesma região que o bucket S3 de destino de exportação de métricas.
6. Em Key policy (Política de chave), escolha Switch to policy view (Alternar para visualização de política).
7. Para atualizar a política de chave, escolha Edit (Editar).
8. Em Edit key policy (Editar política de chave), adicione a seguinte política de chave à existente. Para usar essa política, substitua os *`user input placeholders`* por suas próprias informações.

```
{
    "Sid": "Allow Amazon S3 Storage Lens use of the KMS key",
     "Effect": "Allow",
    "Principal": {
        "Service": "storage-lens.s3.amazonaws.com"
    },
    "Action": [
        "kms:GenerateDataKey"
    ],
    "Resource": "*",
    "Condition": {
       "StringEquals": {
           "aws:SourceArn": "arn:aws:s3:us-east-1:source-account-id:storage-
lens/your-dashboard-name",
           "aws:SourceAccount": "source-account-id"
        }
     }
}
```

9. Escolha Salvar alterações.

Para obter mais informações sobre como criar chaves gerenciadas pelo cliente e usar políticas de chave, consulte os seguintes tópicos no Guia do desenvolvedor do AWS Key Management Service:

- Conceitos básicos
- Usar políticas de chaves no AWS KMS

Você também pode usar a operação de API PUT de política de chaves do AWS KMS (PutKeyPolicy) para copiar a política de chaves para as chaves gerenciadas pelo cliente que deseja usar para criptografar as exportações de métricas usando a API REST, a AWS CLI e SDKs.

O que é um manifesto de exportação do S3 Storage Lens?

Dada a grande quantidade de dados agregados, uma exportação de métricas diárias do S3 Storage Lens pode ser dividida em vários arquivos. O arquivo de manifesto `manifest.json` descreve onde as métricas que exportam arquivos para esse dia estão localizadas. Sempre que uma nova exportação é entregue, ela é acompanhada por um novo manifesto. Cada manifesto contido no `manifest.json` fornece metadados e outras informações básicas sobre a exportação.

As informações do manifesto incluem as seguintes propriedades:

- `sourceAccountId` — O ID da conta do proprietário da configuração.
- `configId` – Um identificador exclusivo do painel.
- `destinationBucket` — O bucket de destino do Amazon Resource Name (ARN) no qual a exportação das métricas é colocada.
- `reportVersion` — A versão da exportação.
- `reportDate` — A data do relatório.
- `reportFormat` – O formato do relatório.
- `reportSchema` — O esquema do relatório.
- `reportFiles` — A lista real dos arquivos de relatório de exportação que estão no bucket de destino.

Veja a seguir um exemplo de manifesto em um arquivo `manifest.json` para um inventário em formato CSV.

```
{
   "sourceAccountId":"123456789012",
   "configId":"my-dashboard-configuration-id",
   "destinationBucket":"arn:aws:s3:::amzn-s3-demo-destination-bucket",
   "reportVersion":"V_1",
   "reportDate":"2020-11-03",
   "reportFormat":"CSV",

 "reportSchema":"version_number,configuration_id,report_date,aws_account_number,aws_region,stor
   "reportFiles":[
        {
            "key":"DestinationPrefix/StorageLens/123456789012/my-dashboard-
configuration-id/V_1/reports/dt=2020-11-03/a38f6bc4-2e3d-4355-ac8a-e2fdcf3de158.csv",
            "size":1603959,
            "md5Checksum":"2177e775870def72b8d84febe1ad3574"
        }
      ]
}
```

Veja a seguir um exemplo de manifesto em um arquivo `manifest.json` para uma exportação em formato Parquet.

```
{
```

```
   "sourceAccountId":"123456789012",
   "configId":"my-dashboard-configuration-id",
   "destinationBucket":"arn:aws:s3:::amzn-s3-demo-destination-bucket",
   "reportVersion":"V_1",
   "reportDate":"2020-11-03",
   "reportFormat":"Parquet",
   "reportSchema":"message s3.storage.lens { required string version_number;
 required string configuration_id; required string report_date; required string
 aws_account_number; required string aws_region; required string storage_class;
 required string record_type; required string record_value; required string
 bucket_name; required string metric_name; required long metric_value; }",
   "reportFiles":[
      {
         "key":"DestinationPrefix/StorageLens/123456789012/my-dashboard-configuration-
id/V_1/reports/dt=2020-11-03/bd23de7c-b46a-4cf4-bcc5-b21aac5be0f5.par",
         "size":14714,
         "md5Checksum":"b5c741ee0251cd99b90b3e8eff50b944"
      }
}
```

Você pode configurar a exportação de métricas para serem geradas como parte da configuração do painel no console do Amazon S3 ou usando a API REST do Amazon S3, a AWS CLI e os SDKs.

Compreendendo o esquema de exportação do Amazon S3 Storage Lens

A tabela a seguir contém o esquema da exportação de métricas do S3 Storage Lens.

Nome do atributo	Tipo de dados	Nome da coluna	Descrição
`VersionNumber`	String	`version_number`	A versão das métricas do S3 Storage Lens que está sendo usada.
`ConfigurationId`	String	`configuration_id`	O `configuration_id` da configuração da Lente de Armazenamento do S3.

Nome do atributo	Tipo de dados	Nome da coluna	Descrição
`ReportDate`	String	`report_date`	A data em que as métricas foram monitoradas.
`AwsAccountNumber`	String	`aws_account_number`	Número da sua Conta da AWS.
`AwsRegion`	String	`aws_region`	A Região da AWS para a qual as métricas estão sendo rastreadas.
`StorageClass`	String	`storage_class`	A classe de armazenamento do bucket em questão.
`RecordType`	ENUM	`record_type`	O tipo de artefato que está sendo relatado (CONTA, BUCKET ou PREFIXO).
`RecordValue`	String	`record_value`	O valor do artefato `RecordType`. **Note** O `record_value` é codificado em URL.
`BucketName`	String	`bucket_name`	O nome do intervalo que está sendo relatado.

Nome do atributo	Tipo de dados	Nome da coluna	Descrição
`MetricName`	String	`metric_name`	O nome da métrica que está sendo relatada.
`MetricValue`	Longo	`metric_value`	O valor da métrica que está sendo relatada.

Exemplo de exportação de métricas do S3 Storage Lens

Veja a seguir um exemplo de uma exportação de métricas do S3 Storage Lens com base nesse esquema.

> **Note**
>
> Você pode identificar métricas para grupos da Lente de Armazenamento procurando os valores `STORAGE_LENS_GROUP_BUCKET` ou `STORAGE_LENS_GROUP_ACCOUNT` na coluna `record_type`. A coluna `record_value` exibirá o nome do recurso da Amazon (ARN) para o grupo da Lente de Armazenamento, por exemplo, `arn:aws:s3:us-east-1:123456789012:storage-lens-group/slg-1`.

version_r	configuration_id	report_date	aws_account_number	aws_region	storage_class	record_type	record_value	bucket_name	metric_name	metric_value
V_1	sample-cmh-exclude	11/3/2020	546264889236	eu-west-1	STANDARD	ACCOUNT			StorageBytes	2478830621
V_1	sample-cmh-exclude	11/3/2020	546264889236	eu-west-1	STANDARD	ACCOUNT			ObjectCount	1598962
V_1	sample-cmh-exclude	11/3/2020	546264889236	eu-west-1	STANDARD	ACCOUNT			ReplicatedStorageBytes	20000
V_1	sample-cmh-exclude	11/3/2020	546264889236	eu-west-1	STANDARD	ACCOUNT			ReplicatedObjectCount	20
V_1	sample-cmh-exclude	11/3/2020	546264889236	eu-west-1	STANDARD	ACCOUNT			EncryptedStorageBytes	2478828742
V_1	sample-cmh-exclude	11/3/2020	546264889236	eu-west-1	STANDARD	ACCOUNT			EncryptedObjectCount	1598961
V_1	sample-cmh-exclude	11/3/2020	546264889236	eu-west-1	STANDARD	ACCOUNT			DeleteMarkerObjectCount	1500
V_1	sample-cmh-exclude	11/3/2020	546264889236	eu-west-1	STANDARD	ACCOUNT			ObjectLockEnabledStorageBytes	0
V_1	sample-cmh-exclude	11/3/2020	546264889236	eu-west-1	STANDARD	ACCOUNT			ObjectLockEnabledObjectCount	0
V_1	sample-cmh-exclude	11/3/2020	546264889236	eu-west-1	STANDARD	ACCOUNT			CurrentVersionStorageBytes	2478830621
V_1	sample-cmh-exclude	11/3/2020	546264889236	eu-west-1	STANDARD	ACCOUNT			CurrentVersionObjectCount	1598962
V_1	sample-cmh-exclude	11/3/2020	546264889236	eu-west-1	STANDARD	ACCOUNT			NonCurrentVersionStorageBytes	0
V_1	sample-cmh-exclude	11/3/2020	546264889236	eu-west-1	STANDARD	ACCOUNT			NonCurrentVersionObjectCount	0
V_1	sample-cmh-exclude	11/3/2020	546264889236	eu-west-1	STANDARD	ACCOUNT			IncompleteMultipartUploadStorageBytes	0
V_1	sample-cmh-exclude	11/3/2020	546264889236	eu-west-1	STANDARD	ACCOUNT			IncompleteMultipartUploadObjectCount	0
V_1	sample-cmh-exclude	11/3/2020	546264889236	us-west-1	STANDARD	PREFIX	AWSLogs%2F546264889236%2FCloudTrail%2Fus	cloudtrail-log-sf	StorageBytes	29996800
V_1	sample-cmh-exclude	11/3/2020	546264889236	us-west-1	STANDARD	PREFIX	AWSLogs%2F546264889236%2FCloudTrail%2Fus	cloudtrail-log-sf	ObjectCount	12264
V_1	sample-cmh-exclude	11/3/2020	546264889236	us-west-1	STANDARD	PREFIX	AWSLogs%2F546264889236%2FCloudTrail%2Fus	cloudtrail-log-sf	ReplicatedStorageBytes	0
V_1	sample-cmh-exclude	11/3/2020	546264889236	us-west-1	STANDARD	PREFIX	AWSLogs%2F546264889236%2FCloudTrail%2Fus	cloudtrail-log-sf	ReplicatedObjectCount	0
V_1	sample-cmh-exclude	11/3/2020	546264889236	us-west-1	STANDARD	PREFIX	AWSLogs%2F546264889236%2FCloudTrail%2Fus	cloudtrail-log-sf	EncryptedStorageBytes	29996800
V_1	sample-cmh-exclude	11/3/2020	546264889236	us-west-1	STANDARD	PREFIX	AWSLogs%2F546264889236%2FCloudTrail%2Fus	cloudtrail-log-sf	EncryptedObjectCount	12264
V_1	sample-cmh-exclude	11/3/2020	546264889236	us-west-1	STANDARD	PREFIX	AWSLogs%2F546264889236%2FCloudTrail%2Fus	cloudtrail-log-sf	DeleteMarkerObjectCount	0
V_1	sample-cmh-exclude	11/3/2020	546264889236	us-west-1	STANDARD	PREFIX	AWSLogs%2F546264889236%2FCloudTrail%2Fus	cloudtrail-log-sf	ObjectLockEnabledStorageBytes	0
V_1	sample-cmh-exclude	11/3/2020	546264889236	us-west-1	STANDARD	PREFIX	AWSLogs%2F546264889236%2FCloudTrail%2Fus	cloudtrail-log-sf	ObjectLockEnabledObjectCount	0
V_1	sample-cmh-exclude	11/3/2020	546264889236	us-west-1	STANDARD	PREFIX	AWSLogs%2F546264889236%2FCloudTrail%2Fus	cloudtrail-log-sf	CurrentVersionStorageBytes	29996800
V_1	sample-cmh-exclude	11/3/2020	546264889236	us-west-1	STANDARD	PREFIX	AWSLogs%2F546264889236%2FCloudTrail%2Fus	cloudtrail-log-sf	CurrentVersionObjectCount	12264
V_1	sample-cmh-exclude	11/3/2020	546264889236	us-west-1	STANDARD	PREFIX	AWSLogs%2F546264889236%2FCloudTrail%2Fus	cloudtrail-log-sf	NonCurrentVersionStorageBytes	0
V_1	sample-cmh-exclude	11/3/2020	546264889236	us-west-1	STANDARD	PREFIX	AWSLogs%2F546264889236%2FCloudTrail%2Fus	cloudtrail-log-sf	NonCurrentVersionObjectCount	0
V_1	sample-cmh-exclude	11/3/2020	546264889236	us-west-1	STANDARD	PREFIX	AWSLogs%2F546264889236%2FCloudTrail%2Fus	cloudtrail-log-sf	IncompleteMultipartUploadStorageBytes	0
V_1	sample-cmh-exclude	11/3/2020	546264889236	us-west-1	STANDARD	PREFIX	AWSLogs%2F546264889236%2FCloudTrail%2Fus	cloudtrail-log-sf	IncompleteMultipartUploadObjectCount	0

Veja a seguir um exemplo de exportação de métricas da Lente de Armazenamento do S3 com dados de grupos da Lente de Armazenamento.

version_numbe	configuration_id	report_date	aws_account_num	aws_region	storage_class	record_type	record_value	bucket_name	metric_name	metric_value
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		StorageBytes	3128548856
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		ObjectCount	4440
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		ReplicatedStorageBytes	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		ReplicatedObjectCount	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		EncryptedStorageBytes	3128548856
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		EncryptedObjectCount	4440
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		DeleteMarkerObjectCount	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		ObjectLockEnabledStorageBytes	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		ObjectLockEnabledObjectCount	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		CurrentVersionStorageBytes	3128548856
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		CurrentVersionObjectCount	4440
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		NonCurrentVersionStorageBytes	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		NonCurrentVersionObjectCount	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		IncompleteMultipartUploadStorageBytes	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		IncompleteMultipartUploadObjectCount	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		DeleteMarkerStorageBytes	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		ReplicatedStorageBytesSource	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		ReplicatedObjectCountSource	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		IncompleteMPUStorageBytesOlderThan7Days	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		IncompleteMPUObjectCountOlderThan7Days	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	StorageBytes	676863200
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	ObjectCount	3000
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	ReplicatedStorageBytes	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	ReplicatedObjectCount	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	EncryptedStorageBytes	676863200
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	EncryptedObjectCount	3000
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	DeleteMarkerObjectCount	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	ObjectLockEnabledStorageBytes	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	ObjectLockEnabledObjectCount	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	CurrentVersionStorageBytes	676863200
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	CurrentVersionObjectCount	3000
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	NonCurrentVersionStorageBytes	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	NonCurrentVersionObjectCount	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	IncompleteMultipartUploadStorageBytes	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	IncompleteMultipartUploadObjectCount	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	DeleteMarkerStorageBytes	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	ReplicatedStorageBytesSource	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	ReplicatedObjectCountSource	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	IncompleteMPUStorageBytesOlderThan7Days	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	IncompleteMPUObjectCountOlderThan7Days	0

Monitorar métricas do S3 Storage Lens no CloudWatch

É possível publicar métricas da Lente de Armazenamento do S3 no Amazon CloudWatch para criar uma visão unificada de sua integridade operacional nos painéis do CloudWatch. Também é possível usar os recursos do CloudWatch, como alarmes e ações acionadas, matemática métrica e detecção de anomalias, para monitorar e realizar ações sobre as métricas da Lente de Armazenamento do S3. Além disso, as operações de API do CloudWatch permitem que aplicações, inclusive provedores de terceiros, acessem as métricas da Lente de Armazenamento do S3. Para obter mais informações sobre os recursos do CloudWatch, consulte o Guia do usuário do Amazon CloudWatch Events.

Você pode habilitar a opção de publicação no CloudWatch para configurações de painéis novos ou existentes usando o console do Amazon S3, a API REST do Amazon S3, a AWS CLI e os AWS SDKs. Painéis atualizados para métricas e recomendações avançadas do S3 Storage Lens podem usar a opção de publicação no CloudWatch. Para saber mais sobre o preço das métricas e recomendações avançadas da Lente de Armazenamento do S3, consulte Definição de preço do Amazon S3. Não são aplicadas cobranças adicionais para publicação de métricas no CloudWatch, mas outras cobranças do CloudWatch, como painéis, alarmes e chamadas de API, são aplicáveis. Para obter mais informações, consulte Preço do Amazon CloudWatch.

As métricas do S3 Storage Lens são publicadas no CloudWatch na conta proprietária da configuração do S3 Storage Lens. Depois de habilitar a opção de publicação no CloudWatch em

métricas e recomendações avançadas, você pode acessar as métricas por organização, conta e bucket no CloudWatch. As métricas de nível prefixo não estão disponíveis no CloudWatch.

> **Note**
>
> As métricas do S3 Storage Lens são métricas diárias e são publicadas no CloudWatch uma vez por dia. Quando você consulta métricas do S3 Storage Lens no CloudWatch, o período para a consulta deve ser de 1 dia (86.400 segundos). Depois que as métricas diárias do S3 Storage Lens são exibidas no painel do S3 Storage Lens no console do Amazon S3, essas mesmas métricas podem demorar algumas horas para serem exibidas no CloudWatch. Quando você habilita a opção de publicação do CloudWatch para métricas do S3 Storage Lens pela primeira vez, as métricas podem levar até 24 horas para serem publicadas no CloudWatch.

Depois de habilitar a opção de publicação do CloudWatch, você pode usar os seguintes recursos do CloudWatch para monitorar e analisar os dados do S3 Storage Lens:

- Painéis: use os painéis do CloudWatch para criar painéis personalizados do S3 Storage Lens. Compartilhe seu painel do CloudWatch com pessoas que não têm acesso direto à sua Conta da AWS, com equipes, com partes interessadas e com pessoas externas às suas organizações.
- Alarmes e ações acionadas: configure alarmes que monitoram métricas e realizam ações quando um limite é violado. Por exemplo, é possível configurar um alarme que envia uma notificação do Amazon SNS quando a métrica Incomplete Multipart Upload Bytes (Bytes de multipart uploads incompletos) exceder 1 GB por três dias consecutivos.
- Detecção de anomalias: habilite a detecção de anomalias para analisar continuamente métricas, determinar linhas de base normais e anomalias. Você pode criar um alarme de detecção de anomalias com base no valor esperado de uma métrica. Por exemplo, é possível monitorar anomalias na métrica Object Lock Enabled Bytes (Bytes de Bloqueio de Objeto ativado) para detectar a remoção não autorizada das configurações de Bloqueio de Objeto.
- Matemática métrica: você também pode usar a matemática métrica para consultar várias métricas do S3 Storage Lens e usar expressões matemáticas para criar novas séries temporais de acordo com essas métricas. Por exemplo, você pode criar uma métrica para obter o tamanho médio de objetos dividindo `StorageBytes` por `ObjectCount`.

Para obter mais informações sobre a opção de publicação no CloudWatch para métricas do S3 Storage Lens, consulte os tópicos a seguir.

Tópicos

- Métricas e dimensões do S3 Storage Lens
- Habilitar publicação no CloudWatch para o S3 Storage Lens
- Trabalhar com métricas do S3 Storage Lens no CloudWatch

Métricas e dimensões do S3 Storage Lens

Para enviar métricas do S3 Storage Lens ao CloudWatch, você deve habilitar a opção de publicação no CloudWatch nas métricas e recomendações avançadas do S3 Storage Lens. Com as métricas avançadas habilitadas, é possível usar os painéis do CloudWatch para monitorar as métricas da Lente de Armazenamento do S3 juntamente com métricas de outras aplicações e criar uma visão unificada de sua integridade operacional. Você pode usar dimensões para filtrar as métricas do S3 Storage Lens no CloudWatch por organização, conta, bucket, classe de armazenamento, região e ID de configuração de métricas.

As métricas do S3 Storage Lens são publicadas no CloudWatch na conta proprietária da configuração do S3 Storage Lens. Depois de habilitar a opção de publicação no CloudWatch em métricas e recomendações avançadas, você pode acessar as métricas por organização, conta e bucket no CloudWatch. As métricas de nível prefixo não estão disponíveis no CloudWatch.

> **Note**
>
> As métricas do S3 Storage Lens são métricas diárias e são publicadas no CloudWatch uma vez por dia. Quando você consulta métricas do S3 Storage Lens no CloudWatch, o período para a consulta deve ser de 1 dia (86.400 segundos). Depois que as métricas diárias do S3 Storage Lens são exibidas no painel do S3 Storage Lens no console do Amazon S3, essas mesmas métricas podem demorar algumas horas para serem exibidas no CloudWatch. Quando você habilita a opção de publicação do CloudWatch para métricas do S3 Storage Lens pela primeira vez, as métricas podem levar até 24 horas para serem publicadas no CloudWatch.

Para obter mais informações sobre métricas e dimensões do S3 Storage Lens no CloudWatch, consulte os tópicos a seguir.

Tópicos

- Métricas
- Dimensões

Métricas

As métricas da Lente de Armazenamento do S3 estão disponíveis como métricas no CloudWatch. As métricas do S3 Storage Lens são publicadas no namespace `AWS/S3/Storage-Lens` do CloudWatch. Este namespace serve apenas para métricas do S3 Storage Lens. As métricas de bucket, solicitação e replicação do Amazon S3 são publicadas no namespace `AWS/S3`.

As métricas do S3 Storage Lens são publicadas no CloudWatch na conta proprietária da configuração do S3 Storage Lens. Depois de habilitar a opção de publicação no CloudWatch em métricas e recomendações avançadas, você pode acessar as métricas por organização, conta e bucket no CloudWatch. As métricas de nível prefixo não estão disponíveis no CloudWatch.

No S3 Storage Lens, as métricas são agregadas e armazenadas somente na região inicial designada. As métricas do S3 Storage Lens também são publicadas no CloudWatch na região inicial especificada na configuração do S3 Storage Lens.

Para obter uma lista completa das métricas do S3 Storage Lens, inclusive uma lista dessas métricas disponíveis no CloudWatch, consulte Glossário de métricas de lente de armazenamento do Amazon S3.

> **Note**
>
> A estatística válida para métricas do S3 Storage Lens no CloudWatch é Average. Para obter mais informações sobre estatísticas no CloudWatch, consulte Definições de estatísticas do CloudWatch no Guia do usuário do Amazon CloudWatch.

Detalhamento das métricas do S3 Storage Lens no CloudWatch

O S3 Storage Lens oferece métricas com detalhamento de organização, conta, bucket e prefixo. O S3 Storage Lens publica métricas do S3 Storage Lens em nível de organização, conta e bucket no CloudWatch. As métricas de nível prefixo do S3 Storage não estão disponíveis no CloudWatch.

Para obter mais informações sobre o detalhamento das métricas do S3 Storage Lens disponíveis no CloudWatch, consulte a lista a seguir:

- Organização: métricas agregadas entre as contas dos membros de sua organização. O S3 Storage Lens publica métricas de contas de membros no CloudWatch na conta de gerenciamento.
  - Organização e conta: métricas de contas de membros de sua organização.
  - Organização e bucket: métricas de buckets do Amazon S3 de contas de membros de sua organização.
- Conta (nível não organizacional): métricas agregadas entre os buckets de sua conta.
- Bucket (nível não organizacional): métricas de um bucket específico. No CloudWatch, o S3 Storage Lens publica essas métricas na Conta da AWS que criou a configuração do S3 Storage Lens. O S3 Storage Lens publica essas métricas somente de configurações não organizacionais.

Dimensões

Quando a Lente de Armazenamento do S3 envia dados para o CloudWatch, dimensões são anexadas a cada métrica. As dimensões são categorias que descrevem as características das métricas. Você pode usar dimensões para filtrar os resultados que o CloudWatch retorna.

Por exemplo, todas as métricas do S3 Storage Lens no CloudWatch têm a dimensão `configuration_id`. É possível usar essa dimensão para diferenciar as métricas associadas a uma configuração específica do S3 Storage Lens. O `organization_id` identifica métricas no nível da organização. Para obter mais informações sobre dimensões no CloudWatch, consulte Dimensões no Guia do usuário do CloudWatch.

Há diferentes dimensões disponíveis para métricas da Lente de Armazenamento do S3, conforme o detalhamento das métricas. Por exemplo, você pode usar a dimensão `organization_id` para filtrar métricas no nível da organização pelo ID do AWS Organizations. No entanto, não é possível usar essa dimensão para métricas de bucket e conta. Para obter mais informações, consulte Filtrar métricas usando dimensões.

Para ver quais dimensões estão disponíveis para sua configuração do S3 Storage Lens, consulte a tabela a seguir.

Dimensão	Descrição	Bucket	Conta	Organização e bucket	Organização e conta
`configuration_id`	O nome do painel para a configuração da Lente de Armazenamento do S3 relatada nas métricas	.	.	.	.
`metrics_version`	A versão das métricas da Lente de Armazenamento do S3. A versão das métricas tem um valor fixo de `1.0`.	.	.	.	.
`organization_id`	O ID do AWS Organizations das métricas	.	.	.	.
`aws_account_number`	A Conta da AWS associada às métricas.	.	.	.	.
`aws_region`	A Região da AWS das métricas	.	.	.	.
`bucket_name`	O nome do bucket do S3 relatado nas métricas	.	.	.	.
`storage_class`	A classe de armazenamento do bucket relatado nas métricas	.	.	.	.
`record_type`	O detalhamento das métricas: ORGANIZATION, ACCOUNT, BUCKET	BUCKET	ACCOUNT	ORGANIZATION	.

Habilitar publicação no CloudWatch para o S3 Storage Lens

É possível publicar métricas da Lente de Armazenamento do S3 no Amazon CloudWatch para criar uma visão unificada de sua integridade operacional nos painéis do CloudWatch. Também é possível usar os recursos do CloudWatch, como alarmes e ações acionadas, matemática métrica e detecção de anomalias, para monitorar e realizar ações sobre as métricas da Lente de Armazenamento do S3. Além disso, as operações de API do CloudWatch permitem que aplicações, inclusive provedores de

terceiros, acessem as métricas da Lente de Armazenamento do S3. Para obter mais informações sobre os recursos do CloudWatch, consulte o Guia do usuário do Amazon CloudWatch Events.

As métricas do S3 Storage Lens são publicadas no CloudWatch na conta proprietária da configuração do S3 Storage Lens. Depois de habilitar a opção de publicação no CloudWatch em métricas e recomendações avançadas, você pode acessar as métricas por organização, conta e bucket no CloudWatch. As métricas de nível prefixo não estão disponíveis no CloudWatch.

Você pode habilitar o suporte do CloudWatch a configurações de painéis novos ou existentes usando o console do S3, as APIs REST do Amazon S3, a AWS CLI e os AWS SDKs. A opção de publicação no CloudWatch está disponível para painéis com upgrade para métricas e recomendações avançadas da Lente de Armazenamento do S3. Para saber mais sobre o preço das métricas e recomendações avançadas da Lente de Armazenamento do S3, consulte Definição de preço do Amazon S3. Não são aplicadas cobranças adicionais para publicação de métricas no CloudWatch, mas outras cobranças do CloudWatch, como painéis, alarmes e chamadas de API, são aplicáveis.

Para habilitar a opção de publicação de métricas do S3 Storage Lens no CloudWatch, consulte os tópicos a seguir.

> **Note**
>
> As métricas do S3 Storage Lens são métricas diárias e são publicadas no CloudWatch uma vez por dia. Quando você consulta métricas do S3 Storage Lens no CloudWatch, o período para a consulta deve ser de 1 dia (86.400 segundos). Depois que as métricas diárias do S3 Storage Lens são exibidas no painel do S3 Storage Lens no console do Amazon S3, essas mesmas métricas podem demorar algumas horas para serem exibidas no CloudWatch. Quando você habilita a opção de publicação do CloudWatch para métricas do S3 Storage Lens pela primeira vez, as métricas podem levar até 24 horas para serem publicadas no CloudWatch.
>
> No momento, as métricas da Lente de Armazenamento do S3 não podem ser consumidas por fluxos do CloudWatch.

Usar o console do S3

Ao atualizar um painel da Lente de Armazenamento do S3, não é possível alterar o nome do painel nem a região inicial. Também não é possível alterar o escopo do painel padrão, que está definido como o armazenamento de toda a sua conta.

Como atualizar um painel da Lente de Armazenamento do S3 para habilitar a publicação no CloudWatch

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação esquerdo, escolha S3 Storage Lens (Lente de Armazenamento do S3) e Dashboards (Painéis).
3. Escolha o painel que você deseja editar e escolha Edit (Editar).
4. Em Metrics selection (Seleção de métricas), escolha Advanced metrics and recommendations (Métricas e recomendações avançadas).

   As métricas e recomendações avançadas estão disponíveis mediante cobranças adicionais. As métricas e recomendações avançadas incluem um período de 15 meses para consultas de dados, métricas de uso agregadas por prefixo, métricas de atividade agregadas por bucket, opção de publicação no CloudWatch e recomendações contextuais que ajudam a otimizar os custos de armazenamento e aplicar as práticas recomendadas de proteção de dados. Para obter mais informações, consulte Preço do Amazon S3.
5. Em Select Advanced metrics and recommendations features, (Selecionar recursos de métricas e recomendações avançadas), escolha CloudWatch publishing (Publicação no CloudWatch).

   > **Important**
   >
   > Se a configuração permitir a agregação de prefixos para métricas de uso, as métricas de nível de prefixo não serão publicadas no CloudWatch. Somente métricas em nível de organização, conta e bucket do S3 Storage Lens são publicadas no CloudWatch.
6. Escolha Salvar alterações.

Para criar um novo painel do S3 Storage Lens que habilite o suporte ao CloudWatch

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação esquerdo, escolha Storage Lens (Lente de Armazenamento) e Dashboards (Painéis).
3. Escolha Create dashboard (Criar painel).
4. Em General (Geral), defina as seguintes opções de configuração:

a. Em Dashboard name (Nome do painel), insira o nome do painel.

   Os nomes do painel devem ter menos de 65 caracteres e não devem conter caracteres ou espaços especiais. Não é possível alterar o nome do painel depois que o painel é criado.

b. Escolha a Home Region (Região inicial) do painel.

   As métricas de todas as regiões incluídas neste escopo do painel são armazenadas centralmente nesta região inicial designada. No CloudWatch, as métricas do S3 Storage Lens também estão disponíveis na região inicial. Não é possível alterar a região inicial depois que o painel é criado.

5. (Opcional) Para adicionar etiquetas, escolha Add tag (Adicionar etiqueta) e insira a Key (Chave) e o Value (Valor) da etiqueta.

> **Note**
>
> Você pode adicionar até 50 tags à configuração do painel.

6. Defina o escopo de sua configuração:

a. Se você estiver criando uma configuração no nível da organização, escolha as contas a serem incluídas na configuração: Include all accounts in your configuration (Incluir todas as contas na configuração) ou Limit the scope to your signed-in account (Limitar o escopo à sua conta conectada).

> **Note**
>
> Ao criar uma configuração no nível da organização que inclui todas as contas, não será possível incluir ou excluir buckets, apenas regiões.

b. Escolha as regiões e os buckets que deseja que a Lente de Armazenamento do S3 inclua na configuração do painel fazendo o seguinte:

- Para incluir todas as regiões, selecione Include Regions and buckets (Incluir regiões e buckets).
- Para incluir regiões específicas, desmarque a opção Include all Regions (Incluir todas as regiões). Em Choose Regions to include (Escolher regiões a serem incluídas), escolha as regiões que deseja que o S3 Storage Lens inclua no painel.

- Para incluir bucket específicos, desmarque a opção Include all buckets (Incluir todos os buckets). Em Choose buckets to include (Escolher buckets a serem incluídos), escolha os buckets que deseja que o S3 Storage Lens inclua no painel.

> **Note**
>
> Você pode escolher até 50 buckets.

7. Em Metrics selection (Seleção de métricas), escolha Advanced metrics and recommendations (Métricas e recomendações avançadas).

   Para obter mais informações sobre o preço das métricas e recomendações avançadas, consulte Preços do Amazon S3.

8. Em Advanced metrics and recommendations features (Recursos de métricas e recomendações avançadas), selecione as opções que deseja habilitar:

   - Advanced metrics (Métricas avançadas)
   - Publicação no CloudWatch

   > **Important**
   >
   > Se você habilitar a agregação de prefixos na configuração do S3 Storage Lens, as métricas de nível de prefixo não serão publicadas no CloudWatch. Somente métricas em nível de organização, conta e bucket do S3 Storage Lens são publicadas no CloudWatch.

   - Agregação de prefixo

   > **Note**
   >
   > Para obter mais informações sobre os recursos de métricas e recomendações avançadas, consulte Seleção de métricas.

9. Se você ativou Advanced metrics (Métricas avançadas), selecione as Advanced metrics categories (Categorias de métricas avançadas) que deseja exibir no painel da Lente de Armazenamento do S3:

   - Métricas de atividade

- Detailed status code metrics (Métricas detalhadas do código de status)
- Advanced cost optimization metrics (Métricas avançadas de otimização de custos)
- Advanced data protection metrics (Métricas avançadas de proteção de dados)

Para obter mais informações sobre categorias de métricas, consulte Categorias de métricas. Para obter uma lista completa de métricas, consulte Glossário de métricas de lente de armazenamento do Amazon S3.

10. (Opcional) Configure a exportação de métricas.

    Para obter mais informações sobre como configurar a exportação de métricas, consulte Usar o console do S3.

11. Escolha Create dashboard (Criar painel).

Como usar o AWS CLI

O seguinte exemplo da AWS CLI habilita a opção de publicação no CloudWatch usando uma configuração de métricas e recomendações avançadas em nível de organização da Lente de Armazenamento do S3. Para usar esse exemplo, substitua os *`user input placeholders`* por suas próprias informações.

```
aws s3control put-storage-lens-configuration --account-id=555555555555 --config-
id=your-configuration-id --region=us-east-1 --storage-lens-configuration=file://./
config.json

config.json
{
  "Id": "SampleS3StorageLensConfiguration", //Use this property to identify your S3
 Storage Lens configuration.
  "AwsOrg": { //Use this property when enabling S3 Storage Lens for AWS Organizations.
    "Arn": "arn:aws:organizations::123456789012:organization/o-abcdefgh"
  },
  "AccountLevel": {
    "ActivityMetrics": {
      "IsEnabled":true
    },
    "AdvancedCostOptimizationMetrics": {
      "IsEnabled":true
    },
    "AdvancedDataProtectionMetrics": {
```

```
      "IsEnabled":true
    },
    "DetailedStatusCodesMetrics": {
      "IsEnabled":true
    },
    "BucketLevel": {
      "ActivityMetrics": {
        "IsEnabled":true //Mark this as false if you want only free metrics.
      },
      "ActivityMetrics": {
        "IsEnabled":true //Mark this as false if you want only free metrics.
      },
      "AdvancedCostOptimizationMetrics": {
        "IsEnabled":true //Mark this as false if you want only free metrics.
      },
      "DetailedStatusCodesMetrics": {
        "IsEnabled":true //Mark this as false if you want only free metrics.
      },
      "PrefixLevel":{
        "StorageMetrics":{
          "IsEnabled":true, //Mark this as false if you want only free metrics.
          "SelectionCriteria":{
            "MaxDepth":5,
            "MinStorageBytesPercentage":1.25,
            "Delimiter":"/"
          }
        }
      }
    }
  },
  "Exclude": { //Replace with "Include" if you prefer to include Regions.
    "Regions": [
      "eu-west-1"
    ],
    "Buckets": [ //This attribute is not supported for AWS Organizations-level
configurations.
      "arn:aws:s3:::amzn-s3-demo-source-bucket "
    ]
  },
  "IsEnabled": true, //Whether the configuration is enabled
  "DataExport": { //Details about the metrics export
    "S3BucketDestination": {
      "OutputSchemaVersion": "V_1",
      "Format": "CSV", //You can add "Parquet" if you prefer.
```

```
      "AccountId": "111122223333",
      "Arn": "arn:aws:s3:::amzn-s3-demo-destination-bucket", // The destination
 bucket for your metrics export must be in the same Region as your S3 Storage Lens
 configuration.
      "Prefix": "prefix-for-your-export-destination",
      "Encryption": {
        "SSES3": {}
      }
    },
    "CloudWatchMetrics": {
      "IsEnabled": true //Mark this as false if you want to export only free metrics.
    }
  }
}
```

Usar o AWS SDK for Java

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import com.amazonaws.services.s3control.model.AccountLevel;
import com.amazonaws.services.s3control.model.ActivityMetrics;
import com.amazonaws.services.s3control.model.BucketLevel;
import com.amazonaws.services.s3control.model.CloudWatchMetrics;
import com.amazonaws.services.s3control.model.Format;
import com.amazonaws.services.s3control.model.Include;
import com.amazonaws.services.s3control.model.OutputSchemaVersion;
import com.amazonaws.services.s3control.model.PrefixLevel;
import com.amazonaws.services.s3control.model.PrefixLevelStorageMetrics;
import com.amazonaws.services.s3control.model.PutStorageLensConfigurationRequest;
import com.amazonaws.services.s3control.model.S3BucketDestination;
import com.amazonaws.services.s3control.model.SSES3;
import com.amazonaws.services.s3control.model.SelectionCriteria;
import com.amazonaws.services.s3control.model.StorageLensAwsOrg;
import com.amazonaws.services.s3control.model.StorageLensConfiguration;
import com.amazonaws.services.s3control.model.StorageLensDataExport;
import com.amazonaws.services.s3control.model.StorageLensDataExportEncryption;
import com.amazonaws.services.s3control.model.StorageLensTag;
```

```
import java.util.Arrays;
import java.util.List;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class CreateAndUpdateDashboard {

    public static void main(String[] args) {
        String configurationId = "ConfigurationId";
        String sourceAccountId = "Source Account ID";
        String exportAccountId = "Destination Account ID";
        String exportBucketArn = "arn:aws:s3:::amzn-s3-demo-destination-bucket"; //
 The destination bucket for your metrics export must be in the same Region as your S3
 Storage Lens configuration.
        String awsOrgARN = "arn:aws:organizations::123456789012:organization/o-
abcdefgh";
        Format exportFormat = Format.CSV;

        try {
            SelectionCriteria selectionCriteria = new SelectionCriteria()
                    .withDelimiter("/")
                    .withMaxDepth(5)
                    .withMinStorageBytesPercentage(10.0);
            PrefixLevelStorageMetrics prefixStorageMetrics = new
 PrefixLevelStorageMetrics()
                    .withIsEnabled(true)
                    .withSelectionCriteria(selectionCriteria);
            BucketLevel bucketLevel = new BucketLevel()
                    .withActivityMetrics(new ActivityMetrics().withIsEnabled(true))
                    .withAdvancedCostOptimizationMetrics(new
 AdvancedCostOptimizationMetrics().withIsEnabled(true))
                    .withAdvancedDataProtectionMetrics(new
 AdvancedDataProtectionMetrics().withIsEnabled(true))
                    .withDetailedStatusCodesMetrics(new
 DetailedStatusCodesMetrics().withIsEnabled(true))
                    .withPrefixLevel(new
 PrefixLevel().withStorageMetrics(prefixStorageMetrics));
            AccountLevel accountLevel = new AccountLevel()
                    .withActivityMetrics(new ActivityMetrics().withIsEnabled(true))
                    .withAdvancedCostOptimizationMetrics(new
 AdvancedCostOptimizationMetrics().withIsEnabled(true))
                    .withAdvancedDataProtectionMetrics(new
 AdvancedDataProtectionMetrics().withIsEnabled(true))
```

```
                    .withDetailedStatusCodesMetrics(new
DetailedStatusCodesMetrics().withIsEnabled(true))
                    .withBucketLevel(bucketLevel);

            Include include = new Include()
                    .withBuckets(Arrays.asList("arn:aws:s3:::amzn-s3-demo-bucket"))
                    .withRegions(Arrays.asList("us-west-2"));

            StorageLensDataExportEncryption exportEncryption = new
StorageLensDataExportEncryption()
                    .withSSES3(new SSES3());
            S3BucketDestination s3BucketDestination = new S3BucketDestination()
                    .withAccountId(exportAccountId)
                    .withArn(exportBucketArn)
                    .withEncryption(exportEncryption)
                    .withFormat(exportFormat)
                    .withOutputSchemaVersion(OutputSchemaVersion.V_1)
                    .withPrefix("Prefix");
            CloudWatchMetrics cloudWatchMetrics = new CloudWatchMetrics()
                    .withIsEnabled(true);
            StorageLensDataExport dataExport = new StorageLensDataExport()
                    .withCloudWatchMetrics(cloudWatchMetrics)
                    .withS3BucketDestination(s3BucketDestination);

            StorageLensAwsOrg awsOrg = new StorageLensAwsOrg()
                    .withArn(awsOrgARN);

            StorageLensConfiguration configuration = new StorageLensConfiguration()
                    .withId(configurationId)
                    .withAccountLevel(accountLevel)
                    .withInclude(include)
                    .withDataExport(dataExport)
                    .withAwsOrg(awsOrg)
                    .withIsEnabled(true);

            List<StorageLensTag> tags = Arrays.asList(
                    new StorageLensTag().withKey("key-1").withValue("value-1"),
                    new StorageLensTag().withKey("key-2").withValue("value-2")
            );

            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(US_WEST_2)
                    .build();
```

```
            s3ControlClient.putStorageLensConfiguration(new
 PutStorageLensConfigurationRequest()
                    .withAccountId(sourceAccountId)
                    .withConfigId(configurationId)
                    .withStorageLensConfiguration(configuration)
                    .withTags(tags)
            );
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Uso da API REST

Para habilitar a opção de publicação no CloudWatch usando a API REST do Amazon S3, use PutStorageLensConfiguration.

Próximas etapas

Depois de habilitar a opção de publicação no CloudWatch, você poderá acessar as métricas do S3 Storage Lens no CloudWatch. Você também pode utilizar os recursos do CloudWatch para monitorar e analisar os dados do S3 Storage Lens no CloudWatch. Para obter mais informações, consulte os tópicos a seguir.

- Métricas e dimensões do S3 Storage Lens
- Trabalhar com métricas do S3 Storage Lens no CloudWatch

Trabalhar com métricas do S3 Storage Lens no CloudWatch

É possível publicar métricas da Lente de Armazenamento do S3 no Amazon CloudWatch para criar uma visão unificada de sua integridade operacional nos painéis do CloudWatch. Também é possível usar os recursos do CloudWatch, como alarmes e ações acionadas, matemática métrica e detecção de anomalias, para monitorar e realizar ações sobre as métricas da Lente de Armazenamento do S3.

Além disso, as operações de API do CloudWatch permitem que aplicações, inclusive provedores de terceiros, acessem as métricas da Lente de Armazenamento do S3. Para obter mais informações sobre os recursos do CloudWatch, consulte o Guia do usuário do Amazon CloudWatch Events.

Você pode habilitar a opção de publicação no CloudWatch para configurações de painéis novos ou existentes usando o console do Amazon S3, as APIs REST do Amazon S3, a AWS CLI e os AWS SDKs. A opção de publicação no CloudWatch está disponível para painéis com upgrade para métricas e recomendações avançadas da Lente de Armazenamento do S3. Para saber mais sobre o preço das métricas e recomendações avançadas da Lente de Armazenamento do S3, consulte Definição de preço do Amazon S3. Não são aplicadas cobranças adicionais para publicação de métricas no CloudWatch, mas outras cobranças do CloudWatch, como painéis, alarmes e chamadas de API, são aplicáveis. Para obter mais informações, consulte Preço do Amazon CloudWatch.

As métricas do S3 Storage Lens são publicadas no CloudWatch na conta proprietária da configuração do S3 Storage Lens. Depois de habilitar a opção de publicação no CloudWatch em métricas e recomendações avançadas, você pode acessar as métricas por organização, conta e bucket no CloudWatch. As métricas de nível prefixo não estão disponíveis no CloudWatch.

> **Note**
>
> As métricas do S3 Storage Lens são métricas diárias e são publicadas no CloudWatch uma vez por dia. Quando você consulta métricas do S3 Storage Lens no CloudWatch, o período para a consulta deve ser de 1 dia (86.400 segundos). Depois que as métricas diárias do S3 Storage Lens são exibidas no painel do S3 Storage Lens no console do Amazon S3, essas mesmas métricas podem demorar algumas horas para serem exibidas no CloudWatch. Quando você habilita a opção de publicação do CloudWatch para métricas do S3 Storage Lens pela primeira vez, as métricas podem levar até 24 horas para serem publicadas no CloudWatch.
>
> No momento, as métricas da Lente de Armazenamento do S3 não podem ser consumidas por fluxos do CloudWatch.

Para obter mais informações sobre como trabalhar com métricas do S3 Storage Lens no CloudWatch, consulte os tópicos a seguir.

Tópicos

- Trabalhar com painéis do CloudWatch
- Definir alarmes, acionar ações e usar detecção de anomalias

- Filtrar métricas usando dimensões
- Calcular novas métricas com matemática métrica
- Usar expressões de pesquisa em gráficos

Trabalhar com painéis do CloudWatch

É possível usar os painéis do CloudWatch para monitorar as métricas do S3 Storage Lens juntamente com métricas de outras aplicações e criar uma visão unificada de sua integridade operacional. Os painéis são páginas iniciais personalizáveis no console do CloudWatch que você pode usar para monitorar seus recursos em uma única visualização.

O CloudWatch tem amplo controle de permissões que não oferece suporte ao limite de acesso a um conjunto específico de métricas ou dimensões. Os usuários de sua conta ou organização que têm acesso ao CloudWatch terão acesso a métricas para todas as configurações do S3 Storage Lens em que a opção de suporte do CloudWatch estiver habilitada. Não é possível gerenciar permissões para painéis específicos, como pode ser feito no S3 Storage Lens. Para obter mais informações sobre permissões do CloudWatch, consulte Gerenciamento de permissões de acesso a seus recursos do CloudWatch no Guia do usuário do Amazon CloudWatch.

Para obter mais informações sobre como usar painéis do CloudWatch e configurar permissões, consulte Usar painéis do Amazon CloudWatch e Compartilhar painéis do CloudWatch no Guia do usuário do Amazon CloudWatch.

Definir alarmes, acionar ações e usar detecção de anomalias

Você pode configurar alarmes do CloudWatch que monitoram as métricas do S3 Storage Lens no CloudWatch e realizam ações quando um limite é violado. Por exemplo, é possível configurar um alarme que envia uma notificação do Amazon SNS quando a métrica Incomplete Multipart Upload Bytes (Bytes de multipart uploads incompletos) exceder 1 GB por três dias consecutivos.

Também é possível habilitar a detecção de anomalias para analisar continuamente as métricas do S3 Storage Lens, determinar linhas de base normais e apontar anomalias. Você pode criar um alarme de detecção de anomalias com base no valor esperado de uma métrica. Por exemplo, é possível monitorar anomalias na métrica Object Lock Enabled Bytes (Bytes de Bloqueio de Objeto ativado) para detectar a remoção não autorizada das configurações de Bloqueio de Objeto.

Para obter mais informações e exemplos, consulte Usar alarmes do Amazon CloudWatch e Criar um alarme da métrica em um grafo no Guia do usuário do Amazon CloudWatch.

Filtrar métricas usando dimensões

Use dimensões para filtrar métricas do S3 Storage Lens no console do CloudWatch. Por exemplo, é possível filtrar por `configuration_id`, `aws_account_number`, `aws_region`, `bucket_name` e muito mais.

O S3 Storage Lens oferece suporte a várias configurações de painel por conta. Isso significa que configurações diferentes podem incluir o mesmo bucket. Quando essas métricas forem publicadas no CloudWatch, o bucket terá métricas duplicadas no CloudWatch. Para exibir métricas somente para uma configuração específica do S3 Storage Lens no CloudWatch, você pode usar a dimensão `configuration_id`. Ao filtrar por `configuration_id`, você visualiza apenas métricas associadas à configuração que você identificou.

Para obter mais informações sobre filtragem por ID de configuração, consulte Procurar as métricas disponíveis no Guia do usuário do Amazon CloudWatch.

Calcular novas métricas com matemática métrica

Você pode usar a matemática métrica para consultar várias métricas do S3 Storage Lens e usar expressões matemáticas para criar novas séries temporais de acordo com essas métricas. Por exemplo, é possível criar uma nova métrica para objetos não criptografados subtraindo os objetos criptografados da contagem de objetos. Também é possível criar uma métrica para obter o tamanho médio de objetos dividindo `StorageBytes` por `ObjectCount`, ou o número de bytes acessados em um dia dividindo `BytesDownloaded` por `StorageBytes`.

Para obter mais informações, consulte Usar matemática métrica no Guia do usuário do Amazon CloudWatch.

Usar expressões de pesquisa em gráficos

Com as métricas da Lente de Armazenamento do S3, é possível criar uma expressão de pesquisa. Por exemplo, é possível criar uma expressão de pesquisa para todas as métricas chamadas IncompleteMultipartUploadStorageBytes e adicionar `SUM` à expressão. Com essa expressão de pesquisa, é possível visualizar o total de bytes de multipart uploads incompletos em todas as dimensões do armazenamento em uma única métrica.

Este exemplo mostra a sintaxe que você usaria para criar uma expressão de pesquisa para todas as métricas chamadas IncompleteMultipartUploadStorageBytes.

```
SUM(SEARCH('{AWS/S3/Storage-
Lens,aws_account_number,aws_region,configuration_id,metrics_version,record_type,storage_class}
 MetricName="IncompleteMultipartUploadStorageBytes"', 'Average',86400))
```

Para obter mais informações sobre essa sintaxe, consulte Sintaxe de expressão de pesquisa do CloudWatch no Guia do usuário do Amazon CloudWatch. Para criar um grafo do CloudWatch com uma expressão de pesquisa, consulte Criar um grafo do CloudWatch com uma expressão de pesquisa no Guia do usuário do Amazon CloudWatch.

Casos de uso das métricas da Lente de Armazenamento do Amazon S3

Você pode usar o painel da Lente de Armazenamento do Amazon S3 para visualizar insights e tendências, sinalizar discrepâncias e receber recomendações. As métricas da Lente de Armazenamento do S3 são organizadas em categorias que estão alinhadas aos principais casos de uso. Você pode usar essas métricas para fazer o seguinte:

- Identificar oportunidades para otimização de custos
- Aplicar práticas recomendadas para proteção de dados
- Aplicar práticas recomendadas para gerenciamento de acesso
- Melhorar a performance das workloads de aplicações

Por exemplo, com as métricas de otimização de custos, você pode identificar oportunidades para reduzir os custos de armazenamento do Amazon S3. Você pode identificar buckets com multipart uploads existentes há mais de 7 dias ou buckets que estão acumulando versões desatualizadas.

Da mesma forma, você pode usar métricas de proteção de dados para identificar buckets que não estão seguindo as práticas recomendadas para proteção de dados em sua organização. Por exemplo, você pode identificar buckets que não usam chaves do AWS Key Management Service (SSE-KMS) para criptografia padrão ou que não têm o Versionamento do S3 ativado.

Com as métricas de gerenciamento de acesso da Lente de Armazenamento do S3, você pode identificar as configurações de bucket para a Propriedade de Objeto do S3 a fim de migrar as permissões da lista de controle de acesso (ACL) para políticas de bucket e desativar as ACLs.

Se a opção S3 Storage Lens advanced metrics (Métricas avançadas da Lente de Armazenamento do S3) estiver ativada, você poderá usar as métricas detalhadas de código de status para obter contagens de solicitações bem-sucedidas ou malsucedidas, que podem ser usadas para solucionar problemas de acesso ou performance.

Com métricas avançadas, você também pode acessar métricas adicionais de otimização de custos e proteção de dados que podem ser usadas com o intuito de identificar oportunidades para reduzir ainda mais os custos gerais de armazenamento do S3 e se alinhar melhor às práticas recomendadas para proteção de dados. Por exemplo, as métricas avançadas de otimização de custos incluem contagens de regras de ciclo de vida que podem ser usadas para identificar buckets que não têm regras de ciclo de vida para expirar multipart uploads incompletos com mais de 7 dias. As métricas avançadas de proteção de dados incluem contagens de regras de replicação.

Para obter mais informações sobre categorias de métricas, consulte Categorias de métricas. Para obter uma lista completa de métricas da Lente de Armazenamento do S3, consulte Glossário de métricas de lente de armazenamento do Amazon S3.

Tópicos

- Como usar o Amazon S3 Storage Lens para otimizar seus custos de armazenamento
- Usar a Lente de Armazenamento do S3 para proteger seus dados
- Como usar a Lente de Armazenamento do S3 para auditar configurações da Propriedade de Objeto
- Usar a Lente de Armazenamento do S3 para melhorar a performance

Como usar o Amazon S3 Storage Lens para otimizar seus custos de armazenamento

Você pode usar as métricas de otimização de custos da Lente de Armazenamento do S3 para reduzir seu custo geral de armazenamento do S3. As métricas de otimização de custos podem ajudar você a confirmar que configurou o Amazon S3 de forma econômica e de acordo com as práticas recomendadas. Por exemplo, você pode identificar as seguintes oportunidades de otimização de custos:

- Buckets com multipart uploads incompletos com mais de 7 dias
- Buckets que estão acumulando várias versões desatualizadas
- Buckets que não têm regras de ciclo de vida para anular multipart uploads incompletos
- Buckets que não têm regras de ciclo de vida para expirar objetos de versões desatualizadas
- Buckets que não têm regras de ciclo de vida para migrar objetos para uma classe de armazenamento diferente

Depois, você pode usar esses dados para adicionar outras regras de ciclo de vida aos seus buckets.

Os exemplos a seguir mostram como você pode usar as métricas de otimização de custos no painel da Lente de Armazenamento do S3 para otimizar seus custos de armazenamento.

Tópicos

- Identifique os seus maiores buckets do S3
- Descubra buckets inativos do Amazon S3
- Localize uploads fracionados incompletos
- Reduza o número de versões não atuais retidas
- Identificar buckets que não têm regras de ciclo de vida e revisar as contagens de regras de ciclo de vida

Identifique os seus maiores buckets do S3

Você paga para armazenar objetos em buckets do S3. A taxa cobrada depende do tamanho dos seus objetos, por quanto tempo você os armazena e quais são as classes de armazenamento. Com a Lente de Armazenamento do S3, você tem uma visualização centralizada de todos os buckets em sua conta. Para ver todos os buckets em todas as contas da sua organização, é possível configurar um painel do S3 Storage Lens no nível do AWS Organizations. Nessa visualização do painel, você pode identificar os seus maiores buckets.

Etapa 1: Identificar os seus maiores buckets

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação esquerdo, escolha Storage Lens (Lente de Armazenamento) e Dashboards (Painéis).
3. Na lista Dashboards (Painéis), escolha o painel que deseja visualizar.

   Quando o painel é aberto, você pode ver a data mais recente em que a Lente de Armazenamento do S3 coletou métricas. Seu painel sempre carrega a data mais recente para a qual há métricas disponíveis.
4. Para ver a classificação dos seus maiores buckets de acordo com a métrica Total storage (Armazenamento total) para um intervalo de datas selecionado, role para baixo até a seção Top N overview for date (Visão geral dos N principais para data).

   Você pode alternar a ordem de classificação para mostrar os buckets menores. Você também pode ajustar a seleção de Metric (Métrica) para classificar seus buckets de acordo com qualquer

uma das métricas disponíveis. A seção Top N overview for date (Visão geral dos N principais para data) também mostra a variação percentual em relação ao dia ou semana anterior e uma linha em spark para visualizar a tendência. Essa tendência é de 14 dias para métricas gratuitas e 30 dias para métricas e recomendações avançadas.

> **Note**
>
> Com métricas e recomendações avançadas da Lente de Armazenamento do S3, as métricas ficam disponíveis para consultas por 15 meses. Para obter mais informações, consulte Seleção de métricas.

5. Para obter informações mais detalhadas sobre seus buckets, role até o topo da página e escolha a guia Bucket.

   Na guia Bucket, você pode ver detalhes como a taxa de crescimento recente, o tamanho médio do objeto, os maiores prefixos e o número de objetos.

Etapa 2: Navegar até os buckets e investigar

Depois de identificar seus maiores buckets do S3, você pode navegar até cada bucket no console do S3 para visualizar os objetos no bucket, entender a workload associada ao bucket e identificar os proprietários internos. Você pode entrar em contato com os proprietários do bucket para descobrir se o crescimento é esperado ou se precisa de monitoramento e controle adicionais.

Descubra buckets inativos do Amazon S3

Se você tiver métricas avançadas do S3 Storage Lens habilitadas, poderá usar métricas de atividade para entender o quão inativos seus buckets do S3 estão. Um bucket inativo é aquele cujo armazenamento deixou de ter acesso (ou é acessado raramente). Essa falta de atividade normalmente indica que os objetos do bucket não são acessados com frequência.

As métricas de atividade, como solicitações GET e bytes de download, indicam com que frequência os seus buckets são acessados todos os dias. Para entender a consistência do padrão de acesso e identificar buckets que deixaram de ser acessados, você pode fazer uma tendência desses dados ao longo de vários meses. A métrica de taxa de recuperação, computada como bytes de download/armazenamento total, indica a proporção de armazenamento em um bucket acessado diariamente.

> **Note**
>
> Os bytes de download são duplicados nos casos em que há download do mesmo objeto várias vezes em um dia.

Pré-requisito

Para ver as métricas de atividade no painel da Lente de Armazenamento do S3, você deve ativar a opção Advanced metrics and recommendations (Métricas e recomendações avançadas) da Lente de Armazenamento do S3 e selecionar Activity metrics (Métricas de atividade). Para obter mais informações, consulte Usar o console do S3.

Etapa 1: Identificar os buckets ativos

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação esquerdo, escolha Storage Lens (Lente de Armazenamento) e Dashboards (Painéis).
3. Na lista Dashboards (Painéis), escolha o painel que deseja visualizar.
4. Escolha a guia Bucket, depois role para baixo até a seção Bubble analysis by buckets for date (Análise de bolhas por buckets para data).

   Na seção Bubble analysis by buckets for date (Análise de bolhas por buckets para data), você pode plotar seus buckets em várias dimensões usando três métricas quaisquer para representar o X-axis (Eixo X), Y-axis (Eixo Y) e Size (Tamanho) da bolha.
5. Para encontrar buckets que ficaram inativos, para X-axis (Eixo X), Y-axis (Eixo Y) e Size (Tamanho), escolha as métricas Total storage (Armazenamento total), % retrieval rate (% da taxa de recuperação) e Average object size (Tamanho médio dos objetos).
6. Na seção Bubble analysis by buckets for date (Análise de bolhas por buckets para data), encontre os buckets com taxas de recuperação iguais a zero (ou próximas de zero) e um tamanho de armazenamento relativo maior, depois escolha a bolha que representa o bucket.

   Uma caixa aparecerá com opções para obter insights mais granulares. Execute um destes procedimentos:

   a. Para atualizar a guia Bucket para exibir métricas somente para o bucket selecionado, escolha Drill Down (Detalhar) e Apply (Aplicar).

b. Para agregar os dados de bucket por conta, Região da AWS, classe de armazenamento ou bucket, escolha Analyze by (Analisar por), depois selecione uma opção em Dimension (Dimensão). Por exemplo, para agregar por classe de armazenamento, escolha Storage class (Classe de armazenamento) em Dimension (Dimensão).

Para encontrar os buckets que se tornaram inativos, faça uma análise em bolhas usando as métricas Total storage (Armazenamento total), % retrieval rate (% de taxa de recuperação) e Average object size (Tamanho médio do objeto). Procure por buckets com taxas zero de recuperação (ou próximas a zero) e um tamanho maior de armazenamento relativo.

A guia Bucket do seu painel é atualizada para exibir os dados da agregação ou filtro selecionado. Se você agregou por classe de armazenamento ou outra dimensão, essa nova guia é aberta em seu painel (por exemplo, a guia Storage class (Classe de armazenamento)).

Etapa 2: Investigar os buckets inativos

Aqui, você pode identificar os proprietários de buckets inativos em sua conta ou organização e descobrir se esse armazenamento ainda é necessário. Depois, é possível otimizar os custos definindo as configurações de validade de ciclo de vida para esses buckets ou arquivando os dados em uma das classes de armazenamento do Amazon S3 Glacier.

Para impedir que o problema de buckets inativos prossiga, você pode fazer a transição dos seus dados de forma automática usando configurações do ciclo de vida do S3 em seus buckets, ou habilitar o arquivamento automático com o S3 Intelligent-Tiering.

Você também pode usar a etapa 1 para identificar os buckets ativos. Depois, você pode garantir que esses buckets usem a classe de armazenamento do S3 correta para garantir que atendam às solicitações com mais eficiência em termos de performance e custo.

Localize uploads fracionados incompletos

Você pode usar multipart uploads para fazer upload de objetos muito grandes (até 5 TB) como um conjunto de partes para obter uma throughput aprimorada e uma recuperação mais rápida diante de problemas de rede. Quando o processo de multipart upload não termina, as partes incompletas permanecem no bucket (em um estado inutilizável). Essas partes incompletas incorrem em custos de armazenamento até que o processo de upload seja concluído, ou até que as partes incompletas sejam removidas. Para obter mais informações, consulte Carregar e copiar objetos usando upload fracionado no Amazon S3.

Com a Lente de Armazenamento do S3, você pode identificar o número de bytes de multipart uploads incompletos em sua conta ou em toda a sua organização, incluindo multipart uploads incompletos há mais de 7 dias. Para obter uma lista completa de métricas de multipart uploads incompletos, consulte Glossário de métricas de lente de armazenamento do Amazon S3.

Uma prática recomendada é configurar regras de ciclo de vida para expirar multipart uploads incompletos há mais de determinada quantidade de dias. Ao criar uma regra de ciclo de vida para expirar multipart uploads incompletos, recomendamos 7 dias como um bom ponto de partida.

Etapa 1: Analise as tendências gerais de multipart uploads incompletos

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação esquerdo, escolha Storage Lens (Lente de Armazenamento) e Dashboards (Painéis).
3. Na lista Dashboards (Painéis), escolha o painel que deseja visualizar.
4. Na seção Snapshot for date (Snapshot para data), em Metrics categories (Categorias de métricas), escolha Cost optimization (Otimização de custos).

   A seção Snapshot for date (Snapshot para data) é atualizada para exibir métricas de Cost optimization (Otimização de custos), que incluem Incomplete multipart upload bytes greater than 7 days old (Bytes de multipart uploads incompletos há mais de 7 dias).

   Em qualquer gráfico no painel da Lente de Armazenamento do S3, você pode ver métricas para multipart uploads incompletos. Você pode usar essas métricas para avaliar ainda mais o impacto dos bytes de multipart uploads incompletos no seu armazenamento, incluindo a contribuição deles para as tendências gerais de crescimento. Você também pode detalhar níveis mais profundos de agregação usando as guias Account (Conta), Região da AWS, Bucket ou Storage class (Classe de armazenamento) para uma análise mais profunda de seus dados. Para obter um exemplo, consulte Descubra buckets inativos do Amazon S3.

Etapa 2: Identificar os buckets que têm o maior número de bytes de multipart uploads incompletos, mas não têm regras de ciclo de vida para anular multipart uploads incompletos

Pré-requisito

Para ver a métrica Abort incomplete multipart upload lifecycle rule count (Contagem de regras de ciclo de vida para anulação de multipart uploads incompletos) no painel da Lente de Armazenamento

do S3, ative Advanced metrics and recommendations (Métricas e recomendações avançadas) da Lente de Armazenamento do S3, depois selecione Advanced cost optimization metrics (Métricas avançadas de otimização de custos). Para obter mais informações, consulte Usar o console do S3.

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação esquerdo, escolha Storage Lens (Lente de Armazenamento) e Dashboards (Painéis).
3. Na lista Dashboards (Painéis), escolha o painel que deseja visualizar.
4. Para identificar buckets específicos com multipart uploads incompletos acumulados há mais de 7 dias, acesse a seção Top N overview for date (Visão geral dos N principais para data).

   Por padrão, a seção Top N overview for date (Visão geral dos N principais para data) exibe métricas para os 3 principais buckets. Você pode aumentar ou diminuir o número de buckets no campo Top N (N principais). A seção Top N overview for date (Visão geral dos N principais para data) também mostra a variação percentual em relação ao dia ou semana anterior e uma linha em spark para visualizar a tendência. (Essa tendência é de 14 dias para métricas gratuitas e 30 dias para métricas e recomendações avançadas.)

   > **Note**
   >
   > Com métricas e recomendações avançadas da Lente de Armazenamento do S3, as métricas ficam disponíveis para consultas por 15 meses. Para obter mais informações, consulte Seleção de métricas.

5. Em Metric (Métrica), escolha Incomplete multipart upload bytes greater than 7 days old (Bytes de multipart uploads incompletos há mais de 7 dias) na categoria Cost optimization (Otimização de custos).

   Em Top number buckets (Número buckets principais), você pode ver os buckets com a maior quantidade de bytes armazenados de multipart uploads incompletos há mais de 7 dias.
6. Para ver métricas mais detalhadas por bucket para multipart uploads incompletos, vá até o topo da página e escolha a guia Bucket.
7. Role para baixo até a seção Buckets. Em Metrics categories (Categorias de métricas), selecione Cost optimization (Otimização de custos). Depois, desmarque Summary (Resumo).

A lista Buckets é atualizada para exibir todas as métricas de Cost optimization (Otimização de custos) disponíveis para os buckets mostrados.

8. Para filtrar a lista Buckets a fim de exibir somente métricas específicas de otimização de custos, escolha o ícone de preferências ().
9. Desmarque todas as métricas de otimização de custos exceto Incomplete multipart upload bytes greater than 7 days old (Bytes de multipart uploads incompletos há mais de 7 dias) e Abort incomplete multipart upload lifecycle rule count (Contagem de regras de ciclo de vida para anulação de multipart uploads incompletos).
10. (Opcional) Em Page size (Tamanho da página), escolha o número de buckets a serem exibidos na lista.
11. Escolha Confirmar.

    A lista Buckets é atualizada para exibir métricas por bucket para multipart uploads incompletos e contagens de regras de ciclo de vida. Você pode usar esses dados para identificar os buckets com mais bytes de multipart uploads incompletos há mais de 7 dias e que não têm regras de ciclo de vida para anular multipart uploads incompletos. Depois, você pode navegar até esses buckets no console do S3 e adicionar regras de ciclo de vida para excluir os multipart uploads incompletos que ficaram esquecidos.

Etapa 3: Adicionar uma regra de ciclo de vida para excluir multipart uploads incompletos depois de 7 dias

Para gerenciar uploads incompletos de várias partes automaticamente, use o console do S3 para criar uma configuração de ciclo de vida para expirar bytes de uploads incompletos de várias partes em um bucket após determinado número de dias. Para obter mais informações, consulte Configurar uma política de ciclo de vida de bucket para anular uploads incompletos de várias partes.

Reduza o número de versões não atuais retidas

Quando habilitado, o Versionamento do S3 retém várias cópias distintas do mesmo objeto que podem ser usadas para recuperar dados rapidamente se um objeto for acidentalmente excluído ou substituído. Se você habilitou o Versionamento do S3 sem configurar regras de ciclo de vida para fazer a transição ou expirar versões desatualizadas, um grande número de versões anteriores desatualizadas pode se acumular, o que pode ter implicações no custo do armazenamento. Para obter mais informações, consulte Reter várias versões de objetos com o Versionamento do S3.

Etapa 1: Identificar os buckets com mais versões de objetos desatualizadas

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação esquerdo, escolha Storage Lens (Lente de Armazenamento) e Dashboards (Painéis).
3. Na lista Dashboards (Painéis), escolha o painel que deseja visualizar.
4. Na seção Snapshot for date (Snapshot para data), em Metrics categories (Categorias de métricas), escolha Cost optimization (Otimização de custos).

   A seção Snapshot for date (Snapshot para data) é atualizada para exibir as métricas de Cost optimization (Otimização de custos), que incluem a métrica % noncurrent version bytes (% de bytes de versões desatualizadas). A métrica % noncurrent version bytes (% de bytes de versões desatualizadas) representa a proporção do total de bytes de armazenamento que é atribuída a versões desatualizadas, dentro do escopo do painel e para a data selecionada.

   > **Note**
   >
   > Se a sua % noncurrent version bytes (% de bytes de versões desatualizadas) for superior a 10% do seu armazenamento por conta, talvez você esteja armazenando muitas versões de objetos.

5. Para identificar buckets específicos que estão acumulando um grande número de versões desatualizadas:

   a. Role para baixo até a seção Top N overview for date (Visão geral dos N principais para data). Em Top N (N principais), insira o número de buckets para os quais deseja ver dados.

   b. Em Metric (Métrica), escolha % noncurrent version bytes (% de bytes de versões desatualizadas).

      Em Top number buckets (Número buckets principais), você pode ver os buckets (para o número especificado) com a maior % noncurrent version bytes (% de bytes de versões desatualizadas). A seção Top N overview for date (Visão geral dos N principais para data) também mostra a variação percentual em relação ao dia ou semana anterior e uma linha em spark para visualizar a tendência. Essa tendência é de 14 dias para métricas gratuitas e 30 dias para métricas e recomendações avançadas.

> **Note**
>
> Com métricas e recomendações avançadas da Lente de Armazenamento do S3, as métricas ficam disponíveis para consultas por 15 meses. Para obter mais informações, consulte Seleção de métricas.

c. Para ver métricas mais detalhadas por bucket para versões de objetos desatualizadas, vá até o topo da página e escolha a guia Bucket.

   Em qualquer gráfico ou visualização no painel da Lente de Armazenamento do S3, você pode detalhar níveis mais profundos de agregação usando as guias Account (Conta), Região da AWS, Storage class (Classe de armazenamento) ou Bucket. Para obter um exemplo, consulte Descubra buckets inativos do Amazon S3.

d. Na seção Buckets, para Metric categories (Categorias de métricas), selecione Cost optimization (Otimização de custos). Depois, desmarque Summary (Resumo).

   Agora é possível ver a métrica % noncurrent version bytes (% de bytes de versões desatualizadas) ao lado de outras métricas relacionadas às versões desatualizadas.

Etapa 2: Identificar buckets que não têm regras de ciclo de vida de transição e expiração para gerenciar versões desatualizadas

Pré-requisito

Para ver as métricas Noncurrent version transition lifecycle rule count (Contagem de regras de ciclo de vida para transição de versões desatualizadas) e Noncurrent version expiration lifecycle rule count (Contagem de regras de ciclo de vida para validade de versões desatualizadas) no painel da Lente de Armazenamento do S3, ative a opção Advanced metrics and recommendations (Métricas e recomendações avançadas) da Lente de Armazenamento do S3 e selecione Advanced cost optimization metrics (Métricas avançadas de otimização de custos). Para obter mais informações, consulte Usar o console do S3.

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação esquerdo, escolha Storage Lens (Lente de Armazenamento) e Dashboards (Painéis).
3. Na lista Dashboards (Painéis), escolha o painel que deseja visualizar.

4. No painel da Lente de Armazenamento, escolha a guia Bucket.
5. Role para baixo até a seção Buckets. Em Metrics categories (Categorias de métricas), selecione Cost optimization (Otimização de custos). Depois, desmarque Summary (Resumo).

   A lista Buckets é atualizada para exibir todas as métricas de Cost optimization (Otimização de custos) disponíveis para os buckets mostrados.
6. Para filtrar a lista Buckets a fim de exibir somente métricas específicas de otimização de custos, escolha o ícone de preferências
   ().
7. Desmarque todas as métricas de otimização de custos, exceto:

   - % noncurrent version bytes (% de bytes de versões desatualizadas)
   - Noncurrent version transition lifecycle rule count (Contagem de regras de ciclo de vida para transição de versões desatualizadas)
   - Noncurrent version expiration lifecycle rule count (Contagem de regras de ciclo de vida para validade de versões desatualizadas)
8. (Opcional) Em Page size (Tamanho da página), escolha o número de buckets a serem exibidos na lista.
9. Escolha Confirmar.

   A lista Buckets é atualizada para exibir as métricas de bytes de versões desatualizadas e contagens de regras de ciclo de vida de versões desatualizadas. Você pode usar esses dados para identificar buckets que têm uma alta porcentagem de bytes de versões desatualizadas, mas que não têm regras de ciclo de vida de transição e validade. Depois, você pode navegar até esses buckets no console do S3 e adicionar regras de ciclo de vida a esses buckets.

Etapa 3: Adicionar regras de ciclo de vida para fazer a transição ou expirar versões de objetos desatualizadas

Depois de determinar quais buckets exigem investigação adicional, você pode navegar até os buckets no console do S3 e adicionar uma regra de ciclo de vida para expirar versões desatualizadas depois de um número especificado de dias. Alternativamente, para reduzir custos mantendo as versões desatualizadas, você pode configurar uma regra de ciclo de vida para fazer a transição das versões desatualizadas para uma das classes de armazenamento do Amazon S3 Glacier. Para obter mais informações, consulte Especificar uma regra de ciclo de vida para um bucket com versionamento habilitado.

Identificar buckets que não têm regras de ciclo de vida e revisar as contagens de regras de ciclo de vida

A Lente de Armazenamento do S3 fornece métricas de contagem de regras do Ciclo de Vida do S3 que você pode usar para identificar buckets que não têm regras de ciclo de vida. Para encontrar buckets que não têm regras de ciclo de vida, você pode usar a métrica Total buckets without lifecycle rules (Total de buckets sem regras de ciclo de vida). Um bucket sem o Ciclo de Vida do S3 configurado pode ter armazenamento que não é mais necessário ou pode ser migrado para uma classe de armazenamento de menor custo. Você também pode usar métricas de contagem de regras de ciclo de vida para identificar buckets que não têm tipos específicos de regras de ciclo de vida, como regras de validade ou transição.

Pré-requisito

Para ver métricas de contagem de regras de ciclo de vida e a métrica Total buckets without lifecycle rules (Total de buckets sem regras de ciclo de vida) no painel da Lente de Armazenamento do S3, ative Advanced metrics and recommendations (Métricas e recomendações avançadas) da Lente de Armazenamento do S3, depois selecione Advanced cost optimization metrics (Métricas avançadas de otimização de custos). Para obter mais informações, consulte Usar o console do S3.

Etapa 1: Identificar buckets sem regras de ciclo de vida

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação esquerdo, escolha Storage Lens (Lente de Armazenamento) e Dashboards (Painéis).
3. Na lista Dashboards (Painéis), escolha o painel que deseja visualizar.
4. Para identificar buckets específicos sem regras de ciclo de vida, role para baixo até a seção Top N overview for datas (Visão geral dos N principais para data).

   Por padrão, a seção Top N overview for date (Visão geral dos N principais para data) exibe métricas para os 3 principais buckets. No campo Top N (N principais), você pode aumentar o número de buckets. A seção Top N overview for date (Visão geral dos N principais para data) também mostra a variação percentual em relação ao dia ou semana anterior e uma linha em spark para visualizar a tendência. Essa tendência é de 14 dias para métricas gratuitas e 30 dias para métricas e recomendações avançadas.

> **Note**
>
> Com métricas e recomendações avançadas da Lente de Armazenamento do S3, as métricas ficam disponíveis para consultas por 15 meses. Para obter mais informações, consulte Seleção de métricas.

5. Em Metric (Métrica), escolha Total buckets without lifecycle rules (Total de buckets sem regras de ciclo de vida) na categoria Cost optimization (Otimização de custos).
6. Analise os dados a seguir para Total buckets without lifecycle rules (Total de buckets sem regras de ciclo de vida):

   - Top number accounts (Número contas principais): veja as contas que têm mais buckets sem regras de ciclo de vida.
   - Top number Regions (Número regiões principais): veja um detalhamento dos buckets sem regras de ciclo de vida por região.
   - Top number buckets (Número buckets principais): veja os buckets que não têm regras de ciclo de vida.

   Em qualquer gráfico ou visualização no painel da Lente de Armazenamento do S3, você pode detalhar níveis mais profundos de agregação usando as guias Account (Conta), Região da AWS, Storage class (Classe de armazenamento) ou Bucket. Para obter um exemplo, consulte Descubra buckets inativos do Amazon S3.

   Depois de identificar quais buckets não têm regras de ciclo de vida, você também pode revisar contagens específicas de regras de ciclo de vida para os buckets.

Etapa 2: Revisar a contagem de regras do ciclo de vida dos buckets

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação esquerdo, escolha Storage Lens (Lente de Armazenamento) e Dashboards (Painéis).
3. Na lista Dashboards (Painéis), escolha o painel que deseja visualizar.
4. No painel da Lente de Armazenamento do S3, escolha a guia Bucket.

5. Role para baixo até a seção Buckets. Em Metrics categories (Categorias de métricas), selecione Cost optimization (Otimização de custos). Depois, desmarque Summary (Resumo).

   A lista Buckets é atualizada para exibir todas as métricas de Cost optimization (Otimização de custos) disponíveis para os buckets mostrados.

6. Para filtrar a lista Buckets a fim de exibir somente métricas específicas de otimização de custos, escolha o ícone de preferências
   ().

7. Desmarque todas as métricas de otimização de custos, exceto:

   - Transition lifecycle rule count (Contagem de regras de ciclo de vida para transição)
   - Expiration lifecycle rule count (Contagem de regras de ciclo de vida para validade)
   - Noncurrent version transition lifecycle rule count (Contagem de regras de ciclo de vida para transição de versões desatualizadas)
   - Noncurrent version expiration lifecycle rule count (Contagem de regras de ciclo de vida para validade de versões desatualizadas)
   - Abort incomplete multipart upload lifecycle rule count (Contagem de regras de ciclo de vida para anulação de multipart uploads incompletos)
   - Total lifecycle rule count (Contagem total de regras de ciclo de vida)

8. (Opcional) Em Page size (Tamanho da página), escolha o número de buckets a serem exibidos na lista.

9. Escolha Confirmar.

   A lista Buckets é atualizada para exibir as métricas de contagem de regras de ciclo de vida para os buckets. Você pode usar esses dados para identificar buckets sem regras de ciclo de vida ou que não tenham tipos específicos de regras de ciclo de vida; por exemplo, regras de validade ou transição. Depois, você pode navegar até esses buckets no console do S3 e adicionar regras de ciclo de vida a esses buckets.

Etapa 3: Adicionar regras de ciclo de vida

Depois de identificar buckets sem regras de ciclo de vida, você pode adicionar regras de ciclo de vida. Para obter mais informações, consulte Definir uma configuração do Ciclo de Vida do S3 em um bucket e Exemplos de configurações do Ciclo de Vida do S3.

Usar a Lente de Armazenamento do S3 para proteger seus dados

Você pode usar as métricas de proteção de dados da Lente de Armazenamento do Amazon S3 para identificar buckets nos quais as práticas recomendadas de proteção de dados não foram aplicadas. Você pode usar essas métricas para agir e aplicar configurações padrão que se alinham às práticas recomendadas para proteger seus dados em todos os buckets de sua conta ou organização. Por exemplo, você pode usar métricas de proteção de dados para identificar buckets que não usam chaves do AWS Key Management Service (AWS KMS) para criptografia padrão ou solicitações que usam o AWS Signature Version 2 (SigV2).

Os casos de uso a seguir fornecem estratégias para usar o painel da Lente de Armazenamento do S3 para identificar valores discrepantes e aplicar as práticas recomendadas de proteção de dados em seus bucket da Lente de Armazenamento do S3.

Tópicos

- Identificar buckets que não usam a criptografia do lado do servidor com AWS KMS como criptografia padrão (SSE-KMS)
- Identificar buckets com o Versionamento do S3 ativado
- Identificar solicitações que usam o AWS Signature Version 2 (SigV2)
- Contar o número total de regras de replicação para cada bucket
- Identificar a porcentagem de bytes do Bloqueio de Objeto

Identificar buckets que não usam a criptografia do lado do servidor com AWS KMS como criptografia padrão (SSE-KMS)

Com a criptografia padrão do Amazon S3, você pode definir o comportamento de criptografia padrão para um bucket do S3. Para obter mais informações, consulte the section called “Definir criptografia de bucket padrão”.

Você pode usar as métricas SSE-KMS enabled bucket count (Contagem de buckets habilitados para SSE-KMS) e % SSE-KMS enabled buckets (% de buckets habilitados para SSE-KMS) para identificar buckets que usam criptografia do lado do servidor com chaves do AWS KMS (SSE-KMS) como criptografia padrão. A Lente de Armazenamento do S3 também fornece métricas para bytes não criptografados, objetos não criptografados, bytes criptografados e objetos criptografados. Para obter uma lista completa de métricas, consulte Glossário de métricas de lente de armazenamento do Amazon S3.

Você pode analisar as métricas de criptografia do SSE-KMS no contexto das métricas gerais de criptografia para identificar buckets que não usam SSE-KMS. Se você quiser usar SSE-KMS para todos os buckets em sua conta ou organização, poderá atualizar as configurações de criptografia padrão desses buckets para usar SSE-KMS. Além de SSE-KMS, você pode usar a criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3) ou chaves fornecidas pelo cliente (SSE-C). Para obter mais informações, consulte Proteger dados com criptografia.

Etapa 1: Identificar quais buckets estão usando SSE-KMS como criptografia padrão

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação esquerdo, escolha Storage Lens (Lente de Armazenamento) e Dashboards (Painéis).
3. Na lista Dashboards (Painéis), escolha o nome do painel que deseja visualizar.
4. Na seção Trends and distributions (Tendências e distribuições), escolha % SSE-KMS enabled bucket count (% de contagem de buckets habilitados para SSE-KMS) como métrica primária e % encrypted bytes (% de bytes criptografados) como métrica secundária.

   O gráfico Trend for date (Tendências para data) é atualizado para exibir tendências de SSE-KMS e bytes criptografados.
5. Para ver insights mais granulares por bucket para SSE-KMS:

   a. Escolha um ponto no gráfico. Uma caixa aparecerá com opções para obter insights mais granulares.

   b. Escolha a dimensão Buckets. Em seguida, escolha Aplicar.
6. No gráfico Distribution by buckets for date (Distribuição por buckets para data), escolha a métrica SSE-KMS enabled bucket count (Contagem de buckets habilitados para SSE-KMS).
7. Agora você pode ver quais buckets têm SSE-KMS habilitada e quais não.

Etapa 2: Atualizar as configurações de criptografia padrão do bucket

Agora que você determinou quais buckets usam SSE-KMS no contexto de % encrypted bytes (% de bytes criptografados), você pode identificar buckets que não usam SSE-KMS. Depois, opcionalmente, você pode navegar até esses buckets no console do S3 e atualizar suas configurações de criptografia padrão para usar SSE-KMS ou SSE-S3. Para obter mais informações, consulte Configurar a criptografia padrão.

Identificar buckets com o Versionamento do S3 ativado

Quando habilitado, o recurso de versionamento do S3 retém várias versões do mesmo objeto que podem ser usadas para recuperar dados rapidamente se um objeto for acidentalmente excluído ou substituído. Você pode usar a métrica Versioning-enabled bucket count (Contagem de buckets habilitados para Versionamento) para ver quais buckets usam o Versionamento do S3. Depois, você pode usar o console do S3 para ativar o Versionamento do S3 para outros buckets.

Etapa 1: Identificar buckets com o Versionamento do S3 ativado

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação, escolha Storage Lens (Lente de Armazenamento) e Dashboards (Painéis).
3. Na lista Dashboards (Painéis), escolha o nome do painel que deseja visualizar.
4. Na seção Trends and distributions (Tendências e distribuições), escolha Versioning-enabled bucket count (Contagem de buckets habilitados para Versionamento) como métrica primária e Buckets como métrica secundária.

   O gráfico Trend for date (Tendência para data) é atualizado para exibir tendências dos buckets com Versionamento do S3 ativado. Logo abaixo da linha de tendências, você pode ver as subseções Storage class distribution (Distribuição por classe de armazenamento) e Region distribution (Distribuição por região).
5. Para ver informações mais granulares de qualquer um dos buckets exibidos no gráfico Trend for date (Tendência para data) com o intuito de realizar uma análise mais profunda, faça o seguinte:

   a. Escolha um ponto no gráfico. Uma caixa aparecerá com opções para obter insights mais granulares.

   b. Escolha uma dimensão para aplicar aos dados para uma análise mais profunda: Account (Conta), Região da AWS, Storage class (Classe de armazenamento) ou Bucket. Em seguida, escolha Aplicar.
6. Na seção Bubble analysis by buckets for date (Análise de bolhas por buckets para data), escolha as métricas Versioning-enabled bucket count (Contagem de buckets habilitados para Versionamento), Buckets e Active buckets (Buckets ativos).

   A seção Bubble analysis by buckets for date (Análise de bolhas por buckets para data) é atualizada para exibir dados das métricas que você selecionou. Você pode usar esses dados

para ver quais buckets estão com o Versionamento do S3 ativado no contexto da sua contagem total de buckets. Na seção Bubble analysis by buckets for date (Análise de bolhas por buckets para data), você pode plotar seus buckets em várias dimensões usando três métricas quaisquer para representar o X-axis (Eixo X), Y-axis (Eixo Y) e Size (Tamanho) da bolha.

Etapa 2: Habilitar o Versionamento do S3

Depois de identificar os buckets com Versionamento do S3 ativado, você pode identificar os buckets que nunca tiveram o Versionamento do S3 ativado ou que estão com o versionamento suspenso. Depois, opcionalmente, você pode ativar o versionamento para esses buckets no console S3. Para obter mais informações, consulte Habilitar o versionamento em buckets.

Identificar solicitações que usam o AWS Signature Version 2 (SigV2)

Você pode usar a métrica All unsupported signature requests (Todas as solicitações de assinatura incompatíveis) para identificar solicitações que usam o AWS Signature Version 2 (SigV2). Esses dados podem ajudar você a identificar aplicações específicas que usam o SigV2. Depois, você pode migrar essas aplicações para o AWS Signature Version 4 (SigV4).

O SigV4 é o método de assinatura recomendado para todas as novas aplicações do S3. O SigV4 oferece segurança aprimorada e é compatível com todas as Regiões da AWS. Para obter mais informações, consulte Atualização do Amazon S3 – Período de defasagem do SigV2 estendido e modificado.

Pré-requisito

Para ver All unsupported signature requests (Todas as solicitações de assinatura incompatíveis) no painel da Lente de Armazenamento do S3, você deve ativar a opção Advanced metrics and recommendations (Métricas e recomendações avançadas) da Lente de Armazenamento do S3 e selecionar Advanced data protection metrics (Métricas avançadas de proteção de dados). Para obter mais informações, consulte Usar o console do S3.

Etapa 1: Examinar as tendências de assinatura do SigV2 por Conta da AWS, região e bucket

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação esquerdo, escolha Storage Lens (Lente de Armazenamento) e Dashboards (Painéis).
3. Na lista Dashboards (Painéis), escolha o nome do painel que deseja visualizar.

4. Para identificar buckets, contas e regiões específicos com solicitações que usam SigV2:

   a. Em Top N overview for date (Visão geral dos N principais para data), em Top N (N principais), insira o número de buckets para os quais deseja ver dados.

   b. Em Metric (Métrica), escolha All unsupported signature requests (Todas as solicitações de assinatura incompatíveis) na categoria Data protection (Proteção de dados).

   A seção Top N overview for date (Visão geral dos N principais para data) é atualizada para exibir dados de solicitações SigV2 por conta, Região da AWS e bucket. A seção Top N overview for date (Visão geral dos N principais para data) também mostra a variação percentual em relação ao dia ou semana anterior e uma linha em spark para visualizar a tendência. Essa tendência é de 14 dias para métricas gratuitas e 30 dias para métricas e recomendações avançadas.

   > **Note**
   >
   > Com métricas e recomendações avançadas da Lente de Armazenamento do S3, as métricas ficam disponíveis para consultas por 15 meses. Para obter mais informações, consulte Seleção de métricas.

Etapa 2: Identificar buckets que são acessados por aplicações por meio de solicitações SigV2

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação esquerdo, escolha Storage Lens (Lente de Armazenamento) e Dashboards (Painéis).
3. Na lista Dashboards (Painéis), escolha o nome do painel que deseja visualizar.
4. No painel da Lente de Armazenamento, escolha a guia Bucket.
5. Role para baixo até a seção Buckets. Em Metrics categories (Categorias de métricas), escolha Data protection (Proteção de dados). Depois, desmarque Summary (Resumo).

   A lista Buckets é atualizada para exibir todas as métricas de Data protection (Proteção de dados) disponíveis para os buckets mostrados.
6. Para filtrar a lista Buckets a fim de exibir somente métricas específicas de proteção de dados, escolha o ícone de preferências
   ( ).

7. Desmarque todas as métricas de proteção de dados, exceto:
   - All unsupported signature requests (Todas as solicitações de assinatura incompatíveis)
   - % all unsupported signature requests (% de todas as solicitações de assinatura incompatíveis)
8. (Opcional) Em Page size (Tamanho da página), escolha o número de buckets a serem exibidos na lista.
9. Escolha Confirmar.

   A lista Buckets é atualizada para exibir métricas por bucket para solicitações SigV2. Você pode usar esses dados para identificar buckets específicos que têm solicitações SigV2. Depois, você pode usar essas informações para migrar aplicações para SigV4. Para obter mais informações, consulte Autenticação de solicitações (AWS Signature Version 4)) na Referência de APIs do Amazon Simple Storage Service.

Contar o número total de regras de replicação para cada bucket

A Replicação do S3 permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3. Os buckets configurados para replicação de objetos podem pertencer à mesma conta da Conta da AWS ou a contas diferentes. Para obter mais informações, consulte Replicar objetos dentro de uma região e entre regiões.

Você pode usar as métricas de contagem de regras de replicação da Lente de Armazenamento do S3 para obter informações detalhadas por bucket sobre os buckets que estão configurados para replicação. Essas informações incluem regras de replicação dentro e entre buckets e regiões.

Pré-requisito

Para ver as métricas de contagem de regras de replicação no painel da Lente de Armazenamento do S3, você deve ativar a opção Advanced metrics and recommendations (Métricas e recomendações avançadas) da Lente de Armazenamento do S3 e selecionar Advanced data protection metrics (Métricas avançadas de proteção de dados). Para obter mais informações, consulte Usar o console do S3.

Etapa 1: Contar o número total de regras de replicação para cada bucket

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação esquerdo, escolha Storage Lens (Lente de Armazenamento) e Dashboards (Painéis).

3. Na lista Dashboards (Painéis), escolha o nome do painel que deseja visualizar.
4. No painel da Lente de Armazenamento, escolha a guia Bucket.
5. Role para baixo até a seção Buckets. Em Metrics categories (Categorias de métricas), escolha Data protection (Proteção de dados). Depois, desmarque Summary (Resumo).
6. Para filtrar a lista Buckets para exibir somente métricas de contagem de regras de replicação, escolha o ícone de preferências ().
7. Desmarque todas as métricas de proteção de dados, exceto as métricas de contagem de regras de replicação:
   - Same-Region Replication rule count (Contagem de regras de replicação na mesma região)
   - Cross-Region Replication rule count (Contagem de regras de replicação entre regiões)
   - Same-account replication rule count (Contagem de regras de replicação na mesma conta)
   - Cross-account replication rule count (Contagem de regras de replicação entre contas)
   - Total replication rule count (Contagem total de regras de replicação)
8. (Opcional) Em Page size (Tamanho da página), escolha o número de buckets a serem exibidos na lista.
9. Escolha Confirmar.

Etapa 2: Adicionar regras de replicação

Depois de ter a contagem de regras de replicação por bucket, você pode, opcionalmente, criar regras de replicação adicionais. Para obter mais informações, consulte Exemplos para configurar a replicação em tempo real.

Identificar a porcentagem de bytes do Bloqueio de Objeto

Com o Bloqueio de Objeto do S3, é possível armazenar objetos usando um modelo gravar uma vez, ler muitas (WORM). Use o Bloqueio de Objeto para ajudar a evitar que um objeto seja excluído ou substituído por um período fixo ou indefinidamente. Só é possível ativar o Bloqueio de Objeto ao criar um bucket e ao ativar o Versionamento do S3. No entanto, você pode editar o período de retenção para versões individuais de objetos ou aplicar retenções legais para buckets com o Bloqueio de Objeto ativado. Para obter mais informações, consulte Bloquear objetos com o Bloqueio de Objetos.

Você pode usar as métricas do Bloqueio de Objeto na Lente de Armazenamento do S3 para ver a métrica % Object Lock bytes (% de bytes do Bloqueio de Objeto) para sua conta ou organização.

Você pode usar essas informações para identificar buckets em sua conta ou organização que não estejam seguindo as práticas recomendadas de proteção de dados.

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação esquerdo, escolha Storage Lens (Lente de Armazenamento) e Dashboards (Painéis).
3. Na lista Dashboards (Painéis), escolha o nome do painel que deseja visualizar.
4. Na seção Snapshot, em Metrics categories (Categorias de métricas), escolha Data protection (Proteção de dados).

   A seção Snapshot é atualizada para exibir as métricas de proteção de dados, incluindo a métrica % Object Lock bytes (% de bytes do Bloqueio de Objeto). Você pode ver a porcentagem geral de bytes do Bloqueio de Objeto para sua conta ou organização.
5. Para ver a métrica % Object Lock bytes (% de bytes do Bloqueio de Objeto) por bucket, role para baixo até a seção Top N overview (Visão geral dos N principais).

   Para obter dados por objeto para o Bloqueio de Objeto, você também pode usar as métricas Object Lock object count (Contagem de objetos do Bloqueio de Objeto) e % Object Lock objects (% de objetos do Bloqueio de Objeto).
6. Em Metric (Métrica), escolha % Object Lock bytes (% de bytes do Bloqueio de Objeto) na categoria Data protection (Proteção de dados).

   Por padrão, a seção Top N overview for date (Visão geral dos N principais para data) exibe métricas para os 3 principais buckets. No campo Top N (N principais), você pode aumentar o número de buckets. A seção Top N overview for date (Visão geral dos N principais para data) também mostra a variação percentual em relação ao dia ou semana anterior e uma linha em spark para visualizar a tendência. Essa tendência é de 14 dias para métricas gratuitas e 30 dias para métricas e recomendações avançadas.

   > **Note**
   >
   > Com métricas e recomendações avançadas da Lente de Armazenamento do S3, as métricas ficam disponíveis para consultas por 15 meses. Para obter mais informações, consulte Seleção de métricas.
7. Revise os seguintes dados para % Object Lock bytes (% de bytes do Bloqueio de Objeto):

- Top number accounts (Número contas principais): veja quais contas têm o maior e o menor valor para % Object Lock bytes (% de bytes do Bloqueio de Objeto).
- Top number Regions (Número regiões principais): veja um detalhamento de % Object Lock bytes (% de bytes do Bloqueio de Objeto) por região.
- Top number buckets (Número buckets principais): veja quais buckets têm o maior e o menor valor para % Object Lock bytes (% de bytes do Bloqueio de Objeto).

Como usar a Lente de Armazenamento do S3 para auditar configurações da Propriedade de Objeto

A Propriedade de Objeto do S3 é uma configuração por bucket do S3 que você pode usar para desabilitar as listas de controle de acesso (ACLs) e controlar a propriedade dos objetos em seu bucket. Se você definir a Propriedade de Objeto como Imposto pelo proprietário do bucket, poderá desabilitar as listas de controle de acesso (ACLs) e assumir a propriedade de todos os objetos de seu bucket. Essa abordagem simplifica o gerenciamento de acesso aos dados armazenados no Amazon S3.

Por padrão, quando outra Conta da AWS carrega um objeto no bucket do S3, essa conta (que gravou o objeto) é a proprietária do objeto, tem acesso a ele e pode conceder acesso a outros usuários por meio de ACLs. Você pode usar o Object Ownership para alterar esse comportamento padrão.

A maioria dos casos de uso modernos no Amazon S3 não exige mais o uso de ACLs. Portanto, recomendamos desabilitar as ACLs, exceto em circunstâncias incomuns em que seja necessário controlar o acesso para cada objeto individualmente. Ao definir a Propriedade de Objeto como Imposto pelo proprietário do bucket, você pode desabilitar as ACLs e confiar em políticas para controle de acesso. Para obter mais informações, consulte Controlar a propriedade de objetos e desabilitar ACLs para seu bucket.

Com as métricas de gerenciamento de acesso da Lente de Armazenamento do S3, você pode identificar buckets que não estão com as ACLs desativadas. Depois de identificar esses buckets, você pode migrar as permissões de ACL para políticas e desativar as ACLs para esses buckets.

Tópicos

- Etapa 1: Identificar tendências gerais para as configurações da Propriedade de Objeto
- Etapa 2: Identificar tendências por bucket para as configurações da Propriedade de Objeto
- Etapa 3: Atualizar sua configuração da Propriedade de Objeto para Imposto pelo proprietário do bucket a fim de desativar as ACLs

Etapa 1: Identificar tendências gerais para as configurações da Propriedade de Objeto

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação esquerdo, escolha Storage Lens (Lente de Armazenamento) e Dashboards (Painéis).
3. Na lista Dashboards (Painéis), escolha o nome do painel que deseja visualizar.
4. Na seção Snapshot for date (Snapshot para data), em Metrics categories (Categorias de métricas), escolha Access management (Gerenciamento de acesso).

   A seção Snapshot for date (Snapshot para data) é atualizada para exibir a métrica % Object Ownership bucket owner enforced (% de Imposto pelo proprietário do bucket para Propriedade de Objeto). Você pode ver a porcentagem de buckets em sua conta ou organização que usam a configuração Imposto pelo proprietário do bucket na Propriedade de Objeto para desabilitar ACLs.

Etapa 2: Identificar tendências por bucket para as configurações da Propriedade de Objeto

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação esquerdo, escolha Storage Lens (Lente de Armazenamento) e Dashboards (Painéis).
3. Na lista Dashboards (Painéis), escolha o nome do painel que deseja visualizar.
4. Para ver métricas mais detalhadas por bucket, escolha a guia Bucket.
5. Na seção Distribution by buckets for date (Distribuição por buckets para data), escolha a métrica % Object Ownership bucket owner enforced (% de Imposto pelo proprietário do bucket para Propriedade de Objeto).

   O gráfico é atualizado para mostrar uma divisão por bucket para % Object Ownership bucket owner enforced (% de Imposto pelo proprietário do bucket para Propriedade de Objeto). Você pode ver quais buckets usam a configuração Imposto pelo proprietário do bucket para a Propriedade de Objeto a fim de desabilitar ACLs.
6. Para ver as configurações Imposto pelo proprietário do bucket no contexto, role para baixo até a seção Buckets. Em Metrics categories (Categorias de métricas), selecione Access management (Gerenciamento de acesso). Depois, desmarque Summary (Resumo).

A lista Buckets exibe dados para as três configurações da Propriedade de Objeto: Imposto pelo proprietário do bucket, Proprietário do bucket preferido e Autor do objeto.

7. Para filtrar a lista Buckets a fim de exibir métricas somente para uma configuração específica da Propriedade de Objeto, escolha o ícone de preferências ().
8. Desmarque as métricas que não deseja visualizar.
9. (Opcional) Em Page size (Tamanho da página), escolha o número de buckets a serem exibidos na lista.
10. Escolha Confirmar.

Etapa 3: Atualizar sua configuração da Propriedade de Objeto para Imposto pelo proprietário do bucket a fim de desativar as ACLs

Depois de identificar os buckets que usam as configurações Autor do objeto e Proprietário do bucket preferido para Propriedade de Objeto, você pode migrar suas permissões de ACL para políticas de bucket. Quando terminar de migrar suas permissões de ACL, você poderá atualizar suas configurações da Propriedade de Objeto para Imposto pelo proprietário do bucket a fim de desativar as ACLs. Para obter mais informações, consulte Pré-requisitos para desabilitar ACLs.

Usar a Lente de Armazenamento do S3 para melhorar a performance

Se a opção S3 Storage Lens advanced metrics (Métricas avançadas da Lente de Armazenamento do S3) estiver ativada, você poderá usar as métricas detalhadas de código de status para obter contagens de solicitações bem-sucedidas ou malsucedidas. Você pode usar essas informações para solucionar problemas de acesso ou performance. As métricas detalhadas de código de status mostram contagens para códigos de status HTTP, como 403 Proibido e 503 Serviço Indisponível. Você pode examinar as tendências gerais para obter métricas detalhadas de código de status em buckets do S3, contas e organizações. Depois, você pode detalhar as métricas por bucket para identificar workloads que estão acessando esses buckets e causando erros.

Por exemplo, você pode observar a métrica 403 Forbidden error count (Contagem de erros 403 Proibido) para identificar workloads que estão acessando buckets sem as permissões corretas em vigor. Depois de identificar essas workloads, você pode analisar em mais detalhes fora da Lente de Armazenamento do S3 para solucionar os erros 403 Proibido.

Este exemplo mostra como fazer uma análise de tendência para o erro 403 Proibido usando as métricas 403 Forbidden error count (Contagem de erros 403 Proibido) e % 403 Forbidden errors

(% de erros 403 Proibido). Você pode usar essas métricas para identificar workloads que estão acessando buckets sem as permissões corretas em vigor. Você pode fazer uma análise de tendência semelhante para qualquer uma das outras Detailed status code metrics (Métricas de códigos de status detalhados). Para obter mais informações, consulte Glossário de métricas de lente de armazenamento do Amazon S3.

Pré-requisito

Para ver Detailed status code metrics (Métricas de códigos de status detalhados) no painel da Lente de Armazenamento do S3, você deve ativar a opção Advanced metrics and recommendations (Métricas e recomendações avançadas) da Lente de Armazenamento do S3 e selecionar Detailed status code metrics (Métricas de códigos de status detalhados). Para obter mais informações, consulte Usar o console do S3.

Tópicos

- Etapa 1: Fazer uma análise de tendências para um código de status HTTP individual
- Etapa 2: Analisar a contagem de erros por bucket
- Etapa 3: Solucionar problemas

Etapa 1: Fazer uma análise de tendências para um código de status HTTP individual

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação esquerdo, escolha Storage Lens (Lente de Armazenamento) e Dashboards (Painéis).
3. Na lista Dashboards (Painéis), escolha o nome do painel que deseja visualizar.
4. Na seção Trends and distributions (Tendências e distribuições), em Primary metric (Métrica primária), escolha 403 Forbidden error count (Contagem de erros 403 Proibido) na categoria Detailed status codes (Códigos de status detalhados). Em Secondary metric (Métrica secundária), escolha % 403 Forbidden errors (% de erros 403 Proibido).
5. Role para baixo até a seção Top N overview for date (Visão geral dos N principais para data). Em Metrics (Métrica), escolha 403 Forbidden error count (Contagem de erros 403 Proibido) ou % 403 Forbidden errors (% de erros 403 Proibido) na categoria Detailed status codes (Códigos de status detalhados).

   A seção Top N overview for date (Visão geral dos N principais para data) para exibir as principais contagens de erros 403 Proibido por conta, Região da AWS e bucket.

Etapa 2: Analisar a contagem de erros por bucket

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação esquerdo, escolha Storage Lens (Lente de Armazenamento) e Dashboards (Painéis).
3. Na lista Dashboards (Painéis), escolha o nome do painel que deseja visualizar.
4. No painel da Lente de Armazenamento, escolha a guia Bucket.
5. Role para baixo até a seção Buckets. Em Metrics categories (Categorias de métricas), selecione as métricas Detailed status code (Códigos de status detalhados). Depois, desmarque Summary (Resumo).

   A lista Buckets é atualizada para exibir todas as métricas disponíveis para códigos de status detalhados. Você pode usar essas informações para ver quais buckets têm uma grande proporção de determinados códigos de status HTTP e quais códigos de status são comuns entre os buckets.
6. Para filtrar a lista Buckets a fim de exibir somente métricas específicas de códigos de status detalhados, escolha o ícone de preferências ().
7. Desmarque todas as métricas de códigos de status detalhados que não quiser ver na lista Buckets.
8. (Opcional) Em Page size (Tamanho da página), escolha o número de buckets a serem exibidos na lista.
9. Escolha Confirmar.

   A lista Buckets exibe métricas de contagem de erros para o número de buckets especificado. Você pode usar essas informações para identificar buckets específicos que estão apresentando muitos erros e solucionar erros por bucket.

Etapa 3: Solucionar problemas

Depois de identificar os buckets que estão com alta proporção de códigos de status HTTP específicos, você pode solucionar esses erros. Para obter mais informações, consulte:

- Por que estou recebendo o erro 403 Proibido quando tento fazer upload de arquivos no Amazon S3?

- Por que estou recebendo o erro 403 Proibido quando tento modificar uma política de bucket no Amazon S3?
- Como soluciono os erros 403 Proibido do meu bucket do Amazon S3 onde todos os recursos são da mesma Conta da AWS?
- Como soluciono um erro HTTP 500 ou 503 do Amazon S3?

Usar o Amazon S3 Storage Lens com AWS Organizations

A Lente de Armazenamento do Amazon S3 é um recurso de análise de armazenamento em nuvem que você pode usar para obter visibilidade em toda a organização sobre o uso e a atividade do armazenamento de objetos. Use as métricas da Lente de Armazenamento do S3 para gerar insights resumidos, como descobrir quanto armazenamento você tem em toda a organização ou quais são os buckets e prefixos que mais crescem. Você também pode usar a Lente de Armazenamento do Amazon S3 para coletar métricas de armazenamento e dados de uso de todas as Contas da AWS que fazem parte da hierarquia do AWS Organizations. Para fazer isso, use o AWS Organizations e habilite o acesso confiável da Lente de Armazenamento do S3 utilizando sua conta de gerenciamento do AWS Organizations.

Depois de habilitar o acesso confiável, adicione acesso de administrador delegado às contas em sua organização. As contas de administrador delegado são usadas para criar configurações e painéis da Lente de Armazenamento do S3 que coletam métricas de armazenamento e dados de usuários em toda a organização. Para obter mais informações sobre como habilitar o acesso confiável, consulte Amazon S3 Storage Lens e AWS Organizations no Guia do usuário do AWS Organizations.

Tópicos

- Ativando acesso confiável para o S3 Storage Lens
- Desativação do acesso confiável para o S3 Storage Lens
- Registro de um administrador delegado para o S3 Storage Lens
- Cancelamento do registro de um administrador delegado para o S3 Storage Lens

Ativando acesso confiável para o S3 Storage Lens

Ao habilitar o acesso confiável, você permite que a Lente de Armazenamento do Amazon S3 tenha acesso à sua hierarquia do AWS Organizations, associação e estrutura por meio das operações de API do AWS Organizations. A Lente de Armazenamento do S3 se torna um serviço confiável para toda a estrutura de sua organização.

Sempre que uma configuração de painel é criada, a Lente de Armazenamento do S3 cria funções vinculadas a serviços nas contas de gerenciamento ou administrador delegado da sua organização. O perfil vinculado ao serviço concede à Lente de Armazenamento do S3 permissão para realizar as seguintes ações:

- Descrever organizações
- Listar contas
- Verificar uma lista de acesso AWS service (Serviço da AWS) para as organizações
- Obter administradores delegados para as organizações

A Lente de Armazenamento do S3 pode garantir que tenha acesso para coletar as métricas entre contas de sua organização. Para obter mais informações, consulte Usar funções vinculadas a serviço do Amazon S3 Storage Lens.

Depois de habilitar o acesso confiável, você pode atribuir acesso de administrador delegado a contas em sua organização. Quando uma conta é marcada como administrador delegado para um serviço, a conta recebe autorização para acessar todas as operações de API da organização somente leitura. Esse acesso oferece a visibilidade de administrador delegado aos membros e estruturas de sua organização para que também possam criar painéis da Lente de Armazenamento do S3.

> **Note**
>
> - O acesso confiável só pode ser ativado pela conta de gerenciamento.
> - Somente a conta de gerenciamento e os administradores delegados podem criar painéis ou configurações do S3 Storage Lens para sua organização.

Usar o console do S3

Como permitir que a Lente de Armazenamento do S3 tenha acesso confiável do AWS Organizations

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, acesse Lente de Armazenamento.
3. Escolha Configurações do AWS Organizations. A página Acesso do AWS Organizations à Lente de Armazenamento é exibida.

4. Em Acesso confiável do AWS Organizations, escolha Editar.

   A página de Acesso do AWS Organizations é exibida.

5. Selecione Habilitar para habilitar o acesso confiável para o painel da Lente de Armazenamento do S3.
6. Escolha Salvar alterações.

Como usar o AWS CLI

Example

O exemplo a seguir mostra como habilitar o acesso confiável do AWS Organizations para a Lente de Armazenamento do S3 na AWS CLI.

```
aws organizations enable-aws-service-access --service-principal storage-
lens.s3.amazonaws.com
```

Usar o AWS SDK para Java

Example – Habilitar o acesso confiável do AWS Organizations para a Lente de Armazenamento do S3 usando o SDK para Java

O exemplo a seguir mostra como habilitar o acesso confiável para a Lente de Armazenamento do S3 no SDK para Java. Para usar esse exemplo, substitua os *user input placeholders* por suas próprias informações.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.organizations.AWSOrganizations;
import com.amazonaws.services.organizations.AWSOrganizationsClient;
import com.amazonaws.services.organizations.model.EnableAWSServiceAccessRequest;

public class EnableOrganizationsTrustedAccess {
 private static final String S3_STORAGE_LENS_SERVICE_PRINCIPAL = "storage-
lens.s3.amazonaws.com";

 public static void main(String[] args) {
  try {
```

```
            AWSOrganizations organizationsClient = AWSOrganizationsClient.builder()
                .withCredentials(new ProfileCredentialsProvider())
                .withRegion(Regions.US_EAST_1)
                .build();

            organizationsClient.enableAWSServiceAccess(new
 EnableAWSServiceAccessRequest()
                .withServicePrincipal(S3_STORAGE_LENS_SERVICE_PRINCIPAL));
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but AWS Organizations couldn't
 process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // AWS Organizations couldn't be contacted for a response, or the client
            // couldn't parse the response from AWS Organizations.
            e.printStackTrace();
        }
 }
}
```

Desativação do acesso confiável para o S3 Storage Lens

Remover uma conta como administrador delegado ou desabilitar o acesso confiável limita as métricas do painel da Lente de Armazenamento do S3 do proprietário da conta para funcionar apenas no nível de conta. Assim, cada titular da conta só pode ver os benefícios da Lente de Armazenamento do S3 com base no escopo limitado de sua conta, e não de toda a organização.

Quando você desabilita o acesso confiável na Lente de Armazenamento do S3, todos os painéis que requerem acesso confiável não são mais atualizados. Todos os painéis organizacionais criados também não são mais atualizados. Em vez disso, você só pode consultar dados históricos para o painel da Lente de Armazenamento do S3, enquanto os dados ainda estão disponíveis.

> **Note**
>
> - A desativação do acesso confiável para a Lente de Armazenamento do S3 também impede automaticamente que todos os painéis da organização coletem e agreguem métricas de armazenamento. Isso ocorre porque a Lente de Armazenamento do S3 não tem mais acesso confiável às contas da organização.

- Suas contas de gerenciamento e de administrador delegado ainda poderão ver os dados históricos de painéis desabilitados. Elas também podem consultar esses dados históricos enquanto eles ainda estão disponíveis.

Usar o console do S3

Para desativar o acesso confiável para o S3 Storage Lens

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, acesse Lente de Armazenamento.
3. Escolha Configurações do AWS Organizations. A página Acesso do AWS Organizations à Lente de Armazenamento é exibida.
4. Em Acesso confiável do AWS Organizations, escolha Editar.

   A página de Acesso do AWS Organizations é exibida.
5. Selecione Desabilitar para desabilitar o acesso confiável para o painel da Lente de Armazenamento do S3.
6. Escolha Salvar alterações.

Como usar o AWS CLI

Example

O exemplo a seguir desabilita o acesso confiável para a Lente de Armazenamento do S3 usando a AWS CLI.

```
aws organizations disable-aws-service-access --service-principal storage-
lens.s3.amazonaws.com
```

Usar o AWS SDK para Java

Example – Desabilitar o acesso confiável do AWS Organizations para a Lente de Armazenamento do S3

O exemplo a seguir mostra como desabilitar o acesso confiável do AWS Organizations para a Lente de Armazenamento do S3 no SDK para Java. Para usar esse exemplo, substitua os *user input placeholders* por suas próprias informações.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.organizations.AWSOrganizations;
import com.amazonaws.services.organizations.AWSOrganizationsClient;
import com.amazonaws.services.organizations.model.DisableAWSServiceAccessRequest;

public class DisableOrganizationsTrustedAccess {
 private static final String S3_STORAGE_LENS_SERVICE_PRINCIPAL = "storage-
lens.s3.amazonaws.com";

 public static void main(String[] args) {
  try {
            AWSOrganizations organizationsClient = AWSOrganizationsClient.builder()
                .withCredentials(new ProfileCredentialsProvider())
                .withRegion(Regions.US_EAST_1)
                .build();

            // Make sure to remove any existing delegated administrator for S3 Storage
 Lens
            // before disabling access; otherwise, the request will fail.
            organizationsClient.disableAWSServiceAccess(new
 DisableAWSServiceAccessRequest()
                .withServicePrincipal(S3_STORAGE_LENS_SERVICE_PRINCIPAL));
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but AWS Organizations couldn't
 process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // AWS Organizations couldn't be contacted for a response, or the client
            // couldn't parse the response from AWS Organizations.
            e.printStackTrace();
        }
 }
}
```

Registro de um administrador delegado para o S3 Storage Lens

Você pode criar painéis no nível da organização usando a conta de gerenciamento da sua organização ou uma conta de administrador delegado. As contas de administrador delegado

permitem que outras contas além da sua conta de gerenciamento criem painéis no nível da organização. A conta mestre de uma organização pode registrar e cancelar o registro de outras contas como administradores delegados da organização.

Depois de habilitar o acesso confiável, você pode registrar o acesso de administrador delegado às contas em sua organização usando a API REST do AWS Organizations, a AWS CLI ou SDKs da conta de gerenciamento. (Consulte mais informações em RegisterDelegatedAdministrator na Referência de API do AWS Organizations.) Quando uma conta é registrada como administrador delegado, ela recebe autorização para acessar todas as operações de API somente leitura do AWS Organizations. Isso fornece visibilidade aos membros e estruturas da sua organização para que eles possam criar painéis do S3 Storage Lens em seu nome.

> **Note**
>
> Antes de designar um administrador delegado usando a API REST do AWS Organizations, a AWS CLI ou SDKs, você deve chamar a operação EnableAWSOrganizationsAccess.

Usar o console do S3

Para registrar administradores delegados para o S3 Storage Lens

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, acesse Lente de Armazenamento.
3. Escolha Configurações do AWS Organizations.
4. Em Administradores delegados, escolha Registrar conta.
5. Adicione um ID de Conta da AWS para registrar a conta como administrador delegado. O administrador delegado pode criar painéis no nível da organização para todas as contas e armazenamentos em sua organização.
6. Escolha Registrar conta.

Como usar o AWS CLI

Example

O exemplo a seguir mostra como registrar os administradores delegados do Organizations para a Lente de Armazenamento do S3 usando a AWS CLI. Para usar esse exemplo, substitua os *user input placeholders* por suas próprias informações.

```
aws organizations register-delegated-administrator --service-principal storage-
lens.s3.amazonaws.com --account-id 111122223333
```

Usar o AWS SDK para Java

Example – Registrar administradores delegados do Organizations para a Lente de Armazenamento do S3

O exemplo a seguir mostra como registrar os administradores delegados do AWS Organizations para a Lente de Armazenamento do S3 no SDK para Java. Para usar esse exemplo, substitua os *user input placeholders* por suas próprias informações.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.organizations.AWSOrganizations;
import com.amazonaws.services.organizations.AWSOrganizationsClient;
import
 com.amazonaws.services.organizations.model.RegisterDelegatedAdministratorRequest;

public class RegisterOrganizationsDelegatedAdministrator {
 private static final String S3_STORAGE_LENS_SERVICE_PRINCIPAL = "storage-
lens.s3.amazonaws.com";

 public static void main(String[] args) {
  try {
            String delegatedAdminAccountId = "111122223333"; // Account Id for the
 delegated administrator.
            AWSOrganizations organizationsClient = AWSOrganizationsClient.builder()
                .withCredentials(new ProfileCredentialsProvider())
                .withRegion(Regions.US_EAST_1)
                .build();
```

```
            organizationsClient.registerDelegatedAdministrator(new
 RegisterDelegatedAdministratorRequest()
                .withAccountId(delegatedAdminAccountId)
                .withServicePrincipal(S3_STORAGE_LENS_SERVICE_PRINCIPAL));
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but AWS Organizations couldn't
 process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // AWS Organizations couldn't be contacted for a response, or the client
            // couldn't parse the response from AWS Organizations.
            e.printStackTrace();
        }
 }
}
```

Cancelamento do registro de um administrador delegado para o S3 Storage Lens

Depois de habilitar o acesso confiável, você também pode cancelar o registro do acesso de administrador delegado às contas em sua organização. As contas de administrador delegado permitem que outras contas além da sua conta de gerenciamento criem painéis no nível da organização. Somente a conta de gerenciamento de uma organização pode cancelar o registro de contas como administradores delegados para a organização.

É possível cancelar o registro de um administrador delegado usando o AWS Management Console do AWS Organizations, a API REST, a AWS CLI ou SDKs da AWS da conta de gerenciamento. Para obter mais informações, consulte DeregisterDelegatedAdministrator na Referência de APIs do AWS Organizations.

Quando uma conta tem o registro do administrador delegado cancelado, ela perde o acesso a:

- Todas as operações de API somente leitura do AWS Organizations que fornecem visibilidade aos membros e estruturas da organização.
- Todos os painéis no nível da organização criados pelo administrador delegado. O cancelamento do registro de um administrador delegado também impede automaticamente que todos os painéis da organização criados por esse administrador delegado agreguem novas métricas de armazenamento.

> **Note**
>
> O administrador delegado que tiver o registro cancelado ainda poderá ver os dados históricos dos painéis desabilitados que foram criados se os dados ainda estiverem disponíveis para consulta.

Usar o console do S3

Como cancelar o registro de administradores delegados para a Lente de Armazenamento do S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, acesse Lente de Armazenamento.
3. Escolha Configurações do AWS Organizations.
4. Em Administradores delegados, selecione a conta da qual deseja cancelar o registro.
5. Escolha Cancelar o registro da conta. A conta com o registro cancelado não é mais um administrador delegado e agora não pode criar painéis no nível da organização para todas as contas e armazenamentos na organização.
6. Escolha Registrar conta.

Como usar o AWS CLI

Example

O exemplo a seguir mostra como cancelar o registro dos administradores delegados do Organizations para a Lente de Armazenamento do S3 usando a AWS CLI. Para usar esse exemplo, substitua *111122223333* pelo ID de sua Conta da AWS.

```
aws organizations deregister-delegated-administrator --service-principal storage-lens.s3.amazonaws.com --account-id 111122223333
```

Usar o AWS SDK para Java

Example – Cancelar o registro de administradores delegados do Organizations para a Lente de Armazenamento do S3

O exemplo a seguir mostra como cancelar o registro dos administradores delegados do Organizations para a Lente de Armazenamento do S3 usando o SDK para Java. Para usar esse exemplo, substitua os *`user input placeholders`* por suas próprias informações.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.organizations.AWSOrganizations;
import com.amazonaws.services.organizations.AWSOrganizationsClient;
import
 com.amazonaws.services.organizations.model.DeregisterDelegatedAdministratorRequest;

public class DeregisterOrganizationsDelegatedAdministrator {
 private static final String S3_STORAGE_LENS_SERVICE_PRINCIPAL = "storage-
lens.s3.amazonaws.com";

 public static void main(String[] args) {
  try {
            String delegatedAdminAccountId = "111122223333"; // Account Id for the
 delegated administrator.
            AWSOrganizations organizationsClient = AWSOrganizationsClient.builder()
                .withCredentials(new ProfileCredentialsProvider())
                .withRegion(Regions.US_EAST_1)
                .build();

            organizationsClient.deregisterDelegatedAdministrator(new
 DeregisterDelegatedAdministratorRequest()
                .withAccountId(delegatedAdminAccountId)
                .withServicePrincipal(S3_STORAGE_LENS_SERVICE_PRINCIPAL));
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but AWS Organizations couldn't
 process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // AWS Organizations couldn't be contacted for a response, or the client
            // couldn't parse the response from AWS Organizations.
```

```
            e.printStackTrace();
        }
    }
}
```

Trabalhar com grupos da Lente de Armazenamento do S3 para filtrar e agregar métricas

Um grupo da Lente de Armazenamento do Amazon S3 agrega métricas usando filtros personalizados com base nos metadados do objeto. Os grupos da Lente de Armazenamento ajudam a detalhar as características dos dados, como distribuição de objetos por idade, tipos de arquivo mais comuns e muito mais. Por exemplo, você pode filtrar métricas por tag de objeto para identificar conjuntos de dados de crescimento mais rápido ou visualizar armazenamento com base no tamanho e na idade do objeto para informar a estratégia de arquivamento de armazenamento. Como resultado, os grupos da Lente de Armazenamento do Amazon S3 ajudam a entender e otimizar o armazenamento do S3.

Ao usar grupos da Lente de Armazenamento, você pode analisar e filtrar as métricas da Lente de Armazenamento do S3 usando metadados de objetos, como prefixos, sufixos, tags de objetos, tamanho do objeto ou idade do objeto. Também é possível aplicar uma combinação desses filtros. Depois de anexar o grupo da Lente de Armazenamento ao painel da Lente de Armazenamento do S3, você pode visualizar as métricas da Lente de Armazenamento do S3 agregadas pelos grupos da Lente de Armazenamento do Amazon S3 diretamente no seu painel.

Você também pode filtrar métricas por tamanho de objeto ou faixa etária para determinar qual parte do armazenamento consiste em objetos pequenos. Você pode usar essas informações com o S3 Intelligent-Tiering ou o S3 Lifecycle para fazer a transição de objetos pequenos para diferentes classes de armazenamento a fim de otimizar custos e armazenamento.

Tópicos

- Como funcionam os grupos de Lente de Armazenamento do S3
- Uso de grupos da Lente de Armazenamento

Como funcionam os grupos de Lente de Armazenamento do S3

Você pode usar grupos da Lente de Armazenamento para agregar métricas usando filtros personalizados com base em metadados de objetos. Ao definir um filtro personalizado, você pode usar prefixos, sufixos, tags de objeto, tamanhos de objeto, idade do objeto ou uma combinação

desses filtros personalizados. Durante a criação do grupo da Lente de Armazenamento, você também pode incluir um único filtro ou várias condições de filtro. Para especificar várias condições de filtro, você usa os operadores lógicos `And` ou `Or`.

Ao criar e configurar um grupo da Lente de Armazenamento, o próprio grupo da Lente de Armazenamento atua como um filtro personalizado no painel ao qual você anexa o grupo. No painel, você pode usar o filtro de grupo da Lente de Armazenamento para obter métricas de armazenamento com base no filtro personalizado definido no grupo.

Para visualizar os dados do grupo da Lente de Armazenamento no painel da Lente de Armazenamento do S3, você deve anexar o grupo ao painel depois de criá-lo. Depois que o grupo da Lente de Armazenamento for anexado ao painel da Lente de Armazenamento, o painel coletará métricas de uso de armazenamento em 48 horas. Visualize dados no painel da Lente de Armazenamento ou exporte por meio de uma exportação de métricas. Caso você se esqueça de anexar um grupo da Lente de Armazenamento a um painel, os dados do grupo da Lente de Armazenamento não serão capturados nem exibidos em nenhum lugar.

> **Note**
>
> - Ao criar um grupo da Lente de Armazenamento do S3, você está criando um recurso AWS. Portanto, cada grupo da Lente de Armazenamento tem o próprio nome do recurso da Amazon (ARN), que você pode especificar ao anexá-lo ou excluí-lo de um painel da Lente de Armazenamento do S3.
> - Se o seu grupo da Lente de Armazenamento não estiver anexado a um painel, você não incorrerá em nenhuma cobrança adicional pela criação de um grupo da Lente de Armazenamento.
> - A Lente de Armazenamento do S3 agrega métricas de uso de um objeto em todos os grupos da Lente de Armazenamento correspondentes. Portanto, se um objeto corresponder às condições de filtro de dois ou mais grupos da Lente de Armazenamento, você verá contagens repetidas do mesmo objeto em todo o uso do armazenamento.

Você pode criar um grupo da Lente de Armazenamento no nível da conta em uma região inicial especificada (na lista de suportes Regiões da AWS). Em seguida, você pode anexar seu grupo da Lente de Armazenamento a vários painéis da Lente de Armazenamento, desde que os painéis estejam no mesmo Conta da AWS e região inicial. Você pode criar até 50 grupos da Lente de Armazenamento por região inicial em cada Conta da AWS.

Você pode criar e gerenciar grupos de Lente de Armazenamento do S3 usando o console do Amazon S3, AWS Command Line Interface (AWS CLI), AWS SDKs ou a API REST do Amazon S3.

Tópicos

- Ver métricas agregadas do grupo da Lente de Armazenamento
- Permissões de grupos de Lente de Armazenamento
- Configuração de grupos da Lente de Armazenamento
- Tags de recursos AWS
- Exportação de métricas de grupos da Lente de Armazenamento

Ver métricas agregadas do grupo da Lente de Armazenamento

Você pode ver as métricas agregadas dos seus grupos da Lente de Armazenamento ao anexar os grupos a um painel. Os grupos da Lente de Armazenamento que deseja anexar devem estar na região inicial designada na conta do painel.

Para anexar um grupo da Lente de Armazenamento a um painel, você deve especificar o grupo na Seção de agregação do grupo da Lente de Armazenamento da configuração do seu painel. Se você tiver vários grupos da Lente de Armazenamento, poderá filtrar os resultados da agregação do grupo da Lente de Armazenamento para incluir ou excluir apenas os grupos desejados. Para obter mais informações sobre como anexar grupos aos seus painéis, consulte the section called “Anexe ou remova um grupo da Lente de Armazenamento”.

Depois de anexar seus grupos, você verá os dados adicionais de agregação de grupos da Lente de Armazenamento em seu painel dentro de 48 horas.

> **Note**
>
> Para ver métricas agregadas para seu grupo da Lente de Armazenamento, você deve anexar o grupo a um painel da Lente de Armazenamento do S3.

Permissões de grupos de Lente de Armazenamento

Os grupos de Lente de Armazenamento exigem determinadas permissões no AWS Identity and Access Management (IAM) para autorizar o acesso às ações do grupo de Lente de Armazenamento do S3. Para conceder essas permissões, você pode usar uma política do IAM baseada em

identidade. Você pode vincular essa política a usuários, grupos ou funções do IAM para conceder permissões. Essas permissões podem incluir a capacidade de criar ou excluir grupos da Lente de Armazenamento, visualizar suas configurações ou gerenciar suas tags.

O usuário ou função do IAM ao qual você concede permissões deve pertencer à conta que criou ou é proprietária do grupo da Lente de Armazenamento.

Para usar grupos da Lente de Armazenamento e ver as métricas dos grupos da Lente de Armazenamento, primeiro você deve ter as permissões apropriadas para usar a Lente de Armazenamento do S3. Para obter mais informações, consulte the section called “Configuração de permissões”.

Para criar e gerenciar grupos da Lente de Armazenamento do S3, você deve ter as seguintes permissões do IAM, dependendo das ações que deseja executar:

Ação	Permissões do IAM
Criar grupo da Lente de Armazenamento	`s3:CreateStorageLensGroup`
Criar grupo da Lente de Armazenamento com tags	`s3:CreateStorageLensGroup` , `s3:TagResource`
Atualizar um grupo da Lente de Armazenamento existente	`s3:UpdateStorageLensGroup`
Gerar os detalhes de uma configuração de grupo da Lente de Armazenamento	`s3:GetStorageLensGroup`
Listar todos os grupos da Lente de Armazenamento na região de origem	`s3:ListStorageLensGroups`
Excluir um grupo da Lente de Armazenamento	`s3:DeleteStorageLensGroup`
Listar as tags que foram adicionadas ao seu grupo da Lente de Armazenamento	`s3:ListTagsForResource`
Adicionar ou atualizar uma tag de grupo da Lente de Armazenamento para um grupo da Lente de Armazenamento existente	`s3:TagResource`

Ação	Permissões do IAM
Excluir uma tag de um grupo da Lente de Armazenamento	`s3:UntagResource`

Veja um exemplo de como configurar a política do IAM na conta que cria o grupo da Lente de Armazenamento. Para usar essa política, substitua *`us-east-1`* pela região inicial em que seu grupo e Lente de Armazenamento está localizado. Substitua *`111122223333`* pelo seu Conta da AWS ID e substitua *`example-storage-lens-group`* pelo nome do seu grupo da Lente de Armazenamento. Para aplicar essas permissões a todos os grupos da Lente de Armazenamento, substitua *`example-storage-lens-group`* por *`*`*.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EXAMPLE-Statement-ID",
            "Effect": "Allow",
            "Action": [
                "s3:CreateStorageLensGroup",
                "s3:UpdateStorageLensGroup",
                "s3:GetStorageLensGroup",
                "s3:ListStorageLensGroups",
                "s3:DeleteStorageLensGroup,
                "s3:TagResource",
                "s3:UntagResource",
                "s3:ListTagsForResource"
                ],
            "Resource": "arn:aws:s3:us-east-1:111122223333:storage-lens-group/example-storage-lens-group"
        }
    ]
}
```

Para obter mais informações sobre as permissões de Lente de Armazenamento do S3, consulte Configurar permissões da Lente de Armazenamento do Amazon S3. Para obter mais informações sobre a linguagem da política do IAM, consulte Políticas e permissões no Amazon S3.

Configuração de grupos da Lente de Armazenamento

Nome do grupo da Lente de Armazenamento do S3

Recomendamos dar nomes aos grupos da Lente de Armazenamento que indiquem a finalidade para determinar quais grupos anexar aos seus painéis. Para anexar um grupo da Lente de Armazenamento a um painel, você deve especificar o grupo na Seção de agregação do grupo da Lente de Armazenamento da configuração do painel.

Os nomes dos grupos de Lente de Armazenamento devem ser exclusivos na conta. Eles não devem exceder 64 caracteres e podem conter apenas letras (a–z, A–Z), números (0–9), hifens (-) e sublinhados (_).

Região inicial

A região inicial é a Região da AWS em que o grupo da Lente de Armazenamento é criado e mantido. O grupo da Lente de Armazenamento é criado na mesma região inicial do painel da Lente de Armazenamento do Amazon S3. A configuração e as métricas do grupo da Lente de Armazenamento também são armazenadas nessa região. Você pode criar até 50 grupos da Lente de Armazenamento em uma região local.

Depois de criar seu grupo da Lente de Armazenamento, você não poderá editar a região inicial.

Escopo

Para incluir objetos no grupo da Lente de Armazenamento, eles devem estar no escopo do painel da Lente de Armazenamento do Amazon S3. O escopo do painel da Lente de Armazenamento é determinado pelos buckets incluídos no Escopo do painel da configuração do painel da Lente de Armazenamento do S3.

Você pode usar filtros diferentes para seus objetos a fim de definir o escopo do seu grupo da Lente de Armazenamento. Para ver essas métricas de grupo da Lente de Armazenamento no painel da Lente de Armazenamento do S3, os objetos devem corresponder aos filtros incluídos nos grupos da Lente de Armazenamento. Por exemplo, suponha que seu grupo da Lente de Armazenamento inclua objetos com o prefixo `marketing` e o sufixo `.png`, mas nenhum objeto corresponda a esses critérios. Nesse caso, as métricas desse grupo da Lente de Armazenamento não serão geradas na exportação diária de métricas e nenhuma métrica desse grupo ficará visível no seu painel.

Filtros

Você pode usar os seguintes filtros em um grupo da Lente de Armazenamento do S3:

- Prefixos: especifica o prefixo dos objetos incluídos, que é uma sequência de caracteres no início do nome da chave do objeto. Por exemplo, um valor de `images` para o filtro Prefixos inclui objetos com qualquer um dos seguintes prefixos: `images/`, `images-marketing` e `images/production`. O comprimento máximo de um prefixo é 1.024 bytes.
- Sufixos: especifica o sufixo dos objetos incluídos (por exemplo, `.png`, `.jpeg` ou `.csv`). O comprimento máximo de um sufixo é 1.024 bytes.
- Tags de objeto: especifica a lista de tags de objeto que você deseja filtrar. Uma chave de tag não pode exceder 128 caracteres Unicode, e um valor de tag não pode exceder 256 caracteres Unicode. Se o campo de valor da etiqueta do objeto ficar vazio, os grupos da Lente de Armazenamento do S3 só associarão o objeto a outros objetos que também tenham valores de etiqueta vazios.
- Idade: especifica o intervalo de idade do objeto incluído em dias. Somente números inteiros são compatíveis.
- Tamanho: especifica o intervalo de tamanho dos objetos incluídos em bytes. Somente números inteiros são compatíveis. O valor máximo permitido é 5 TB.

Tags de objeto do grupo da Lente de Armazenamento

Você pode criar um grupo da Lente de Armazenamento que inclua até 10 filtros de tags de objetos. O exemplo a seguir inclui dois pares de valores-chave de tags de objeto como filtros para um grupo da Lente de Armazenamento denominado *`Marketing-Department`*. Para usar esse exemplo, substitua *`Marketing-Department`* pelo nome do seu grupo e substitua *`object-tag-key-1`*, *`object-tag-value-1`* e assim por diante pelos pares de valores-chave da tag de objeto que você deseja filtrar.

```
{
    "Name": "Marketing-Department",
    "Filter": {
     "MatchAnyTag":[
                {
                    "Key": "object-tag-key-1",
                    "Value": "object-tag-value-1"
                },
                {
                    "Key": "object-tag-key-2",
                    "Value": "object-tag-value-2"
                }
            ]
```

```
    }
}
```

Operadores lógicos (**`And`** ou **`Or`**)

Para incluir diversas condições de filtro em seu grupo da Lente de Armazenamento, use operadores lógicos (tanto `And` quanto `Or`). No exemplo a seguir, o grupo e Lente de Armazenamento *`Marketing-Department`* contém um operador `And` com os filtros `Prefix`, `ObjectAge` e `ObjectSize`. Como um operador `And` é usado, somente objetos que correspondam a todas as condições de filtro serão incluídos no escopo do grupo da Lente de Armazenamento.

Para usar esse exemplo, substitua *`user input placeholders`* pelos valores que você deseja filtrar.

```
{
    "Name": "Marketing-Department",
    "Filter": {
        "And": {
            "MatchAnyPrefix": [
                "prefix-1",
                "prefix-2",
                "prefix-3/sub-prefix-1"
            ],
             "MatchObjectAge": {
                "DaysGreaterThan": 10,
                "DaysLessThan": 60
            },
            "MatchObjectSize": {
                "BytesGreaterThan": 10,
                "BytesLessThan": 60
            }
        }
    }
}
```

> **Note**
>
> Se desejar incluir objetos que correspondam a qualquer uma das condições nos filtros, substitua o operador lógico `And` pelo operador lógico `Or` deste exemplo.

Tags de recursos AWS

Cada grupo da Lente de Armazenamento do S3 é contado como um recurso AWS com seu próprio nome do recurso da Amazon (ARN). Portanto, ao configurar o grupo da Lente de Armazenamento, você tem a opção de adicionar tags de recursos AWS ao grupo. Você pode adicionar até 50 tags para cada grupo da Lente de Armazenamento. Para criar um grupo da Lente de Armazenamento com tags, você deve ter as permissões `s3:CreateStorageLensGroup` e `s3:TagResource`.

Use tags de recursos AWS para categorizar os recursos de acordo com o departamento, a linha de negócios ou o projeto. Fazer isso é útil quando você tem muitos recursos do mesmo tipo. Ao aplicar tags, é possível identificar rapidamente um grupo específico da Lente de Armazenamento com base nas tags atribuídas a ele. Você também pode usar tags para rastrear e alocar custos.

Além disso, ao adicionar uma tag de recursos AWS ao grupo da Lente de Armazenamento, você ativa o controle de acesso por atributo (ABAC). ABAC é uma estratégia de autorização que define permissões com base em atributos, neste caso, tags. É possível usar condições que especificam tags de recursos nas políticas do IAM para controlar o acesso aos recursos AWS.

É possível editar chaves de tags e valores e é possível remover as tags de um recurso a qualquer momento. Além disso, esteja ciente das seguintes limitações:

- As chaves e os valores das tags diferenciam maiúsculas de minúsculas.
- Ao adicionar uma tag que tenha a mesma chave de uma tag existente nesse recurso, o novo valor substituirá o antigo.
- Se você excluir um recurso, todas as tags do recurso também serão excluídas.
- Não inclua dados privados ou confidenciais nas tags de recursos AWS.
- As tags do sistema (ou tags com chaves de tag que começam com `aws:`) não são compatíveis.
- O comprimento de cada chave de tag não pode exceder 128 caracteres. O comprimento de cada valor de tag não pode exceder 256 caracteres.

Exportação de métricas de grupos da Lente de Armazenamento

As métricas do grupo da Lente de Armazenamento do S3 estão incluídas na exportação de métricas de lente de armazenamento do Amazon S3 para o painel ao qual o grupo da Lente de Armazenamento está anexado. Para obter informações gerais sobre o recurso de exportação de métricas da Lente de Armazenamento, consulte Exibição de métricas de lente de armazenamento do Amazon S3 usando uma exportação de dados.

A exportação de métricas para grupos da Lente de Armazenamento inclui quaisquer métricas da Lente de Armazenamento do S3 que estejam no escopo do painel ao qual você anexou o grupo da Lente de Armazenamento. A exportação também inclui dados de métricas adicionais para grupos da Lente de Armazenamento.

Depois de criar seu grupo da Lente de Armazenamento, sua exportação de métricas será enviada diariamente para o bucket selecionado ao configurar a exportação de métricas para o painel ao qual seu grupo está anexado. Pode levar até 48 horas para você receber a primeira exportação de métricas.

Para gerar métricas na exportação diária, os objetos devem corresponder aos filtros incluídos nos grupos da Lente de Armazenamento. Se nenhum objeto corresponder aos filtros incluídos no grupo da Lente de Armazenamento, nenhuma métrica será gerada. No entanto, se um objeto corresponder a dois ou mais grupos da Lente de Armazenamento, o objeto será listado separadamente para cada grupo quando aparecer na exportação de métricas.

Você pode identificar métricas para grupos da Lente de Armazenamento procurando um dos seguintes valores na coluna `record_type` de exportação de métricas do seu painel:

- `STORAGE_LENS_GROUP_BUCKET`
- `STORAGE_LENS_GROUP_ACCOUNT`

A coluna `record_value` mostra o ARN do recurso para o grupo da Lente de Armazenamento (por exemplo, `arn:aws:s3:`*`us-east-1`*`:`*`111122223333`*`:storage-lens-group/`*`Marketing-Department`*).

Uso de grupos da Lente de Armazenamento

A Lente de Armazenamento do Amazon S3 agrega métricas usando filtros personalizados com base nos metadados do objeto. Você pode analisar e filtrar as métricas da Lente de Armazenamento do S3 usando prefixos, sufixos, tags de objetos, tamanho do objeto ou idade do objeto. Com grupos da Lente de Armazenamento do Amazon S3, você também pode categorizar seu uso dentro de buckets e por meio deles no Amazon S3. Consequentemente, você poderá entender e otimizar melhor o armazenamento S3.

Para começar a visualizar os dados de um grupo da Lente de Armazenamento, você deve primeiro anexar o grupo da Lente de Armazenamento a um painel da Lente de Armazenamento do S3. Se precisar gerenciar grupos da Lente de Armazenamento no painel, edite a configuração do painel. Para verificar quais grupos da Lente de Armazenamento estão na sua conta, você pode listá-los.

Para verificar quais grupos da Lente de Armazenamento estão anexados ao seu painel, verifique a guia Grupos da Lente de Armazenamento no painel. Para revisar ou atualizar o escopo de um grupo da Lente de Armazenamento existente, visualize os detalhes. Você também pode excluir permanentemente um grupo da Lente de Armazenamento.

Para gerenciar permissões, você pode criar e adicionar tags de recursos AWS definidas pelo usuário aos seus grupos da Lente de Armazenamento. Use tags de recursos AWS para categorizar os recursos de acordo com o departamento, a linha de negócios ou o projeto. Fazer isso é útil quando você tem muitos recursos do mesmo tipo. Ao aplicar tags, é possível identificar rapidamente um grupo específico da Lente de Armazenamento com base nas tags atribuídas a ele.

Além disso, ao adicionar uma tag de recursos AWS ao grupo da Lente de Armazenamento, você ativa o controle de acesso por atributo (ABAC). ABAC é uma estratégia de autorização que define permissões com base em atributos, neste caso, tags. É possível usar condições que especificam tags de recursos nas políticas do IAM para controlar o acesso aos recursos AWS.

Tópicos

- Criação de grupo da Lente de Armazenamento
- Anexar ao painel ou remover do painel grupos da Lente de Armazenamento do S3
- Visualização de dados dos grupos da Lente de Armazenamento
- Atualização do grupo da Lente de Armazenamento
- Gerenciamento de tags de recursos AWS com grupos da Lente de Armazenamento
- Listagem de todos os grupos da Lente de Armazenamento
- Visualização de detalhes do grupo da Lente de Armazenamento
- Exclusão de grupo da Lente de Armazenamento

Criação de grupo da Lente de Armazenamento

Os exemplos a seguir demonstram como criar um grupo da Lente de Armazenamento do Amazon S3 usando o console do Amazon S3AWS Command Line Interface, (AWS CLI) e AWS SDK para Java.

Usar o console do S3

Para criar um grupo da Lente de Armazenamento

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.

2. Na barra de navegação na parte superior da página, escolha o nome da região da AWS exibida no momento. Em seguida, escolha a região para a qual você deseja mudar.
3. No painel de navegação à esquerda, selecione Grupos de Lente de Armazenamento.
4. Selecione Criar grupo da Lente de Armazenamento.
5. Em Geral, visualize sua Região de origem e insira o Nome do grupo do Storage Lens.
6. Em Escopo, selecione o filtro para aplicar ao seu grupo da Lente de Armazenamento. Para aplicar vários filtros, selecione os filtros e, em seguida, escolha o operador lógico AND ou OR.

   - Para o filtro Prefixos, selecione Prefixos e insira uma sequência de prefixo. Para adicionar vários prefixos, selecione Adicionar prefixo. Para remover um prefixo, selecione Remover ao lado do prefixo para remover.
   - Para o filtro Tags de objeto, selecione Tags de objeto e insira o par de valores-chave para seu objeto. Selecione Adicionar tag. Para remover uma tag, selecione Remover ao lado da tag para remover.
   - Para o filtro Sufixos, selecione Sufixos e insira uma sequência de sufixo. Para adicionar vários sufixos, selecione Adicionar sufixo. Para remover um sufixo, selecione Remover ao lado do sufixo para remover.
   - Para o filtro Idade, especifique a faixa etária do objeto em dias. Selecione Especificar idade mínima do objeto e insira a idade mínima do objeto. Em seguida, selecione Especificar idade máxima do objeto e insira a idade máxima do objeto.
   - Para o filtro Tamanho, especifique a faixa de tamanho do objeto e a unidade de medida. Selecione Especificar tamanho mínimo do objeto e insira o tamanho mínimo do objeto. Selecione Especificar tamanho máximo do objeto e insira o tamanho máximo do objeto.
7. (Opcional) Para tags de recursos AWS, adicione o par de valores-chave e selecione Adicionar tag.
8. Selecione Criar grupo da Lente de Armazenamento.

Como usar o AWS CLI

O comando de exemplo AWS CLI a seguir cria um grupo de Lente de Armazenamento. Para usar esse exemplo de comando, substitua os *user input placeholders* por suas próprias informações.

```
aws s3control create-storage-lens-group --account-id 111122223333 \
--region us-east-1 --storage-lens-group=file://./marketing-department.json
```

O comando de exemplo AWS CLI a seguir cria um grupo da Lente de Armazenamento com duas tags de recursos AWS. Para usar esse exemplo de comando, substitua os *user input placeholders* por suas próprias informações.

```
aws s3control create-storage-lens-group --account-id 111122223333 \
--region us-east-1 --storage-lens-group=file://./marketing-department.json \
--tags Key=k1,Value=v1 Key=k2,Value=v2
```

Para obter configurações de exemplo JSON, consulte Configuração de grupos da Lente de Armazenamento.

Usar o AWS SDK para Java

O exemplo AWS SDK para Java a seguir cria um grupo da Lente de Armazenamento Para usar esse exemplo, substitua os *user input placeholders* por suas próprias informações.

Example — Crie um grupo da Lente de Armazenamento com um único filtro

O exemplo a seguir cria um grupo de Lente de Armazenamento chamado *Marketing-Department*. Esse grupo tem um filtro de idade do objeto que especifica a faixa etária em *30* para *90* dias. Para usar esse exemplo, substitua os *user input placeholders* por suas próprias informações.

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.CreateStorageLensGroupRequest;
import software.amazon.awssdk.services.s3control.model.MatchObjectAge;
import software.amazon.awssdk.services.s3control.model.StorageLensGroup;
import software.amazon.awssdk.services.s3control.model.StorageLensGroupFilter;

public class CreateStorageLensGroupWithObjectAge {
    public static void main(String[] args) {
        String storageLensGroupName = "Marketing-Department";
        String accountId = "111122223333";

        try {
            StorageLensGroupFilter objectAgeFilter = StorageLensGroupFilter.builder()
```

```
                    .matchObjectAge(MatchObjectAge.builder()
                            .daysGreaterThan(30)
                            .daysLessThan(90)
                            .build())
                    .build();

            StorageLensGroup storageLensGroup = StorageLensGroup.builder()
                    .name(storageLensGroupName)
                    .filter(objectAgeFilter)
                    .build();

            CreateStorageLensGroupRequest createStorageLensGroupRequest =
 CreateStorageLensGroupRequest.builder()
                    .storageLensGroup(storageLensGroup)
                    .accountId(accountId).build();

            S3ControlClient s3ControlClient = S3ControlClient.builder()
                    .region(Region.US_WEST_2)
                    .credentialsProvider(ProfileCredentialsProvider.create())
                    .build();
            s3ControlClient.createStorageLensGroup(createStorageLensGroupRequest);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Example — Crie um grupo da Lente de Armazenamento com um operador **AND** que inclua vários filtros

O exemplo a seguir cria um grupo de Lente de Armazenamento chamado *Marketing-Department*. Este grupo utiliza o operador AND para indicar que os objetos devem corresponder a todas as condições de filtro. Para usar esse exemplo, substitua os *user input placeholders* por suas próprias informações.

```
package aws.example.s3control;
```

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.CreateStorageLensGroupRequest;
import software.amazon.awssdk.services.s3control.model.MatchObjectAge;
import software.amazon.awssdk.services.s3control.model.MatchObjectSize;
import software.amazon.awssdk.services.s3control.model.S3Tag;
import software.amazon.awssdk.services.s3control.model.StorageLensGroup;
import software.amazon.awssdk.services.s3control.model.StorageLensGroupAndOperator;
import software.amazon.awssdk.services.s3control.model.StorageLensGroupFilter;


public class CreateStorageLensGroupWithAndFilter {
    public static void main(String[] args) {
        String storageLensGroupName = "Marketing-Department";
        String accountId = "111122223333";

        try {
            // Create object tags.
            S3Tag tag1 = S3Tag.builder()
                    .key("object-tag-key-1")
                    .value("object-tag-value-1")
                    .build();
            S3Tag tag2 = S3Tag.builder()
                    .key("object-tag-key-2")
                    .value("object-tag-value-2")
                    .build();

            StorageLensGroupAndOperator andOperator =
 StorageLensGroupAndOperator.builder()
                    .matchAnyPrefix("prefix-1", "prefix-2", "prefix-3/sub-prefix-1")
                    .matchAnySuffix(".png", ".gif", ".jpg")
                    .matchAnyTag(tag1, tag2)
                    .matchObjectAge(MatchObjectAge.builder()
                            .daysGreaterThan(30)
                            .daysLessThan(90).build())
                    .matchObjectSize(MatchObjectSize.builder()
                            .bytesGreaterThan(1000L)
                            .bytesLessThan(6000L).build())
                    .build();

            StorageLensGroupFilter andFilter = StorageLensGroupFilter.builder()
```

```
                    .and(andOperator)
                    .build();

            StorageLensGroup storageLensGroup = StorageLensGroup.builder()
                    .name(storageLensGroupName)
                    .filter(andFilter)
                    .build();

            CreateStorageLensGroupRequest createStorageLensGroupRequest =
 CreateStorageLensGroupRequest.builder()
                    .storageLensGroup(storageLensGroup)
                    .accountId(accountId).build();

            S3ControlClient s3ControlClient = S3ControlClient.builder()
                    .region(Region.US_WEST_2)
                    .credentialsProvider(ProfileCredentialsProvider.create())
                    .build();
            s3ControlClient.createStorageLensGroup(createStorageLensGroupRequest);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Example — Crie um grupo da Lente de Armazenamento com um operador **OR** que inclua vários filtros

O exemplo a seguir cria um grupo de Lente de Armazenamento chamado *Marketing-Department*. Este grupo usa um operador OR para aplicar um filtro de prefixo (*prefix-1*, *prefix-2*, *prefix3/sub-prefix-1*) ou um filtro de tamanho de objeto com intervalo de tamanho entre *1000* bytes e *6000* bytes. Para usar esse exemplo, substitua os *user input placeholders* por suas próprias informações.

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;
```

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.CreateStorageLensGroupRequest;
import software.amazon.awssdk.services.s3control.model.MatchObjectSize;
import software.amazon.awssdk.services.s3control.model.StorageLensGroup;
import software.amazon.awssdk.services.s3control.model.StorageLensGroupFilter;
import software.amazon.awssdk.services.s3control.model.StorageLensGroupOrOperator;

public class CreateStorageLensGroupWithOrFilter {
    public static void main(String[] args) {
        String storageLensGroupName = "Marketing-Department";
        String accountId = "111122223333";

        try {
            StorageLensGroupOrOperator orOperator =
 StorageLensGroupOrOperator.builder()
                    .matchAnyPrefix("prefix-1", "prefix-2", "prefix-3/sub-prefix-1")
                    .matchObjectSize(MatchObjectSize.builder()
                            .bytesGreaterThan(1000L)
                            .bytesLessThan(6000L)
                            .build())
                    .build();

            StorageLensGroupFilter orFilter = StorageLensGroupFilter.builder()
                    .or(orOperator)
                    .build();

            StorageLensGroup storageLensGroup = StorageLensGroup.builder()
                    .name(storageLensGroupName)
                    .filter(orFilter)
                    .build();

            CreateStorageLensGroupRequest createStorageLensGroupRequest =
 CreateStorageLensGroupRequest.builder()
                    .storageLensGroup(storageLensGroup)
                    .accountId(accountId).build();

            S3ControlClient s3ControlClient = S3ControlClient.builder()
                    .region(Region.US_WEST_2)
                    .credentialsProvider(ProfileCredentialsProvider.create())
                    .build();
            s3ControlClient.createStorageLensGroup(createStorageLensGroupRequest);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
```

```
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Example – Crie um grupo da Lente de Armazenamento com um único filtro e duas tags de recursos AWS

O exemplo a seguir cria um grupo da Lente de Armazenamento chamado *Marketing-Department*, que tem um filtro de sufixo. Este exemplo também adiciona duas tags de recursos AWS ao grupo da Lente de Armazenamento. Para usar esse exemplo, substitua os *user input placeholders* por suas próprias informações.

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.CreateStorageLensGroupRequest;
import software.amazon.awssdk.services.s3control.model.StorageLensGroup;
import software.amazon.awssdk.services.s3control.model.StorageLensGroupFilter;
import software.amazon.awssdk.services.s3control.model.Tag;

public class CreateStorageLensGroupWithResourceTags {
    public static void main(String[] args) {
        String storageLensGroupName = "Marketing-Department";
        String accountId = "111122223333";

        try {
            // Create AWS resource tags.
            Tag resourceTag1 = Tag.builder()
                    .key("resource-tag-key-1")
                    .value("resource-tag-value-1")
                    .build();
            Tag resourceTag2 = Tag.builder()
                    .key("resource-tag-key-2")
```

```
                    .value("resource-tag-value-2")
                    .build();

            StorageLensGroupFilter suffixFilter = StorageLensGroupFilter.builder()
                    .matchAnySuffix(".png", ".gif", ".jpg")
                    .build();

            StorageLensGroup storageLensGroup = StorageLensGroup.builder()
                    .name(storageLensGroupName)
                    .filter(suffixFilter)
                    .build();

            CreateStorageLensGroupRequest createStorageLensGroupRequest =
 CreateStorageLensGroupRequest.builder()
                    .storageLensGroup(storageLensGroup)
                    .tags(resourceTag1, resourceTag2)
                    .accountId(accountId).build();

            S3ControlClient s3ControlClient = S3ControlClient.builder()
                    .region(Region.US_WEST_2)
                    .credentialsProvider(ProfileCredentialsProvider.create())
                    .build();
            s3ControlClient.createStorageLensGroup(createStorageLensGroupRequest);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Para obter configurações de exemplo JSON, consulte Configuração de grupos da Lente de Armazenamento.

Anexar ao painel ou remover do painel grupos da Lente de Armazenamento do S3

Depois de atualizar para o nível avançado na Lente de Armazenamento do Amazon S3, você poderá anexar um grupo da Lente de Armazenamento ao seu painel. Se você tiver vários grupos da Lente de Armazenamento, poderá incluir ou excluir os grupos desejados.

Seus grupos da Lente de Armazenamento devem residir na região inicial designada na conta do painel. Depois de anexar um grupo da Lente de Armazenamento ao painel, você receberá os dados adicionais de agregação do grupo da Lente de Armazenamento na exportação de métricas em até 48 horas.

> **Note**
>
> Para visualizar métricas agregadas ao grupo da Lente de Armazenamento, você deve anexá-las ao painel da Lente de Armazenamento. Para obter exemplos de arquivos de configuração JSON do grupo da Lente de Armazenamento, consulte Exemplo de configuração da Lente de Armazenamento do S3 com grupos da Lente de Armazenamento em JSON.

Usar o console do S3

Para anexar um grupo da Lente de Armazenamento a um painel da Lente de Armazenamento

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, em Lente de Armazenamento, selecione Painéis.
3. Selecione botão de opção para o painel da Lente de Armazenamento ao qual você deseja anexar um grupo da Lente de Armazenamento.
4. Escolha Editar.
5. Em Seleção de métricas, escolha Métricas e recomendações avançadas.
6. Selecione a opção Agregação do grupo da Lente de Armazenamento.

   > **Note**
   >
   > Por padrão, a opção Métricas avançadas também é selecionada. No entanto, você também pode desmarcar essa configuração, pois ela não é necessária para agregar dados de grupos da Lente de Armazenamento.

7. Role para baixo até Agregação do grupo da Lente de Armazenamento e especifique o grupo ou grupos da Lente de Armazenamento que você deseja incluir ou excluir na agregação de dados. Você pode usar as seguintes opções de filtro:

- Para incluir determinados grupos da Lente de Armazenamento, escolha Incluir grupos da Lente de Armazenamento. Em Grupos da Lente de Armazenamento a serem incluídos, selecione seus grupos da Lente de Armazenamento.
- Para incluir todos os grupos da Lente de Armazenamento, selecione Incluir todos os grupos da Lente de Armazenamento na região de origem nesta conta.
- Para excluir determinados grupos da Lente de Armazenamento, selecione Excluir grupos da Lente de Armazenamento. Em Grupos da Lente de Armazenamento a serem excluídos, selecione os grupos da Lente de Armazenamento que você deseja excluir.

8. Escolha Salvar alterações. Se tiver configurado seus grupos da Lente de Armazenamento corretamente, você verá os dados adicionais de agregação do grupo da Lente de Armazenamento em seu painel dentro de 48 horas.

Como remover um grupo da Lente de Armazenamento de um painel da Lente de Armazenamento do S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, em Lente de Armazenamento, selecione Painéis.
3. Selecione o botão de opção para o painel da Lente de Armazenamento do qual você deseja remover um grupo da Lente de Armazenamento.
4. Selecione Exibir configuração do painel.
5. Escolha Editar.
6. Role para baixo até a seção Seleção de métricas.
7. Em Agregação de grupo da Lente de Armazenamento, selecione o X ao lado do grupo da Lente de Armazenamento que você deseja remover. Isso remove o grupo da Lente de Armazenamento.

   Se você tiver incluído todos os grupos da Lente de Armazenamento em seu painel, desmarque a caixa de seleção ao lado de Incluir todos os grupos da Lente de Armazenamento na região inicial nesta conta.
8. Escolha Salvar alterações.

> **Note**
>
> Levará até 48 horas para que seu painel mostre as atualizações de configuração.

Usar o AWS SDK para Java

Example – Anexar todos os grupos da Lente de Armazenamento a um painel

O exemplo de SDK para Java a seguir anexa todos os grupos da Lente de Armazenamento na conta *111122223333* ao painel *DashBoardConfigurationId*:

```
package aws.example.s3control;


import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import com.amazonaws.services.s3control.model.BucketLevel;
import com.amazonaws.services.s3control.model.PutStorageLensConfigurationRequest;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.model.AccountLevel;
import com.amazonaws.services.s3control.model.StorageLensConfiguration;
import com.amazonaws.services.s3control.model.StorageLensGroupLevel;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class CreateDashboardWithStorageLensGroups {
    public static void main(String[] args) {
        String configurationId = "ExampleDashboardConfigurationId";
        String sourceAccountId = "111122223333";

        try {
            StorageLensGroupLevel storageLensGroupLevel = new StorageLensGroupLevel();

            AccountLevel accountLevel = new AccountLevel()
                    .withBucketLevel(new BucketLevel())
                    .withStorageLensGroupLevel(storageLensGroupLevel);

            StorageLensConfiguration configuration = new StorageLensConfiguration()
                    .withId(configurationId)
```

```
                    .withAccountLevel(accountLevel)
                    .withIsEnabled(true);

            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(US_WEST_2)
                    .build();

            s3ControlClient.putStorageLensConfiguration(new
 PutStorageLensConfigurationRequest()
                    .withAccountId(sourceAccountId)
                    .withConfigId(configurationId)
                    .withStorageLensConfiguration(configuration)
            );
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Example – Anexar dois grupos da Lente de Armazenamento a um painel

O exemplo AWS SDK para Java a seguir anexa dois grupos da Lente de Armazenamento (*StorageLensGroupName1* e *StorageLensGroupName2*) ao painel *ExampleDashboardConfigurationId*.

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import com.amazonaws.services.s3control.model.AccountLevel;
import com.amazonaws.services.s3control.model.BucketLevel;
import com.amazonaws.services.s3control.model.PutStorageLensConfigurationRequest;
import com.amazonaws.services.s3control.model.StorageLensConfiguration;
```

```
import com.amazonaws.services.s3control.model.StorageLensGroupLevel;
import com.amazonaws.services.s3control.model.StorageLensGroupLevelSelectionCriteria;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class CreateDashboardWith2StorageLensGroups {
    public static void main(String[] args) {
        String configurationId = "ExampleDashboardConfigurationId";
        String storageLensGroupName1 = "StorageLensGroupName1";
        String storageLensGroupName2 = "StorageLensGroupName2";
        String sourceAccountId = "111122223333";

        try {
            StorageLensGroupLevelSelectionCriteria selectionCriteria = new
 StorageLensGroupLevelSelectionCriteria()
                    .withInclude(
                            "arn:aws:s3:" + US_WEST_2.getName() + ":" + sourceAccountId
 + ":storage-lens-group/" + storageLensGroupName1,
                            "arn:aws:s3:" + US_WEST_2.getName() + ":" + sourceAccountId
 + ":storage-lens-group/" + storageLensGroupName2);

            System.out.println(selectionCriteria);
            StorageLensGroupLevel storageLensGroupLevel = new StorageLensGroupLevel()
                    .withSelectionCriteria(selectionCriteria);

            AccountLevel accountLevel = new AccountLevel()
                    .withBucketLevel(new BucketLevel())
                    .withStorageLensGroupLevel(storageLensGroupLevel);

            StorageLensConfiguration configuration = new StorageLensConfiguration()
                    .withId(configurationId)
                    .withAccountLevel(accountLevel)
                    .withIsEnabled(true);

            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(US_WEST_2)
                    .build();

            s3ControlClient.putStorageLensConfiguration(new
 PutStorageLensConfigurationRequest()
                    .withAccountId(sourceAccountId)
                    .withConfigId(configurationId)
                    .withStorageLensConfiguration(configuration)
```

```
            );
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Example – Anexar todos os grupos da Lente de Armazenamento com exclusões

O exemplo de SDK para Java a seguir anexa todos os grupos da Lente de Armazenamento ao painel *ExampleDashboardConfigurationId*, exceto os dois especificados (*StorageLensGroupName1* e *StorageLensGroupName2*):

```
package aws.example.s3control;


import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import com.amazonaws.services.s3control.model.AccountLevel;
import com.amazonaws.services.s3control.model.BucketLevel;
import com.amazonaws.services.s3control.model.PutStorageLensConfigurationRequest;
import com.amazonaws.services.s3control.model.StorageLensConfiguration;
import com.amazonaws.services.s3control.model.StorageLensGroupLevel;
import com.amazonaws.services.s3control.model.StorageLensGroupLevelSelectionCriteria;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class CreateDashboardWith2StorageLensGroupsExcluded {
    public static void main(String[] args) {
        String configurationId = "ExampleDashboardConfigurationId";
        String storageLensGroupName1 = "StorageLensGroupName1";
        String storageLensGroupName2 = "StorageLensGroupName2";
        String sourceAccountId = "111122223333";
```

```
        try {
            StorageLensGroupLevelSelectionCriteria selectionCriteria = new
StorageLensGroupLevelSelectionCriteria()
                    .withInclude(
                            "arn:aws:s3:" + US_WEST_2.getName() + ":" + sourceAccountId
+ ":storage-lens-group/" + storageLensGroupName1,
                            "arn:aws:s3:" + US_WEST_2.getName() + ":" + sourceAccountId
+ ":storage-lens-group/" + storageLensGroupName2);

            System.out.println(selectionCriteria);
            StorageLensGroupLevel storageLensGroupLevel = new StorageLensGroupLevel()
                    .withSelectionCriteria(selectionCriteria);

            AccountLevel accountLevel = new AccountLevel()
                    .withBucketLevel(new BucketLevel())
                    .withStorageLensGroupLevel(storageLensGroupLevel);

            StorageLensConfiguration configuration = new StorageLensConfiguration()
                    .withId(configurationId)
                    .withAccountLevel(accountLevel)
                    .withIsEnabled(true);

            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(US_WEST_2)
                    .build();

            s3ControlClient.putStorageLensConfiguration(new
PutStorageLensConfigurationRequest()
                    .withAccountId(sourceAccountId)
                    .withConfigId(configurationId)
                    .withStorageLensConfiguration(configuration)
            );
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
```

```
}
```

Visualização de dados dos grupos da Lente de Armazenamento

Visualize os dados dos grupos da Lente de Armazenamento anexando o grupo ao painel da Lente de Armazenamento do Amazon S3. Depois de incluir o grupo da Lente de Armazenamento na agregação do grupo na configuração do painel, pode levar até 48 horas para que os dados do grupo da Lente de Armazenamento sejam exibidos no painel.

Depois que a configuração do painel for atualizada, todos os grupos da Lente de Armazenamento recém-anexados aparecerão na lista de recursos disponíveis, na guia Grupos da Lente de Armazenamento. Você também pode analisar melhor o uso do armazenamento na guia Visão geral. É só dividir os dados em outra dimensão. Por exemplo, você pode selecionar um dos itens listados nas três principais categorias e escolher Analisar por para dividir os dados em outra dimensão. Não é possível aplicar a mesma dimensão do próprio filtro.

> **Note**
>
> Não é possível aplicar um filtro de grupo e Lente de Armazenamento junto com um filtro de prefixo e vice-versa. Você também não pode analisar de maneira mais aprofundada um grupo da Lente de Armazenamento usando um filtro de prefixo.

Você pode usar a guia Grupos da Lente de Armazenamento no painel da Lente de Armazenamento do Amazon S3 para personalizar a visualização de dados para os grupos da Lente de Armazenamento anexados ao seu painel. Você pode visualizar os dados de alguns grupos da Lente de Armazenamento que estão anexados ao seu painel ou de todos eles.

Ao visualizar os dados do grupo da Lente de Armazenamento no painel da Lente de Armazenamento do S3, esteja ciente do seguinte:

- A Lente de Armazenamento do S3 agrega métricas de uso de um objeto em todos os grupos da Lente de Armazenamento correspondentes. Portanto, se um objeto corresponder às condições de filtro de dois ou mais grupos da Lente de Armazenamento, você verá contagens repetidas do mesmo objeto em todo o uso do armazenamento.
- Os objetos devem corresponder aos filtros incluídos nos grupos da Lente de Armazenamento. Se nenhum objeto corresponder aos filtros incluídos no grupo da Lente de Armazenamento, nenhuma métrica será gerada. Para determinar se há objetos não atribuídos, verifique a contagem total de objetos no painel no nível da conta e do bucket.

Atualização do grupo da Lente de Armazenamento

Os exemplos a seguir demonstram como atualizar um grupo da Lente de Armazenamento do Amazon S3. Você pode atualizar um grupo da Lente de Armazenamento usando o console Amazon S3, AWS Command Line Interface (AWS CLI) e AWS SDK para Java.

Usar o console do S3

Para atualizar um grupo da Lente de Armazenamento

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, selecione Grupos de Lente de Armazenamento.
3. Em Grupos da Lente de Armazenamento, selecione o grupo a ser atualizado.
4. Em Escopo, selecione Editar.
5. Na página Escopo, selecione o filtro a ser aplicado no grupo da Lente de Armazenamento. Para aplicar vários filtros, selecione os filtros e escolha o operador lógico AND ou OR.
   - Para o filtro Prefixos, selecione Prefixos e insira uma sequência de prefixo. Para adicionar vários prefixos, selecione Adicionar prefixo. Para remover um prefixo, selecione Remover ao lado do prefixo para remover.
   - Para o filtro Tags de objeto, insira o par de valores-chave ao objeto. Selecione Adicionar tag. Para remover uma tag, selecione Remover ao lado da tag para remover.
   - Para o filtro Sufixos, selecione Sufixos e insira uma sequência de sufixo. Para adicionar vários sufixos, selecione Adicionar sufixo. Para remover um sufixo, selecione Remover ao lado do sufixo para remover.
   - Para o filtro Idade, especifique a faixa etária do objeto em dias. Selecione Especificar idade mínima do objeto e insira a idade mínima do objeto. Em Especificar idade máxima do objeto, insira a idade máxima do objeto.
   - Para o filtro Tamanho, especifique a faixa de tamanho do objeto e a unidade de medida. Selecione Especificar tamanho mínimo do objeto e insira o tamanho mínimo do objeto. Em Especificar tamanho máximo do objeto, insira o tamanho máximo do objeto.
6. Escolha Salvar alterações. A página de detalhes do grupo da Lente de Armazenamento é exibida.
7. (Opcional) Para adicionar uma nova tag de recursos AWS, acesse a seção Tags de recursos AWS e selecione Adicionar tags. A página Adicionar tags é exibida.

Adicione o novo par de valores-chave e selecione Salvar alterações. A página de detalhes do grupo da Lente de Armazenamento é exibida.

8. (Opcional) Para remover uma tag de recursos existente AWS, acesse a seção Tags de recurso AWS e selecione a tag de recursos. Em seguida, selecione Excluir. A caixa de diálogo Excluir tags AWS é exibida.

   Selecione Excluir novamente para excluir permanentemente a tag de recursos AWS.

   > **Note**
   >
   > Depois de excluir permanentemente uma tag de recursos AWS, ela não poderá ser restaurada.

Como usar o AWS CLI

O comando de exemplo AWS CLI a seguir mostra os detalhes da configuração de um grupo da Lente de Armazenamento *marketing-department*. Para usar esse exemplo de comando, substitua os *user input placeholders* por suas próprias informações.

```
aws s3control get-storage-lens-group --account-id 111122223333 \
--region us-east-1 --name marketing-department
```

O exemplo AWS CLI a seguir atualiza um grupo da Lente de Armazenamento. Para usar esse exemplo de comando, substitua os *user input placeholders* por suas próprias informações.

```
aws s3control update-storage-lens-group --account-id 111122223333 \
--region us-east-1 --storage-lens-group=file://./marketing-department.json
```

Para obter configurações de exemplo JSON, consulte Configuração de grupos da Lente de Armazenamento.

Usar o AWS SDK para Java

O exemplo AWS SDK para Java a seguir mostra os detalhes da configuração do grupo da Lente de Armazenamento *Marketing-Department* na conta *111122223333*. Para usar esse exemplo, substitua os *user input placeholders* por suas próprias informações.

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.GetStorageLensGroupRequest;
import software.amazon.awssdk.services.s3control.model.GetStorageLensGroupResponse;

public class GetStorageLensGroup {
    public static void main(String[] args) {
        String storageLensGroupName = "Marketing-Department";
        String accountId = "111122223333";

        try {
            GetStorageLensGroupRequest getRequest =
 GetStorageLensGroupRequest.builder()
                    .name(storageLensGroupName)
                    .accountId(accountId).build();
            S3ControlClient s3ControlClient = S3ControlClient.builder()
                    .region(Region.US_WEST_2)
                    .credentialsProvider(ProfileCredentialsProvider.create())
                    .build();
            GetStorageLensGroupResponse response =
 s3ControlClient.getStorageLensGroup(getRequest);
            System.out.println(response);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

O exemplo a seguir atualiza o grupo da Lente de Armazenamento *Marketing-Department* na conta *111122223333*. Esse exemplo atualiza o escopo do painel para incluir objetos que

correspondam a qualquer um dos seguintes sufixos: *.png*, *.gif*, *.jpg* ou *.jpeg*. Para usar esse exemplo, substitua os *user input placeholders* por suas próprias informações.

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.StorageLensGroup;
import software.amazon.awssdk.services.s3control.model.StorageLensGroupFilter;
import software.amazon.awssdk.services.s3control.model.UpdateStorageLensGroupRequest;

public class UpdateStorageLensGroup {
    public static void main(String[] args) {
        String storageLensGroupName = "Marketing-Department";
        String accountId = "111122223333";

        try {
            // Create updated filter.
            StorageLensGroupFilter suffixFilter = StorageLensGroupFilter.builder()
                    .matchAnySuffix(".png", ".gif", ".jpg", ".jpeg")
                    .build();

            StorageLensGroup storageLensGroup = StorageLensGroup.builder()
                    .name(storageLensGroupName)
                    .filter(suffixFilter)
                    .build();

            UpdateStorageLensGroupRequest updateStorageLensGroupRequest =
 UpdateStorageLensGroupRequest.builder()
                    .name(storageLensGroupName)
                    .storageLensGroup(storageLensGroup)
                    .accountId(accountId)
                    .build();

            S3ControlClient s3ControlClient = S3ControlClient.builder()
                    .region(Region.US_WEST_2)
                    .credentialsProvider(ProfileCredentialsProvider.create())
                    .build();
            s3ControlClient.updateStorageLensGroup(updateStorageLensGroupRequest);
        } catch (AmazonServiceException e) {
```

```
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Para obter configurações de exemplo JSON, consulte Configuração de grupos da Lente de Armazenamento.

Gerenciamento de tags de recursos AWS com grupos da Lente de Armazenamento

Cada grupo da Lente de Armazenamento do Amazon S3 é contado como um recurso AWS com o próprio nome do recurso da Amazon (ARN). Portanto, ao configurar o grupo da Lente de Armazenamento, você tem a opção de adicionar tags de recursos AWS ao grupo. Você pode adicionar até 50 tags para cada grupo da Lente de Armazenamento. Para criar um grupo da Lente de Armazenamento com tags, você deve ter as permissões `s3:CreateStorageLensGroup` e `s3:TagResource`.

Use tags de recursos AWS para categorizar os recursos de acordo com o departamento, a linha de negócios ou o projeto. Fazer isso é útil quando você tem muitos recursos do mesmo tipo. Ao aplicar tags, é possível identificar rapidamente um grupo específico da Lente de Armazenamento com base nas tags atribuídas a ele. Você também pode usar tags para rastrear e alocar custos.

Além disso, ao adicionar uma tag de recursos AWS ao grupo da Lente de Armazenamento, você ativa o controle de acesso por atributo (ABAC). ABAC é uma estratégia de autorização que define permissões com base em atributos, neste caso, tags. É possível usar condições que especificam tags de recursos nas políticas do IAM para controlar o acesso aos recursos AWS.

É possível editar chaves de tags e valores e é possível remover as tags de um recurso a qualquer momento. Além disso, esteja ciente das seguintes limitações:

- As chaves e os valores das tags diferenciam maiúsculas de minúsculas.
- Ao adicionar uma tag que tenha a mesma chave de uma tag existente nesse recurso, o novo valor substituirá o antigo.
- Se você excluir um recurso, todas as tags do recurso também serão excluídas.

- Não inclua dados privados ou confidenciais nas tags de recursos AWS.
- As tags do sistema (com chaves de tags que começam com `aws:`) não são compatíveis.
- O comprimento de cada chave de tag não pode exceder 128 caracteres. O comprimento de cada valor de tag não pode exceder 256 caracteres.

Os exemplos a seguir demonstram como usar tags de recursos AWS com grupos da Lente de Armazenamento.

Tópicos

- Adicionar tag de recursos AWS a um grupo da Lente de Armazenamento
- Atualização dos valores das tags de grupo da Lente de Armazenamento
- Exclusão de tag de recursos AWS do grupo da Lente de Armazenamento
- Listagem de tags de grupo da Lente de Armazenamento

Adicionar tag de recursos AWS a um grupo da Lente de Armazenamento

Os exemplos a seguir demonstram como adicionar tags de recursos AWS a um grupo da Lente de Armazenamento do Amazon S3. Adicione tags de recurso usando o console do Amazon S3, AWS Command Line Interface (AWS CLI) e AWS SDK para Java.

Usar o console do S3

Para adicionar uma tag de recursos AWS a um grupo da Lente de Armazenamento

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, selecione Grupos de Lente de Armazenamento.
3. Em Grupos da Lente de Armazenamento, selecione o grupo a ser atualizado.
4. Em Tags de recursos AWS, selecione Adicionar tags.
5. Na página Adicionar tags, adicione o novo par de valores-chave.

> **Note**
>
> Adicionar uma nova tag com a mesma chave de tag existente substitui o valor da tag anterior.

6. (Opcional) Para adicionar mais de uma tag nova, selecione Adicionar tag novamente para continuar adicionando novas entradas. Você pode adicionar até 50 tags de recursos AWS ao seu grupo da Lente de Armazenamento.
7. (Opcional) Para remover uma entrada recém-adicionada, selecione Remover ao lado da tag que você deseja remover.
8. Escolha Salvar alterações.

Como usar o AWS CLI

O comando de exemplo AWS CLI a seguir adiciona duas tags de recursos a um grupo da Lente de Armazenamento existente chamado *marketing-department*. Para usar esse exemplo de comando, substitua os *user input placeholders* por suas próprias informações.

```
aws s3control tag-resource --account-id 111122223333 \
--resource-arn arn:aws:s3:us-east-1:111122223333:storage-lens-group/marketing-
department \
--region us-east-1 --tags Key=k1,Value=v1 Key=k2,Value=v2
```

Usar o AWS SDK para Java

O exemplo AWS SDK para Java a seguir adiciona duas tags de recursos AWS a um grupo da Lente de Armazenamento existente. Para usar esse exemplo, substitua os *user input placeholders* por suas próprias informações.

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.Tag;
import software.amazon.awssdk.services.s3control.model.TagResourceRequest;

public class TagResource {
    public static void main(String[] args) {
        String resourceARN = "Resource_ARN";
        String accountId = "111122223333";

        try {
```

```
            Tag resourceTag1 = Tag.builder()
                .key("resource-tag-key-1")
                .value("resource-tag-value-1")
                .build();
            Tag resourceTag2 = Tag.builder()
                    .key("resource-tag-key-2")
                    .value("resource-tag-value-2")
                    .build();
            TagResourceRequest tagResourceRequest = TagResourceRequest.builder()
                    .resourceArn(resourceARN)
                    .tags(resourceTag1, resourceTag2)
                    .accountId(accountId)
                    .build();
            S3ControlClient s3ControlClient = S3ControlClient.builder()
                    .region(Region.US_WEST_2)
                    .credentialsProvider(ProfileCredentialsProvider.create())
                    .build();
            s3ControlClient.tagResource(tagResourceRequest);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Atualização dos valores das tags de grupo da Lente de Armazenamento

Os exemplos a seguir demonstram como atualizar os valores das tags de grupo da Lente de Armazenamento usando o console Amazon S3, AWS Command Line Interface (AWS CLI) e AWS SDK para Java.

Usar o console do S3

Para atualizar uma tag de recursos AWS de um grupo da Lente de Armazenamento

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, selecione Grupos de Lente de Armazenamento.

3. Em Grupos da Lente de Armazenamento, selecione o grupo a ser atualizado.
4. Em Tags de recursos AWS, selecione a tag a ser atualizada.
5. Adicione o novo valor da tag usando a mesma chave do par de valores-chave que você deseja atualizar. Escolha o ícone da marca de seleção para atualizar o valor da tag.

   > **Note**
   >
   > Adicionar uma nova tag com a mesma chave de tag existente substitui o valor da tag anterior.

6. (Opcional) Para adicionar novas tags, selecione Adicionar tag para adicionar novas entradas. A página Adicionar tags é exibida.

   Adicione até 50 tags de recursos AWS ao grupo da Lente de Armazenamento. Quando terminar de adicionar tags, selecione Salvar alterações.
7. (Opcional) Para remover uma entrada recém-adicionada, selecione Remover ao lado da tag que você deseja remover. Ao finalizar a remoção de tags, selecione Salvar alterações.

Como usar o AWS CLI

O comando de exemplo AWS CLI a seguir atualiza dois valores de tags para o grupo da Lente de Armazenamento *marketing-department*. Para usar esse exemplo de comando, substitua os *user input placeholders* por suas próprias informações.

```
aws s3control tag-resource --account-id 111122223333 \
--resource-arn arn:aws:s3:us-east-1:111122223333:storage-lens-group/marketing-
department \
--region us-east-1 --tags Key=k1,Value=v3 Key=k2,Value=v4
```

Usar o AWS SDK para Java

O exemplo AWS SDK para Java a seguir atualiza dois valores de tags do grupo da Lente de Armazenamento. Para usar esse exemplo, substitua os *user input placeholders* por suas próprias informações.

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
```

```
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.Tag;
import software.amazon.awssdk.services.s3control.model.TagResourceRequest;

public class UpdateTagsForResource {
    public static void main(String[] args) {
        String resourceARN = "Resource_ARN";
        String accountId = "111122223333";

        try {
            Tag updatedResourceTag1 = Tag.builder()
                .key("resource-tag-key-1")
                .value("resource-tag-updated-value-1")
                .build();
            Tag updatedResourceTag2 = Tag.builder()
                    .key("resource-tag-key-2")
                    .value("resource-tag-updated-value-2")
                    .build();
            TagResourceRequest tagResourceRequest = TagResourceRequest.builder()
                    .resourceArn(resourceARN)
                    .tags(updatedResourceTag1, updatedResourceTag2)
                    .accountId(accountId)
                    .build();
            S3ControlClient s3ControlClient = S3ControlClient.builder()
                    .region(Region.US_WEST_2)
                    .credentialsProvider(ProfileCredentialsProvider.create())
                    .build();
            s3ControlClient.tagResource(tagResourceRequest);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Exclusão de tag de recursos AWS do grupo da Lente de Armazenamento

Os exemplos a seguir demonstram como excluir uma tag de recursos AWS de um grupo da Lente de Armazenamento. Exclua tags usando o console do Amazon S3, AWS Command Line Interface (AWS CLI) e AWS SDK para Java.

Usar o console do S3

Para excluir uma tags de recurso AWS de um grupo da Lente de Armazenamento

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, selecione Grupos de Lente de Armazenamento.
3. Em Grupos da Lente de Armazenamento, selecione o grupo a ser atualizado.
4. Em Tags de recursos AWS, selecione o par de valores-chave a ser excluído.
5. Escolha Excluir. A caixa de diálogo Excluir tags de recursos AWS é exibida.

> **Note**
>
> Se tags forem usadas para controlar o acesso, prosseguir com essa ação poderá afetar os recursos relacionados. Depois de excluir permanentemente uma tag, ela não poderá ser restaurada.

6. Selecione Excluir para excluir permanentemente o par de valores-chave.

Como usar o AWS CLI

O comando AWS CLI a seguir exclui duas tags de recursos AWS de um grupo da Lente de Armazenamento existente: para usar esse comando de exemplo, substitua *`user input placeholders`* por suas próprias informações.

```
aws s3control untag-resource --account-id 111122223333 \
--resource-arn arn:aws:s3:us-east-1:111122223333:storage-lens-group/Marketing-Department \
--region us-east-1 --tag-keys k1 k2
```

Usar o AWS SDK para Java

O exemplo AWS SDK para Java a seguir exclui duas tags de recursos AWS do nome do recurso da Amazon (ARN) do grupo da Lente de Armazenamento especificado na conta *111122223333*. Para usar esse exemplo, substitua os *user input placeholders* por suas próprias informações.

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.UntagResourceRequest;

public class UntagResource {
    public static void main(String[] args) {
        String resourceARN = "Resource_ARN";
        String accountId = "111122223333";

        try {
            String tagKey1 = "resource-tag-key-1";
            String tagKey2 = "resource-tag-key-2";
            UntagResourceRequest untagResourceRequest = UntagResourceRequest.builder()
                    .resourceArn(resourceARN)
                    .tagKeys(tagKey1, tagKey2)
                    .accountId(accountId)
                    .build();
            S3ControlClient s3ControlClient = S3ControlClient.builder()
                    .region(Region.US_WEST_2)
                    .credentialsProvider(ProfileCredentialsProvider.create())
                    .build();
            s3ControlClient.untagResource(untagResourceRequest);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
```

```
}
```

Listagem de tags de grupo da Lente de Armazenamento

Os exemplos a seguir demonstram como listar as tags de recursos AWS associadas ao grupo da Lente de Armazenamento. Você pode listar as tags usando o console do Amazon S3, AWS Command Line Interface (AWS CLI) e AWS SDK para Java.

Usar o console do S3

Para revisar a lista de tags e valores de tags para o grupo da Lente de Armazenamento

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, selecione Grupos de Lente de Armazenamento.
3. Em Grupos da Lente de Armazenamento, selecione o grupo da Lente de Armazenamento da sua preferência.
4. Role para baixo até a seção Tags de recursos AWS. Todas as tags de recursos AWS definidas pelo usuário que são adicionadas ao grupo da Lente de Armazenamento são listadas junto com os valores de tag.

Como usar o AWS CLI

O comando de exemplo AWS CLI a seguir lista todos os valores de tag do grupo da Lente de Armazenamento para o grupo da Lente de Armazenamento *marketing-department*. Para usar esse exemplo de comando, substitua os *user input placeholders* por suas próprias informações.

```
aws s3control list-tags-for-resource --account-id 111122223333 \
--resource-arn arn:aws:s3:us-east-1:111122223333:storage-lens-group/marketing-
department \
--region us-east-1
```

Usar o AWS SDK para Java

O exemplo AWS SDK para Java a seguir lista os valores de tag do grupo da Lente de Armazenamento para o nome do recurso da Amazon (ARN) do grupo da Lente de Armazenamento que você especifica. Para usar esse exemplo, substitua os *user input placeholders* por suas próprias informações.

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.ListTagsForResourceRequest;
import software.amazon.awssdk.services.s3control.model.ListTagsForResourceResponse;

public class ListTagsForResource {
    public static void main(String[] args) {
        String resourceARN = "Resource_ARN";
        String accountId = "111122223333";

        try {
            ListTagsForResourceRequest listTagsForResourceRequest =
 ListTagsForResourceRequest.builder()
                    .resourceArn(resourceARN)
                    .accountId(accountId)
                    .build();
            S3ControlClient s3ControlClient = S3ControlClient.builder()
                    .region(Region.US_WEST_2)
                    .credentialsProvider(ProfileCredentialsProvider.create())
                    .build();
            ListTagsForResourceResponse response =
 s3ControlClient.listTagsForResource(listTagsForResourceRequest);
            System.out.println(response);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Listagem de todos os grupos da Lente de Armazenamento

Os exemplos a seguir demonstram como listar todos os grupos da Lente de Armazenamento do Amazon S3 em uma Conta da AWS e região local. Esses exemplos mostram como listar todos os grupos da Lente de Armazenamento usando o console do Amazon S3, AWS Command Line Interface (AWS CLI) e AWS SDK para Java.

Usar o console do S3

Para listar todos os grupos da Lente de Armazenamento em uma conta e região local

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, selecione Grupos de Lente de Armazenamento.
3. Em Grupos da Lente de Armazenamento, a lista é exibida na sua conta.

Como usar o AWS CLI

O exemplo AWS CLI a seguir lista todos os grupos da Lente de Armazenamento da sua conta. Para usar esse exemplo de comando, substitua os *user input placeholders* por suas próprias informações.

```
aws s3control list-storage-lens-groups --account-id 111122223333 \
--region us-east-1
```

Usar o AWS SDK para Java

O exemplo AWS SDK para Java a seguir lista os grupos da Lente de Armazenamento da sua conta *111122223333*. Para usar esse exemplo, substitua os *user input placeholders* por suas próprias informações.

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.ListStorageLensGroupsRequest;
```

```
import software.amazon.awssdk.services.s3control.model.ListStorageLensGroupsResponse;

public class ListStorageLensGroups {
    public static void main(String[] args) {
        String accountId = "111122223333";

        try {
            ListStorageLensGroupsRequest listStorageLensGroupsRequest =
 ListStorageLensGroupsRequest.builder()
                    .accountId(accountId)
                    .build();
            S3ControlClient s3ControlClient = S3ControlClient.builder()
                    .region(Region.US_WEST_2)
                    .credentialsProvider(ProfileCredentialsProvider.create())
                    .build();
            ListStorageLensGroupsResponse response =
 s3ControlClient.listStorageLensGroups(listStorageLensGroupsRequest);
            System.out.println(response);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Visualização de detalhes do grupo da Lente de Armazenamento

Os exemplos a seguir demonstram como visualizar detalhes de configuração do grupo da Lente de Armazenamento do Amazon S3. Visualize os detalhes usando o console do Amazon S3, AWS Command Line Interface (AWS CLI) e AWS SDK para Java.

Usar o console do S3

Para visualizar detalhes de configuração do grupo da Lente de Armazenamento

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.

2. No painel de navegação à esquerda, selecione Grupos de Lente de Armazenamento.
3. Em Grupos da Lente de Armazenamento, selecione o botão ao lado do grupo da Lente de Armazenamento da sua preferência.
4. Escolha Exibir detalhes. Agora, você pode analisar os detalhes do grupo da Lente de Armazenamento.

Como usar o AWS CLI

O exemplo AWS CLI a seguir replica os detalhes da configuração do grupo da Lente de Armazenamento. Para usar esse exemplo de comando, substitua os *user input placeholders* por suas próprias informações.

```
aws s3control get-storage-lens-group --account-id 111122223333 \
--region us-east-1 --name marketing-department
```

Usar o AWS SDK para Java

O exemplo AWS SDK para Java a seguir replica os detalhes de configuração do grupo da Lente de Armazenamento *Marketing-Department* na conta *111122223333*. Para usar esse exemplo, substitua os *user input placeholders* por suas próprias informações.

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.GetStorageLensGroupRequest;
import software.amazon.awssdk.services.s3control.model.GetStorageLensGroupResponse;

public class GetStorageLensGroup {
    public static void main(String[] args) {
        String storageLensGroupName = "Marketing-Department";
        String accountId = "111122223333";

        try {
            GetStorageLensGroupRequest getRequest =
 GetStorageLensGroupRequest.builder()
                    .name(storageLensGroupName)
```

```
                    .accountId(accountId).build();
            S3ControlClient s3ControlClient = S3ControlClient.builder()
                    .region(Region.US_WEST_2)
                    .credentialsProvider(ProfileCredentialsProvider.create())
                    .build();
            GetStorageLensGroupResponse response =
 s3ControlClient.getStorageLensGroup(getRequest);
            System.out.println(response);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Exclusão de grupo da Lente de Armazenamento

Os exemplos a seguir demonstram como excluir um grupo da Lente de Armazenamento do Amazon S3 usando o console do Amazon S3AWS Command Line Interface, (AWS CLI) e AWS SDK para Java.

Usar o console do S3

Para excluir um grupo da Lente de Armazenamento

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, selecione Grupos de Lente de Armazenamento.
3. Em Grupos da Lente de Armazenamento, selecione o botão ao lado do grupo da Lente de Armazenamento para excluir.
4. Escolha Excluir. Uma caixa de diálogo Excluir grupo da Lente de Armazenamento é exibida.
5. Selecione Excluir novamente para excluir permanentemente o grupo da Lente de Armazenamento.

> **Note**
>
> Depois de excluir um grupo da Lente de Armazenamento, ele não poderá ser restaurado.

Como usar o AWS CLI

O exemplo AWS CLI a seguir exclui o grupo de Lente de Armazenamento *marketing-department*. Para usar esse exemplo de comando, substitua os *user input placeholders* por suas próprias informações.

```
aws s3control delete-storage-lens-group --account-id 111122223333 \
--region us-east-1 --name marketing-department
```

Usar o AWS SDK para Java

O exemplo AWS SDK para Java a seguir exclui o grupo da Lente de Armazenamento *Marketing-Department* na conta *111122223333*. Para usar esse exemplo, substitua os *user input placeholders* por suas próprias informações.

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.DeleteStorageLensGroupRequest;

public class DeleteStorageLensGroup {
    public static void main(String[] args) {
        String storageLensGroupName = "Marketing-Department";
        String accountId = "111122223333";

        try {
            DeleteStorageLensGroupRequest deleteStorageLensGroupRequest =
 DeleteStorageLensGroupRequest.builder()
                    .name(storageLensGroupName)
                    .accountId(accountId).build();
```

```
            S3ControlClient s3ControlClient = S3ControlClient.builder()
                    .region(Region.US_WEST_2)
                    .credentialsProvider(ProfileCredentialsProvider.create())
                    .build();
            s3ControlClient.deleteStorageLensGroup(deleteStorageLensGroupRequest);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Catalogar e analisar seus dados com o Inventário S3

É possível usar o Inventário Amazon S3 para ajudar a gerenciar o armazenamento. Por exemplo, você pode usá-lo para auditar e gerar relatórios sobre o status da replicação e criptografia de seus objetos para os negócios, a conformidade e as necessidades normativas. Também é possível simplificar e acelerar os fluxos de trabalho de negócios e os trabalhos de big data usando o Inventário Amazon S3, que fornece uma alternativa programada para as operações síncronas da API `List` do Amazon S3. O Inventário Amazon S3 não usa as operações de API `List` para auditar os objetos e não afeta a taxa de solicitação do bucket.

O Inventário Amazon S3 fornece arquivos de saída nos formatos CSV (valores separados por vírgulas), Apache ORC (colunar de linhas otimizado do Apache) ou Apache Parquet que listam os objetos e os metadados correspondentes, diária ou semanalmente, para um bucket do S3 ou objetos com prefixo compartilhado (ou seja, objetos que tenham nomes que comecem com uma string comum). Se você configurar um inventário semana, um relatório será gerado todo domingo (no fuso horário UTC) depois do relatório inicial. Para obter mais informações sobre preços do Amazon S3 Inventory, consulte Preços do Amazon S3.

Você pode configurar várias listas de inventário para um bucket. Ao configurar uma lista de inventário, é possível especificar o seguinte:

- Quais metadados de objeto incluir no inventário
- Se deve listar todas as versões do objeto ou somente as versões atuais

- Onde armazenar a saída do arquivo da lista de inventário
- Se o inventário deve ser gerado diariamente ou semanalmente
- Se o arquivo da lista de inventário deve ser criptografado

É possível consultar o Inventário Amazon S3 com consultas SQL padrão usando o Amazon Athena, o Amazon Redshift Spectrum e outras ferramentas, como Presto, Apache Hive e Apache Spark. Para obter mais informações sobre como usar o Athena para consultar os arquivos de inventário, consulte the section called “Consultar o inventário com o Athena”.

> **Note**
>
> Pode levar até 48 horas para o Amazon S3 entregar o primeiro relatório de inventário.

Buckets de origem e destino

O bucket para o qual o inventário lista objetos é chamado de bucket de origem. O bucket em que o arquivo de lista de inventários é armazenado é chamado de bucket de destino.

Bucket de origem

O inventário lista os objetos armazenados no bucket de origem. É possível obter uma lista de inventários de um bucket inteiro ou filtrar a lista pelo prefixo do nome da chave do objeto.

O bucket de origem:

- Contém os objetos que estão listados no inventário
- Contém a configuração para o inventário

Bucket de destino

Os arquivos de lista do Amazon S3 Inventory são gravados no bucket de destino. Você pode especificar um prefixo de destino na configuração do inventário para agrupar todos os arquivos de lista de inventários em um local comum no bucket de destino.

O bucket de destino:

- Contém as listas de arquivos de inventário.

- Contém os arquivos manifestos que relacionam todos os arquivos de listas de inventários armazenados no bucket de destino. Para obter mais informações, consulte Manifesto de inventário.
- Deve haver uma política de bucket para dar permissão ao Amazon S3 para verificar a propriedade do bucket e permissão para gravar arquivos no bucket.
- Deve estar na mesma Região da AWS do bucket de origem.
- Pode ser igual ao bucket de origem.
- Pode pertencer a uma Conta da AWS diferente da conta que é proprietária do bucket de origem.

Lista do Amazon S3 Inventory

Um arquivo de lista de inventários contém uma lista dos objetos no bucket de origem e os metadados de cada objeto. Um arquivo da lista de inventários é armazenado no bucket de destino com um dos seguintes formatos:

- Um arquivo CSV compactado com GZIP
- Como um arquivo colunar de linha otimizado (ORC) do Apache compactado com ZLIB
- Como um arquivo Apache Parquet compactado com Snappy

> **Note**
>
> Não há garantia de classificação em nenhuma ordem dos objetos nos relatórios do Amazon S3 Inventory.

Um arquivo de lista de inventários contém uma lista dos objetos no bucket de origem e os metadados de cada objeto listado:

- Nome do bucket: o nome do bucket a que o inventário se refere.
- Key name (Nome da chave): o nome da chave de objeto (ou chave) que identifica cada objeto no bucket. Ao usar o formato de arquivo CSV, o nome da chave é codificado em URL e deve ser decodificado para que possa ser usado.
- Version ID (ID da versão): o ID de versão do objeto. Quando você habilita o versionamento em um bucket, o Amazon S3 atribui um número de versão aos objetos adicionados ao bucket. Para

obter mais informações, consulte Reter várias versões de objetos com o Versionamento do S3. (O campo não é incluído caso a lista seja configurada somente para a versão atual dos objetos.)

- IsLatest: definido como `True` se o objeto for a versão atual do objeto. (O campo não é incluído caso a lista seja configurada somente para a versão atual dos objetos.)
- Delete marker (Marcador de exclusão): definido como `True` se o objeto for um marcador de exclusão. Para obter mais informações, consulte Reter várias versões de objetos com o Versionamento do S3. (Este campo é adicionado automaticamente ao seu relatório se você configurou o relatório para incluir todas as versões dos seus objetos).
- Tamanho: o tamanho do objeto em bytes, sem incluir o tamanho de uploads incompletos de várias partes, metadados de objetos e marcadores de exclusão.
- Last modified date (Data da última modificação) – a data de criação do objeto ou data da última modificação, a mais atual entre as duas.
- ETag: a tag de entidade (ETag) é um hash do objeto. O ETag reflete as alterações apenas no conteúdo de um objeto, não em seus metadados. A ETag pode ser um resumo MD5 dos dados do objeto. Tudo depende de como o objeto foi criado e de como está criptografado. Para obter mais informações, consulte Object na Referência da API do Amazon Simple Storage Service.
- Classe de armazenamento: a classe de armazenamento usada para armazenar o objeto. Defina como `STANDARD`, `REDUCED_REDUNDANCY`, `STANDARD_IA`, `ONEZONE_IA`, `INTELLIGENT_TIERING`, `GLACIER`, `DEEP_ARCHIVE`, `OUTPOSTS`, `GLACIER_IR` ou `SNOW`. Para obter mais informações, consulte Compreender e gerenciar classes de armazenamento do Amazon S3.

  > **Note**
  >
  > O Inventário S3 não é compatível com a classe S3 Express One Zone.

- Sinalizador de multipart upload: definido como `True` se o objeto foi carregado como um multipart upload. Para obter mais informações, consulte Carregar e copiar objetos usando upload fracionado no Amazon S3.
- Replication status (Status da replicação): defina como`PENDING`, `COMPLETED`, `FAILED`, ou`REPLICA`. Para obter mais informações, consulte Obtenção de informações sobre o status da replicação.
- Status da criptografia: o status da criptografia do lado do servidor, dependendo do tipo de chave de criptografia usada, criptografia do lado do servidor com chaves gerenciadas do Amazon S3 (SSE-S3), criptografia do lado do servidor com chaves do AWS Key Management Service (AWS KMS)

(SSE-KMS), criptografia de camada dupla do lado do servidor com chaves do AWS KMS (DSSE-KMS) ou criptografia do lado do servidor com chaves fornecidas pelo cliente (SSE-C). Defina como `SSE-S3`, `SSE-KMS`, `DSSE-KMS`, `SSE-C` ou `NOT-SSE`. Um status `NOT-SSE` significa que o objeto não foi criptografado com a criptografia no lado do servidor. Para obter mais informações, consulte Proteger dados com criptografia.

- Prazo de retenção do bloqueio de objetos do S3: a data até a qual o objeto bloqueado não pode ser excluído. Para obter mais informações, consulte Bloquear objetos com o Bloqueio de Objetos.
- Modo de retenção do bloqueio de objetos do S3: defina como `Governance` ou `Compliance` para objetos bloqueados. Para obter mais informações, consulte Bloquear objetos com o Bloqueio de Objetos.
- Status de retenção legal do bloqueio de objetos do S3: definido como `On` caso uma retenção legal tenha sido aplicada a um objeto. Caso contrário, ele será definido como `Off`. Para obter mais informações, consulte Bloquear objetos com o Bloqueio de Objetos.
- Nível de acesso S3 Intelligent-Tiering: nível de acesso (frequente ou infrequente) do objeto se armazenado na classe de armazenamento S3 Intelligent-Tiering. Defina como `FREQUENT`, `INFREQUENT`, `ARCHIVE_INSTANT_ACCESS`, `ARCHIVE` ou `DEEP_ARCHIVE`. Para obter mais informações, consulte Classe de armazenamento para otimizar automaticamente dados com padrões de acesso alterados ou desconhecidos.
- S3 Bucket Key Status (Status da chave do bucket do S3): defina como `ENABLED` ou `DISABLED`. Indica se o objeto usa a uma chave de bucket do S3 para SSE-KMS. Para obter mais informações, consulte Uso de chaves de bucket do Amazon S3.
- Algoritmo de soma de verificação: indica o algoritmo usado para criar a soma de verificação do objeto. Para obter mais informações, consulte Usar algoritmos de soma de verificação compatíveis.
- Lista de controle de acesso de objetos: uma lista de controle de acesso (ACL) para cada objeto que define quais Contas da AWS ou grupos recebem acesso a esse objeto e o tipo de acesso concedido. O campo ACL de objetos é definido no formato JSON. Um relatório da funcionalidade Inventário S3 inclui ACLs associadas a objetos no bucket de origem, mesmo quando as ACLs estão desabilitadas para o bucket. Para obter mais informações, consulte Trabalhar com o campo ACL de objetos e Visão geral da lista de controle de acesso (ACL).

> **Note**
>
> O campo ACL de objetos é definido no formato JSON. Um relatório de inventário exibe o valor do campo ACL de objetos como uma string codificada em base64.

Por exemplo, suponha que você tenha o seguinte campo ACL de objetos no formato JSON:

```
{
        "version": "2022-11-10",
        "status": "AVAILABLE",
        "grants": [{
            "canonicalId": "example-canonical-user-ID",
            "type": "CanonicalUser",
            "permission": "READ"
        }]
}
```

O campo ACL de objetos é codificado e mostrado como a seguinte string codificada em base64:

```
eyJ2ZXJzaW9uIjoiMjAyMi0xMS0xMCIsInN0YXR1cyI6IkFWQUlMQUJMRSIsImdyYW50cyI6W3siY2Fub25pY2Fs
```

Para obter o valor decodificado em JSON para o campo ACL de objetos, você pode consultar esse campo no Amazon Athena. Para obter exemplos de consultas, consulte Consulta do Amazon S3 Inventory com o Amazon Athena.

- Proprietário do objeto: o ID de usuário canônico do proprietário do objeto. Para ter mais informações, consulte Find the canonical user ID for your AWS account no Guia de referência de gerenciamento de contas da AWS.

> **Note**
>
> Quando um objeto atinge o fim de seu ciclo de vida, com base em sua configuração de ciclo de vida, o Amazon S3 o coloca em uma fila para remoção e o remove assincronamente. Assim, pode haver um atraso entre a data de expiração e a data em que o Amazon S3 remove um objeto. O relatório de inventário inclui os objetos que expiraram, mas ainda não foram removidos. Para obter mais informações sobre as ações de expiração no ciclo de vida do S3, consulte Expirando objetos.

Veja a seguir um exemplo de relatório de inventário com campos de metadados adicionais que consistem em quatro registros.

```
amzn-s3-demo-bucket1    example-object-1    EXAMPLEDC8l.XJCENlF7LePaNIIvs001    TRUE
     1500    2024-08-15T15:28:26.0004    EXAMPLE21e1518b92f3d92773570f600    STANDARD
  FALSE    COMPLETED    SSE-KMS    2025-01-25T15:28:26.000Z    COMPLIANCE    Off
 ENABLED
 eyJ2ZXJzaW9uIjoiMjAyMi0xMS0xMCIsInN0YXR1cyI6IkFWQUlMQUJMRSIsImdyYW50cyI6W3sicGVybWlzc2lvbiI6Ik
    EXAMPLE766e8f6b115d93d41df2eac420aa4a465d177c1398bc6a088c76b7000
amzn-s3-demo-bucket1    example-object-2    EXAMPLEDC8l.XJCENlF7LePaNIIvs002
 TRUE        200    2024-08-21T15:28:26.000Z    EXAMPLE21e1518b92f3d92773570f601
  INTELLIGENT_TIERING    FALSE    COMPLETED    SSE-KMS    2025-01-25T15:28:26.000Z
    COMPLIANCE    Off    INFREQUENT    ENABLED    SHA-256
 eyJ2ZXJzaW9uIjoiMjAyMi0xMS0xMCIsInN0YXR1cyI6IkFWQUlMQUJMRSIsImdyYW50cyI6W3sicGVybWlzc2lvbiI6Ik
    EXAMPLE766e8f6b115d93d41df2eac420aa4a465d177c1398bc6a088c76b7001
amzn-s3-demo-bucket1    example-object-3    EXAMPLEDC8l.XJCENlF7LePaNIIvs003    TRUE
      12500    2023-01-15T15:28:30.000Z    EXAMPLE21e1518b92f3d92773570f602    STANDARD
    FALSE    REPLICA    SSE-KMS    2025-01-25T15:28:26.000Z    GOVERNANCE    On
 ENABLED
 eyJ2ZXJzaW9uIjoiMjAyMi0xMS0xMCIsInN0YXR1cyI6IkFWQUlMQUJMRSIsImdyYW50cyI6W3sicGVybWlzc2lvbiI6Ik
    EXAMPLE766e8f6b115d93d41df2eac420aa4a465d177c1398bc6a088c76b7002
amzn-s3-demo-bucket1    example-object-4    EXAMPLEDC8l.XJCENlF7LePaNIIvs004    TRUE
      100    2021-02-15T15:28:27.000Z    EXAMPLE21e1518b92f3d92773570f603    STANDARD
  FALSE    COMPLETED    SSE-KMS    2025-01-25T15:28:26.000Z    COMPLIANCE    Off
 ENABLED
 eyJ2ZXJzaW9uIjoiMjAyMi0xMS0xMCIsInN0YXR1cyI6IkFWQUlMQUJMRSIsImdyYW50cyI6W3sicGVybWlzc2lvbiI6Ik
    EXAMPLE766e8f6b115d93d41df2eac420aa4a465d177c1398bc6a088c76b7003
```

Recomendamos que você crie uma política de ciclo de vida que exclua listas de inventário antigas. Para obter mais informações, consulte Gerenciar o ciclo de vida dos objetos.

Com `s3:PutInventoryConfiguration`, o usuário tem permissão para selecionar todos os campos de metadados listados anteriormente para cada objeto ao configurar uma lista de inventário e especificar o bucket de destino para armazenar o inventário. Um usuário com acesso de leitura aos objetos no bucket de destino pode acessar todos os campos de metadados do objeto que estão disponíveis na lista de inventário. Para restringir o acesso a um relatório de inventário, consulte Conceder permissões para o Inventário do S3 e análises do S3.

Consistência de inventário

Todos os seus objetos podem não aparecer em cada lista de inventários. A lista de inventários fornece uma consistência eventual para solicitações PUT (de objetos novos e substituídos) e para solicitações `DELETE`. Cada lista de inventário de um bucket é um snapshot dos itens do bucket.

Essas listas acabam sendo consistentes (ou seja, uma lista pode não incluir objetos adicionados ou excluídos recentemente).

Para validar o estado de um objeto antes de você realizar uma ação no objeto, recomendamos que faça uma solicitação `HeadObject` da API REST para recuperar metadados do objeto ou verifique suas propriedades no console do Amazon S3. Você também pode verificar metadados do objeto com a AWS CLI ou os AWS SDKs. Para obter mais informações, consulte `HeadObject` na Referência da API do Amazon Simple Storage Service.

Para obter mais informações sobre como trabalhar com o Amazon S3 Inventory, consulte os tópicos a seguir.

Tópicos

- Configurar o inventário do Amazon S3
- Localização de lista de inventário
- Configuração de notificações de eventos do Amazon S3 para conclusão de inventário
- Consulta do Amazon S3 Inventory com o Amazon Athena
- Converter strings de ID de versão vazias nos relatórios do Amazon S3 Inventory em cadeias de caracteres null
- Trabalhar com o campo ACL de objetos

Configurar o inventário do Amazon S3

O Amazon S3 Inventory oferece uma lista de arquivos sem formatação de seus objetos e metadados, de acordo com um agendamento que você define. Você pode usar o Amazon S3 Inventory como uma alternativa agendada para a operação `List` da API síncrona. O S3 Inventory fornece arquivos de saída no formato de valores separados por vírgulas (CSV), em colunas de linhas otimizados para Apache (ORC) ou Apache Parquet (Parquet), que listam seus objetos e os metadados correspondentes.

É possível configurar o S3 Inventory para criar listas de inventário, diária ou semanalmente, para um bucket do S3 ou para os objetos que compartilham um prefixo (objetos com nomes que começam com a mesma string). Para obter mais informações, consulte Catalogar e analisar seus dados com o Inventário S3.

Esta seção descreve como configurar um inventário, incluindo detalhes sobre seus buckets de origem e destino do inventário.

Tópicos

- Visão geral
- Criação de uma política de bucket de destino
- Conceder permissão para que o Amazon S3 use a sua chave gerenciada pelo cliente para criptografia
- Configurar um inventário usando o console do S3
- Usar a API REST para trabalhar com o Inventário S3

Visão geral

O Amazon S3 Inventory ajuda você a gerenciar seu armazenamento, criando listas dos objetos em um bucket do S3 em uma programação definida. Você pode configurar várias listas de inventário para um bucket. As listas de inventários são publicadas em arquivos CSV, ORC ou Parquet em um bucket de destino.

A maneira mais fácil de configurar um inventário é usando o console do Amazon S3, mas você também pode usar a API REST do Amazon S3, a AWS Command Line Interface (AWS CLI) ou SDKs da AWS. O console realiza a primeira etapa do procedimento a seguir para você: adicionar uma política de bucket ao bucket de destino.

Para configurar o Amazon S3 nventory para um bucket do S3

1. Adicionar uma política do bucket para o bucket de destino.

   É necessário criar uma política de bucket no bucket de destino que conceda permissões ao Amazon S3 para gravar objetos no bucket no local definido. Para ver um exemplo de política, consulte Conceder permissões para o Inventário do S3 e análises do S3.
2. Configurar um inventário para relacionar objetos em um bucket de origem e publicar a lista em um bucket de destino.

   Ao configurar uma lista de inventários para um bucket de origem, você especifica o bucket de destino no qual deseja que a lista seja armazenada e se quer gerar a lista diária ou semanalmente. Você também pode configurar se devem ser listadas todas as versões de objetos ou somente as versões atuais e quais metadados de objetos devem ser incluídos.

   Alguns campos de metadados de objetos nas configurações de relatório do Inventário S3 são opcionais, o que significa que estão disponíveis por padrão, mas podem ser restritos quando você

concede a permissão `s3:PutInventoryConfiguration` a um usuário. É possível controlar se os usuários podem incluir esses campos de metadados opcionais em seus relatórios usando a chave de condição `s3:InventoryAccessibleOptionalFields`.

Consulte mais informações sobre os campos de metadados opcionais disponíveis no Inventário S3 em OptionalFields na Referência de API do Amazon Simple Storage Service. Consulte mais informações sobre como restringir o acesso a certos campos de metadados opcionais em uma configuração de inventário em Controlar a criação da configuração de relatórios do Inventário S3.

É possível especificar que o arquivo da lista de inventário seja criptografado usando a criptografia do lado do servidor com uma chave gerenciada do Amazon S3 (SSE-S3) ou uma chave gerenciada pelo cliente do AWS Key Management Service (AWS KMS) (SSE-KMS).

> **Note**
>
> A Chave gerenciada pela AWS (`aws/s3`) não é compatível com a criptografia SSE-KMS com o S3 Inventory.

Para obter mais informações sobre SSE-S3 e SSE-KMS, consulte Proteger os dados usando criptografia do lado do servidor. Se você pretende usar a criptografia de SSE-KMS, consulte a Etapa 3.

- Para obter informações sobre como usar o console para configurar uma lista de inventário, consulte Configurar um inventário usando o console do S3.
- Para usar a API do Amazon S3 para configurar uma lista de inventários, use a operação da API REST PutBucketInventoryConfiguration ou o equivalente pela AWS CLI ou por AWS SDKs.

3. Para criptografar o arquivo da lista de inventários com o SSE-KMS, conceda permissão para que o Amazon S3 use a AWS KMS key.

   Você pode configurar a criptografia do arquivo da lista de inventários usando o console do Amazon S3, a API REST do Amazon S3 a AWS CLI ou SDKs da AWS. Independentemente do que você escolher, é necessário conceder permissão para que o Amazon S3 use a chave gerenciada pelo cliente para criptografar o arquivo de inventário. Conceda permissão ao Amazon S3 modificando a política de chave da chave gerenciada pelo cliente que você deseja usar para criptografar o arquivo de inventário. Para obter mais informações, consulte Conceder permissão para que o Amazon S3 use a sua chave gerenciada pelo cliente para criptografia.

O bucket de destino que armazena o arquivo da lista de inventário pode ser de propriedade de uma Conta da AWS diferente da conta que possui o bucket de origem. Se você usa a criptografia SSE-KMS para as operações entre contas do Inventário Amazon S3, recomendamos usar um ARN de chave do KMS totalmente qualificado ao configurar o Inventário S3. Para obter mais informações, consulte Usar criptografia SSE-KMS para operações entre contas e ServerSideEncryptionByDefault na Referência da API do Amazon Simple Storage Service.

Criação de uma política de bucket de destino

Se você criar a configuração de inventário pelo console do Amazon S3, o Amazon S3 criará automaticamente uma política de bucket no bucket de destino que concede ao Amazon S3 permissão de gravação para o bucket. No entanto, se você criar a configuração de inventário pela AWS CLI, por SDKs da AWS ou pela API REST do Amazon S3, será necessário adicionar manualmente uma política de bucket no bucket de destino. A política do bucket de destino do Inventário S3 permite que o Amazon S3 grave dados para os relatórios de inventário no bucket.

Veja a seguir um exemplo de política de bucket.

```
{
      "Version": "2012-10-17",
      "Statement": [
        {
            "Sid": "InventoryExamplePolicy",
            "Effect": "Allow",
            "Principal": {
                "Service": "s3.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": [
                "arn:aws:s3:::DOC-EXAMPLE-DESTINATION-BUCKET/*"
            ],
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:s3:::DOC-EXAMPLE-SOURCE-BUCKET"
                },
                "StringEquals": {
                    "aws:SourceAccount": "source-account-id",
                    "s3:x-amz-acl": "bucket-owner-full-control"
                }
```

```
            }
        }
    ]
}
```

Para obter mais informações, consulte Conceder permissões para o Inventário do S3 e análises do S3.

Se ocorrer um erro quando você tentar criar a política do bucket, você receberá instruções sobre como corrigi-lo. Por exemplo, se você escolher um bucket de destino em outra Conta da AWS e não tiver as permissões para ler e gravar na política do bucket, você verá uma mensagem de erro.

Nesse caso, o proprietário do bucket de destino deve adicionar a política do bucket ao bucket de destino. Se a política não for adicionada ao bucket de destino, você não terá um relatório de inventário, pois o Amazon S3 não tem permissão para gravar no bucket de destino. Se o bucket de origem pertencer a outra conta que não seja a do usuário atual, o ID de conta correto do bucket de origem deverá ser substituído na política.

> **Note**
>
> Garanta que não haja declarações de negação adicionadas à política de bucket de destino que impeçam a entrega de relatórios de inventário nesse bucket. Para ter mais informações, consulte Não consigo gerar um relatório de inventário do Amazon S3. Por que isto está acontecendo? .

Conceder permissão para que o Amazon S3 use a sua chave gerenciada pelo cliente para criptografia

Para conceder permissão para que o Amazon S3 use sua chave gerenciada pelo cliente do AWS Key Management Service (AWS KMS) para criptografia no lado do servidor, é necessário usar uma política de chave. Para atualizar sua política de chaves para que você possa usar uma chave gerenciada pelo cliente, siga este procedimento.

Como conceder permissões ao Amazon S3 para criptografia usando a chave gerenciada pelo cliente

1. Usando a Conta da AWS proprietária da chave gerenciada pelo cliente, faça login no AWS Management Console.
2. Abra o console do AWS KMS em https://console.aws.amazon.com/kms.

3. Para alterar o Região da AWS, use o seletor de Região no canto superior direito da página.
4. No painel de navegação esquerdo, escolha Customer managed keys (Chaves gerenciadas pelo cliente).
5. Em Chaves gerenciadas pelo cliente, selecione a chave gerenciada pelo cliente que você deseja usar para criptografar os arquivos de inventário.
6. Na seção Key Policy (Política de chaves), selecione Switch to policy view (Alternar para a visualização da política).
7. Para atualizar a política de chave, escolha Edit (Editar).
8. Na página Editar a política de chaves, adicione as seguintes linhas à política de chave existente. Para *source-account-id* e *amzn-s3-demo-source-bucket*, forneça os valores apropriados para seu caso de uso.

```
{
    "Sid": "Allow Amazon S3 use of the customer managed key",
    "Effect": "Allow",
    "Principal": {
        "Service": "s3.amazonaws.com"
    },
    "Action": [
        "kms:GenerateDataKey"
    ],
    "Resource": "*",
    "Condition":{
      "StringEquals":{
         "aws:SourceAccount":"source-account-id"
     },
      "ArnLike":{
        "aws:SourceARN": "arn:aws:s3:::amzn-s3-demo-source-bucket"
     }
   }
}
```

9. Escolha Salvar alterações.

Para obter mais informações sobre como criar chaves gerenciadas pelo cliente e usar políticas de chaves, consulte os links a seguir no Guia do desenvolvedor do AWS Key Management Service:

- Managing keys
- Key policies in AWS KMS

> **Note**
>
> Garanta que não haja declarações de negação adicionadas à política de bucket de destino que impeçam a entrega de relatórios de inventário nesse bucket. Para ter mais informações, consulte Não consigo gerar um relatório de inventário do Amazon S3. Por que isto está acontecendo? .

Configurar um inventário usando o console do S3

Use estas instruções para configurar o inventário usando o console do S3.

> **Note**
>
> Pode levar até 48 horas para o Amazon S3 entregar o primeiro relatório de inventário.

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets de uso geral.
3. Na lista de buckets, escolha o nome do bucket para o qual deseja configurar a funcionalidade Inventário Amazon S3.
4. Escolha a guia Management.
5. Em Inventory configurations (Configurações de inventário), escolha Create inventory configuration (Criar configuração de inventário).
6. Em Nome da configuração do inventário, insira um nome.
7. Em Escopo de inventário, faça o seguinte:
   - Insira um prefixo opcional.
   - Escolha quais versões de objeto incluir, Somente versões atuais ou Incluir todas as versões.
8. Em Report details (Detalhes do relatório), escolha o local da Conta da AWS em que deseja salvar os relatórios: This account (Esta conta) ou A different account (Uma conta diferente).
9. Em Destino, selecione o bucket de destino no qual deseja salvar os relatórios de inventário.

   O bucket de destino deve estar na mesma Região da AWS que o bucket para o qual você está configurando o inventário. O bucket de destino pode estar em uma Conta da AWS diferente. Ao

especificar o bucket de destino, você também pode incluir um prefixo opcional para agrupar os relatórios de inventário.

No campo de bucket Destino, você verá a declaração Permissão do bucket de destino que é adicionada à política de bucket de destino para permitir que o Amazon S3 coloque dados nesse bucket. Para obter mais informações, consulte Criação de uma política de bucket de destino.

10. Em Frequência, escolha a frequência com que o relatório será gerado, Diário ou Semanal.
11. Em Formato da saída, escolha um dos seguintes formatos para o relatório:

    - CSV: se você planeja usar esse relatório de inventário com as Operações em Lote do S3 ou se quiser analisar esse relatório em outra ferramenta, como o Microsoft Excel, escolha CSV.
    - Apache ORC
    - Apache Parquet
12. Em Status, escolha Enable (Ativar) ou Disable (Desabilitar).
13. Para configurar a criptografia no lado do servidor, em Criptografia de relatório do Inventory, siga estas etapas:

    a. Em Criptografia do lado do servidor, selecione Não especificar uma chave de criptografia ou Especificar uma chave de criptografia para criptografar dados.

    - Para manter as configurações de bucket para a criptografia padrão de objetos no lado do servidor ao armazená-los no Amazon S3, selecione Não especificar uma chave de criptografia. Desde que o destino do bucket tenha o recurso de chaves de bucket do S3 ativado, a operação de cópia aplicará uma chave de bucket do S3 ao bucket de destino.

    > **Note**
    >
    > Se a política de bucket para o destino especificado exigir que os objetos sejam criptografados antes de armazená-los no Amazon S3, você deverá escolher Especificar uma chave de criptografia. Caso contrário, ocorrerá uma falha na cópia de objetos no destino.

    - Para criptografar objetos antes de armazená-los no Amazon S3, selecione Especificar uma chave de criptografia.

    b. Se você escolheu Especificar uma chave de criptografia, em Tipo de criptografia, é necessário selecionar Chave gerenciada pelo Amazon S3 (SSE-S3) ou Chave do AWS Key Management Service (SSE-KMS).

A SSE-S3 usa uma das criptografias de bloco mais fortes: o padrão de criptografia avançada de 256 bits (AES-256) para criptografar cada objeto. A SSE-KMS oferece mais controle sobre sua chave. Para ter mais informações sobre SSE-S3, consulte Usar a criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3). Para obter mais informações sobre SSE-KMS, consulte Usar criptografia do lado do servidor com o AWS KMS (SSE-KMS).

> **Note**
>
> Para criptografar o arquivo da lista de inventário com a SSE-KMS, conceda permissão para que o Amazon S3 use a chave gerenciada pelo cliente. Para obter instruções, consulte Conceder permissão para o Amazon S3 criptografar usando chaves do KMS.

c. Se você escolheu chave do AWS Key Management Service (SSE-KMS), em AWS KMS key, poderá especificar a chave do AWS KMS por meio de uma das opções a seguir.

> **Note**
>
> Se o bucket de destino que armazena o arquivo da lista de inventários pertencer a outra Conta da AWS, use um ARN de chave do KMS totalmente qualificado para especificar a chave do KMS.

- Para fazer sua escolha em uma lista de chaves do KMS disponíveis, selecione Escolha entre suas chaves do AWS KMS e escolha uma chave do KMS de criptografia simétrica na lista de chaves disponíveis. Verifique se a chave do KMS está na mesma região do bucket.

  > **Note**
  >
  > A Chave gerenciada pela AWS (`aws/s3`) e as chaves gerenciadas pelo cliente são exibidas na lista. No entanto, a Chave gerenciada pela AWS (`aws/s3`) não é compatível com a criptografia SSE-KMS com o S3 Inventory.

- Para inserir o ARN da chave do KMS, selecione Inserir ARN da chave do AWS KMS e insira o ARN da chave do KMS no campo exibido.

- Para criar uma chave gerenciada pelo cliente no console do AWS KMS, selecione Criar uma chave do KMS.

14. Em Campos adicionais de metadados, selecione um ou mais dos seguintes campos para adicionar ao relatório de inventário:

- Tamanho: o tamanho do objeto em bytes, sem incluir o tamanho de uploads incompletos de várias partes, metadados de objetos e marcadores de exclusão.
- Last modified date (Data da última modificação) – a data de criação do objeto ou data da última modificação, a mais atual entre as duas.
- Multipart upload – especifica se o objeto foi carregado como um multipart upload. Para obter mais informações, consulte Carregar e copiar objetos usando upload fracionado no Amazon S3.
- Replication status (Status da replicação) – o status de replicação do objeto. Para obter mais informações, consulte Obtenção de informações sobre o status da replicação.
- Status da criptografia: o tipo da criptografia do lado do servidor usada para criptografar o objeto. Para obter mais informações, consulte Proteger os dados usando criptografia do lado do servidor.
- Status da chave de bucket: indica se uma chave no nível do bucket gerada pelo AWS KMS se aplica ao objeto. Para obter mais informações, consulte Redução do custo do SSE-KMS com chaves de bucket do Amazon S3.
- Lista de controle de acesso de objetos: uma lista de controle de acesso (ACL) para cada objeto que define quais Contas da AWS ou grupos recebem acesso a esse objeto e o tipo de acesso concedido. Para obter mais informações sobre esse campo, consulte Trabalhar com o campo ACL de objetos. Para obter mais informações sobre ACLs, consulte Visão geral da lista de controle de acesso (ACL).
- Proprietário do objeto: o dono do objeto.
- Classe de armazenamento: a classe de armazenamento usada para armazenar o objeto.
- Intelligent Tiering: nível de acesso: indica o nível de acesso (frequente ou infrequente) do objeto se armazenado na classe de armazenamento S3 Intelligent-Tiering. Para obter mais informações, consulte Classe de armazenamento para otimizar automaticamente dados com padrões de acesso alterados ou desconhecidos.
- ETag: a tag de entidade (ETag) é um hash do objeto. O ETag reflete as alterações apenas no conteúdo de um objeto, não em seus metadados. O ETag pode ou não ser um digest MD5 do objeto de dados. Tudo depende de como o objeto foi criado e de como está criptografado.

Para obter mais informações, consulte Object na Referência da API do Amazon Simple Storage Service.

- Algoritmo de soma de verificação: indica o algoritmo usado para criar a soma de verificação do objeto. Para obter mais informações, consulte Usar algoritmos de soma de verificação compatíveis.
- Todas as configurações de bloqueio de objetos: o status do bloqueio de objetos, incluindo as seguintes configurações:
  - Bloqueio de objetos: modo de retenção: o nível de proteção aplicado ao objeto, Governança ou Conformidade.
  - Bloqueio de objetos: prazo de retenção: a data até a qual o objeto bloqueado não pode ser excluído.
  - Bloqueio de objetos: status da retenção jurídica: o status de retenção jurídica do objeto bloqueado.

  Para obter mais informações sobre bloqueio de objetos do S3, consulte Como o bloqueio de objetos do S3 funciona.

Para obter mais informações sobre o conteúdo de um relatório de inventário, consulte Lista do Amazon S3 Inventory.

Consulte mais informações sobre como restringir o acesso a certos campos de metadados opcionais em uma configuração de inventário em Controlar a criação da configuração de relatórios do Inventário S3.

15. Escolha Criar.

Usar a API REST para trabalhar com o Inventário S3

Veja a seguir as operações REST que você pode usar para trabalhar com o Inventário Amazon S3.

- DeleteBucketInventoryConfiguration
- GetBucketInventoryConfiguration
- ListBucketInventoryConfigurations
- PutBucketInventoryConfiguration

Localização de lista de inventário

Quando uma lista de inventários é publicada, os arquivos manifestos são publicados no seguinte local no bucket de destino.

```
destination-prefix/amzn-s3-demo-source-bucket/config-ID/YYYY-MM-DDTHH-MMZ/manifest.json
 destination-prefix/amzn-s3-demo-source-bucket/config-ID/YYYY-MM-DDTHH-MMZ/
manifest.checksum
 destination-prefix/amzn-s3-demo-source-bucket/config-ID/hive/dt=YYYY-MM-DD-HH-MM/
symlink.txt
```

- *destination-prefix* é o prefixo do nome da chave do objeto que é especificado opcionalmente na configuração do inventário. É possível usar esse prefixo para agrupar todos os arquivos da lista de inventários em um local comum no bucket de destino.
- *amzn-s3-demo-source-bucket* é o bucket de origem ao qual a lista de inventário se refere. O nome do bucket de origem é adicionado para evitar colisões quando vários relatórios do inventário de diferentes buckets de origem são enviados ao mesmo bucket de destino.
- O *config-ID* é adicionado para evitar colisões com vários relatórios do inventário do mesmo bucket de origem que são enviados ao mesmo bucket de destino. O *config-ID* vem da configuração do relatório de inventário e é o nome do relatório definido durante a configuração.
- *YYYY-MM-DDTHH-MMZ* é o carimbo de data/hora que consiste na data e hora de início em que o processo de geração do relatório de inventário começa a verificar o bucket. Por exemplo, `2016-11-06T21-32Z`.
- `manifest.json` é o arquivo manifesto.
- `manifest.checksum` é o hash MD5 do conteúdo do arquivo `manifest.json`.
- `symlink.txt` é o arquivo de manifesto compatível com o Apache Hive.

As listas de inventários são publicadas diária ou semanalmente no seguinte local do bucket de destino.

```
destination-prefix/amzn-s3-demo-source-bucket/config-ID/data/example-file-name.csv.gz
...
destination-prefix/amzn-s3-demo-source-bucket/config-ID/data/example-file-name-1.csv.gz
```

- *destination-prefix* é o prefixo do nome da chave do objeto que é especificado opcionalmente na configuração do inventário. É possível usar esse prefixo para agrupar todos os arquivos da lista de inventários em um local comum no bucket de destino.
- *amzn-s3-demo-source-bucket* é o bucket de origem ao qual a lista de inventário se refere. O nome do bucket de origem é adicionado para evitar colisões quando vários relatórios do inventário de diferentes buckets de origem são enviados ao mesmo bucket de destino.
- *example-file-name*`.csv.gz` é um dos arquivos de inventário em formato CSV. Os nomes de inventário ORC terminam com a extensão do nome do arquivo `.orc`, e os nomes de inventário do Parquet terminam com a extensão de nome de arquivo `.parquet`.

Manifesto de inventário

Os arquivos manifestos `manifest.json` e `symlink.txt` descrevem onde os arquivos de inventário estão localizados. Sempre que uma nova lista de inventários é entregue, um novo conjunto de arquivos manifestos a acompanha. Esses arquivos podem se sobrepor. Em buckets habilitados para versionamento, o Amazon S3 cria versões dos arquivos de manifesto.

Cada manifesto contido no arquivo `manifest.json` fornece metadados e outras informações básicas sobre um inventário. Essas informações incluem:

- O nome do bucket de origem
- O nome do bucket de destino
- A versão do inventário
- O carimbo de data/hora de criação no formato de data de referência (epoch) que consiste na hora de início e na data em que o processo de geração do relatório de inventário começa a verificar o bucket
- O formato e o esquema de arquivos de inventário
- Uma lista dos arquivos de inventário que estão no bucket de destino

Sempre que um arquivo `manifest.json` é gravado, ele é acompanhado por um arquivo `manifest.checksum`, que representa o hash MD5 do conteúdo do arquivo `manifest.json`.

Example Manifesto de inventário em um arquivo **`manifest.json`**

Os exemplos a seguir mostram um manifesto de inventário em um arquivo `manifest.json` para inventários nos formatos CSV, ORC e Parquet.

CSV

Veja a seguir um exemplo de manifesto em um arquivo `manifest.json` para um inventário em formato CSV.

```
{
    "sourceBucket": "amzn-s3-demo-source-bucket",
    "destinationBucket": "arn:aws:s3:::example-inventory-destination-bucket",
    "version": "2016-11-30",
    "creationTimestamp" : "1514944800000",
    "fileFormat": "CSV",
    "fileSchema": "Bucket, Key, VersionId, IsLatest, IsDeleteMarker,
 Size, LastModifiedDate, ETag, StorageClass, IsMultipartUploaded,
 ReplicationStatus, EncryptionStatus, ObjectLockRetainUntilDate, ObjectLockMode,
 ObjectLockLegalHoldStatus, IntelligentTieringAccessTier, BucketKeyStatus,
 ChecksumAlgorithm, ObjectAccessControlList, ObjectOwner",
    "files": [
        {
            "key": "Inventory/amzn-s3-demo-source-bucket/2016-11-06T21-32Z/
files/939c6d46-85a9-4ba8-87bd-9db705a579ce.csv.gz",
            "size": 2147483647,
            "MD5checksum": "f11166069f1990abeb9c97ace9cdfabc"
        }
    ]
}
```

ORC

Veja a seguir um exemplo de manifesto em um arquivo `manifest.json` para um inventário em formato ORC.

```
{
    "sourceBucket": "amzn-s3-demo-source-bucket",
    "destinationBucket": "arn:aws:s3:::example-destination-bucket",
    "version": "2016-11-30",
    "creationTimestamp" : "1514944800000",
    "fileFormat": "ORC",
    "fileSchema":
 "struct<bucket:string,key:string,version_id:string,is_latest:boolean,is_delete_marker:boole
    "files": [
        {
            "key": "inventory/amzn-s3-demo-source-bucket/data/
d794c570-95bb-4271-9128-26023c8b4900.orc",
```

```
            "size": 56291,
            "MD5checksum": "5925f4e78e1695c2d020b9f6eexample"
        }
    ]
}
```

Parquet

Veja a seguir um exemplo de manifesto em um arquivo `manifest.json` para um inventário em formato Parquet.

```
{
    "sourceBucket": "amzn-s3-demo-source-bucket",
    "destinationBucket": "arn:aws:s3:::example-destination-bucket",
    "version": "2016-11-30",
    "creationTimestamp" : "1514944800000",
    "fileFormat": "Parquet",
    "fileSchema": "message s3.inventory { required binary bucket (UTF8);
 required binary key (UTF8); optional binary version_id (UTF8); optional boolean
 is_latest; optional boolean is_delete_marker; optional int64 size; optional
 int64 last_modified_date (TIMESTAMP_MILLIS); optional binary e_tag (UTF8);
 optional binary storage_class (UTF8); optional boolean is_multipart_uploaded;
 optional binary replication_status (UTF8); optional binary encryption_status
 (UTF8); optional int64 object_lock_retain_until_date (TIMESTAMP_MILLIS); optional
 binary object_lock_mode (UTF8); optional binary object_lock_legal_hold_status
 (UTF8); optional binary intelligent_tiering_access_tier (UTF8); optional binary
 bucket_key_status (UTF8); optional binary checksum_algorithm (UTF8); optional
 binary object_access_control_list (UTF8); optional binary object_owner (UTF8);}",
    "files": [
        {
           "key": "inventory/amzn-s3-demo-source-bucket/data/
d754c470-85bb-4255-9218-47023c8b4910.parquet",
            "size": 56291,
            "MD5checksum": "5825f2e18e1695c2d030b9f6eexample"
        }
    ]
}
```

O `symlink.txt` é um arquivo manifesto compatível com o Apache Hive permitindo que o Hive detecte automaticamente arquivos de inventário e os arquivos de dados associados. O manifesto compatível com o Hive funciona com os serviços compatíveis com o Hive, o Athena

e o Amazon Redshift Spectrum. Ele também funciona com aplicações compatíveis com o Hive, incluindo Presto, Apache Hive, Apache Spark e muitos outros.

> **Important**
>
> O arquivo manifesto `symlink.txt` compatível com Apache Hive atualmente não funciona com o AWS Glue.
> Ler o arquivo `symlink.txt` com Apache Hive e Apache Spark não é compatível com arquivos de inventário no formato Parquet e ORC.

Configuração de notificações de eventos do Amazon S3 para conclusão de inventário

É possível configurar uma notificação de evento do Amazon S3 para receber um aviso quando o arquivo de soma de verificação do manifesto for criado, o que indica que uma lista de inventários foi adicionada ao bucket de destino. O manifesto é uma lista atualizada de todas as listas de inventário no local de destino.

O Amazon S3 pode publicar eventos em um tópico do Amazon Simple Notification Service (Amazon SNS), em uma fila do Amazon Simple Queue Service (Amazon SQS) ou em uma função do AWS Lambda. Para obter mais informações, consulte Notificações de eventos do Amazon S3.

A configuração de notificação a seguir define que todos os arquivos `manifest.checksum` recém-adicionados ao bucket de destino são processados pela AWS Lambda do `cloud-function-list-write`.

```
<NotificationConfiguration>
  <QueueConfiguration>
      <Id>1</Id>
      <Filter>
          <S3Key>
              <FilterRule>
                  <Name>prefix</Name>
                  <Value>destination-prefix/source-bucket</Value>
              </FilterRule>
              <FilterRule>
                  <Name>suffix</Name>
                  <Value>checksum</Value>
              </FilterRule>
```

```
          </S3Key>
      </Filter>
      <CloudFunction>arn:aws:lambda:us-west-2:222233334444:cloud-function-list-write</
CloudFunction>
      <Event>s3:ObjectCreated:*</Event>
    </QueueConfiguration>
    </NotificationConfiguration>
```

Para obter mais informações, consulte Uso do AWS Lambda com o Amazon S3 no Guia do desenvolvedor do AWS Lambda.

Consulta do Amazon S3 Inventory com o Amazon Athena

É possível consultar arquivos do Inventário Amazon S3 com consultas SQL padrão usando o Amazon Athena em todas as regiões onde o Athena esteja disponível. Para verificar a disponibilidade da Região da AWS, consulte a Tabela de Região da AWS.

O Athena pode consultar arquivos do Inventário Amazon S3 no formato colunar de linhas otimizado (ORC) do Apache, Apache Parquet ou valores separados por vírgula (CSV). Quando você usar o Athena para consultar arquivos de inventário, use arquivos de inventário no formato ORC ou Parquet. Os formatos ORC e Parquet têm uma performance de consulta mais rápida e custos mais baixos de consulta. ORC e Parquet são formatos de arquivo colunares do tipo autodescritivo projetados para o Apache Hadoop. O formato colunar permite que o leitor leia, descompacte e processe apenas as colunas necessárias para a consulta atual. Os formatos ORC e Parquet para o Inventário Amazon S3 estão disponíveis em todas as Regiões da AWS.

Para usar o Athena para consultar arquivos do Inventário Amazon S3

1. Crie uma tabela do Athena. Para obter informações sobre como criar uma tabela, consulte Criar tabelas no Amazon Athena no Guia do usuário do Amazon Athena.
2. Crie sua consulta usando um dos exemplos de modelos de consulta a seguir, dependendo se você está consultando um relatório de inventário no formato ORC, Parquet ou CSV.

   - Ao usar o Athena para consultar um relatório de inventário no formato ORC, use o exemplo de consulta a seguir como modelo.

     O exemplo de consulta a seguir inclui todos os campos opcionais no relatório de inventário no formato ORC.

     Para usar esse exemplo de consulta, faça o seguinte:

- Substitua *your_table_name* pelo nome da tabela do Athena que você criou.
- Remova todos os campos opcionais que você não selecionou no inventário para que a consulta corresponda aos campos escolhidos.
- Substitua o nome do bucket a seguir e o local do inventário (o ID de configuração) conforme apropriado para sua configuração.

  `s3://`*amzn-s3-demo-bucket*`/`*config-ID*`/hive/`
- Substitua a data *2022-01-01-00-00* abaixo de `projection.dt.range` com o primeiro dia do intervalo de tempo em que você particiona os dados no Athena. Para obter mais informações, consulte Particionamento de dados no Athena.

```
CREATE EXTERNAL TABLE your_table_name(
         bucket string,
         key string,
         version_id string,
         is_latest boolean,
         is_delete_marker boolean,
         size bigint,
         last_modified_date timestamp,
         e_tag string,
         storage_class string,
         is_multipart_uploaded boolean,
         replication_status string,
         encryption_status string,
         object_lock_retain_until_date bigint,
         object_lock_mode string,
         object_lock_legal_hold_status string,
         intelligent_tiering_access_tier string,
         bucket_key_status string,
         checksum_algorithm string,
         object_access_control_list string,
         object_owner string
) PARTITIONED BY (
        dt string
)
ROW FORMAT SERDE 'org.apache.hadoop.hive.ql.io.orc.OrcSerde'
  STORED AS INPUTFORMAT 'org.apache.hadoop.hive.ql.io.SymlinkTextInputFormat'
  OUTPUTFORMAT 'org.apache.hadoop.hive.ql.io.IgnoreKeyTextOutputFormat'
  LOCATION 's3://source-bucket/config-ID/hive/'
  TBLPROPERTIES (
    "projection.enabled" = "true",
```

```
    "projection.dt.type" = "date",
    "projection.dt.format" = "yyyy-MM-dd-HH-mm",
    "projection.dt.range" = "2022-01-01-00-00,NOW",
    "projection.dt.interval" = "1",
    "projection.dt.interval.unit" = "HOURS"
  );
```

- Ao usar o Athena para consultar um relatório de inventário no formato Parquet, use a consulta de amostra para um relatório no formato ORC. No entanto, use o seguinte Parquet SerDe no lugar do ORC SerDe na declaração `ROW FORMAT SERDE`.

```
ROW FORMAT SERDE 'org.apache.hadoop.hive.ql.io.parquet.serde.ParquetHiveSerDe'
```

- Ao usar o Athena para consultar um relatório de inventário no formato CSV, use o exemplo de consulta a seguir como modelo.

  O exemplo de consulta a seguir inclui todos os campos opcionais no relatório de inventário no formato CSV.

  Para usar esse exemplo de consulta, faça o seguinte:

  - Substitua *`your_table_name`* pelo nome da tabela do Athena que você criou.
  - Remova todos os campos opcionais que você não selecionou no inventário para que a consulta corresponda aos campos escolhidos.
  - Substitua o nome do bucket a seguir e o local do inventário (o ID de configuração) conforme apropriado para sua configuração.

    `s3://`*`amzn-s3-demo-bucket`*`/`*`config-ID`*`/hive/`
  - Substitua a data *`2022-01-01-00-00`* abaixo de `projection.dt.range` com o primeiro dia do intervalo de tempo em que você particiona os dados no Athena. Para obter mais informações, consulte Particionamento de dados no Athena.

```
CREATE EXTERNAL TABLE your_table_name(
         bucket string,
         key string,
         version_id string,
         is_latest boolean,
         is_delete_marker boolean,
         size string,
         last_modified_date string,
         e_tag string,
```

```
         storage_class string,
         is_multipart_uploaded boolean,
         replication_status string,
         encryption_status string,
         object_lock_retain_until_date string,
         object_lock_mode string,
         object_lock_legal_hold_status string,
         intelligent_tiering_access_tier string,
         bucket_key_status string,
         checksum_algorithm string,
         object_access_control_list string,
         object_owner string
) PARTITIONED BY (
        dt string
)
ROW FORMAT SERDE 'org.apache.hadoop.hive.serde2.OpenCSVSerde'
  STORED AS INPUTFORMAT 'org.apache.hadoop.hive.ql.io.SymlinkTextInputFormat'
  OUTPUTFORMAT 'org.apache.hadoop.hive.ql.io.IgnoreKeyTextOutputFormat'
  LOCATION 's3://source-bucket/config-ID/hive/'
  TBLPROPERTIES (
    "projection.enabled" = "true",
    "projection.dt.type" = "date",
    "projection.dt.format" = "yyyy-MM-dd-HH-mm",
    "projection.dt.range" = "2022-01-01-00-00,NOW",
    "projection.dt.interval" = "1",
    "projection.dt.interval.unit" = "HOURS"
  );
```

3. Agora você pode executar várias consultas no inventário, conforme mostrado nos exemplos a seguir. Substitua cada *user input placeholder* por suas próprias informações.

```
# Get a list of the latest inventory report dates available.
SELECT DISTINCT dt FROM your_table_name ORDER BY 1 DESC limit 10;

# Get the encryption status for a provided report date.
SELECT encryption_status, count(*) FROM your_table_name WHERE dt = 'YYYY-MM-DD-HH-
MM' GROUP BY encryption_status;

# Get the encryption status for inventory report dates in the provided range.
SELECT dt, encryption_status, count(*) FROM your_table_name
WHERE dt > 'YYYY-MM-DD-HH-MM' AND dt < 'YYYY-MM-DD-HH-MM' GROUP BY dt,
 encryption_status;
```

Quando você configura o Inventário S3 para adicionar o campo Lista de controle de acesso de objetos (ACL de objetos) a um relatório de inventário, o relatório exibe o valor do campo ACL de objetos como uma string codificada em base64. Para obter o valor decodificado em JSON para o campo ACL de objetos, você pode consultar esse campo usando o Athena. Veja os exemplos de consulta a seguir. Para obter mais informações sobre o campo ACL do objeto, consulte Trabalhar com o campo ACL de objetos.

```
# Get the S3 keys that have Object ACL grants with public access.
WITH grants AS (
    SELECT key,
        CAST(
            json_extract(from_utf8(from_base64(object_access_control_list)),
 '$.grants') AS ARRAY(MAP(VARCHAR, VARCHAR))
        ) AS grants_array
    FROM your_table_name
)
SELECT key,
       grants_array,
       grant
FROM grants, UNNEST(grants_array) AS t(grant)
WHERE element_at(grant, 'uri') = 'http://acs.amazonaws.com/groups/global/AllUsers'
```

```
# Get the S3 keys that have Object ACL grantees in addition to the object owner.
WITH grants AS
    (SELECT key,
    from_utf8(from_base64(object_access_control_list)) AS
 object_access_control_list,
         object_owner,
         CAST(json_extract(from_utf8(from_base64(object_access_control_list)),
         '$.grants') AS ARRAY(MAP(VARCHAR, VARCHAR))) AS grants_array
    FROM your_table_name)
SELECT key,
       grant,
       objectowner
FROM grants, UNNEST(grants_array) AS t(grant)
WHERE cardinality(grants_array) > 1 AND element_at(grant, 'canonicalId') !=
 object_owner;
```

```
# Get the S3 keys with READ permission that is granted in the Object ACL.
WITH grants AS (
    SELECT key,
        CAST(
            json_extract(from_utf8(from_base64(object_access_control_list)),
 '$.grants') AS ARRAY(MAP(VARCHAR, VARCHAR))
        ) AS grants_array
    FROM your_table_name
)
SELECT key,
       grants_array,
       grant
FROM grants, UNNEST(grants_array) AS t(grant)
WHERE element_at(grant, 'permission') = 'READ';
```

```
# Get the S3 keys that have Object ACL grants to a specific canonical user ID.
WITH grants AS (
    SELECT key,
        CAST(
            json_extract(from_utf8(from_base64(object_access_control_list)),
 '$.grants') AS ARRAY(MAP(VARCHAR, VARCHAR))
        ) AS grants_array
    FROM your_table_name
)
SELECT key,
       grants_array,
       grant
FROM grants, UNNEST(grants_array) AS t(grant)
WHERE element_at(grant, 'canonicalId') = 'user-canonical-id';
```

```
# Get the number of grantees on the Object ACL.
SELECT key,
       object_access_control_list,
       json_array_length(json_extract(object_access_control_list,'$.grants')) AS
 grants_count
FROM your_table_name;
```

Para obter mais informações sobre como usar o Athena, consulte o Guia do usuário do Amazon Athena.

Converter strings de ID de versão vazias nos relatórios do Amazon S3 Inventory em cadeias de caracteres null

> **Note**
>
> O procedimento a seguir se aplica somente aos relatórios do Amazon S3 Inventory que incluem todas as versões e somente se os relatórios “todas as versões” forem usados como manifestos para o S3 Batch Operations em buckets que têm o versionamento do S3 habilitado. Não é necessário converter strings para relatórios do S3 Inventory que especificam somente a versão atual.

Você pode usar relatórios do S3 Inventory como manifestos para o S3 Batch Operations. Porém, quando o versionamento S3 está habilitado em um bucket, os relatórios do S3 Inventory que incluem todas as versões marcam qualquer objeto com versionamento nulo com strings vazias no campo de ID da versão. Quando um relatório de inventário inclui todas as IDs de versão do objeto, o Batch Operations reconhece strings `null` como IDs de versão, mas não strings vazias.

Quando um trabalho do S3 Batch Operations usa um relatório “all versions” (todas as versões) do S3 Inventory como manifesto, ele falha em todas as tarefas em objetos que têm uma string vazia no campo de ID da versão. Para converter cadeias de caracteres vazias no campo ID da versão do relatório do S3 Inventory para strings `null` do Batch Operations, use o procedimento a seguir.

Atualize um relatório do Amazon S3 Inventory para uso com o Batch Operations

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Navegue até o relatório do S3 Inventory. O relatório de inventário está localizado no bucket de destino especificado durante a configuração do relatório de inventário. Para obter mais informações sobre a localização de relatórios de inventário, consulte Localização de lista de inventário.
    a. Escolha o bucket de destino.
    b. Escolha a pasta . A pasta tem o nome do bucket de origem original.
    c. Escolha a pasta com o nome da configuração do inventário.

d. Marque a caixa de seleção ao lado da pasta chamada hive. Na parte superior da página, escolha Copy S3 URI (Copiar URI do S3) para copiar a URI do S3 para a pasta.

3. Abra o console do Amazon Athena em https://console.aws.amazon.com/athena/.

4. No editor de consultas, escolha Settings (Configurações) e escolha Manage (Gerenciar). Na página Manage settings (Gerenciar configurações), em Location of query result (Local do resultado da consulta), escolha um bucket do S3 para armazenar os resultados da consulta.

5. No editor de consultas, crie uma tabela do Athena para manter os dados no relatório de inventário usando o comando a seguir. Substitua *table_name* pelo nome de sua preferência, e na cláusula `LOCATION`, insira a URI do S3 que você copiou anteriormente. Em seguida, escolha Run (Executar) para executar a consulta.

```
CREATE EXTERNAL TABLE table_name(bucket string, key string,
 version_id string) PARTITIONED BY (dt string)ROW FORMAT SERDE
 'org.apache.hadoop.hive.serde2.OpenCSVSerde'STORED AS INPUTFORMAT
 'org.apache.hadoop.hive.ql.io.SymlinkTextInputFormat' OUTPUTFORMAT
 'org.apache.hadoop.hive.ql.io.IgnoreKeyTextOutputFormat' LOCATION 'Copied S3 URI';
```

6. Para limpar o editor de consultas, escolha Clear (Limpar). Então carregue o relatório de inventário na tabela usando o comando a seguir. Substitua *table_name* pelo que você escolheu na etapa anterior. Em seguida, escolha Run (Executar) para executar a consulta.

```
MSCK REPAIR TABLE table_name;
```

7. Para limpar o editor de consultas, escolha Clear (Limpar). Execute a seguinte consulta `SELECT` para recuperar todas as entradas no relatório de inventário original e substituir quaisquer IDs de versão vazias por strings `null`. Substitua *table_name* pelo que você escolheu anteriormente e substitua *YYYY-MM-DD-HH-MM* na cláusula `WHERE` pela data do relatório de inventário em que você deseja que essa ferramenta seja executada. Em seguida, escolha Run (Executar) para executar a consulta.

```
SELECT bucket as Bucket, key as Key, CASE WHEN version_id = '' THEN 'null' ELSE
 version_id END as VersionId FROM table_name WHERE dt = 'YYYY-MM-DD-HH-MM';
```

8. Retorne ao console do Amazon S3 (https://console.aws.amazon.com/s3/) e navegue até o bucket do S3 que você escolheu para Location of query result (Local do resultado da consulta) anteriormente. Dentro dele, deve haver uma série de pastas terminando com a data.

Por exemplo, você verá algo parecido com s3://*amzn-s3-demo-bucket*/*query-result-location*/Unsaved/2021/10/07/. Haverá arquivos `.csv` contendo os resultados da consulta `SELECT` que você executou.

Escolha o arquivo CSV com a data de modificação mais recente. Baixe esse arquivo na máquina local para a próxima etapa.

9. O arquivo CSV gerado contém uma linha de cabeçalho. Para usar esse arquivo CSV como entrada para um trabalho do S3 Batch Operations, é necessário remover a linha de cabeçalho, pois o Batch Operations não é compatível com linhas de cabeçalho em manifestos CSV.

   Para remover a linha do cabeçalho, execute um dos comandos a seguir no arquivo. Substitua *file.csv* pelo nome de seu arquivo CSV.

   Para máquinas macOS e Linux, execute o comando `tail` em uma janela Terminal.

   ```
   tail -n +2 file.csv > tmp.csv && mv tmp.csv file.csv
   ```

   Para máquinas Windows, execute o script a seguir em uma janela do Windows PowerShell. Substitua *File-location* pelo caminho do arquivo e *file.csv* pelo nome do arquivo.

   ```
   $ins = New-Object System.IO.StreamReader File-location\file.csv
   $outs = New-Object System.IO.StreamWriter File-location\temp.csv
   try {
       $skip = 0
       while ( !$ins.EndOfStream ) {
           $line = $ins.ReadLine();
           if ( $skip -ne 0 ) {
               $outs.WriteLine($line);
           } else {
               $skip = 1
           }
       }
   } finally {
       $outs.Close();
       $ins.Close();
   }
   Move-Item File-location\temp.csv File-location\file.csv -Force
   ```

10. Depois de remover a linha de cabeçalho do arquivo CSV, você estará pronto para usá-lo como manifesto em um trabalho do S3 Batch Operations. Carregue o arquivo CSV para um bucket do

S3 ou local de sua preferência e crie um trabalho do Batch Operations usando o arquivo CSV como manifesto.

Para obter mais informações sobre como criar um trabalho do Batch Operations, consulte Criar um trabalho de operações em lote do S3.

Trabalhar com o campo ACL de objetos

Um relatório do Inventário Amazon S3 contém uma lista dos objetos no bucket de origem do S3 e os metadados de cada objeto. O campo lista de controle de acesso (ACL) de objetos é um campo de metadados que está disponível no Inventário Amazon S3. Especificamente, o campo ACL de objetos contém a lista de controle de acesso (ACL) para cada objeto. A ACL de um objeto define quais Contas da AWS ou grupos recebem acesso a esse objeto e ao tipo de acesso concedido. Para obter mais informações, consulte Visão geral da lista de controle de acesso (ACL) e Lista do Amazon S3 Inventory.

O campo ACL de objetos nos relatórios do Inventário Amazon S3 é definido no formato JSON. Os dados JSON incluem os seguintes campos:

- `version`: a versão do formato do campo ACL de objetos nos relatórios de inventário. Está no formato de data `yyyy-mm-dd`.
- `status`: os valores possíveis são `AVAILABLE` ou `UNAVAILABLE` para indicar se uma ACL de objetos está disponível para um objeto. Quando o status da ACL de objetos é `UNAVAILABLE`, o valor do campo Proprietário do objeto no relatório de inventário também é `UNAVAILABLE`.
- `grants`: pares de concessão e permissão que listam o status da permissão de cada beneficiário da ACL de objetos. Os valores disponíveis para um beneficiário são `CanonicalUser` e `Group`. Para obter mais informações sobre os beneficiários, consulte Beneficiários em listas de controle de acesso.

  Para um beneficiário com o tipo `Group`, um par de concessão e permissão inclui os seguintes atributos:

  - `uri`: um grupo predefinido do Amazon S3.
  - `permission`: as permissões de ACL concedidas ao objeto. Para obter mais informações, consulte Permissões de ACL em um objeto.
  - `type`: o tipo `Group`, o que indica que o beneficiário é um grupo.

Para um beneficiário com o tipo `CanonicalUser`, um par de concessão e permissão inclui os seguintes atributos:

- `canonicalId`: uma forma ofuscada do ID da Conta da AWS. O ID de usuário canônico de uma Conta da AWS é específico dessa conta. Você pode recuperar o ID de usuário canônico. Para ter mais informações, consulte Find the canonical user ID for your Conta da AWS no Guia de referência de gerenciamento de contas da AWS.

  > **Note**
  >
  > Se um beneficiário em uma ACL for o endereço de e-mail de uma Conta da AWS, o Inventário S3 usa o `canonicalId` dessa Conta da AWS e o tipo `CanonicalUser` para especificar esse beneficiário. Para obter mais informações, consulte Beneficiários em listas de controle de acesso.

- `permission`: as permissões de ACL concedidas ao objeto. Para obter mais informações, consulte Permissões de ACL em um objeto.
- `type`: o tipo `CanonicalUser`, o que indica que o beneficiário é uma Conta da AWS.

O exemplo a seguir mostra os valores possíveis para o campo ACL de objetos no formato JSON:

```
{
    "version": "2022-11-10",
    "status": "AVAILABLE",
    "grants": [{
        "uri": "http://acs.amazonaws.com/groups/global/AllUsers",
        "permission": "READ",
        "type": "Group"
    }, {
        "canonicalId": "example-canonical-id",
        "permission": "FULL_CONTROL",
        "type": "CanonicalUser"
    }]
}
```

> **Note**
>
> O campo ACL de objetos é definido no formato JSON. Um relatório de inventário exibe o valor do campo ACL de objetos como uma string codificada em base64.

Por exemplo, suponha que você tenha o seguinte campo ACL de objetos no formato JSON:

```
{
        "version": "2022-11-10",
        "status": "AVAILABLE",
        "grants": [{
            "canonicalId": "example-canonical-user-ID",
            "type": "CanonicalUser",
            "permission": "READ"
        }]
}
```

O campo ACL de objetos é codificado e mostrado como a seguinte string codificada em base64:

```
eyJ2ZXJzaW9uIjoiMjAyMi0xMS0xMCIsInN0YXR1cyI6IkFWQUlMQUJMRSIsImdyYW50cyI6W3siY2Fub25pY2FsSW
```

Para obter o valor decodificado em JSON para o campo ACL de objetos, você pode consultar esse campo no Amazon Athena. Para obter exemplos de consultas, consulte Consulta do Amazon S3 Inventory com o Amazon Athena.

Padrões de design de melhores práticas: otimização do desempenho do Amazon S3

As aplicações podem executar facilmente milhares de transações por segundo em performance de solicitação ao fazer upload e recuperar armazenamento do Amazon S3. O Amazon S3 escala automaticamente para taxas de solicitações elevadas. Por exemplo, a aplicação pode atingir pelo menos 3,5 mil solicitações PUT/COPY/POST/DELETE ou 5,5 mil solicitações GET/HEAD por segundo por prefixo particionado do Amazon S3. Não há limite para o número de prefixos em um bucket. Você pode melhorar a performance de leitura ou gravação usando paralelização. Por exemplo, se você criar 10 prefixos em um bucket do Amazon S3 para paralelizar leituras, poderá escalar a performance de leitura para 55.000 solicitações de leitura por segundo. Da mesma forma, você pode dimensionar as operações de gravação gravando em vários prefixos. O ajuste de escala, no caso de operações de leitura e gravação, ocorre gradualmente e não é imediato. Além disso, o desempenho real varia de acordo com as características específicas da workload, os padrões de uso e a configuração do sistema. Embora o Amazon S3 esteja escalando para sua nova taxa de solicitação mais alta, você pode ver alguns erros 503 (desaceleração). Esses erros serão dissipados quando o ajuste de escala for concluído. Para obter mais informações sobre como criar e usar prefixos, consulte Organizar objetos usando prefixos.

Por exemplo, algumas aplicações de data lake no Amazon S3 verificam milhões ou bilhões de objetos para consultas que são executadas em petabytes de dados. Essas aplicações de data lake atingem taxas de transferência de instância única que maximizam o uso da interface de rede para a instância do Amazon EC2, que podem ser de até 100 Gb/s em uma única instância. Esses aplicativos então agregam a taxa de transferência em várias instâncias para obter vários terabits por segundo.

Outros aplicativos são sensíveis à latência, como aplicativos de mensagem de mídias sociais. Essas aplicações podem atingir latências consistentes de objetos pequenos (e latências de saída de primeiro byte para objetos maiores) de aproximadamente 100 a 200 milissegundos.

Outros serviços da AWS também podem ajudar a acelerar a performance para diferentes arquiteturas de aplicação. Por exemplo, para obter taxas de transferência mais altas em uma única conexão HTTP ou latências de um dígito de milissegundos, use o Amazon CloudFront ou o Amazon ElastiCache para armazenar em cache com o Amazon S3.

Além disso, se você quiser um transporte de dados rápido em longas distâncias entre um cliente e um bucket do S3, use Configurar transferências de arquivos rápidas e seguras usando o Amazon S3

Transfer Acceleration. O Transfer Acceleration usa os pontos de presença distribuídos globalmente no CloudFront para acelerar o transporte de dados em distâncias geográficas. Se a workload do Amazon S3 usa criptografia do lado do servidor com o AWS KMS, consulte Limites do AWS KMS no Guia do desenvolvedor do AWS Key Management Service para obter informações sobre as taxas de solicitações compatíveis com seu caso de uso.

Os tópicos a seguir descrevem as diretrizes de melhores práticas e os padrões de design para otimizar a performance de aplicações que usam o Amazon S3. Consulte Diretrizes de desempenho para o Amazon S3 e Padrões de design de desempenho do Amazon S3 para obter as informações mais recentes sobre a otimização de performance do Amazon S3.

> **Note**
>
> Para obter mais informações sobre o uso da classe de armazenamento Amazon S3 Express One Zone com buckets de diretório, consulte S3 Express One Zone e Trabalhar com buckets de diretório.

Tópicos

- Diretrizes de desempenho para o Amazon S3
- Padrões de design de desempenho do Amazon S3

Diretrizes de desempenho para o Amazon S3

Ao criar aplicações que fazem upload e recuperam objetos do Amazon S3, siga as diretrizes de melhores práticas para otimizar a performance. Também oferecemos mais detalhado Padrões de design de desempenho do Amazon S3 .

Para obter a melhor performance para a aplicação no Amazon S3, recomendamos as seguintes diretrizes.

Tópicos

- Avalie a performance
- Escalar conexões de armazenamento horizontalmente
- Usar consultas na escala de bytes

- Solicitações de repetição para aplicações sensíveis à latência
- Associar o Amazon S3 (armazenamento) e o Amazon EC2 (computação) na mesma Região da AWS
- Usar a Aceleração de Transferências do Amazon S3 para minimizar a latência causada pela distância
- Usar a versão mais recente dos SDKs da AWS

Avalie a performance

Ao otimizar a performance, observe os requisitos de throughput de rede, CPU e DRAM. Dependendo da combinação de demandas desses recursos diferentes, convém avaliar os diferentes tipos de instância do Amazon EC2. Para obter mais informações sobre os tipos de instância, consulte Tipos de instância no Guia do usuário do Amazon EC2.

Também é útil observar o tempo de pesquisa de DNS, a latência e a velocidade de transferência dos dados usando ferramentas de análise de HTTP ao avaliar a performance.

Para entender os requisitos de performance e otimizar a performance da aplicação, você também pode monitorar as respostas de erro 503 que você recebe. O monitoramento de determinadas métricas de performance pode gerar despesas adicionais. Para obter mais informações, consulte Preço do Amazon S3.

Monitore o número de respostas de erro de status 503 (desaceleração)

Para monitorar o número de respostas de erro de status 503 que você recebe, use uma das seguintes opções:

- Use métricas de solicitação do Amazon CloudWatch para o Amazon S3. As métricas de solicitação do CloudWatch incluem uma métrica para respostas de status 5xx. Para obter mais informações sobre métricas de solicitação do CloudWatch, consulte Monitoramento de métricas com o Amazon CloudWatch.
- Use a contagem de erros 503 (Serviço indisponível) disponível na seção de métricas avançadas da Lente de Armazenamento do Amazon S3. Para obter mais informações, consulte Usar a Lente de Armazenamento do S3 para melhorar a performance.
- Use o registro em log de acesso ao servidor do Amazon S3. Com o registro de acesso ao servidor, é possível filtrar e revisar todas as solicitações que recebem respostas 503 (erro interno). Você também pode usar o Amazon Athena para analisar logs. Para obter mais informações sobre o

registro em log de acesso ao servidor, consulte Registrar em log as solicitações com registro em log de acesso ao servidor.

Ao monitorar o número de códigos de erro de status HTTP 503, muitas vezes você pode obter informações valiosas sobre quais prefixos, chaves ou buckets estão recebendo mais solicitações de controle de utilização.

Escalar conexões de armazenamento horizontalmente

A distribuição de solicitações em muitas conexões é um padrão de design comum para dimensionamento horizontal da performance. Ao criar aplicações de alta performance, pense no Amazon S3 como um sistema distribuído muito grande, não como um único endpoint de rede de um servidor de armazenamento tradicional. Para atingir a melhor performance, emita várias solicitações simultâneas para o Amazon S3. Espalhe essas solicitações em conexões separadas para maximizar a largura de banda acessível do Amazon S3. O Amazon S3 não tem limites para o número de conexões feitas ao bucket.

Usar consultas na escala de bytes

Usando o cabeçalho HTTP `Range` em uma solicitação de Objeto GET, é possível consultar um objeto em escala de bytes, transferindo somente a parte especificada. É possível usar conexões simultâneas ao Amazon S3 para buscar diferentes escalas de bytes no mesmo objeto. Isso ajuda a atingir um throughput agregado maior em comparação com uma única solicitação de objeto inteiro. A consulta de escalas menores de um objeto grande também permite que o aplicativo melhore os tempos de repetição quando as solicitações são interrompidas. Para obter mais informações, consulte Baixar objetos.

Os tamanhos típicos das solicitações de escala de bytes são 8 MB ou 16 MB. Se os objetos usarem a solicitação PUT com um upload de várias partes, é recomendado usar a solicitação GET nos mesmos tamanhos de parte (ou pelo menos de acordo com os limites de parte) para obter a melhor performance. As solicitações GET podem abordar partes individuais diretamente; por exemplo, `GET ?partNumber=N.`

Solicitações de repetição para aplicações sensíveis à latência

Repetições e tempos limite agressivos ajudam a obter uma latência consistente. Devido à grande escala do Amazon S3, se a primeira solicitação for lenta, uma solicitação repetida provavelmente seguirá um caminho diferente e será bem-sucedida rapidamente. Os AWS SDKs têm valores

configuráveis de tempo limite e repetição que podem ser ajustados de acordo com as tolerâncias da aplicação específica.

Associar o Amazon S3 (armazenamento) e o Amazon EC2 (computação) na mesma Região da AWS

Embora os nomes de buckets do S3 sejam globalmente exclusivos, cada bucket é armazenado em uma região selecionada ao criar o bucket. Para saber mais sobre as diretrizes de nomenclatura de buckets, consulte Visão geral dos buckets e Regras de nomeação de bucket. Para otimizar a performance, recomendamos acessar o bucket nas instâncias do Amazon EC2 na mesma Região da AWS quando possível. Isso ajuda a reduzir os custos de latência de rede e transferência de dados.

Para obter mais informações sobre custos de transferência de dados, consulte Definição de preço do Amazon S3.

Usar a Aceleração de Transferências do Amazon S3 para minimizar a latência causada pela distância

Configurar transferências de arquivos rápidas e seguras usando o Amazon S3 Transfer AccelerationO gerencia transferências de arquivos rápidas, fáceis e seguras em longas distâncias entre o cliente e um bucket do S3. O Transfer Acceleration tira proveito dos pontos de presença distribuídos globalmente no Amazon CloudFront. Conforme os dados chegam a um ponto de presença, eles são roteados para o Amazon S3 por um caminho de rede otimizado. O Transfer Acceleration é ideal para transferir gigabytes a terabytes de dados regularmente entre os continentes. Ele também é útil para clientes que fazem upload em um bucket centralizado do mundo todo.

É possível usar a Ferramenta de comparação de velocidade da Aceleração de Transferências do Amazon S3 para comparar velocidades de upload aceleradas e não aceleradas em regiões do Amazon S3. A ferramenta de comparação de velocidade usa multipart uploads para transferir um arquivo do navegador para várias regiões do Amazon S3 com e sem o uso do Amazon S3 Transfer Acceleration.

Usar a versão mais recente dos SDKs da AWS

Os AWS SDKs fornecem suporte integrado a muitas da diretrizes recomendadas para otimizar a performance do Amazon S3. Os SDKs fornecem uma API mais simples para aproveitar o Amazon S3 em uma aplicação e são atualizados regularmente para seguir as práticas recomendadas mais

recentes. Por exemplo, os SDKs incluem uma lógica para executar automaticamente solicitações de repetição em erros HTTP 503 e estão investindo em código para responder e se adaptar a conexões lentas.

Os SDKs também fornecem o Gerenciador de transferências, que automatiza conexões de dimensionamento horizontal para atingir milhares de solicitações por segundo, usando solicitações na escala de bytes quando apropriado. É importante usar a última versão dos AWS SDKs para obter os recursos mais recentes de otimização de performance.

Também é possível otimizar a performance ao usar solicitações de API REST HTTP. Ao usar a API REST, siga as mesmas práticas recomendadas que fazem parte dos SDKs. Permita tempo limite e repetição em solicitações lentas e que várias conexões consultem dados de objeto em paralelo. Para obter informações sobre como usar a API REST, consulte a Referência da API do Amazon Simple Storage Service.

Padrões de design de desempenho do Amazon S3

Ao projetar aplicações para fazer upload e recuperar objetos do Amazon S3, use nossas melhores práticas e padrões de design para atingir a melhor performance da aplicação. Também oferecemos Diretrizes de desempenho para o Amazon S3 a ser considerado ao planejar a arquitetura da aplicação.

Para otimizar a performance, você pode usar os padrões de design a seguir.

Tópicos

- Usar o armazenamento em cache para conteúdo acessado com frequência
- Tempo limite e repetição para aplicações sensíveis à latência
- Escalabilidade horizontal e paralelização de solicitações para alto throughput
- Usar a Aceleração de Transferências do Amazon S3 para acelerar transferências de dados geograficamente dispersas

Usar o armazenamento em cache para conteúdo acessado com frequência

Muitas aplicações que armazenam dados no Amazon S3 fornecem um “conjunto de trabalho” de dados que são solicitados várias vezes pelos usuários. Se uma workload estiver enviando solicitações GET repetidas para um conjunto comum de objetos, você poderá usar um cache, como o Amazon CloudFront, o Amazon ElastiCache ou o AWS Elemental MediaStore para otimizar a

performance. A adoção bem-sucedida do cache pode resultar em baixar latência e altas taxas de transferência de dados. As aplicações que usam o armazenamento em cache também enviam menos solicitações diretas ao Amazon S3, o que também pode ajudar a reduzir os custos de solicitações.

O Amazon CloudFront é uma rede de entrega de conteúdo (CDN) rápida que armazena os dados do Amazon S3 em cache com transparência em um grande conjunto de pontos de presença (PoPs) distribuídos geograficamente. Quando os objetos podem ser acessados em várias regiões ou pela Internet, o CloudFront permite que os dados sejam armazenados em cache perto dos usuários que estão acessando os objetos. Isso pode resultar na entrega de alta performance de conteúdo popular do Amazon S3. Para obter mais informações sobre o CloudFront, consulte o Guia do desenvolvedor do Amazon CloudFront.

O Amazon ElastiCache é um cache de memória gerenciado. Com o ElastiCache, é possível provisionar instâncias do Amazon EC2 que armazenam objetos em cache na memória. Esse armazenamento em cache resulta em pedidos de redução de magnitude da latência de GET e aumentos significativos no throughput de download. Para usar o ElastiCache, modifique a lógica da aplicação para preencher o cache com objetos dinâmicos e verifique se esses objetos estão presentes no cache antes de solicitá-los do Amazon S3. Para obter exemplos de como usar o ElastiCache para melhorar a performance de GET do Amazon S3, consulte a publicação do blog Turbocharge Amazon S3 with Amazon ElastiCache for Redis.

O AWS Elemental MediaStore é um sistema de armazenamento em cache e de distribuição de conteúdo criado especificamente para fluxos de trabalho de vídeo e entrega de mídia do Amazon S3. O MediaStore fornece APIs de armazenamento completas especificamente para vídeo e é recomendado para workloads de vídeo sensíveis à performance. Para obter informações sobre o MediaStore, consulte o Guia do usuário do AWS Elemental MediaStore.

Tempo limite e repetição para aplicações sensíveis à latência

Há determinadas situações em que uma aplicação recebe uma resposta do Amazon S3 indicando que uma nova tentativa é necessária. O Amazon S3 mapeia nomes de bucket e de objetos para os dados do objeto associados a eles. Se um aplicativo gerar altas taxas de solicitação (normalmente taxas constantes de mais de 5.000 solicitações por segundo para um pequeno número de objetos), ele poderá receber respostas HTTP 503 de lentidão. Se esses erros ocorrerem, cada AWS SDK implementará uma lógica de repetição automática usando o recuo exponencial. Se você não estiver usando um AWS SDK, implemente a lógica de repetição ao receber o erro HTTP 503. Consulte mais informações em Retry behavior no Guia de referência de ferramentas e SDKs da AWS.

O Amazon S3 é dimensionado automaticamente em resposta a novas taxas constantes de solicitação, otimizando a performance dinamicamente. Enquanto o Amazon S3 estiver sendo otimizado internamente para uma nova taxa de solicitação, você receberá respostas de solicitação HTTP 503 temporariamente até a otimização terminar. Depois que o Amazon S3 otimiza a performance internamente para a nova taxa de solicitação, todas as solicitações serão executadas de forma geral sem repetições.

Para aplicações sensíveis à latência, o Amazon S3 recomenda rastrear e repetir agressivamente as operações mais lentas. Ao repetir uma solicitação, recomendamos usar uma nova conexão ao Amazon S3 e executar uma nova pesquisa de DNS.

Ao fazer solicitações de tamanhos variavelmente grandes (por exemplo, mais de 128 MB), recomendamos rastrear o throughput atingido e repetir os 5% mais lentos das solicitações. Ao fazer solicitações menores (por exemplo, menos de 512 KB), onde latências medianas geralmente estão na faixa de dezenas de milissegundos, é recomendado repetir uma operação GET ou PUT depois de 2 segundos. Se outras repetições forem necessárias, é recomendado recuar. Por exemplo, recomendamos emitir uma repetição depois de 2 segundos e uma segunda repetição depois de mais 4 segundos.

Se a aplicação fizer solicitações de tamanho fixo para o Amazon S3, espere tempos de resposta mais consistentes para cada uma dessas solicitações. Nesse caso, uma estratégia simples é identificar o 1% mais lento de solicitações e repetí-las. Uma única repetição consegue reduzir a latência.

Se estiver usando o AWS Key Management Service (AWS KMS) para criptografia do lado do servidor, consulte Quotas no Guia do desenvolvedor do AWS Key Management Service para ter informações sobre as taxas de solicitações compatíveis com seu caso de uso.

Escalabilidade horizontal e paralelização de solicitações para alto throughput

O Amazon S3 é um sistema distribuído muito grande. Para ajudar a aproveitar essa escala, recomendamos dimensionar horizontalmente as solicitações paralelas para os endpoints do serviço Amazon S3. Além de distribuir as solicitações no Amazon S3, esse tipo de abordagem de dimensionamento ajuda a distribuir a carga em vários caminhos na rede.

Para obter altas taxas de transferência, o Amazon S3 recomenda usar aplicações com várias conexões para executar solicitações GET ou PUT paralelas de dados. Por exemplo, isso é compatível com o Amazon S3 Transfer Manager no AWS SDK for Java, e a maioria dos outros

AWS SDKs fornece construções semelhantes. Para alguns aplicativos, você pode atingir conexões paralelas iniciando várias solicitações ao mesmo tempo em diferentes threads de aplicativo ou em diferentes instâncias de aplicativo. A melhor abordagem depende do aplicativo e da estrutura dos objetos acessados.

Você pode usar os AWS SDKs para emitir solicitações GET e PUT diretamente em vez de empregar o gerenciamento de transferências no AWS SDK. Essa abordagem permite ajustar a workload mais diretamente, além de ainda aproveitar o suporte do SDK para repetições e o processamento das eventuais respostas HTTP 503. Como regra geral, ao fazer download de grandes objetos em uma região do Amazon S3 para o Amazon EC2, sugerimos fazer solicitações simultâneas em escalas de bytes de um objeto na granularidade de 8 a 16 MB. Faça uma solicitação simultânea para cada 85 a 90 MB/s da taxa de transferência de rede desejada. Para saturar uma placa de interface de rede (NIC) de 10 Gb/s, você pode usar cerca de 15 solicitações simultâneas em conexões separadas. É possível dimensionar as solicitações simultâneas em mais conexões para saturar NICs mais rápidas, como NICs de 25 Gb/s ou 100 Gb/s.

A avaliação da performance é importante ao ajustar o número de solicitações a serem emitidas ao mesmo tempo. Recomendamos começar com uma única solicitação de cada vez. Meça a largura de banda de rede atingida e o uso de outros recursos que o aplicativo usa no processamento dos dados. Você pode identificar o recurso de gargalo (isto é, o recurso com maior utilização) e, assim, o número de solicitações que provavelmente serão úteis. Por exemplo, se processar uma solicitação por vez usa 25% da CPU, é recomendado acomodar até quatro solicitações simultâneas. A medição é essencial e vale a pena confirmar o uso do recurso conforme a taxa de solicitação aumenta.

Se a aplicação emitir solicitações diretamente para o Amazon S3 usando a API REST, recomendamos usar um grupo de conexões HTTP e reutilizar cada conexão para uma série de solicitações. Evitar a configuração de conexão por solicitação elimina a necessidade de realizar handshakes Secure Sockets Layer (SSL) e TCP de inicialização lenta em cada solicitação. Para obter informações sobre como usar a API REST, consulte a Referência da API do Amazon Simple Storage Service.

Finalmente, vale prestar atenção ao DNS e verificar novamente se as solicitações estão sendo distribuídas em um grande grupo de endereços IP do Amazon S3. As consultas de DNS para o Amazon S3 percorrem uma grande lista de endpoints IP. No entanto, o armazenamento em cache de solucionadores ou código do aplicativo que reutiliza um único endereço IP não aproveita a diversidade de endereços e o balanceamento de carga associados. Ferramentas de utilitário de rede, como a ferramenta de linha de comando `netstat`, podem mostrar os endereços IP usados para comunicação com o Amazon S3, e nós fornecemos diretrizes para as configurações de DNS

que devem ser usadas. Consulte mais informações sobre essas diretrizes em Making requests na Referência da API do Amazon S3.

Usar a Aceleração de Transferências do Amazon S3 para acelerar transferências de dados geograficamente dispersas

Configurar transferências de arquivos rápidas e seguras usando o Amazon S3 Transfer AccelerationO é útil para minimizar ou eliminar a latência causada pela distância geográfica entre clientes distribuídos globalmente e uma aplicação regional que usa o Amazon S3. O Transfer Acceleration usa os pontos de presença distribuídos globalmente no CloudFront para transporte de dados. A rede de borda da AWS tem pontos de presença em mais de 50 locais. Atualmente, ela é usada para distribuir conteúdo por meio do CloudFront e fornecer respostas rápidas para consultas de DNS feitas para o Amazon Route 53.

A rede de borda também ajuda a acelerar transferências de dados enviadas e recebidas do Amazon S3. Ela é ideal para aplicativos que transferem dados em ou entre continentes, possuem uma rápida conexão com a Internet, usam objetos grandes ou possuem muito conteúdo para upload. Conforme os dados chegam em um ponto de presença, eles são roteados para o Amazon S3 por um caminho de rede otimizado. Em geral, quanto mais distante você está de uma região do Amazon S3, maior a melhoria de velocidade que pode esperar do uso do Transfer Acceleration.

Você pode configurar o Transfer Acceleration em buckets novos ou existentes. Use um endpoint separado do Amazon S3 Transfer Acceleration para usar os locais de borda da AWS. A melhor maneira de testar se o Transfer Acceleration ajuda a performance da solicitação do cliente é usar a Ferramenta de comparação de velocidade do Amazon S3 Transfer Acceleration. As configurações e condições de rede variam periodicamente e de um lugar para outro. Portanto, você só é cobrado para transferências em que o Amazon S3 Transfer Acceleration pode melhorar a performance do upload. Para obter informações sobre o uso do Transfer Acceleration com diferentes AWS SDKs, consulte Habilitar e usar o S3 Transfer Acceleration.

Hospedagem de um site estático usando o Amazon S3

Você pode usar o Amazon S3 para hospedar um site estático. Em um site estático, as páginas da Web individuais incluem conteúdo estático. Elas também podem conter scripts do lado do cliente.

> **Note**
>
> Recomendamos que você use o AWS Amplify Hosting para hospedar conteúdo de site estático armazenado no S3. O Amplify Hosting é um serviço totalmente gerenciado que facilita a implantação de seus sites em uma rede de entrega de conteúdo (CDN) disponível globalmente, desenvolvida pelo Amazon CloudFront, permitindo hospedagem segura de site estático.
>
> Com o AWS Amplify Hosting, é possível selecionar a localização dos objetos no bucket de uso geral, implantar o conteúdo em uma CDN gerenciada e gerar um URL HTTPS público para que o site possa ser acessado em qualquer lugar. Consulte mais informações sobre o Amplify Hosting em Implantar um site estático no AWS Amplify Hosting diretamente de um bucket do S3 de uso geral e em Deploying a static website from S3 using the Amplify console no Guia do usuário do console do AWS Amplify.

Para obter mais informações sobre a hospedagem de um site estático no Simple Storage Service (Amazon S3), incluindo instruções e demonstrações detalhadas, consulte os tópicos a seguir.

Tópicos

- Endpoints de site
- Habilitar a hospedagem de sites
- Configurar um documento de índice
- Configurar um documento de erro personalizado
- Configuração de permissões para acesso ao site
- (Opcional) Registrar em log o tráfego da web
- (Opcional) Configurar um redirecionamento de uma página da Web
- Usar o compartilhamento de recursos de origem cruzada (CORS)
- Tutoriais de site estático

Endpoints de site

Quando você configura seu bucket como um site estático, o site fica disponível no endpoint de site específico da Região da AWS do bucket. Os endpoints de site são diferentes dos endpoints para onde você envia solicitações de API REST. Para obter mais informações sobre as diferenças entre os endpoints, consulte Principais diferenças entre um endpoint de site e um endpoint de API REST.

Dependendo da Região, os endpoints de site do Amazon S3 seguem um destes dois formatos.

- Região s3-website dash - `http://bucket-name.s3-website-Region.amazonaws.com`
- s3-website ponto (.) Região - `http://bucket-name.s3-website.Region.amazonaws.com`

Esses URLs retornam o documento de indexação padrão configurado para o site. Para obter uma lista completa dos endpoints do site do Amazon S3, consulte Endpoints de site do Amazon S3.

> **Note**
>
> Para aumentar a segurança dos sites estáticos do Amazon S3, os domínios de endpoint do site do Amazon S3 (por exemplo, s3-website-us-east-1.amazonaws.com ou s3-website.ap-south-1.amazonaws.com) são registrados na Lista Pública de Sufixos (PSL). Para maior segurança, recomendamos que você use cookies com um prefiro `__Host-` caso precise definir cookies confidenciais no nome de domínio de sites estáticos do Amazon S3. Essa prática ajudará a defender seu domínio contra tentativas de falsificação de solicitação entre sites (CSRF). Para obter mais informações, consulte a página Set-Cookie na Mozilla Developer Network.

Se você quiser que seu site seja público, será necessário fazer com que seu conteúdo seja publicamente legível para que seus clientes possam acessá-lo no endpoint de site. Para obter mais informações, consulte Configuração de permissões para acesso ao site.

> **Important**
>
> - Os endpoints de site do Amazon S3 não oferecem suporte a HTTPS ou pontos de acesso. Se quiser usar HTTPS, você poderá utilizar uma destas opções:
>   - (Recomendado) Use o AWS Amplify Hosting para hospedar conteúdo de site estático armazenado no S3. O Amplify Hosting é um serviço totalmente gerenciado que facilita

a implantação de seus sites em uma rede de entrega de conteúdo (CDN) disponível globalmente, desenvolvida pelo Amazon CloudFront, permitindo hospedagem segura de site estático.

Com o AWS Amplify Hosting, é possível selecionar a localização dos objetos no bucket de uso geral, implantar o conteúdo em uma CDN gerenciada e gerar um URL HTTPS público para que o site possa ser acessado em qualquer lugar. Consulte mais informações sobre o Amplify Hosting em Implantar um site estático no AWS Amplify Hosting diretamente de um bucket do S3 de uso geral e em Deploying a static website from S3 using the Amplify console no Guia do usuário do console do AWS Amplify.

- Use o Amazon CloudFront para atender a um site estático hospedado no Amazon S3. Para obter mais informações, consulte Como uso o CloudFront para atender a solicitações HTTPS para meu bucket do Amazon S3? Para usar HTTPS com um domínio personalizado, consulte Configuração de um site estático usando um domínio personalizado registrado no Route 53.

- Os buckets de pagamento pelo solicitante não permitem acesso por um endpoint de site. Qualquer solicitação para tal bucket recebe uma resposta 403 Acesso negado. Para obter mais informações, consulte Utilizar buckets de uso geral com pagamento pelo solicitante para transferência e uso de armazenamento.

Tópicos

- Exemplos de endpoint de site
- Adicionar um registro DNS CNAME
- Usar um domínio personalizado com o Route 53
- Principais diferenças entre um endpoint de site e um endpoint de API REST

Exemplos de endpoint de site

Os exemplos a seguir mostram como você pode acessar um bucket do Amazon S3 configurado como um site estático.

Example - solicitação de um objeto no nível raiz

Para solicitar um objeto específico que é armazenado no nível raiz do bucket, use a seguinte estrutura de URL.

```
http://bucket-name.s3-website.Region.amazonaws.com/object-name
```

Por exemplo, o URL a seguir solicita o objeto `photo.jpg` que está armazenado no nível raiz do bucket.

```
http://example-bucket.s3-website.us-west-2.amazonaws.com/photo.jpg
```

Example - solicitação de um objeto em um prefixo

Para solicitar um objeto armazenado em uma pasta em seu bucket, use a seguinte estrutura de URL.

```
http://bucket-name.s3-website.Region.amazonaws.com/folder-name/object-name
```

O URL a seguir solicita o objeto `docs/doc1.html` em seu bucket.

```
http://example-bucket.s3-website.us-west-2.amazonaws.com/docs/doc1.html
```

Adicionar um registro DNS CNAME

Se você tiver um domínio registrado, poderá adicionar uma entrada DNS CNAME para apontar para o endpoint de site do Amazon S3. Por exemplo, se você registrou o domínio `www.example-bucket.com`, pode criar um bucket `www.example-bucket.com` e adicionar um registro DNS CNAME que aponte para `www.example-bucket.com.s3-website.Region.amazonaws.com`. Todas as solicitações a `http://www.example-bucket.com` são redirecionadas para `www.example-bucket.com.s3-website.Region.amazonaws.com`.

Para obter mais informações, consulte Personalizar URLs do Amazon S3 com registros CNAME.

Usar um domínio personalizado com o Route 53

Em vez de acessar o site usando um endpoint de site do Amazon S3, você pode usar seu próprio domínio registrado com Amazon Route 53 para veicular conteúdo, por exemplo, `example.com`. Você pode usar o Amazon S3 com o Route 53 para hospedar um site no domínio raiz. Por exemplo, se você tiver o domínio raiz `example.com` e quiser hospedar seu site no Amazon S3, os visitantes do site poderão acessá-lo no navegador digitando `http://www.example.com` ou `http://example.com`.

Para ver uma demonstração de exemplo, consult Tutorial: Configurar um site estático usando um domínio personalizado registrado no Route 53.

Principais diferenças entre um endpoint de site e um endpoint de API REST

Um endpoint de site do Amazon S3 é otimizado para acesso de um navegador da Web. A tabela a seguir resume as principais diferenças entre um endpoint de API REST e um endpoint de site.

Principal diferença	Endpoint de API REST	Endpoint de site
Controle de acesso	Oferece suporte a conteúdo público e privado	Oferece suporte apenas a conteúdo publicamente legível
Manuseio de mensagens de erro	Retorna uma resposta de erro formatada em XML	Retorna um documento HTML
Suporte a redirecionamento	Não aplicável	Oferece suporte a redirecionamentos no nível do objeto e do bucket
Solicitações com suporte	Oferece suporte a todas as operações de bucket e de objeto	Compatível apenas com solicitações `GET` e `HEAD` em objetos
Responde a solicitações `GET` e `HEAD` na raiz de um bucket	Retorna uma lista de chaves de objeto no bucket	Retorna o documento de índice especificado na configuração de site
Suporte a Secure Sockets Layer (SSL)	Oferece suporte a conexões SSL	Não oferece suporte a conexões SSL

Para obter uma lista completa dos endpoints do Amazon S3, consulte Endpoints e cotas do Amazon S3 na .Referência geral da AWS

Habilitar a hospedagem de sites

Ao configurar um bucket como um site estático, você deve habilitar a hospedagem de sites estáticos, configurar um documento de índice e definir permissões.

Você pode habilitar a hospedagem estática de sites usando o console do Amazon S3, a API REST, os AWS SDKs, a AWS CLI ou o AWS CloudFormation.

Para configurar seu site com um domínio personalizado, consulte Tutorial: Configurar um site estático usando um domínio personalizado registrado no Route 53.

Uso do console do S3

Como habilitar a hospedagem de sites estáticos

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets de uso geral.
3. Na lista de buckets, escolha o nome do bucket para o qual você deseja habilitar a hospedagem de site estático.
4. Escolha Properties (Propriedades).
5. Em Static website hosting (Hospedagem estática de sites), escolha Edit (Editar).
6. Escolha Use this bucket to host a website (Usar este bucket para hospedar um site).
7. Em Static website hosting (Hospedagem estática de sites), escolha Enable (Ativar).
8. Em Index Document (Documento de índice), insira o nome do arquivo do documento de índice, que geralmente é `index.html`.

   O nome do documento de índice diferencia letras maiúsculas de minúsculas e deve corresponder exatamente ao nome do arquivo do documento de índice HTML do qual você planeja fazer upload para o bucket do S3. Quando você configura um bucket para hospedagem de site, deve especificar um documento de índice. O Amazon S3 retorna esse documento de índice quando as solicitações são feitas para o domínio raiz ou alguma subpasta. Para obter mais informações, consulte Configurar um documento de índice.
9. Para fornecer seu próprio documento de erros personalizado para erros da classe 4XX, em Error document (Documento de erros), insira o nome de arquivo do documento de erros personalizado.

O nome do documento de erro diferencia letras maiúsculas de minúsculas e deve corresponder exatamente ao nome do arquivo do documento de erro HTML do qual você planeja fazer upload para o bucket do S3. Se você não especificar um documento de erro personalizado e ocorrer um erro, o Amazon S3 retornará um documento de erro HTML padrão. Para obter mais informações, consulte Configurar um documento de erro personalizado.

10. (Opcional) Se você quiser especificar regras avançadas de redirecionamento em Redirection rules (Regras de redirecionamento), use JSON para descrevê-las.

    Por exemplo, você pode encaminhar solicitações condicionalmente de acordo com nomes de chave de objeto ou prefixos específicos na solicitação. Para obter mais informações, consulte Configurar regras de redirecionamento para usar redirecionamentos condicionais avançados.

11. Selecione Save changes.

    O Amazon S3 permite a hospedagem estática de sites para seu bucket. Na parte inferior da página, em Static website hosting (Hospedagem estática de sites), você verá o endpoint do site do seu bucket.

12. Em Static website hosting (Hospedagem de sites estáticos), anote o Endpoint.

    O Endpoint é o endpoint do site do Amazon S3 para o bucket. Depois de concluir a configuração do bucket como um site estático, é possível usar esse endpoint para testar o site.

Uso dos REST API

Para obter mais informações sobre o envio de solicitações REST diretamente para habilitar a hospedagem estática de sites, consulte as seções a seguir na Referência da API do Amazon Simple Storage Service:

- PUT em site de bucket
- GET em site de bucket
- Site de DELETE Bucket

Uso da SDKs AWS

Para hospedar um site estático no Amazon S3, você configura um bucket do Amazon S3 para hospedagem de sites e faz upload do conteúdo do seu site no bucket. Você também pode usar os AWS SDKs para criar, atualizar e excluir a configuração do site de forma programática. Os SDKs

fornecem classes de wrapper na API REST do Amazon S3. Se seu aplicativo exigir, você pode enviar solicitações de API REST diretamente do seu aplicativo.

.NET

O exemplo a seguir mostra como usar o AWS SDK para .NET para gerenciar a configuração de site para um bucket. Para adicionar uma configuração de site a um bucket, forneça um nome de bucket e uma configuração de site. A configuração de site deve incluir um documento de índice e pode conter um documento de erro opcional. Esses documentos devem ser armazenados no bucket. Para obter mais informações, consulte PUT Bucket website. Para obter mais informações sobre o recurso de site do Amazon S3, consulte Hospedagem de um site estático usando o Amazon S3.

O exemplo de código C# a seguir adiciona uma configuração de site ao bucket especificado. A configuração especifica o documento de índice e os nomes de documento de erros. Para obter informações sobre como configurar e executar exemplos de código, consulte Conceitos básicos do AWS SDK for .NET no Guia do desenvolvedor do AWS SDK for .NET.

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class WebsiteConfigTest
    {
        private const string bucketName = "*** bucket name ***";
        private const string indexDocumentSuffix = "*** index object key ***"; //
 For example, index.html.
        private const string errorDocument = "*** error object key ***"; // For
 example, error.html.
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 client;
        public static void Main()
        {
            client = new AmazonS3Client(bucketRegion);
            AddWebsiteConfigurationAsync(bucketName, indexDocumentSuffix,
 errorDocument).Wait();
```

```
        }

        static async Task AddWebsiteConfigurationAsync(string bucketName,
                                                string indexDocumentSuffix,
                                                string errorDocument)
        {
            try
            {
                // 1. Put the website configuration.
                PutBucketWebsiteRequest putRequest = new PutBucketWebsiteRequest()
                {
                    BucketName = bucketName,
                    WebsiteConfiguration = new WebsiteConfiguration()
                    {
                        IndexDocumentSuffix = indexDocumentSuffix,
                        ErrorDocument = errorDocument
                    }
                };
                PutBucketWebsiteResponse response = await
client.PutBucketWebsiteAsync(putRequest);

                // 2. Get the website configuration.
                GetBucketWebsiteRequest getRequest = new GetBucketWebsiteRequest()
                {
                    BucketName = bucketName
                };
                GetBucketWebsiteResponse getResponse = await
client.GetBucketWebsiteAsync(getRequest);
                Console.WriteLine("Index document: {0}",
getResponse.WebsiteConfiguration.IndexDocumentSuffix);
                Console.WriteLine("Error document: {0}",
getResponse.WebsiteConfiguration.ErrorDocument);
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered on server. Message:'{0}' when
writing an object", e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
writing an object", e.Message);
            }
        }
```

```
    }
}
```

PHP

O exemplo de PHP a seguir adiciona uma configuração de site ao bucket especificado. O método `create_website_config` fornece explicitamente os nomes de documentos de índice e de documentos de erros. O exemplo também recupera a configuração de site e imprime a resposta. Para obter mais informações sobre o recurso de site do Amazon S3, consulte Hospedagem de um site estático usando o Amazon S3.

Para obter mais informações sobre a API do AWS SDK for Ruby, acesse AWS SDK for Ruby Version 2.

```
 require 'vendor/autoload.php';

use Aws\S3\S3Client;

$bucket = '*** Your Bucket Name ***';

$s3 = new S3Client([
    'version' => 'latest',
    'region'  => 'us-east-1'
]);


// Add the website configuration.
$s3->putBucketWebsite([
    'Bucket'                => $bucket,
    'WebsiteConfiguration'  => [
        'IndexDocument' => ['Suffix' => 'index.html'],
        'ErrorDocument' => ['Key' => 'error.html']
    ]
]);

// Retrieve the website configuration.
$result = $s3->getBucketWebsite([
    'Bucket' => $bucket
]);
echo $result->getPath('IndexDocument/Suffix');

// Delete the website configuration.
$s3->deleteBucketWebsite([
```

```
    'Bucket' => $bucket
]);
```

Como usar o AWS CLI

Para obter mais informações sobre como usar a AWS CLI para configurar um bucket do S3 como um site estático, consulte site na Referência de comandos da AWS CLI.

Depois, é necessário configurar o documento de índice e definir permissões. Para obter informações, consulte Configurar um documento de índice e Configuração de permissões para acesso ao site.

Também é possível configurar um documento de erro, o registro em log do tráfego da web ou um redirecionamento.

Configurar um documento de índice

Ao habilitar a hospedagem de sites, você também deve configurar e fazer upload de um documento de índice. Um documento de índice é uma página da Web que o Amazon S3 retorna quando uma solicitação é feita para a raiz de um site ou para qualquer subpasta. Por exemplo, se um usuário insere `http://www.example.com` no navegador, ele não está solicitando nenhuma página específica. Nesse caso, o Amazon S3 exibe o documento de índice, que às vezes é referido como a página padrão.

Quando você habilita a hospedagem de sites estáticos para seu bucket, insere o nome do documento de índice (por exemplo, `index.html`). Depois de habilitar a hospedagem de sites estáticos para seu bucket, faça upload de um arquivo HTML com o nome do documento de índice para o bucket.

A barra no final do URL no nível raiz é opcional. Por exemplo, se você configurar seu site com `index.html` como o documento de índice, qualquer um dos URLs a seguir retornará `index.html`.

```
http://example-bucket.s3-website.Region.amazonaws.com/
http://example-bucket.s3-website.Region.amazonaws.com
```

Para obter mais informações sobre endpoints de site do Amazon S3, consulte Endpoints de site.

Pastas e documentos de índice

No Amazon S3, um bucket é um contêiner de objetos simples. Ele não fornece nenhuma organização hierárquica, já que o sistema de arquivos em seu computador faz isso. No entanto, você pode criar uma hierarquia lógica usando nomes de chaves de objetos que envolvam uma estrutura de pastas.

Por exemplo, considere um bucket com três objetos e que tenha os nomes de chaves a seguir. Embora esses objetos sejam armazenados sem uma organização hierárquica física, você pode pressupor a seguinte estrutura lógica de pastas com base nos nomes das chaves.

- `sample1.jpg`: o objeto está na raiz do bucket.
- `photos/2006/Jan/sample2.jpg`: o objeto está na subpasta `photos/2006/Jan`.
- `photos/2006/Feb/sample3.jpg`: o objeto está na subpasta `photos/2006/Feb`.

No console do Amazon S3, você também pode criar uma pasta em um bucket. Por exemplo, você pode criar uma pasta chamada `photos`. Você pode fazer upload de objetos no bucket ou na pasta `photos` no bucket. Se você adicionar o objeto `sample.jpg` ao bucket, o nome da chave será `sample.jpg`. Se você fizer upload do objeto na pasta `photos`, o nome da chave de objeto será `photos/sample.jpg`.

Se você criar um estrutura de pastas em seu bucket, deverá ter um documento de índice em cada nível. Em cada pasta, o documento de índice deve ter o mesmo nome, por exemplo, `index.html`. Quando um usuário especificar um URL que se assemelhe a uma consulta de pasta, a presença ou a ausência de uma barra no final determinará o comportamento do site. Por exemplo, o URL a seguir, com uma barra no final, retorna o documento de índice `photos/index.html`.

```
http://bucket-name.s3-website.Region.amazonaws.com/photos/
```

Contudo, se você excluir a barra no final do URL anterior, o Amazon S3 procurará primeiro um objeto `photos` no bucket. Se o objeto `photos` não for encontrado, ele procurará um documento de índice, `photos/index.html`. Se esse documento for encontrado, o Amazon S3 retornará uma mensagem `302 Found` e apontará para a chave `photos/`. Para solicitações subsequentes a `photos/`, o Amazon S3 retorna `photos/index.html`. Se o documento de índice não for encontrado, o Amazon S3 retornará um erro.

Configurar um documento de índice

Para configurar um documento de índice usando o console do S3, use o procedimento a seguir. Você também pode configurar um documento de índice usando a API REST, os AWS SDKs, a AWS CLI ou o AWS CloudFormation.

> **Note**
>
> Em um bucket com versionamento habilitado, é possível carregar várias cópias do `index.html`, mas somente a versão mais recente será resolvida. Para obter mais informações sobre como usar o versionamento do S3, consulte Reter várias versões de objetos com o Versionamento do S3.

Quando você habilita a hospedagem de sites estáticos para seu bucket, insere o nome do documento de índice (por exemplo, **`index.html`**). Depois de habilitar a hospedagem de sites estáticos para seu bucket, faça upload de um arquivo HTML com esse nome de documento de índice para o bucket.

Como configurar o documento de índice

1. Criar um arquivo `index.html`

   Se você não tiver um arquivo `index.html`, poderá usar o HTML a seguir para criar um:

   ```
   <html xmlns="http://www.w3.org/1999/xhtml" >
   <head>
       <title>My Website Home Page</title>
   </head>
   <body>
     <h1>Welcome to my website</h1>
     <p>Now hosted on Amazon S3!</p>
   </body>
   </html>
   ```

2. Salve o arquivo de índice localmente.

   O nome do documento de índice deve corresponder exatamente ao nome do documento de índice que você inseriu na caixa de diálogo Hospedagem de site estático. O nome do documento de índice diferencia maiúsculas de minúsculas. Por exemplo, se você inserir `index.html` no

nome do Documentos de índice na caixa de diálogo Hospedagem de site estático, o nome do arquivo do documento de índice também deverá ser `index.html` e não `Index.html`.

3. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
4. No painel de navegação à esquerda, escolha Buckets de uso geral.
5. Na lista de buckets, escolha o nome do bucket que você deseja usar para hospedar um site estático.
6. Habilite a hospedagem de sites estáticos para seu bucket e insira o nome exato do documento de índice (por exemplo, `index.html`). Para obter mais informações, consulte Habilitar a hospedagem de sites.

   Depois de habilitar a hospedagem estática do site, vá para a etapa 6.
7. Para fazer upload do documento de índice para o bucket, siga um destes procedimentos:

   - Arraste e solte o arquivo de índice na listagem de buckets do console.
   - Escolha Upload (Fazer upload) e siga as instruções para escolher e fazer upload do arquivo de índice.

   Para obter instruções detalhadas, consulte Fazer upload de objetos.
8. (Opcional) Faça upload do conteúdo de outro site para o seu bucket.

Depois, é necessário definir permissões para acesso ao site. Para mais informações, consulte Configuração de permissões para acesso ao site.

Também é possível configurar um documento de erro, o registro em log do tráfego da web ou um redirecionamento.

Configurar um documento de erro personalizado

Depois de configurar o bucket como um site estático, quando ocorre um erro, o Amazon S3 retorna um documento de erro HTML. Opcionalmente, você pode configurar seu bucket com um documento de erro personalizado para que o Amazon S3 retorne esse documento quando ocorrer um erro.

> **Note**
>
> Quando um erro ocorre, alguns navegadores exibem sua própria mensagem, ignorando o documento de erro que o Amazon S3 retorna. Por exemplo, quando ocorre um erro HTTP 404 Not Found, o Google Chrome pode ignorar o documento de erro que o Amazon S3 retorna e exibir seu próprio erro.

Tópicos

- Códigos de resposta HTTP do Amazon S3
- Configurar um documento de erro personalizado

Códigos de resposta HTTP do Amazon S3

A tabela a seguir lista o subconjunto de códigos de resposta HTTP que o Amazon S3 retorna quando ocorre um erro.

Código de erro HTTP	Descrição
301 Moved Permanently (301 movido permanentemente)	Quando um usuário enviar uma solicitação diretamente a endpoints de site do Amazon S3 (`http://s3-website.` *`Region`*`.amazonaws.com/`), o Amazon S3 retornará uma resposta 301 Moved Permanently e redirecionará essas solicitações para `https://aws.amazon.com/s3/` .
302 Found (302 Encontrado)	Quando o Amazon S3 recebe uma solicitação para uma chave `x`, `http://`*`bucket-name`*`.s3-website.`*`Region`*`.amazonaws.com/x` , sem uma barra no final, ele tenta localizar o objeto com o nome de chave `x`. Se o objeto não for encontrado, o Amazon S3 determinará que a solicitação é para a subpasta `x` e redirecionará a solicitação adicionando uma barra no final, e retornará 302 Found.
304 Not Modified (304 Não modificado)	Os usuários do Amazon S3 usam cabeçalhos de solicitação `If-Modified-Since` , `If-Unmodified-Since` , `If-Match` e/ou `If-None-M`

Código de erro HTTP	Descrição
	atch para determinar se o objeto solicitado é igual ao da cópia em cache mantida pelo cliente. Se o objeto for o mesmo, o endpoint do site retornará uma resposta 304 Not Modified (304 não modificados).
400 Malformed Request (400 Solicitação malformada)	O endpoint de site responde com 400 Malformed Request (400 Solicitaç ão malformada) quando um usuário tenta acessar um bucket pelo endpoint regional incorreto.
403 Forbidden (403 Proibido)	O endpoint de site responde com 403 Forbidden (403 Proibido) quando uma solicitação de usuário se traduz em um objeto que não é publicamente legível. O proprietário do objeto deve tornar o objeto publicamente legível usando uma política de bucket ou uma ACL.

Código de erro HTTP	Descrição
404 Not Found (404 Não encontrado)	O endpoint de site responde com 404 Not Found (404 Não encontrado) pelos seguintes motivos: • O Amazon S3 determina que o URL do site refere-se a uma chave de objeto que não existe. • O Amazon S3 pressupõe que a solicitação é para um documento de índice que não existe. • Um bucket especificado no URL não existe. • Um bucket especificado no URL existe, mas não é configurado como um site. Você pode criar um documento personalizado que é retornado em caso de 404 Not Found (404 Não encontrado). Certifique-se de que o documento seja carregado no bucket configurado como um site e que a configuração de hospedagem de sites esteja definida para usar o documento. Para obter informações sobre como o Amazon S3 interpreta o URL como uma solicitação de um objeto ou um documento de índice, consulte Configurar um documento de índice.
500 Service Error (500 Erro de serviço)	O endpoint de site responde com 500 Service Error (500 Erro de serviço) quando ocorre um erro interno de servidor.
503 Service Unavailable (503 Serviço não disponível)	O endpoint de site responde com 503 Service Unavailable quando o Amazon S3 determina que você precisa reduzir sua taxa de solicitações.

Para cada um desses erros, o Amazon S3 retorna uma mensagem HTML predefinida. Veja a seguir uma mensagem HTML de exemplo que é retornada para a resposta 403 Forbidden (403 Proibido).



Configurar um documento de erro personalizado

Quando configura seu bucket como um site estático, você pode, opcionalmente, fornecer um documento de erro personalizado que contém uma mensagem de erro fácil de entender e ajuda adicional. O Amazon S3 retorna seu documento de erro personalizado somente para códigos de erro HTTP classe 4XX.

Para configurar um documento de erro personalizado usando o console do S3, siga as etapas abaixo. Você também pode configurar um documento de erro usando a API REST, os AWS SDKs, a AWS CLI ou o AWS CloudFormation. Para obter mais informações, consulte:

- PutBucketWebsite na Referência da API do Amazon Simple Storage Service
- AWS::S3::Bucket WebsiteConfiguration no Guia do usuário do AWS CloudFormation
- put-bucket-website na Referência de comando da AWS CLI

Ao habilitar a hospedagem de site estático para o bucket, insira o nome do documento de erro (por exemplo, **`404.html`**). Depois de habilitar a hospedagem de sites estáticos para seu bucket, faça upload de um arquivo HTML com esse nome de documento de erros para o bucket.

Para configurar um documento de erros

1. Crie um documento de erro, por exemplo `404.html`.

2. Salve o arquivo de documento de erros localmente.

   O nome do documento de erros diferencia maiúsculas e minúsculas e deve corresponder exatamente ao nome que você insere ao habilitar a hospedagem estática do site. Por exemplo, se você inserir `404.html` como o nome do Error document (Documento de erro) na caixa de diálogo Static website hosting (Hospedagem de site estático), o nome de arquivo do documento de erro também deve ser `404.html`.
3. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
4. No painel de navegação à esquerda, escolha Buckets de uso geral.
5. Na lista de buckets, escolha o nome do bucket que você deseja usar para hospedar um site estático.
6. Habilite a hospedagem de site estático para seu bucket e insira o nome exato do documento de erro (por exemplo, `404.html`). Para obter mais informações, consulte Habilitar a hospedagem de sites e Configurar um documento de erro personalizado.

   Depois de habilitar a hospedagem estática do site, vá para a etapa 6.
7. Para fazer upload do documento de erros para o bucket, siga um destes procedimentos:

   - Arraste e solte o arquivo de documento de erros na lista de buckets do console.
   - Escolha Upload (Fazer upload) e siga as instruções para escolher e fazer upload do arquivo de índice.

   Para obter instruções detalhadas, consulte Fazer upload de objetos.

Configuração de permissões para acesso ao site

Ao configurar um bucket como um site estático, se você desejar que seu site seja público, poderá conceder acesso público de leitura. Para tornar o bucket publicamente legível, é necessário desabilitar as configurações de bloqueio de acesso público do bucket e gravar uma política de bucket que conceda acesso público de leitura. Se o bucket contiver objetos que não são do proprietário do bucket, talvez também seja necessário adicionar uma lista de controle de acesso (ACL) de objeto que conceda acesso de leitura a todos.

Se você não quiser desativar as configurações de acesso público de bloqueio para seu bucket, mas ainda quiser que seu site seja público, poderá criar uma distribuição do Amazon CloudFront para

servir seu site estático. Para obter mais informações, consulte Acelerar seu site com o Amazon CloudFront ou Usar uma distribuição do Amazon CloudFront para servir um site estático no Guia do desenvolvedor do Amazon Route 53.

> **Note**
>
> No endpoint de site, se um usuário solicitar um objeto que não existe, o Amazon S3 retornará um código de resposta HTTP `404 (Not Found)`. Se o objeto existir, mas não você não tiver permissão de leitura nele, o endpoint de site retornará o código de resposta HTTP `403 (Access Denied)`. O usuário pode usar o código de resposta para inferir se um objeto específico existe. Se você não quiser esse comportamento, não ative o suporte de site para seu bucket.

Tópicos

- Etapa 1: Editar configurações de bloqueio de acesso público do S3
- Etapa 2: Adicionar uma política de bucket
- Listas de controle de acesso de objetos

Etapa 1: Editar configurações de bloqueio de acesso público do S3

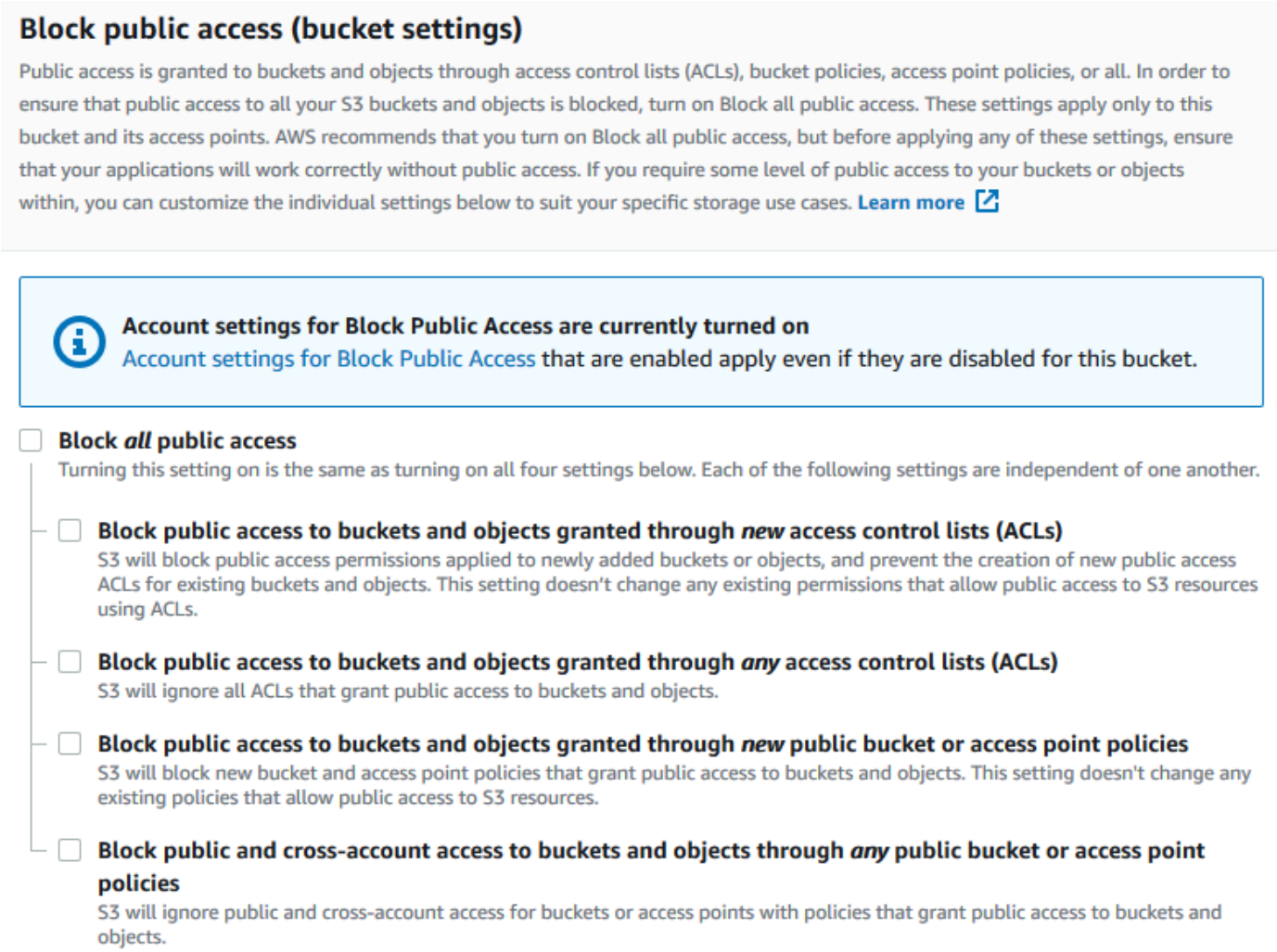
Se quiser configurar um bucket existente como um site estático que tenha acesso público, você deverá editar as configurações de bloqueio de acesso público desse bucket. Você também pode ter que editar suas configurações de bloqueio de acesso público no nível da conta. O Amazon S3 aplica a combinação mais restritiva das configurações de bloqueio de acesso público no nível do bucket e no nível da conta.

Por exemplo, se você permitir o acesso público a um bucket, mas bloquear todo o acesso público no nível da conta, o Amazon S3 continuará a bloquear o acesso público ao bucket. Neste cenário, você precisaria editar as configurações de bloqueio de acesso público no nível do bucket e no nível da conta. Para obter mais informações, consulte Bloquear o acesso público ao armazenamento do Amazon S3.

Por padrão, o Amazon S3 bloqueia o acesso público à sua conta e aos seus buckets. Se quiser usar um bucket para hospedar um site estático, use estas etapas para editar as configurações de bloqueio de acesso público.

> **Warning**
>
> Antes de concluir estas etapas, revise Bloquear o acesso público ao armazenamento do Amazon S3 para garantir que você entenda e aceite os riscos envolvidos em permitir o acesso público. Ao desativar as configurações de bloqueio de acesso público para tornar seu bucket público, qualquer pessoa na Internet pode acessá-lo. Recomendamos que você bloqueie todo o acesso público aos buckets.

1. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Escolha o nome do bucket configurado como um site estático.
3. Escolha Permissions (Permissões).
4. Em Block public access (bucket settings) (Bloqueio de acesso público (configurações de bucket), escolha Edit (Editar).
5. Desmarque Block all public access (Bloquear todo acesso público) e escolha Save changes (Salvar alterações).



O Amazon S3 desativa as configurações do Bloqueio de Acesso Público para o bucket. Para criar um site público estático, talvez também seja necessário editar as configurações do Bloqueio de Acesso Público para sua conta antes de adicionar uma política de bucket. Se as configurações do Bloqueio de Acesso Público da conta estiverem ativadas no momento, você verá uma observação em Bloquear acesso público (configurações de bucket).

Etapa 2: Adicionar uma política de bucket

Para tornar os objetos no bucket publicamente legíveis, você deverá gravar uma política de bucket que conceda a todos a permissão `s3:GetObject`.

Depois de editar as configurações do Bloqueio de acesso público do S3, é possível adicionar uma política de bucket para conceder acesso público de leitura ao bucket. Ao conceder um acesso público de leitura, qualquer pessoa na Internet pode acessar seu bucket.

> **Important**
>
> A política a seguir é somente um exemplo e concede acesso total aos conteúdos do bucket. Antes de prosseguir com esta etapa, revise Como posso proteger os arquivos no meu bucket do Amazon S3? para garantir que você entende as práticas recomendadas a fim de proteger os arquivos no bucket do S3 e os riscos envolvidos na concessão de acesso público.

1. Em Buckets, escolha o nome do seu bucket.
2. Escolha Permissions (Permissões).
3. Em Bucket Policy (Política de bucket), escolha Edit (Editar).
4. Para conceder acesso público de leitura ao site, copie a política de bucket a seguir e cole-a no Bucket policy editor (Editor de política de bucket).

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PublicReadGetObject",
            "Effect": "Allow",
            "Principal": "*",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::Bucket-Name/*"
            ]
        }
    ]
}
```

5. Atualize o `Resource` para o nome do bucket.

   Na política de bucket do exemplo anterior, *`Bucket-Name`* é um espaço reservado para o nome do bucket. Para usar essa política de bucket com seu próprio bucket, você deve atualizar esse nome para corresponder ao nome do seu bucket.

6. Selecione Save changes.

   Uma mensagem é exibida indicando que a política de bucket foi adicionada com sucesso.

Se você vir um erro que diz `Policy has invalid resource`, confirme se o nome do bucket na política de bucket corresponde ao nome do seu bucket. Para obter informações sobre como adicionar uma política de bucket, consulte Como adicionar uma política de bucket do S3?

Se você receber uma mensagem de erro e não puder salvar a política do bucket, verifique suas configurações de acesso público para confirmar que você permite acesso público ao bucket.

Listas de controle de acesso de objetos

É possível usar uma política de bucket para conceder permissão de leitura aos seus objetos. No entanto, a política de bucket se aplica somente a objetos que sejam do proprietário do bucket. Se o seu bucket contiver objetos que não sejam do proprietário do bucket, ele deverá usar a lista de controle de acesso (ACL) do objeto para conceder permissão READ pública nesses objetos.

A Propriedade de objetos do S3 é uma configuração no nível do bucket do Amazon S3 que você pode usar para controlar a propriedade de objetos carregados no bucket e para desabilitar ou habilitar as ACLs. Por padrão, a Propriedade de Objetos está definida com a configuração Imposto pelo proprietário do bucket e todas as ACLs estão desabilitadas. Quando as ACLs são desabilitadas, o proprietário do bucket possui todos os objetos do bucket e gerencia o acesso a eles exclusivamente usando políticas de gerenciamento de acesso.

A maioria dos casos de uso modernos no Amazon S3 não exige mais o uso de ACLs. Recomendamos manter as ACLs desabilitadas, exceto em circunstâncias incomuns em que seja necessário controlar o acesso para cada objeto individualmente. Com as ACLs desabilitadas, é possível usar políticas para controlar o acesso a todos os objetos no bucket, independentemente de quem carregou os objetos para o bucket. Para obter mais informações, consulte Controlar a propriedade de objetos e desabilitar ACLs para seu bucket.

> **Important**
>
> Se o bucket de uso geral utilizar a configuração “Imposto pelo proprietário do bucket” para a Propriedade de objetos do S3, será necessário usar políticas para conceder acesso ao bucket de uso geral e aos objetos contidos nele. Quando a configuração Imposto pelo proprietário do bucket estiver habilitada, as solicitações para definir listas de controle de acesso (ACLs) ou atualizar ACLs falharão e retornarão o código de erro `AccessControlListNotSupported`. Ainda há suporte para solicitações de leitura de ACLs.

Para tornar um objeto publicamente legível usando uma ACL, conceda a permissão READ ao grupo `AllUsers`, como mostrado no elemento de concessão a seguir. Adicione esse elemento de concessão à ACL do objeto. Para obter informações sobre o gerenciamento de ACLs, consulte Visão geral da lista de controle de acesso (ACL).

```
<Grant>
  <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
          xsi:type="Group">
    <URI>http://acs.amazonaws.com/groups/global/AllUsers</URI>
  </Grantee>
  <Permission>READ</Permission>
</Grant>
```

(Opcional) Registrar em log o tráfego da web

Opcionalmente, é possível habilitar o registro em log de acesso ao servidor do Amazon S3 para um bucket configurado como um site estático. O registro em log de acesso ao servidor fornece registros detalhados para as solicitações que são feitas ao bucket. Para obter mais informações, consulte Registrar em log as solicitações com registro em log de acesso ao servidor. Se planeja usar o Amazon CloudFront para acelerar seu site, você também pode usar o registro em log do CloudFront. Para obter mais informações, consulte Configurar e usar logs de acesso no Guia do desenvolvedor do Amazon CloudFront.

Como habilitar o registro em log do acesso ao servidor para o bucket de site estático

1. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Na mesma região onde você criou o bucket configurado como um site estático, crie um bucket de uso geral para registro em log, por exemplo, `logs.example.com`.
3. Crie uma pasta para os arquivos de log do registro em log de acesso ao servidor (por exemplo, `logs`).
4. (Opcional) Se você quiser usar o CloudFront para melhorar oa performance do seu site, crie uma pasta para os arquivos de log do CloudFront (por exemplo, `cdn`).

   Para obter mais informações, consulte Acelerar seu site com o Amazon CloudFront.
5. Na lista Buckets, escolha o bucket.
6. Escolha Properties (Propriedades).
7. Em Server access logging (Registro de acesso ao servidor), selecione Edit (Editar).

8. Escolha Habilitar.
9. No Target bucket (Bucket de destino), escolha o destino do bucket e da pasta para os logs de acesso ao servidor:

   - Navegue até o local da pasta e do bucket:
     1. Escolha Browse S3 (Navegar no S3).
     2. Escolha o nome do bucket e, depois, escolha a pasta de logs.
     3. Selecione Choose path (Escolher caminho).
   - Insira o caminho do bucket do S3, por exemplo, **`s3://logs.example.com/logs/`**.
10. Selecione Save changes.

    No bucket de log, agora você pode acessar seus logs. O Amazon S3 grava os logs de acesso ao site no bucket de log a cada duas horas.

(Opcional) Configurar um redirecionamento de uma página da Web

Se o bucket do Amazon S3 estiver configurado para hospedagem de site estático, você poderá configurar redirecionamentos para seu bucket ou para os objetos nele contidos. As opções a seguir estão disponíveis para a configuração de redirecionamentos.

Tópicos

- Redirecionar solicitações para o endpoint do site do seu bucket para outro bucket ou domínio
- Configurar regras de redirecionamento para usar redirecionamentos condicionais avançados
- Redirecionar solicitações para um objeto

Redirecionar solicitações para o endpoint do site do seu bucket para outro bucket ou domínio

É possível redirecionar todas as solicitações de um endpoint de site de um bucket para outro bucket ou domínio. Se você redirecionar todas as solicitações, qualquer solicitação feita ao endpoint do site será redirecionada ao bucket ou domínio especificado.

Por exemplo, se o seu domínio raiz for `example.com` e você quiser atender a solicitações para `http://example.com` e `http://www.example.com`, é necessário criar dois buckets chamados `example.com` e `www.example.com`. Depois, mantenha o conteúdo no bucket `example.com`

e configure o outro bucket `www.example.com` para redirecionar todas as solicitações ao bucket `example.com`. Para obter mais informações, consulte Configurar um site estático usando um nome de domínio personalizado.

Como redirecionar solicitações para um endpoint de site do bucket

1. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Em Buckets, escolha o nome do bucket do qual você deseja redirecionar solicitações (por exemplo, `www.example.com`).
3. Escolha Properties (Propriedades).
4. Em Static website hosting (Hospedagem estática de sites), escolha Edit (Editar).
5. Selecione Redirect requests for an object (Redirecionar solicitações de um objeto).
6. Na caixa Host name (Nome do host) insira o endpoint do site para seu bucket ou seu domínio personalizado.

   Por exemplo, se você estiver redirecionando para um endereço de domínio raiz, insira **`example.com`**.
7. Para Protocol (Protocolo), escolha o protocolo para as solicitações redirecionadas (none,http, ou https).

   Se você não especificar um protocolo, a opção padrão será none.
8. Selecione Save changes.

Configurar regras de redirecionamento para usar redirecionamentos condicionais avançados

Usando regras de redirecionamentos avançadas, você pode rotear solicitações condicionalmente de acordo com nomes de chave de objeto específicos, prefixos na solicitação ou códigos da resposta. Por exemplo, suponha que você exclua ou dê outro nome a um objeto em seu bucket. Você pode adicionar uma regra de roteamento que redireciona a solicitação a outro objeto. Se você deseja tornar uma pasta indisponível, será possível adicionar uma regra de roteamento para redirecionar a solicitação para outra página da Web. Você também pode adicionar uma regra de roteamento para processar condições de erro, encaminhando solicitações que retornam o erro para outro domínio quando ele é processado.

Ao habilitar a hospedagem de site estático para seu bucket, você pode especificar opcionalmente regras de redirecionamento avançadas. O Amazon S3 tem uma limitação de 50 regras de roteamento por configuração de site. Se você precisar de mais de 50 regras de roteamento, poderá usar o redirecionamento de objetos. Para obter mais informações, consulte Uso do console do S3.

Para obter mais informações sobre como configurar regras de roteamento usando a API REST, consulte PutBucketWebsite na Referência da API do Amazon Simple Storage Service.

> **Important**
>
> Para criar regras de redirecionamento no novo console do Amazon S3, você deve usar o JSON. Para exemplos de JSON, consulte Exemplos de regras de redirecionamento.

Para configurar regras de redirecionamento para um site estático

Para adicionar regras de redirecionamento para um bucket que já tem alojamento de site estático ativado, siga estas etapas.

1. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets de uso geral.
3. Na lista de buckets, escolha o nome do bucket que você configurou como um site estático.
4. Escolha Properties (Propriedades).
5. Em Static website hosting (Hospedagem estática de sites), escolha Edit (Editar).
6. Na caixa Redirection rules (Regras de redirecionamento), insira suas regras de redirecionamento em JSON.

   No console do S3, você descreve as regras usando o JSON. Para exemplos de JSON, consulte Exemplos de regras de redirecionamento. O Amazon S3 tem uma limitação de 50 regras de roteamento por configuração de site.
7. Selecione Save changes.

Elementos de regra de roteamento

Veja a seguir a sintaxe geral para definir as regras de roteamento em uma configuração de site em XML. Para configurar regras de redirecionamento no novo console do S3, use o JSON. Para exemplos de JSON, consulte Exemplos de regras de redirecionamento.

JSON

```
[
    {
      "Condition": {
        "HttpErrorCodeReturnedEquals": "string",
        "KeyPrefixEquals": "string"
      },
      "Redirect": {
        "HostName": "string",
        "HttpRedirectCode": "string",
        "Protocol": "http"|"https",
        "ReplaceKeyPrefixWith": "string",
        "ReplaceKeyWith": "string"
      }
    }
  ]

Note: Redirect must each have at least one child element. You can have either
 ReplaceKeyPrefix with or ReplaceKeyWith but not both.
```

XML

```
<RoutingRules> =
    <RoutingRules>
         <RoutingRule>...</RoutingRule>
         [<RoutingRule>...</RoutingRule>
         ...]
    </RoutingRules>

<RoutingRule> =
   <RoutingRule>
      [ <Condition>...</Condition> ]
      <Redirect>...</Redirect>
   </RoutingRule>

<Condition> =
   <Condition>
      [ <KeyPrefixEquals>...</KeyPrefixEquals> ]
      [ <HttpErrorCodeReturnedEquals>...</HttpErrorCodeReturnedEquals> ]
   </Condition>
    Note: <Condition> must have at least one child element.
```

```
<Redirect> =
   <Redirect>
      [ <HostName>...</HostName> ]
      [ <Protocol>...</Protocol> ]
      [ <ReplaceKeyPrefixWith>...</ReplaceKeyPrefixWith>  ]
      [ <ReplaceKeyWith>...</ReplaceKeyWith> ]
      [ <HttpRedirectCode>...</HttpRedirectCode> ]
   </Redirect>

Note: <Redirect> must have at least one child element. You can have either
 ReplaceKeyPrefix with or ReplaceKeyWith but not both.
```

A tabela a seguir descreve os elementos na regra de roteamento.

Nome	Descrição
`RoutingRules`	Contêiner para um conjunto de elementos `RoutingRule` .
`RoutingRule`	Uma regra que identifica uma condição e o redirecionamento que é aplicado quando a condição é satisfeita. Condição: • Um contêiner `RoutingRules` deve ter pelo menos uma regra de roteamento.
`Condition`	O contêiner para descrever uma condição que deve ser satisfeit a para que o redirecionamento especificado seja aplicado. Se a regra de roteamento não incluir uma condição, a regra será aplicada a todas as solicitações.
`KeyPrefixEquals`	O prefixo do nome da chave de objeto do qual as solicitações são redirecionadas. `KeyPrefixEquals` será obrigatório se `HttpError CodeReturnedEquals` não for especificado. Se `KeyPrefix`

Nome	Descrição
	`Equals` e `HttpErrorCodeReturnedEquals` forem especificados, ambos deverão ser verdadeiros para a condição ser satisfeita.
`HttpErrorCodeReturnedEquals`	O código de erro HTTP que deve corresponder para que o redirecionamento seja aplicado. Se ocorrer um erro, e se o código de erro satisfizer esse valor, o redirecionamento especificado será aplicado. `HttpErrorCodeReturnedEquals` será obrigatório se `KeyPrefixEquals` não for especificado. Se `KeyPrefixEquals` e `HttpErrorCodeReturnedEquals` forem especificados, ambos deverão ser verdadeiros para a condição ser satisfeita.
`Redirect`	O elemento do contêiner que fornece instruções para o redirecionamento da solicitação. Você pode redirecionar solicitações para outro host, ou outra página, ou pode especificar outro protocolo a ser usado. Uma `RoutingRule` deve ter um elemento `Redirect`. Um elemento `Redirect` deve conter pelo menos um dos seguintes elementos irmãos: `Protocol`, `HostName`, `ReplaceKeyPrefixWith`, `ReplaceKeyWith` ou `HttpRedirectCode`.
`Protocol`	O protocolo, `http` ou `https`, que será usado no cabeçalho `Location` que é retornado na resposta. Se um dos irmãos for fornecido, `Protocol` não será obrigatório.
`HostName`	O nome do host a ser usado no cabeçalho `Location` que é retornado na resposta. Se um dos irmãos for fornecido, `HostName` não será obrigatório.

Nome	Descrição
`ReplaceKeyPrefixWith`	O prefixo do nome de chave de objeto que substitui o valor de `KeyPrefixEquals` na solicitação de redirecionamento. Se um dos irmãos for fornecido, `ReplaceKeyPrefixWith` não será obrigatório. Poderá ser fornecido somente se `ReplaceKeyWith` não for fornecido.
`ReplaceKeyWith`	A chave de objeto a ser usada no cabeçalho `Location` que é retornado na resposta. Se um dos irmãos for fornecido, `ReplaceKeyWith` não será obrigatório. Poderá ser fornecido somente se `ReplaceKeyPrefixWith` não for fornecido.
`HttpRedirectCode`	O código de redirecionamento HTTP a ser usado no cabeçalho `Location` que é retornado na resposta. Se um dos irmãos for fornecido, `HttpRedirectCode` não será obrigatório.

Exemplos de regras de redirecionamento

Os seguintes exemplos explicam tarefas comuns de redirecionamento:

> **Important**
>
> Para criar regras de redirecionamento no novo console do Amazon S3, você deve usar o JSON.

Example 1: Redirecionar após trocar o nome de um prefixo de chave

Suponha que seu bucket contenha os seguintes objetos:

- index.html

- docs/article1.html
- docs/article2.html

Você decide renomear a pasta de `docs/` para `documents/`. Depois de fazer essa alteração, você precisará redirecionar as solicitações do prefixo `docs/` para `documents/`. Por exemplo, as solicitações para `docs/article1.html` serão redirecionadas para `documents/article1.html`.

Nesse caso, adicione a seguinte regra de roteamento à configuração do site:

JSON

```
[
    {
        "Condition": {
            "KeyPrefixEquals": "docs/"
        },
        "Redirect": {
            "ReplaceKeyPrefixWith": "documents/"
        }
    }
]
```

XML

```
  <RoutingRules>
    <RoutingRule>
    <Condition>
      <KeyPrefixEquals>docs/</KeyPrefixEquals>
    </Condition>
    <Redirect>
      <ReplaceKeyPrefixWith>documents/</ReplaceKeyPrefixWith>
    </Redirect>
    </RoutingRule>
  </RoutingRules>
```

Example 2: Redirecionar solicitações de uma pasta excluída para uma página

Suponha que você tenha excluído a pasta `images/` (ou seja, você excluiu todos os objetos com o prefixo de chave `images/`). Você pode adicionar uma regra de roteamento que redirecione

as solicitações para os objetos com o prefixo de chave `images/` a uma página chamada `folderdeleted.html`.

JSON

```
[
    {
        "Condition": {
            "KeyPrefixEquals": "images/"
        },
        "Redirect": {
            "ReplaceKeyWith": "folderdeleted.html"
        }
    }
]
```

XML

```
  <RoutingRules>
    <RoutingRule>
    <Condition>
       <KeyPrefixEquals>images/</KeyPrefixEquals>
    </Condition>
    <Redirect>
      <ReplaceKeyWith>folderdeleted.html</ReplaceKeyWith>
    </Redirect>
    </RoutingRule>
  </RoutingRules>
```

Example 3: Redirecionar para um erro HTTP

Suponha que, quando um objeto solicitado não for encontrado, você queira redirecionar solicitações para uma instância do Amazon Elastic Compute Cloud (Amazon EC2). Adicione uma regra de redirecionamento para que, quando um código HTTP de status 404 (não encontrado) for retornado, o visitante do site seja redirecionado para uma instância do Amazon EC2 que processa a solicitação.

O exemplo a seguir também insere o prefixo de chave de objeto `report-404/` no redirecionamento. Por exemplo, se você solicitar uma página `ExamplePage.html` e ela resultar em um erro HTTP 404, a solicitação será redirecionada a uma página `report-404/ExamplePage.html` na instância do Amazon EC2 especificada. Se não houver nenhuma regra de roteamento e o erro HTTP 404 ocorrer, o documento de erro que é especificado na configuração será retornado.

JSON

```
[
    {
        "Condition": {
            "HttpErrorCodeReturnedEquals": "404"
        },
        "Redirect": {
            "HostName": "ec2-11-22-333-44.compute-1.amazonaws.com",
            "ReplaceKeyPrefixWith": "report-404/"
        }
    }
]
```

XML

```
  <RoutingRules>
    <RoutingRule>
    <Condition>
      <HttpErrorCodeReturnedEquals>404</HttpErrorCodeReturnedEquals >
    </Condition>
    <Redirect>
      <HostName>ec2-11-22-333-44.compute-1.amazonaws.com</HostName>
      <ReplaceKeyPrefixWith>report-404/</ReplaceKeyPrefixWith>
    </Redirect>
    </RoutingRule>
  </RoutingRules>
```

Redirecionar solicitações para um objeto

Você pode redirecionar solicitações de um objeto para outro objeto ou URL configurando o local de redirecionamento do site nos metadados do objeto. Você define o redirecionamento adicionando a propriedade `x-amz-website-redirect-location` aos metadados do objeto. Você pode usar o console do Amazon S3 para definir o Website Redirect Location (Local de redirecionamento de site) nos metadados do objeto. Se você usar a API do Amazon S3, defina `x-amz-website-redirect-location`. A seguir, o site interpreta o objeto como um redirecionamento 301.

Para reorientar uma solicitação para outro objeto, você define o local de redirecionamento como a chave do objeto de destino. Para redirecionar uma solicitação para um URL externo, defina o local de

redirecionamento como o URL desejado. Para obter mais informações sobre metadados de objeto, consulte Metadados do objeto definidos pelo sistema.

Quando você define um redirecionamento de página, pode manter ou excluir o conteúdo de objeto de origem. Por exemplo, se você tiver um objeto `page1.html` em seu bucket, poderá redirecionar todas as solicitações para essa página para outro objeto, `page2.html`. Você tem duas opções:

- Mantenha o conteúdo do objeto do `page1.html` e redirecione solicitações de página.
- Exclua o conteúdo de `page1.html` e carregue um objeto de byte zero chamado `page1.html` para substituir o objeto existente e redirecionar solicitações de páginas.

Uso do console do S3

1. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Na lista Buckets, escolha o nome do bucket que você configurou como um site estático (por exemplo, `example.com`).
3. Em Objects (Objetos), selecione seu objeto.
4. Escolha Actions (Ações) e escolha Edit metadata (Editar metadados).
5. Escolha Metadata (Metadados).
6. Escolha Add Metadata (Adicionar metadados).
7. Em Type (Tipo), escolha System Defined (Definido pelo sistema).
8. Em Key (Chave), escolha x-amz-website-redirect-location.
9. Em Value (Valor), insira o nome da chave do objeto o qual deseja redirecionar, por exemplo, `/page2.html`.

   Para outro objeto no mesmo bucket, o prefixo `/` no valor é obrigatório. Você também pode definir o valor para um URL externo, por exemplo, `http://www.example.com`.
10. Escolha Edit metadata (Editar metadados).

Uso dos REST API

As ações da API do Amazon S3 oferecem suporte ao cabeçalho `x-amz-website-redirect-location` na solicitação. O Amazon S3 armazena o valor de cabeçalho nos metadados de objeto como `x-amz-website-redirect-location`.

- Objeto PUT

- Iniciar multipart upload
- Objeto POST
- Objeto PUT - Copiar

Um bucket configurado para hospedagem de sites tem o endpoint de site e o endpoint REST. Uma solicitação para uma página que é configurada como redirecionamento 301 tem os seguintes resultados possíveis, dependendo do endpoint da solicitação:

- Endpoint de site específico da região: o Amazon S3 redireciona a solicitação da página de acordo com o valor da propriedade `x-amz-website-redirect-location`.
- Endpoint REST: o Amazon S3 não redireciona a solicitação da página. Ele retorna o objeto solicitado.

Para obter mais informações sobre os endpoints, consulte Principais diferenças entre um endpoint de site e um endpoint de API REST.

Quando você define um redirecionamento de página, pode manter ou excluir o conteúdo de objeto. Por exemplo, suponha que você tenha um objeto `page1.html` em seu bucket.

- Para manter o conteúdo de `page1.html` e apenas redirecionar as solicitações de página, envie uma solicitação PUT objeto - Copiar para criar um novo objeto `page1.html`que usa o objeto `page1.html` existente como origem. Na sua solicitação, você define o cabeçalho `x-amz-website-redirect-location`. Quando a solicitação for concluída, você terá a página original com o conteúdo inalterado, mas o Amazon S3 redirecionará todas as solicitações da página para o local de redirecionamento especificado.
- Para excluir o conteúdo do objeto `page1.html` e redirecionar as solicitações para a página, envie uma solicitação PUT objeto para fazer upload de um objeto com zero byte com a mesma chave de objeto: `page1.html`. Na solicitação PUT, você define `x-amz-website-redirect-location` para `page1.html`como o novo objeto. Quando a solicitação for concluída, `page1.html` não terá nenhum conteúdo, e as solicitações serão redirecionadas para o local que é especificado por `x-amz-website-redirect-location`.

Quando você recupera o objeto usando a ação GET objeto com outros metadados de objeto, o Amazon S3 retorna o cabeçalho `x-amz-website-redirect-location` na resposta.

Usar o compartilhamento de recursos de origem cruzada (CORS)

O compartilhamento de recursos de origem cruzada (CORS) define uma maneira de os aplicativos web clientes carregados em um domínio interagirem com recursos em outro domínio. Com o suporte do CORS, você pode criar aplicações web no lado do cliente com o Amazon S3 e permitir seletivamente o acesso de origem cruzada aos seus recursos do Amazon S3.

Esta seção fornece uma visão geral do CORS. Os subtópicos descrevem como você pode ativar o CORS usando o console do Amazon S3 ou, programaticamente, usando a API REST do Amazon S3 e os AWS SDKs.

Compartilhamento de recursos de origem cruzada: cenários de caso de uso

Veja a seguir exemplos de cenário de uso do CORS:

Cenário 1

Suponha que você esteja hospedando um site em um bucket do Amazon S3 chamado `website` como descrito em Hospedagem de um site estático usando o Amazon S3. Os usuários carregam o endpoint de site.

```
http://website.s3-website.us-east-1.amazonaws.com
```

Agora você quer usar JavaScript nas páginas da web armazenadas nesse bucket para fazer solicitações GET e PUT autenticadas no mesmo bucket usando o endpoint da API do Amazon S3 para o bucket `website.s3.us-east-1.amazonaws.com`. Um navegador normalmente impediria que o JavaScript permitisse essas solicitações. No entanto, com CORS, é possível configurar seu bucket para permitir explicitamente solicitações de origem cruzada de `website.s3-website.us-east-1.amazonaws.com`.

Cenário 2

Suponha que você queira hospedar uma fonte web de seu bucket do S3. Mais uma vez, os navegadores exigem uma verificação de CORS (também chamada de verificação de simulação) para carregar fontes web. Assim, é preciso configurar o bucket que está hospedando a fonte web para permitir que qualquer origem faça essas solicitações.

Como o Amazon S3 avalia a configuração de CORS em um bucket?

Quando o Amazon S3 recebe uma solicitação de simulação de um navegador, ele avalia a configuração de CORS para o bucket e usa a primeira regra `CORSRule` que corresponde à solicitação de entrada do navegador para permitir uma solicitação de origem cruzada. Para que uma regra seja correspondente, as seguintes condições devem ser satisfeitas:

- O cabeçalho `Origin` em uma solicitação do CORS para seu bucket deve corresponder às origens do elemento `AllowedOrigins` na configuração do CORS.
- Os métodos HTTP especificados no `Access-Control-Request-Method` em uma solicitação de CORS para o bucket devem corresponder ao método ou aos métodos listados no elemento `AllowedMethods` na configuração de CORS.
- Os cabeçalhos listados no cabeçalho `Access-Control-Request-Headers` em uma solicitação de pré-processamento devem corresponder aos cabeçalhos no elemento `AllowedHeaders` na configuração do CORS.

> **Note**
>
> As ACLs e as políticas continuam sendo aplicadas quando você habilita o CORS no bucket.

Como o ponto de acesso do Object Lambda é compatível com o CORS

Ao receber uma solicitação de um navegador ou quando a solicitação inclui um cabeçalho `Origin`, o S3 Object Lambda sempre adiciona um campo de cabeçalho `"AllowedOrigins":"*"`.

Para obter mais informações sobre como usar o CORS, consulte os tópicos a seguir.

Tópicos

- Elementos de uma configuração de CORS
- Configurar o compartilhamento de recursos de origem cruzada (CORS)
- Testar o CORS
- Solução de problemas do CORS

Elementos de uma configuração de CORS

Para configurar seu bucket para permitir solicitações de origem cruzada, crie uma configuração CORS. A configuração de CORS é um documento com elementos que identificam as origens que você permitirá que acessem o bucket, as operações (métodos HTTP) compatíveis com cada origem e outras informações específicas da operação. Você pode adicionar até 100 regras à configuração. Você pode adicionar a configuração CORS como o sub-recurso `cors` ao bucket.

Se você estiver configurando o CORS no console do S3, use o JSON para criar uma configuração CORS. O novo console do S3 oferece suporte somente a configurações JSON CORS.

Para obter mais informações sobre a configuração de CORS e os elementos nele, consulte os tópicos a seguir. Para obter instruções sobre como adicionar uma configuração de CORS, consulte Configurar o compartilhamento de recursos de origem cruzada (CORS).

> **Important**
>
> No novo console do S3, a configuração CORS deve ser JSON.

Tópicos

- Elemento AllowedMethods
- Elemento AllowedOrigins
- Elemento AllowedHeaders
- Elemento ExposeHeaders
- Elemento MaxAgeSeconds
- Exemplos de configurações de CORS

Elemento **`AllowedMethods`**

Na configuração de CORS, você pode especificar os seguintes valores para o elemento `AllowedMethods`.

- GET
- PUT

- POST
- DELETE
- HEAD

Elemento **AllowedOrigins**

No elemento `AllowedOrigins`, você especifica as origens das quais deseja permitir solicitações de domínio cruzado, por exemplo, `http://www.example.com`. A string de origem pode conter somente um caractere curinga `*`, como `http://*.example.com`. É possível especificar `*` como a origem para permitir que todas as origens enviem solicitações de origem cruzada. Você também pode especificar `https` para permitir somente origens confiáveis.

Elemento **AllowedHeaders**

O elemento `AllowedHeaders` especifica quais cabeçalhos são permitidos em uma solicitação de simulação por meio do cabeçalho `Access-Control-Request-Headers`. Cada nome no cabeçalho `Access-Control-Request-Headers` deve coincidir com uma entrada correspondente no elemento. O Amazon S3 enviará somente os cabeçalhos permitidos que foram solicitados em uma resposta. Para obter uma lista de exemplos de cabeçalhos que podem ser usados em solicitações para o Amazon S3, acesse Cabeçalhos de solicitação comuns no guia de Referência da API do Amazon Simple Storage Service.

Cada string de AllowedHeaders na configuração pode conter no máximo um caractere curinga *. Por exemplo, `<AllowedHeader>x-amz-*</AllowedHeader>` permitirá todos os cabeçalhos específicos da Amazon.

Elemento **ExposeHeaders**

Cada elemento `ExposeHeader` identifica um cabeçalho na resposta que você deseja que os clientes acessem de seus aplicativos (por exemplo, de um objeto JavaScript `XMLHttpRequest`). Para obter uma lista de cabeçalhos de resposta comuns do Amazon S3, acesse Cabeçalhos de resposta comuns no guia de Referência da API do Amazon Simple Storage Service .

Elemento **MaxAgeSeconds**

O elemento `MaxAgeSeconds` especifica o tempo em segundos que seu navegador pode armazenar em cache a resposta para uma solicitação de simulação conforme identificado pelo recurso, pelo método HTTP e pela origem.

Exemplos de configurações de CORS

Em vez de acessar um site usando um endpoint do Amazon S3, você pode usar seu próprio domínio, como `example1.com` para distribuir seu conteúdo. Para obter informações sobre como usar seu próprio domínio, consulte Tutorial: Configurar um site estático usando um domínio personalizado registrado no Route 53.

O seguinte exemplo de configuração de CORS tem três regras especificadas como elementos `CORSRule`:

- A primeira regra permite solicitações PUT, POST e DELETE de origem cruzada da origem `http://www.example1.com`. A regra também permite todos os cabeçalhos em uma solicitação OPTIONS de simulação por meio do cabeçalho `Access-Control-Request-Headers`. Em resposta a solicitações OPTIONS de simulação, o Amazon S3 retorna cabeçalhos solicitados.
- A segunda regra permite as mesmas solicitações de origem cruzada da primeira regra, mas a regra se aplica a outra origem, `http://www.example2.com`.
- A terceira regra permite solicitações GET de origem cruzada de todas as origens. O caractere curinga * refere-se a todas as origens.

JSON

```
[
    {
        "AllowedHeaders": [
            "*"
        ],
        "AllowedMethods": [
            "PUT",
            "POST",
            "DELETE"
        ],
        "AllowedOrigins": [
            "http://www.example1.com"
        ],
        "ExposeHeaders": []
    },
    {
        "AllowedHeaders": [
            "*"
        ],
```

```
        "AllowedMethods": [
            "PUT",
            "POST",
            "DELETE"
        ],
        "AllowedOrigins": [
            "http://www.example2.com"
        ],
        "ExposeHeaders": []
    },
    {
        "AllowedHeaders": [],
        "AllowedMethods": [
            "GET"
        ],
        "AllowedOrigins": [
            "*"
        ],
        "ExposeHeaders": []
    }
]
```

XML

```
<CORSConfiguration>
 <CORSRule>
   <AllowedOrigin>http://www.example1.com</AllowedOrigin>

   <AllowedMethod>PUT</AllowedMethod>
   <AllowedMethod>POST</AllowedMethod>
   <AllowedMethod>DELETE</AllowedMethod>

   <AllowedHeader>*</AllowedHeader>
 </CORSRule>
 <CORSRule>
   <AllowedOrigin>http://www.example2.com</AllowedOrigin>

   <AllowedMethod>PUT</AllowedMethod>
   <AllowedMethod>POST</AllowedMethod>
   <AllowedMethod>DELETE</AllowedMethod>

   <AllowedHeader>*</AllowedHeader>
 </CORSRule>
```

```
 <CORSRule>
   <AllowedOrigin>*</AllowedOrigin>
   <AllowedMethod>GET</AllowedMethod>
 </CORSRule>
</CORSConfiguration>
```

A configuração de CORS também permite parâmetros de configuração opcionais, conforme exibido na configuração de CORS a seguir. Neste exemplo, a configuração de CORS permite solicitações PUT, POST e DELETE de origem cruzada da origem `http://www.example.com`.

JSON

```
[
    {
        "AllowedHeaders": [
            "*"
        ],
        "AllowedMethods": [
            "PUT",
            "POST",
            "DELETE"
        ],
        "AllowedOrigins": [
            "http://www.example.com"
        ],
        "ExposeHeaders": [
            "x-amz-server-side-encryption",
            "x-amz-request-id",
            "x-amz-id-2"
        ],
        "MaxAgeSeconds": 3000
    }
]
```

XML

```
<CORSConfiguration>
 <CORSRule>
   <AllowedOrigin>http://www.example.com</AllowedOrigin>
   <AllowedMethod>PUT</AllowedMethod>
   <AllowedMethod>POST</AllowedMethod>
   <AllowedMethod>DELETE</AllowedMethod>
```

```
    <AllowedHeader>*</AllowedHeader>
   <MaxAgeSeconds>3000</MaxAgeSeconds>
   <ExposeHeader>x-amz-server-side-encryption</
ExposeHeader>
   <ExposeHeader>x-amz-request-id</
ExposeHeader>
   <ExposeHeader>x-amz-id-2</ExposeHeader>
  </CORSRule>
</CORSConfiguration>
```

O elemento `CORSRule` na configuração anterior inclui os seguintes elementos opcionais:

- `MaxAgeSeconds`: Especifica o tempo em segundos (neste exemplo, 3000) que o navegador armazena em cache uma resposta do Amazon S3 a uma solicitação OPTIONS de simulação para o recurso especificado. Armazenando a resposta em cache, o navegador não precisará enviar solicitações de simulação ao Amazon S3, caso a solicitação original seja repetida.
- `ExposeHeaders` — Identifica os cabeçalhos de resposta (neste exemplo, `x-amz-server-side-encryption`, `x-amz-request-id` e `x-amz-id-2`) que os clientes podem acessar de seus aplicativos (por exemplo, de um objeto JavaScript `XMLHttpRequest`).

Configurar o compartilhamento de recursos de origem cruzada (CORS)

O compartilhamento de recursos de origem cruzada (CORS) define uma maneira de os aplicativos web clientes carregados em um domínio interagirem com recursos em outro domínio. Com o suporte do CORS, você pode criar aplicações web no lado do cliente com o Amazon S3 e permitir seletivamente o acesso de origem cruzada aos seus recursos do Amazon S3.

Esta seção mostra como habilitar o CORS usando o console do Amazon S3, a API REST do Amazon S3 e os AWS SDKs. Para configurar seu bucket para permitir solicitações de origem cruzada, adicione uma configuração de CORS ao bucket. Uma configuração CORS é um documento que define regras que identificam as origens que você permitirá que acessem seu bucket, as operações (métodos HTTP) compatíveis para cada origem e outras informações específicas da operação. No console do S3, a configuração CORS deve ser um documento JSON.

Para obter exemplos de configurações de CORS em JSON e XML, consulte Elementos de uma configuração de CORS.

Uso do console do S3

Esta seção explica como usar o console do Amazon S3 para adicionar uma configuração de compartilhamento de recursos de origem cruzada (CORS) para um bucket do S3.

Quando você permitir o CORS no bucket, as listas de controle de acesso (ACLs) e outras políticas de permissão de acesso continuarão sendo aplicadas.

> **Important**
>
> No novo console do S3, a configuração CORS deve ser JSON. Para obter exemplos de configurações de CORS em JSON e XML, consulte Elementos de uma configuração de CORS.

Para adicionar uma configuração CORS a um bucket do S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets de uso geral.
3. Na lista de buckets, escolha o nome do bucket para o qual você deseja criar uma política de bucket.
4. Escolha Permissions (Permissões).
5. Na seção Cross-origin resource sharing (CORS) (Compartilhamento de recursos de origem cruzada (CORS)) escolha Edit (Editar).
6. Na caixa de texto CORS configuration editor (Editor de configuração CORS), digite ou copie e cole uma nova configuração CORS, ou edite uma configuração existente.

   A configuração de CORS é um arquivo JSON. O texto que você digita no editor deve ser um JSON válido. Para obter mais informações, consulte Elementos de uma configuração de CORS.
7. Selecione Save changes.

   > **Note**
   >
   > O Amazon S3 exibe o Nome de recurso da Amazon (ARN) para o bucket próximo ao título CORS configuration editor (Editor de configuração CORS). Para obter mais

informações sobre ARNs, consulte Nomes do recurso da Amazon (ARNs) e namespaces do serviço da AWS noReferência geral da Amazon Web Services.

Uso dos SDKs da AWS

Você pode usar o AWS SDK para gerenciar o Cross-Origin Resource Sharing (CORS – Compartilhamento de recursos entre origens) para um bucket. Para obter mais informações sobre CORS, consulte Usar o compartilhamento de recursos de origem cruzada (CORS).

Veja os seguintes exemplos:

- Cria uma configuração do CORS e define a configuração em um bucket
- Recupera a configuração e a altera adicionando uma regra
- Adiciona a configuração modificada ao bucket
- Exclui a configuração

Java

Example

Example

Consulte instruções sobre como criar e testar uma amostra funcional em Getting Started no Guia do desenvolvedor do AWS SDK para Java.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.BucketCrossOriginConfiguration;
import com.amazonaws.services.s3.model.CORSRule;

import java.io.IOException;
import java.util.ArrayList;
import java.util.Arrays;
import java.util.List;
```

```
public class CORS {

    public static void main(String[] args) throws IOException {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "*** Bucket name ***";

        // Create two CORS rules.
        List<CORSRule.AllowedMethods> rule1AM = new
 ArrayList<CORSRule.AllowedMethods>();
        rule1AM.add(CORSRule.AllowedMethods.PUT);
        rule1AM.add(CORSRule.AllowedMethods.POST);
        rule1AM.add(CORSRule.AllowedMethods.DELETE);
        CORSRule rule1 = new
 CORSRule().withId("CORSRule1").withAllowedMethods(rule1AM)
                .withAllowedOrigins(Arrays.asList("http://*.example.com"));

        List<CORSRule.AllowedMethods> rule2AM = new
 ArrayList<CORSRule.AllowedMethods>();
        rule2AM.add(CORSRule.AllowedMethods.GET);
        CORSRule rule2 = new
 CORSRule().withId("CORSRule2").withAllowedMethods(rule2AM)
                .withAllowedOrigins(Arrays.asList("*")).withMaxAgeSeconds(3000)
                .withExposedHeaders(Arrays.asList("x-amz-server-side-encryption"));

        List<CORSRule> rules = new ArrayList<CORSRule>();
        rules.add(rule1);
        rules.add(rule2);

        // Add the rules to a new CORS configuration.
        BucketCrossOriginConfiguration configuration = new
 BucketCrossOriginConfiguration();
        configuration.setRules(rules);

        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(clientRegion)
                    .build();

            // Add the configuration to the bucket.
            s3Client.setBucketCrossOriginConfiguration(bucketName, configuration);

            // Retrieve and display the configuration.
            configuration = s3Client.getBucketCrossOriginConfiguration(bucketName);
```

```
            printCORSConfiguration(configuration);

            // Add another new rule.
            List<CORSRule.AllowedMethods> rule3AM = new
ArrayList<CORSRule.AllowedMethods>();
            rule3AM.add(CORSRule.AllowedMethods.HEAD);
            CORSRule rule3 = new
CORSRule().withId("CORSRule3").withAllowedMethods(rule3AM)
                    .withAllowedOrigins(Arrays.asList("http://www.example.com"));

            rules = configuration.getRules();
            rules.add(rule3);
            configuration.setRules(rules);
            s3Client.setBucketCrossOriginConfiguration(bucketName, configuration);

            // Verify that the new rule was added by checking the number of rules in
the
            // configuration.
            configuration = s3Client.getBucketCrossOriginConfiguration(bucketName);
            System.out.println("Expected # of rules = 3, found " +
configuration.getRules().size());

            // Delete the configuration.
            s3Client.deleteBucketCrossOriginConfiguration(bucketName);
            System.out.println("Removed CORS configuration.");

            // Retrieve and display the configuration to verify that it was
            // successfully deleted.
            configuration = s3Client.getBucketCrossOriginConfiguration(bucketName);
            printCORSConfiguration(configuration);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }

    private static void printCORSConfiguration(BucketCrossOriginConfiguration
configuration) {
        if (configuration == null) {
```

```
            System.out.println("Configuration is null.");
        } else {
            System.out.println("Configuration has " +
 configuration.getRules().size() + " rules\n");

            for (CORSRule rule : configuration.getRules()) {
                System.out.println("Rule ID: " + rule.getId());
                System.out.println("MaxAgeSeconds: " + rule.getMaxAgeSeconds());
                System.out.println("AllowedMethod: " + rule.getAllowedMethods());
                System.out.println("AllowedOrigins: " + rule.getAllowedOrigins());
                System.out.println("AllowedHeaders: " + rule.getAllowedHeaders());
                System.out.println("ExposeHeader: " + rule.getExposedHeaders());
                System.out.println();
            }
        }
    }
}
```

.NET

Example

Para obter informações sobre como configurar e executar exemplos de código, consulte Conceitos básicos do AWS SDK for .NET no Guia do desenvolvedor do AWS SDK for .NET.

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Collections.Generic;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class CORSTest
    {
        private const string bucketName = "*** bucket name ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 s3Client;

        public static void Main()
```

```
        {
            s3Client = new AmazonS3Client(bucketRegion);
            CORSConfigTestAsync().Wait();
        }
        private static async Task CORSConfigTestAsync()
        {
            try
            {
                // Create a new configuration request and add two rules
                CORSConfiguration configuration = new CORSConfiguration
                {
                    Rules = new System.Collections.Generic.List<CORSRule>
                        {
                          new CORSRule
                          {
                            Id = "CORSRule1",
                            AllowedMethods = new List<string> {"PUT", "POST",
 "DELETE"},
                            AllowedOrigins = new List<string> {"http://
*.example.com"}
                          },
                          new CORSRule
                          {
                            Id = "CORSRule2",
                            AllowedMethods = new List<string> {"GET"},
                            AllowedOrigins = new List<string> {"*"},
                            MaxAgeSeconds = 3000,
                            ExposeHeaders = new List<string> {"x-amz-server-side-
encryption"}
                          }
                        }
                };

                // Add the configuration to the bucket.
                await PutCORSConfigurationAsync(configuration);

                // Retrieve an existing configuration.
                configuration = await RetrieveCORSConfigurationAsync();

                // Add a new rule.
                configuration.Rules.Add(new CORSRule
                {
                    Id = "CORSRule3",
                    AllowedMethods = new List<string> { "HEAD" },
```

```
                    AllowedOrigins = new List<string> { "http://www.example.com" }
                });

                // Add the configuration to the bucket.
                await PutCORSConfigurationAsync(configuration);

                // Verify that there are now three rules.
                configuration = await RetrieveCORSConfigurationAsync();
                Console.WriteLine();
                Console.WriteLine("Expected # of rulest=3; found:{0}",
configuration.Rules.Count);
                Console.WriteLine();
                Console.WriteLine("Pause before configuration delete. To continue,
click Enter...");
                Console.ReadKey();

                // Delete the configuration.
                await DeleteCORSConfigurationAsync();

                // Retrieve a nonexistent configuration.
                configuration = await RetrieveCORSConfigurationAsync();
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered on server. Message:'{0}' when
writing an object", e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
writing an object", e.Message);
            }
        }

        static async Task PutCORSConfigurationAsync(CORSConfiguration configuration)
        {

            PutCORSConfigurationRequest request = new PutCORSConfigurationRequest
            {
                BucketName = bucketName,
                Configuration = configuration
            };

            var response = await s3Client.PutCORSConfigurationAsync(request);
```

```
        }

        static async Task<CORSConfiguration> RetrieveCORSConfigurationAsync()
        {
            GetCORSConfigurationRequest request = new GetCORSConfigurationRequest
            {
                BucketName = bucketName

            };
            var response = await s3Client.GetCORSConfigurationAsync(request);
            var configuration = response.Configuration;
            PrintCORSRules(configuration);
            return configuration;
        }

        static async Task DeleteCORSConfigurationAsync()
        {
            DeleteCORSConfigurationRequest request = new
DeleteCORSConfigurationRequest
            {
                BucketName = bucketName
            };
            await s3Client.DeleteCORSConfigurationAsync(request);
        }

        static void PrintCORSRules(CORSConfiguration configuration)
        {
            Console.WriteLine();

            if (configuration == null)
            {
                Console.WriteLine("\nConfiguration is null");
                return;
            }

            Console.WriteLine("Configuration has {0} rules:",
configuration.Rules.Count);
            foreach (CORSRule rule in configuration.Rules)
            {
                Console.WriteLine("Rule ID: {0}", rule.Id);
                Console.WriteLine("MaxAgeSeconds: {0}", rule.MaxAgeSeconds);
                Console.WriteLine("AllowedMethod: {0}", string.Join(", ",
rule.AllowedMethods.ToArray()));
```

```
                Console.WriteLine("AllowedOrigins: {0}", string.Join(", ",
 rule.AllowedOrigins.ToArray()));
                Console.WriteLine("AllowedHeaders: {0}", string.Join(", ",
 rule.AllowedHeaders.ToArray()));
                Console.WriteLine("ExposeHeader: {0}", string.Join(", ",
 rule.ExposeHeaders.ToArray()));
            }
        }
    }
}
```

Uso da API REST

Para definir uma configuração de CORS no bucket, use o AWS Management Console. Se o seu aplicativo exigir, você também pode enviar solicitações REST diretamente. As seções a seguir na Referência da API do Amazon Simple Storage Service descrevem as ações da API REST relacionadas à configuração CORS:

- PutBucketCors
- GetBucketCors
- DeleteBucketCors
- Objeto OPTIONS

Testar o CORS

Para testar a configuração de CORS, uma solicitação de CORS preliminar pode ser enviada com o método `OPTIONS` para que o servidor responda se é aceitável enviar a solicitação. Quando o Amazon S3 recebe uma solicitação preliminar, ele avalia a configuração de CORS para o bucket e usa a primeira regra `CORSRule` correspondente à solicitação de entrada para permitir uma solicitação entre origens. Para que uma regra seja correspondente, as seguintes condições devem ser satisfeitas:

- O cabeçalho `Origin` em uma solicitação do CORS para seu bucket deve corresponder às origens do elemento `AllowedOrigins` na configuração do CORS.
- Os métodos HTTP especificados no `Access-Control-Request-Method` em uma solicitação de CORS para o bucket devem corresponder ao método ou aos métodos listados no elemento `AllowedMethods` na configuração de CORS.

- Os cabeçalhos listados no cabeçalho `Access-Control-Request-Headers` em uma solicitação preliminar devem corresponder aos cabeçalhos no elemento `AllowedHeaders` na configuração de CORS.

Veja a seguir um exemplo de configuração de CORS. Para criar uma configuração de CORS, consulte Configurar CORS. Para ver mais exemplos de configuração de CORS, consulte Elementos de uma configuração de CORS.

Para obter orientação sobre como configurar e solucionar problemas de regras de CORS, consulte Como configuro o CORS no Amazon S3 e confirmo as regras do CORS usando cURL? no Centro de Conhecimento do AWS re:Post.

JSON

```
[
    {
        "AllowedHeaders": [
            "Authorization"
        ],
        "AllowedMethods": [
            "GET",
            "PUT",
            "POST",
            "DELETE"
        ],
        "AllowedOrigins": [
            "http://www.example1.com"
        ],
        "ExposeHeaders":  [
             "x-amz-meta-custom-header"
        ]

    }
]
```

Para testar a configuração de CORS, é possível enviar uma verificação `OPTIONS` preliminar usando o comando CURL a seguir. CURL é uma ferramenta de linha de comando que pode ser usada para interagir com o S3. Para ter mais informações, consulte CURL.

```
curl -v -X OPTIONS \
```

```
  -H "Origin: http://www.example1.com" \
  -H "Access-Control-Request-Method: PUT" \
  -H "Access-Control-Request-Headers: Authorization" \
  -H "Access-Control-Expose-Headers: x-amz-meta-custom-header"\
     "http://bucket_name.s3.amazonaws.com/object_prefix_name"
```

No exemplo acima, o comando `curl -v -x OPTIONS` é usado para enviar uma solicitação preliminar ao S3 e perguntar se o S3 tem permissão para enviar uma solicitação PUT em um objeto por meio do `http://www.example1.com` de origem cruzada. Os cabeçalhos `Access-Control-Request-Headers` e `Access-Control-Expose-Headers` são opcionais.

- Em resposta ao cabeçalho `Access-Control-Request-Method` na solicitação `OPTIONS` preliminar, o Amazon S3 exibe a lista de métodos permitidos quando há correspondência com os métodos solicitados.
- Em resposta ao cabeçalho `Access-Control-Request-Headers` na solicitação `OPTIONS` preliminar, o Amazon S3 exibe a lista de cabeçalhos permitidos quando há correspondência com os cabeçalhos solicitados.
- Em resposta ao cabeçalho `Access-Control-Expose-Headers` na solicitação `OPTIONS` preliminar, o Amazon S3 exibe uma lista de cabeçalhos permitidos quando os cabeçalhos solicitados podem ser acessados por scripts em execução no navegador.

> **Note**
>
> Ao enviar uma solicitação preliminar, se algum dos cabeçalhos da solicitação de CORS não for permitido, nenhum dos cabeçalhos de CORS de resposta será exibido.

Em resposta a essa solicitação `OPTIONS` preliminar, você receberá uma resposta `200 OK`. Para conhecer os códigos de erro comuns recebidos ao testar o CORS e ter mais informações para resolver problemas relacionados ao CORS, consulte Solução de problemas do CORS.

```
< HTTP/1.1 200 OK
< Date: Fri, 12 Jul 2024 00:23:51 GMT
< Access-Control-Allow-Origin: http://www.example1.com
< Access-Control-Allow-Methods: GET, PUT, POST, DELETE
< Access-Control-Allow-Headers: Authorization
< Access-Control-Expose-Headers: x-amz-meta-custom-header
< Access-Control-Allow-Credentials: true
```

```
< Vary: Origin, Access-Control-Request-Headers, Access-Control-Request-Method
< Server: AmazonS3
< Content-Length: 0
```

Solução de problemas do CORS

Os tópicos a seguir podem ajudar a solucionar alguns problemas comuns do CORS relacionados ao S3.

Tópicos

- 403 Erro proibido: o CORS não está habilitado para este bucket.
- 403 Erro proibido: essa solicitação do CORS não é permitida.
- Cabeçalhos não encontrados na resposta do CORS
- Considerações sobre o CORS nas integrações de proxy do S3

403 Erro proibido: o CORS não está habilitado para este bucket.

O erro `403 Forbidden` a seguir ocorre quando uma solicitação de origem cruzada é enviada ao Amazon S3, mas o CORS não está configurado no bucket do S3.

Erro: HTTP/1.1 403 Resposta proibida do CORS: o CORS não está habilitado para esse bucket.

A configuração do CORS é um documento ou uma política com regras que identificam as origens que você permitirá que acessem o bucket, as operações (métodos HTTP) compatíveis com cada origem e outras informações específicas da operação. Veja como configurar o CORS no S3 usando o console do Amazon S3, AWS SDKs e a API REST. Para ter mais informações sobre o CORS e exemplos da configuração correspondente, consulte Elementos do CORS.

403 Erro proibido: essa solicitação do CORS não é permitida.

O erro `403 Forbidden` a seguir é recebido quando uma regra do CORS na configuração correspondente não coincide com os dados da sua solicitação.

Erro: HTTP/1.1 403 Resposta proibida do CORS: essa solicitação do CORS não é permitida.

Como resultado, esse erro `403 Forbidden` pode ocorrer por vários motivos:

- A origem não é permitida.

- Métodos não são permitidos.
- Cabeçalhos solicitados não são permitidos.

Para cada solicitação que o Amazon S3 recebe, é necessário ter uma regra do CORS na configuração correspondente que coincida com os dados na solicitação.

A origem não é permitida

O cabeçalho `Origin` em uma solicitação do CORS para seu bucket deve corresponder às origens do elemento `AllowedOrigins` na configuração do CORS. Um caractere curinga ("`*`") no elemento `AllowedOrigins` corresponderia a todos os métodos HTTP. Para ter mais informações sobre como atualizar o elemento `AllowedOrigins`, consulte Configurar o compartilhamento de recursos de origem cruzada (CORS).

Por exemplo, se somente o domínio `http://www.example1.com` estiver incluído no elemento `AllowedOrigins`, uma solicitação do CORS enviada do domínio `http://www.example2.com` receberá o erro `403 Forbidden`.

O exemplo a seguir mostra parte de uma configuração do CORS que inclui o domínio `http://www.example1.com` no elemento `AllowedOrigins`.

```
"AllowedOrigins":[
   "http://www.example1.com"
]
```

Para que uma solicitação do CORS enviada do domínio `http://www.example2.com` seja bem-sucedida, o domínio `http://www.example2.com` deve ser incluído no elemento `AllowedOrigins` da configuração do CORS.

```
"AllowedOrigins":[
   "http://www.example1.com"
   "http://www.example2.com"
]
```

Métodos não são permitidos

Os métodos HTTP especificados no `Access-Control-Request-Method` em uma solicitação de CORS para o bucket devem corresponder ao método ou aos métodos listados no elemento

`AllowedMethods` na configuração de CORS. Um caractere curinga (`"*"`) em `AllowedMethods` corresponderia a todos os métodos HTTP. Para ter mais informações sobre como atualizar o elemento `AllowedOrigins`, consulte Configurar o compartilhamento de recursos de origem cruzada (CORS).

Na configuração do CORS, é possível especificar os seguintes métodos para o elemento `AllowedMethods`:

- `GET`
- `PUT`
- `POST`
- `DELETE`
- `HEAD`

O exemplo a seguir mostra parte de uma configuração do CORS que inclui o método `GET` no elemento `AllowedMethods`. Somente solicitações que incluíssem o método `GET` seriam bem-sucedidas.

```
"AllowedMethods":[
   "GET"
]
```

Se um método HTTP (por exemplo, `PUT`) fosse usado em uma solicitação do CORS ou incluído em uma solicitação de pré-processamento do CORS no bucket, mas o método não estivesse presente na configuração do CORS, a solicitação geraria um erro `403 Forbidden`. Para permitir essa solicitação do CORS ou a solicitação de pré-processamento do CORS, o método `PUT` deve ser adicionado à sua configuração do CORS.

```
"AllowedMethods":[
   "GET"
   "PUT"
]
```

Cabeçalhos solicitados não são permitidos

Os cabeçalhos listados no cabeçalho `Access-Control-Request-Headers` em uma solicitação de pré-processamento devem corresponder aos cabeçalhos no elemento `AllowedHeaders` na

configuração do CORS. Para ver uma lista de cabeçalhos comuns que podem ser usados em solicitações ao Amazon S3, consulte Common Request Headers. Para ter mais informações sobre como atualizar o elemento `AllowedHeaders`, consulte Configurar o compartilhamento de recursos de origem cruzada (CORS).

O exemplo a seguir mostra parte de uma configuração do CORS que inclui o cabeçalho `Authorization` no elemento `AllowedHeaders`. Somente solicitações para o cabeçalho `Authorization` seriam bem-sucedidas.

```
"AllowedHeaders":  [
    "Authorization"
]
```

Se um cabeçalho, por exemplo, `Content-MD5`, fosse incluído em uma solicitação do CORS, mas o cabeçalho não estivesse presente na configuração correspondente, a solicitação geraria um erro `403 Forbidden`. Para permitir essa solicitação do CORS, o cabeçalho `Content-MD5` deve ser adicionado à sua configuração do CORS. Se você quiser transmitir os cabeçalhos `Authorization` e `Content-MD5` em uma solicitação do CORS para o bucket, confirme se os dois cabeçalhos estão incluídos no elemento `AllowedHeaders` em sua configuração do CORS.

```
"AllowedHeaders":  [
    "Authorization"
    "Content-MD5"
]
```

Cabeçalhos não encontrados na resposta do CORS

O elemento `ExposeHeaders` na configuração do CORS identifica quais cabeçalhos de resposta você gostaria de tornar acessíveis aos scripts e às aplicações executados em navegadores, em resposta a uma solicitação do CORS.

Se os objetos armazenados no bucket do S3 tiverem metadados definidos pelo usuário (por exemplo, `x-amz-meta-custom-header`) além dos dados de resposta, esse cabeçalho personalizado poderá conter metadados ou informações adicionais a serem acessados do código JavaScript do lado do cliente. No entanto, por padrão, os navegadores bloqueiam o acesso a cabeçalhos personalizados por motivos de segurança. Para permitir que o JavaScript do lado do cliente acesse cabeçalhos personalizados, é necessário incluir o cabeçalho na configuração do CORS.

No exemplo abaixo, o cabeçalho `x-amz-meta-custom-header1` está incluído no elemento `ExposeHeaders`. O `x-amz-meta-custom-header2` não está incluído no elemento `ExposeHeaders` e não está presente na configuração do CORS. Na resposta, somente os valores incluídos no elemento `ExposeHeaders` seriam exibidos. Se a solicitação incluísse o cabeçalho `x-amz-meta-custom-header2` no cabeçalho `Access-Control-Expose-Headers`, a resposta ainda exibiria `200 OK`. No entanto, somente o cabeçalho permitido, por exemplo, `x-amz-meta-custom-header`, seria exibido na resposta.

```
"ExposeHeaders":  [
    "x-amz-meta-custom-header1"
]
```

Para garantir que todos os cabeçalhos apareçam na resposta, adicione todos os cabeçalhos permitidos ao elemento `ExposeHeaders` na configuração do CORS, conforme mostrado abaixo.

```
"ExposeHeaders":  [
    "x-amz-meta-custom-header1",
    "x-amz-meta-custom-header2"
]
```

Considerações sobre o CORS nas integrações de proxy do S3

Se você estiver enfrentando erros e já tiver conferido a configuração do CORS no bucket do S3, e a solicitação de origem cruzada for enviada para proxies, como o AWS CloudFront, tente o seguinte:

- Defina as configurações para permitir o método `OPTIONS` para solicitações HTTP.
- Configure o proxy para encaminhar os seguintes cabeçalhos: `Origin`, `Access-Control-Request-Headers` e `Access-Control-Request-Method`.
- Configure as definições de proxy para incluir o cabeçalho de origem na chave de cache. Isso é importante porque os proxies de armazenamento em cache que não incluem o cabeçalho de origem na respectiva chave de cache podem fornecer respostas em cache que não incluem os cabeçalhos de CORS apropriados para origens diferentes.

Alguns proxies fornecem recursos predefinidos para solicitações do CORS. Por exemplo, no CloudFront, você pode configurar uma política que inclua os cabeçalhos

que permitem solicitações de compartilhamento de recursos entre origens (CORS) quando a origem é um bucket do Amazon S3.

Essa política tem as seguintes configurações:

- Cabeçalhos incluídos nas solicitações de origem:

  `Origin`

  `Access-Control-Request-Headers`

  `Access-Control-Request-Method`
- Cookies incluídos nas solicitações de origem: nenhum
- Strings de consulta incluídas em solicitações de origem: nenhuma

Para ter mais informações, consulte Controlar as solicitações de origem com uma política ou Usar políticas de solicitação de origem gerenciadas no Guia do desenvolvedor do CloudFront.

Tutoriais de site estático

Os tutoriais ou as demonstrações a seguir apresentam procedimentos de como criar e configurar um bucket de uso geral do Amazon S3 para hospedagem de site estático e hospedagem de streaming de vídeo sob demanda. O objetivo desses tutoriais é fornecer orientação geral. Esses tutoriais foram projetados para um ambiente de tipo de laboratório e usam nomes de empresas, nomes de usuários e assim por diante. Eles não se destinam ao uso direto em um ambiente de produção sem uma revisão e adaptação cuidadosas para atender às necessidades exclusivas do ambiente da organização.

- Hospedagem de transmissão sob demanda com o Amazon S3, Amazon CloudFront e Amazon Route 53: é possível usar o Amazon S3 com o Amazon CloudFront para hospedar e ver vídeos sob demanda, com segurança e escalabilidade. Quando o vídeo estiver empacotado nos formatos corretos, você poderá armazená-lo em um servidor ou em um bucket de uso geral do S3 e, depois, enviá-lo com o CloudFront conforme solicitado pelos visualizadores. Nesse tutorial, você aprenderá a configurar um bucket de uso geral para hospedar o streaming de vídeo sob demanda usando o CloudFront para entrega e o Amazon Route 53 para gerenciamento de Sistema de Nomes de Domínio (DNS) e de domínio personalizado. O CloudFront veiculará o vídeo de seu cache, recuperando-o do bucket de uso geral somente se ele ainda não estiver armazenado em cache. Esse recurso de gerenciamento de cache acelera a entrega de seu vídeo aos espectadores globalmente, com baixa latência, alto throughput e altas velocidades de transferência. Para mais informações sobre o gerenciamento do cache do CloudFront, consulte Otimizar o armazenamento em cache e a disponibilidade no Guia do desenvolvedor do Amazon CloudFront.

- Configurar um site estático: é possível configurar um bucket de uso geral para funcionar como um site estático. Esse tutorial mostra as etapas de hospedagem de um site no Amazon S3, incluindo como criar um bucket, como habilitar a hospedagem de site estático no console do S3, como criar um documento de índice e como criar um documento de erro. Consulte mais informações em Hospedagem de um site estático usando o Amazon S3.
- Configurar um site estático usando um domínio personalizado registrado no Route 53: é possível criar e configurar um bucket de uso geral para hospedar um site estático e criar redirecionamentos no S3 para um site com um nome de domínio personalizado que é registrado com o Amazon Route 53. Você usa o Route 53 para registrar domínios e definir onde você deseja rotear o tráfego de internet para o seu domínio. Esse tutorial mostra como criar registros de alias do Route 53 que roteia o tráfego para o domínio e o subdomínio ao bucket de uso geral que contém o arquivo HTML. Consulte mais informações em Use your domain for a static website in an Amazon S3 bucket no Guia do desenvolvedor do Amazon Route 53. Depois de concluir esse tutorial, você tem a opção de usar o CloudFront para melhorar o desempenho do seu site. Consulte mais informações em Acelerar seu site com o Amazon CloudFront.
- Deploying a static website to AWS Amplify Hosting from an S3 general purpose bucket: recomendamos que você use o AWS Amplify Hosting para hospedar conteúdo de site estático armazenado no S3. O Amplify Hosting é um serviço totalmente gerenciado que facilita a implantação de seus sites em uma rede de entrega de conteúdo (CDN) disponível globalmente, desenvolvida pelo Amazon CloudFront, permitindo hospedagem segura de sites estáticos sem configuração extensiva. Com o AWS Amplify Hosting, você pode selecionar a localização de seus objetos no bucket de uso geral, implantar seu conteúdo em uma CDN gerenciada e gerar um URL HTTPS público para que seu site possa ser acessado em qualquer lugar. Para obter mais informações, consulte Deploying a static website from S3 using the Amplify console no Guia do usuário do AWS Amplify Hosting.

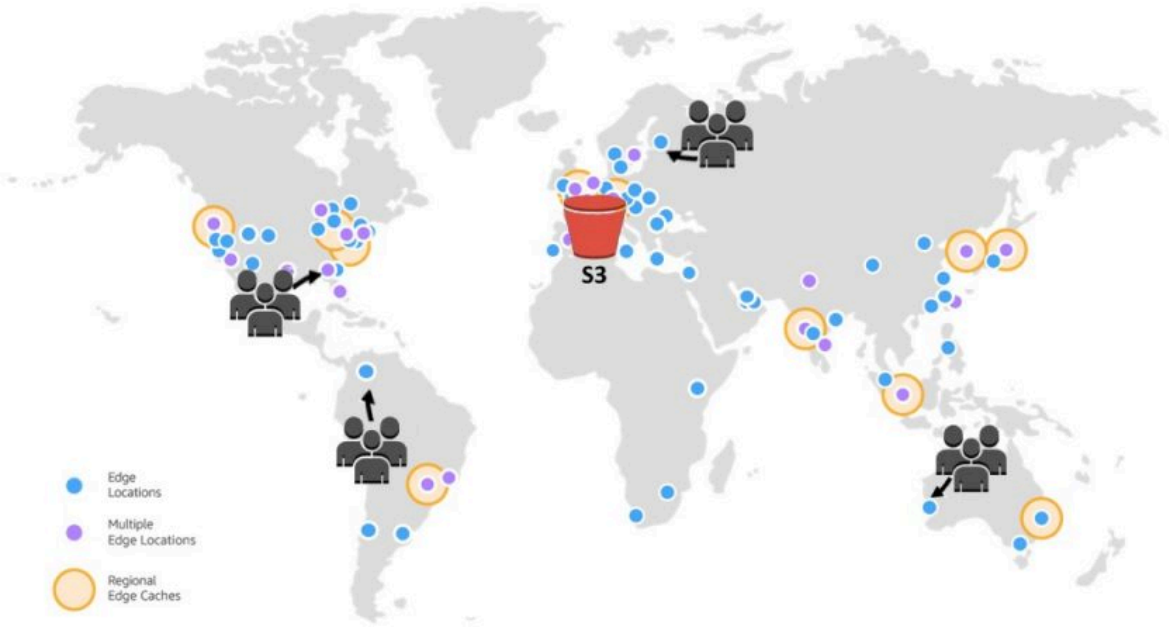
Tutorial: Hospedagem de transmissão sob demanda com o Amazon S3, Amazon CloudFront e Amazon Route 53

Você pode usar o Amazon S3 com o Amazon CloudFront para hospedar vídeos para visualização sob demanda, com segurança e escalabilidade. Transmissão de vídeo sob demanda (VOD - Video On Demand) significa que o conteúdo do vídeo é armazenado em um servidor e os espectadores podem assisti-lo a qualquer momento.

O CloudFront é um serviço de rede de entrega de conteúdo (CDN) rápido, altamente seguro e programável. O CloudFront pode fornecer seu conteúdo de modo seguro por HTTPS a partir de

todos os locais da borda do CloudFront. Para mais informações sobre o CloudFront, consulte O que é o Amazon CloudFront? no Guia do desenvolvedor do Amazon CloudFront.

O cache do CloudFront reduz o número de solicitações às quais seu servidor de origem deve responder diretamente. Quando um espectador (usuário final) solicita um vídeo que você veicula com o CloudFront, a solicitação é encaminhada para o local da borda mais próximo de onde o visualizador está localizado. O CloudFront veicula o vídeo de seu cache, recuperando-o do bucket do S3 somente se ele ainda não estiver armazenado em cache. Esse recurso de gerenciamento de cache acelera a entrega de seu vídeo aos espectadores globalmente, com baixa latência, alto throughput e altas velocidades de transferência. Para mais informações sobre o gerenciamento do cache do CloudFront, consulte Otimizar o armazenamento em cache e a disponibilidade no Guia do desenvolvedor do Amazon CloudFront.



Objetivo

Neste tutorial, você configura um bucket do S3 para hospedar transmissão de vídeo sob demanda usando o CloudFront para entrega e o Amazon Route 53 para gerenciamento de Sistema de Nomes de Domínio (DNS) e de domínio personalizado.

Tópicos

- Pré-requisitos: registrar e configurar um domínio personalizado com o Route 53

- Etapa 1: criar um bucket do S3
- Etapa 2: carregar um vídeo no bucket do S3
- Etapa 3: Criar uma identidade do acesso de origem do CloudFront
- Etapa 4: criar uma distribuição do CloudFront
- Etapa 5: Acessar o vídeo por meio da distribuição do CloudFront
- Etapa 6: Configurar sua distribuição do CloudFront para usar o seu nome de domínio personalizado
- Etapa 7: acessar o vídeo do S3 por meio da distribuição do CloudFront com o nome de domínio personalizado
- (Opcional) Etapa 8: exibir dados sobre solicitações recebidas pela distribuição do CloudFront
- Etapa 9: limpeza
- Próximas etapas

Pré-requisitos: registrar e configurar um domínio personalizado com o Route 53

Antes de iniciar este tutorial, você deve se inscrever e configurar um domínio personalizado (por exemplo, **`example.com`**) no Route 53 para poder configurar sua distribuição do CloudFront para usar um nome de domínio personalizado depois.

Sem um nome de domínio personalizado, seu vídeo do S3 é acessível ao público e hospedado por meio do CloudFront em um URL semelhante a este:

```
https://CloudFront distribution domain name/Path to an S3 video
```

Por exemplo, **`https://d111111abcdef8.cloudfront.net/sample.mp4`**.

Depois de configurar sua distribuição do CloudFront para usar um nome de domínio personalizado configurado com o Route 53, seu vídeo do S3 fica publicamente acessível e hospedado pelo CloudFront em um URL semelhante a este:

```
https://CloudFront distribution alternate domain name/Path to an S3 video
```

Por exemplo, **`https://www.example.com/sample.mp4`**. Um nome de domínio personalizado é mais simples e intuitivo para os espectadores usarem.

Para registrar um nome de domínio personalizado, consulte Registro de um novo nome de domínio usando o Route 53 no Guia do desenvolvedor do Amazon Route 53.

Quando você registra um nome de domínio com o Route 53, ele cria a zona hospedada que você usará posteriormente neste tutorial. Esta zona hospedada é onde você armazena informações sobre como encaminhar o tráfego para seu domínio, por exemplo, para uma instância do Amazon EC2 ou uma distribuição do CloudFront.

Há tarifas associadas ao registro de domínios, à sua zona hospedada e às consultas de DNS recebidas pelo seu domínio. Para obter mais informações, consulte Definição de preço do Amazon Route 53.

> **Note**
>
> Ao registrar um domínio, você gasta dinheiro imediatamente e é irreversível. Você pode escolher não renovar automaticamente o domínio, mas paga antecipadamente e adquire o domínio por um ano). Para obter mais informações, consulte Registrar um novo domínio no Guia do desenvolvedor do Amazon Route 53.

Etapa 1: criar um bucket do S3

Crie um bucket para armazenar o vídeo original que você pretende transmitir.

Para criar um bucket

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Na barra de navegação na parte superior da página, escolha o nome da Região da AWS exibida no momento. Em seguida, escolha a região na qual você deseja criar um bucket.

   > **Note**
   >
   > Para reduzir a latência e os custos e atender aos requisitos regulatórios, selecione uma região perto de você. Os objetos armazenados em uma região nunca saem dessa região, a menos que você os transfira para outra região. Para obter uma lista de Regiões da AWS do Amazon S3, consulte Endpoints de AWS service (Serviço da AWS) no Referência geral da Amazon Web Services.

3. No painel de navegação à esquerda, escolha Buckets de uso geral.
4. Selecione Create bucket (Criar bucket). A página Create bucket (Criar bucket) é aberta.
5. Em Bucket name (Nome do bucket), insira um nome para o seu bucket (por exemplo, **`tutorial-bucket`**).

   Para obter mais informações sobre como nomear buckets no Amazon S3, consulte Regras de nomenclatura de buckets de uso geral.
6. Em Region (Região), escolha a Região da AWS onde deseja que o bucket resida.

   Se possível, você deve escolher a região mais próxima da maioria dos seus espectadores. Para obter mais informações sobre a região do bucket, consulte Visão geral dos buckets de uso geral.
7. Para Block Public Access settings for this bucket (Configurações de acesso de bloqueio público para este bucket), mantenha as configurações padrão (Block allpublic access (Bloquear todo acesso público) está habilitado).

   Mesmo com Block all public access (Bloquear todo acesso público) habilitado, os espectadores ainda podem acessar o vídeo carregado por meio do CloudFront. Esse recurso é uma grande vantagem do uso do CloudFront para hospedar um vídeo armazenado no S3.

   Recomendamos que você mantenha todas as configurações ativadas, a menos que precise desabilitar uma ou mais delas para seu caso de uso. Para obter mais informações sobre como bloquear o acesso público, consulte Bloquear o acesso público ao armazenamento do Amazon S3.
8. Mantenha as configurações restantes definidas conforme os padrões.

   (Opcional) Se quiser definir configurações de bucket adicionais para o caso de uso específico, consulte Criar um bucket de uso geral.
9. Selecione Create bucket (Criar bucket).

Etapa 2: carregar um vídeo no bucket do S3

O procedimento a seguir descreve como carregar um arquivo de vídeo em um bucket do S3 usando o console. Se você for carregar muitos arquivos de vídeo grandes para o S3, pode ser interessante usar o Amazon S3 Transfer Acceleration para configurar transferências de arquivos rápidas e seguras. O Transfer Acceleration pode acelerar o carregamento de vídeo no seu bucket do S3 para transferências de longa distância de vídeos maiores. Para obter mais informações, consulte Configurar transferências de arquivos rápidas e seguras usando o Amazon S3 Transfer Acceleration.

Para carregar o arquivo para o bucket

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets de uso geral.
3. Na lista Buckets de uso geral, escolha o nome do bucket que você criou na Etapa 1 (por exemplo, **`tutorial-bucket`**) para fazer upload do arquivo nele.
4. Na guia Objects (Objetos) do bucket, escolha Upload (Fazer upload).
5. Na página Upload (Carregar), em Files and folders (Arquivos e pastas), escolha Add files (Adicionar arquivos).
6. Escolha um arquivo para carregar e, em seguida, escolha Open (Abrir).

   Por exemplo, você pode carregar um arquivo de vídeo chamado `sample.mp4`.
7. Escolha Carregar.

Etapa 3: Criar uma identidade do acesso de origem do CloudFront

Para restringir o acesso direto ao vídeo a partir do seu bucket do S3, crie um usuário especial do CloudFront denominado identidade do acesso de origem (OAI). Você vai associar a OAI à sua distribuição mais adiante neste tutorial. Usando uma OAI, você garante que os espectadores não possam ignorar o CloudFront e obter o vídeo diretamente do bucket do S3. Somente a OAI do CloudFront pode acessar o arquivo no bucket do S3. Para obter mais informações, consulte Restrição de acesso ao conteúdo do Amazon S3 usando uma OAI no Guia do desenvolvedor do Amazon CloudFront.

Para criar uma OAI do CloudFront

1. Faça login no AWS Management Console e abra o console do CloudFront em https://console.aws.amazon.com/cloudfront/v4/home.
2. Na seção Segurança do painel de navegação esquerdo, escolha Acesso de origem.
3. Na guia Identidades, escolha Criar uma identidade de acesso de origem.
4. Insira um nome (por exemplo, **`S3-OAI`**) para a nova identidade do acesso de origem.
5. Escolha Criar.

Etapa 4: criar uma distribuição do CloudFront

Para usar o CloudFront para oferecer e distribuir o vídeo em seu bucket do S3, você deve criar uma distribuição do CloudFront.

Subetapas

- Crie uma distribuição do CloudFront
- Revise a política de bucket

Crie uma distribuição do CloudFront

1. Faça login no AWS Management Console e abra o console do CloudFront em https://console.aws.amazon.com/cloudfront/v4/home.
2. No painel de navegação esquerdo, escolha Distributions (Distribuições).
3. Escolha Create distribution (Criar distribuição).
4. Na seção Origin (Origem), para Origin domain (Domínio de origem), escolha o nome de domínio de sua origem do S3 que começa com o nome do bucket do S3 criado na Etapa 1 (por exemplo, **`tutorial-bucket`**).
5. Em Acesso de origem, selecione Identidades de acesso herdadas.
6. Em Origin access identity (Identidade do acesso de origem), escolha a identidade do acesso de origem que você criou na Etapa 3 (por exemplo, **`S3-OAI`**).
7. Em Bucket policy (Política de bucket), escolha Yes, update the bucket policy (Sim, atualizar a política de bucket).
8. Para Default cache behavior (Comportamento do cache padrão), em Viewer protocol policy (Política de protocolo do espectador), escolha Redirect HTTP to HTTPS (Redirecionar HTTP para HTTPS).

   Quando você escolhe este recurso, as solicitações de HTTP são automaticamente redirecionadas para HTTPS para proteger seu site e proteger os dados de seus espectadores.
9. Para as outras configurações na seção Default cache behaviors (Configurações de comportamento de cache padrão), mantenha os valores padrão.

   (Opcional) Você pode controlar o tempo de permanência dos arquivos em um cache do CloudFront antes que o CloudFront encaminhe outra solicitação para a origem. A diminuição da duração permite fornecer conteúdo dinâmico. Aumentar a duração significa que os espectadores obtêm uma melhor performance, pois é mais provável que seus arquivos sejam fornecidos

diretamente do cache de borda. Uma duração maior também reduz a carga na origem. Para obter mais informações, consulte Gerenciamento do tempo que o conteúdo permanece em um cache de borda (validade) no Guia do desenvolvedor do Amazon CloudFront.

10. Para as outras seções, mantenha as demais configurações definidas como os padrões.

    Para obter mais informações sobre essas opções de configuração, consulte Valores que você especifica quando cria ou atualiza uma distribuição no Guia do desenvolvedor do Amazon CloudFront.

11. Na parte inferior da página, escolha Create Distribution (Criar distribuição).
12. Na guia General (Geral) da sua distribuição do CloudFront, em Details (Detalhes), o valor da coluna Last modified (Última modificação) para sua distribuição muda de Deploying (Em implantação) para o carimbo de data e hora em que a distribuição foi modificada pela última vez. Normalmente, esse processo leva alguns minutos.

Revise a política de bucket

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets.
3. Na lista Buckets, escolha o nome do bucket que você usou antes, como a origem de sua distribuição do CloudFront (por exemplo, **`tutorial-bucket`**).
4. Escolha a aba Permissões.
5. Na seção Bucket policy (Política de bucket), confirme que você vê uma instrução semelhante à seguinte no texto da política de bucket:

```
{
    "Version": "2008-10-17",
    "Id": "PolicyForCloudFrontPrivateContent",
    "Statement": [
        {
            "Sid": "1",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::cloudfront:user/CloudFront Origin Access
 Identity EH1HDMB1FH2TC"
            },
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::tutorial-bucket/*"
```

```
        }
    ]
}
```

Esta é a instrução que sua distribuição do CloudFront adicionou à sua política de bucket quando você escolheu Yes, update the bucket policy (Sim, atualizar a política de bucket) antes.

Esta atualização de política de bucket indica que você configurou com êxito a distribuição do CloudFront para restringir o acesso ao bucket do S3. Devido a essa restrição, os objetos no bucket só podem ser acessados por meio da distribuição do CloudFront.

Etapa 5: Acessar o vídeo por meio da distribuição do CloudFront

Agora, o CloudFront pode veicular o vídeo armazenado no seu bucket do S3. Para acessar seu vídeo por meio do CloudFront, você deve combinar seu nome de domínio de distribuição do CloudFront com o caminho para o vídeo no bucket do S3.

Para criar um URL para o vídeo do S3 usando o nome de domínio de distribuição do CloudFront

1. Faça login no AWS Management Console e abra o console do CloudFront em https://console.aws.amazon.com/cloudfront/v4/home.
2. No painel de navegação esquerdo, escolha Distributions (Distribuições).
3. Para obter o nome do domínio de distribuição, faça o seguinte:
    a. Na coluna Origins (Origens), encontre a distribuição correta do CloudFront localizando seu nome de origem, que começa com o bucket do S3 que você criou na Etapa 1 (por exemplo, **`tutorial-bucket`**).
    b. Depois de encontrar a distribuição na lista, alargue a coluna Domain name (Nome de domínio) para copiar o valor do nome do domínio para sua distribuição do CloudFront.
4. Em uma nova guia do navegador, cole o nome do domínio de distribuição que você copiou.
5. Retorne à guia do navegador anterior e abra o console do S3 em https://console.aws.amazon.com/s3/.
6. No painel de navegação à esquerda, escolha Buckets.
7. Na lista Buckets, escolha o nome do bucket que você criou na Etapa 1 (por exemplo, **`tutorial-bucket`**).
8. Na lista Objects (Objetos), escolha o nome do vídeo que você carregiu na Etapa 2 (por exemplo, `sample.mp4`).

9. Na página de detalhes do objeto, na seção Object overview (Visão geral do objeto), copie o valor da Key (Chave). Esse valor é o caminho para o objeto de vídeo carregado no bucket do S3.
10. Retorne à guia do navegador onde você colou anteriormente o nome do domínio de distribuição, insira uma barra (**/**) após o nome do domínio de distribuição e, em seguida, cole o caminho do vídeo que você copiou antes (por exemplo,`sample.mp4`).

    Agora, seu vídeo do S3 está acessível ao público e hospedado por meio do CloudFront em um URL semelhante a este:

    ```
    https://CloudFront distribution domain name/Path to the S3 video
    ```

    Substitua *`CloudFront distribution domain name`* (Nome de domínio de distribuição do CloudFront) e *`Path to the S3 video`* (Caminho para o vídeo S3) pelos valores apropriados. O URL do exemplo é: **`https://d111111abcdef8.cloudfront.net/sample.mp4`**.

Etapa 6: Configurar sua distribuição do CloudFront para usar o seu nome de domínio personalizado

Para usar seu próprio nome de domínio em vez do nome de domínio do CloudFront no URL para acessar o vídeo do S3, adicione um nome de domínio alternativo à distribuição do CloudFront.

Subetapas

- Solicitar um certificado SSL
- Adicione um nome de domínio alternativo à distribuição do CloudFront
- Crie um registro do DNS para encaminhar o tráfego do seu nome de domínio alternativo para o nome de domínio da distribuição do CloudFront
- Verifique se o IPv6 está habilitado para sua distribuição e crie outro registro do DNS, se necessário

Solicitar um certificado SSL

Para permitir que seus espectadores usem HTTPS e seu nome de domínio personalizado no URL da transmissão de vídeo, use a AWS Certificate Manager (ACM) para solicitar um certificado Secure Sockets Layer (SSL). O certificado SSL estabelece uma conexão de rede criptografada com o site.

1. Faça login no AWS Management Console e abra o console do ACM em https://console.aws.amazon.com/acm/.

2. Se a página introdutória for exibida, em Provision certificates (Certificados de provisão), escolha Get Started (Conceitos básicos).
3. Na página Request a certificate (Solicitar um certificado), escolha Request a public certificate (Solicitar um certificado público) e depois Request a certificate (Solicitar um certificado).
4. Em Add domain names (Adicionar nomes de domínios) (insira o nome do domínio totalmente qualificado do site que você deseja proteger usando um certificado SSL/TLS. Use um asterisco (*) para solicitar um certificado curinga, que protege vários sites no mesmo domínio. Para este tutorial, insira **`*`** e o nome de domínio personalizado que você configurou em Pré-requisitos. Para este exemplo, insira **`*.example.com`** e escolha Next (Avançar).

   Para obter mais informações, consulte Solicitar um certificado público do ACM (console) no Guia do usuário do AWS Certificate Manager.
5. Na página Select validation method (Selecionar método de validação), escolha DNS validation (Validação de DNS). Em seguida, escolha Next (Próximo).

   Se você puder editar sua configuração de DNS, recomendamos usar a validação de domínio de DNS, em vez da validação de e-mail. A validação de DNS tem vários benefícios em relação à validação de e-mail. Para obter mais informações, consulte Opção 1: Validação de DNS no .Manual do usuário do AWS Certificate Manager.
6. (Opcional) Na página Add tags (Adicionar etiquetas), marque seu certificado com metadados.
7. Escolha Revisar.
8. Na página Review (Revisão), verifique se as informações em Domain name (Nome de domínio) e Validation method (Método de validação) estão corretas. Escolha Confirm and request (Confirmar e solicitar).

   A página Validation (Validação) mostra que sua solicitação está sendo processada e que o domínio de certificado está sendo validado. O certificado que aguarda validação está no estado Pending validation (Validação pendente).
9. Na página Validation (Validação), escolha a seta para baixo à esquerda do seu nome de domínio personalizado e escolha Create record in Route 53 (Criar registro no Route 53) para validar que você é o proprietário do domínio por meio do DNS.

   Isso adiciona um registro CNAME fornecido pelo AWS Certificate Manager na configuração do DNS.
10. Na caixa de diálogo Create record in Route 53 (Criar registro no Route 53), escolha Create (Criar).

A página Validation (Validação) agora deve exibir uma notificação de status de Success (Êxito) na parte inferior.

11. Selecione Continue (Continuar) para visualizar a página da lista Certificates (Certificados).

    O Status de seu novo certificado muda de Pending validation (Validação pendente) para Issued (Emitida) em até 30 minutos.

Adicione um nome de domínio alternativo à distribuição do CloudFront

1. Faça login no AWS Management Console e abra o console do CloudFront em https://console.aws.amazon.com/cloudfront/v4/home.
2. No painel de navegação esquerdo, escolha Distributions (Distribuições).
3. Escolha o ID da distribuição que você criou na Etapa 4.
4. Na guia General (Geral), vá para a seção Settings (Configurações) e escolha Edit (Editar).
5. Na página Edit settings (Editar configurações), para Alternate domain name (CNAME) - optional (Nome de domínio alternativo (CNAME) - opcional), escolha Add item (Adicionar item) para adicionar os nomes de domínio personalizados que você deseja usar no URL para o vídeo do S3 fornecido por essa distribuição do CloudFront.

   Neste tutorial, por exemplo, se você quiser encaminhar o tráfego para um subdomínio, como `www.example.com`, insira o nome do subdomínio (`www`) com o nome do domínio (`example.com`). Especificamente, insira **`www.example.com`**.

   > **Note**
   >
   > O nome de domínio alternativo (CNAME) que você adicionar deve ser coberto pelo certificado SSL que você anexou anteriormente à sua distribuição do CloudFront.

6. Para Custom SSL certificate optional, (Certificado SSL personalizado - opcional), escolha o certificado SSL que você solicitou antes (por exemplo, **`*.example.com`**).

   > **Note**
   >
   > Se você não vir o certificado SSL imediatamente após solicitá-lo, aguarde 30 minutos, e atualize a lista até que o certificado SSL esteja disponível para você selecionar.

7. Mantenha as configurações restantes definidas conforme os padrões. Escolha Salvar alterações.
8. Na guia General (Geral) para a distribuição, aguarde o valor de Last modified (Última modificação) mudar de Deploying (Em implantação) para o carimbo de data ehora em que a distribuição foi modificada pela última vez.

Crie um registro do DNS para encaminhar o tráfego do seu nome de domínio alternativo para o nome de domínio da distribuição do CloudFront

1. Faça login no AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Hosted zones (Zonas hospedadas).
3. Na página Hosted zones (Zonas hospedadas), escolha o nome da zona hospedada que o Route 53 criou para você em Pré-requisitos (por exemplo, **`example.com`**).
4. Selecione Create record (Criar registro) e, em seguida, use Quick create record (Criação rápida de registro).
5. Para Record name (Nome de registro), mantenha o valor do nome do registro igual ao nome de domínio alternativo da distribuição do CloudFront que você adicionou antes.

   Neste tutorial, para encaminhar o tráfego para um subdomínio, como `www.example.com`, insira o nome do subdomínio sem o nome do domínio. Por exemplo, insira somente **`www`** no campo de texto antes do seu nome de domínio personalizado.
6. Em Tipo de registro, selecione A: encaminhar o tráfego para um endereço IPv4 e alguns recursos da AWS.
7. Para Value (Valor), escolha a opção Alias para habilitar o recurso de alias.
8. Em Route traffic to (Encaminhar tráfego para), escolha Alias to CloudFront distribution (Alias para distribuição do CloudFront).
9. Na caixa Choose distribution (Escolher distribuição), escolha o nome de domínio da distribuição do CloudFront que você criou na Etapa 4.

   Para localizar o nome de domínio da sua distribuição do CloudFront, faça o seguinte:

   a. Em uma nova guia do navegador, entre no AWS Management Console e abra o console do CloudFront em https://console.aws.amazon.com/cloudfront/v3/home.
   b. No painel de navegação esquerdo, escolha Distributions (Distribuições).

c. Na coluna Origins (Origens), encontre a distribuição correta do CloudFront localizando seu nome de origem, que começa com o bucket do S3 que você criou na Etapa 1 (por exemplo, **`tutorial-bucket`**).

d. Depois de encontrar a distribuição na lista, amplie a coluna Domain name (Nome de domínio) para ver o valor do nome do domínio para sua distribuição do CloudFront.

10. Na página Create record (Criar registro) no console do Route 53, para as demais configurações, mantenha os padrões.
11. Escolha Criar registros.

Verifique se o IPv6 está habilitado para sua distribuição e crie outro registro do DNS, se necessário

Se o IPv6 estiver habilitado para sua distribuição, você deve criar outro registro do DNS.

1. Para verificar se o IPv6 está habilitado para sua distribuição, faça o seguinte:

   a. Faça login no AWS Management Console e abra o console do CloudFront em https://console.aws.amazon.com/cloudfront/v4/home.

   b. No painel de navegação esquerdo, escolha Distributions (Distribuições).

   c. Escolha o ID da distribuição do CloudFront que você criou na Etapa 4.

   d. Na guia General (Geral), em Settings (Configurações), verifique se IPv6 está definido como Enabled (Habilitado).

   Se o IPv6 estiver habilitado para sua distribuição, você deve criar outro registro do DNS.

2. Se o IPv6 estiver habilitado para sua distribuição, faça o seguinte para criar um registro DNS:

   a. Faça login no AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.

   b. No painel de navegação, escolha Hosted zones (Zonas hospedadas).

   c. Na página Hosted zones (Zonas hospedadas), escolha o nome da zona hospedada que o Route 53 criou para você em Pré-requisitos (por exemplo, **`example.com`**).

   d. Selecione Create record (Criar registro) e, em seguida, use Quick create record (Criação rápida de registro).

   e. Para Record name (Nome de registro), no campo de texto antes do nome de domínio personalizado, digite o mesmo valor que você digitou quando criou antes o registro do DNS do IPv4. Por exemplo, neste tutorial, para encaminhar o tráfego para o subdomínio`www.example.com`, insira apenas **`www`**.

f. Para Record type (Tipo de registro), escolha AAAA - Routes traffic to an IPv6 address and some AWS resources (AAAA - Encaminha o tráfego para um endereço IPv6 e alguns recursos da AWS).

g. Para Value (Valor), escolha a opção Alias para habilitar o recurso de alias.

h. Em Route traffic to (Encaminhar tráfego para), escolha Alias to CloudFront distribution (Alias para distribuição do CloudFront).

i. Na caixa Choose distribution (Escolher distribuição), escolha o nome de domínio da distribuição do CloudFront que você criou na Etapa 4.

j. Mantenha as configurações restantes definidas conforme os padrões.

k. Escolha Criar registros.

Etapa 7: acessar o vídeo do S3 por meio da distribuição do CloudFront com o nome de domínio personalizado

Para acessar o vídeo do S3 usando o URL personalizado, você deve combinar seu nome de domínio alternativo com o caminho para o vídeo no bucket do S3.

Criar um URL personalizado para acessar o vídeo do S3 por meio da distribuição do CloudFront

1. Faça login no AWS Management Console e abra o console do CloudFront em https://console.aws.amazon.com/cloudfront/v4/home.
2. No painel de navegação esquerdo, escolha Distributions (Distribuições).
3. Para obter o nome de domínio alternativo da sua distribuição do CloudFront, faça o seguinte:

   a. Na coluna Origins (Origens), encontre a distribuição correta do CloudFront procurando seu nome de origem, que começa com o nome do bucket do S3 que você criou na Etapa 1 (por exemplo, **`tutorial-bucket`**).

   b. Depois de encontrar a distribuição na lista, alargue a coluna Alternate domain names (Nomes de domínio alternativos) para copiar o valor do nome de domínio alternativo de sua distribuição do CloudFront.
4. Em uma nova guia do navegador, cole o nome de domínio alternativo da distribuição do CloudFront.
5. Retorne à guia anterior do navegador e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
6. Encontre o caminho para o seu vídeo S3, como explicado na Etapa 5.

7. Retorne à guia do navegador onde você colou anteriormente o nome de domínio alternativo, insira uma barra (**/**) e cole o caminho para o vídeo do S3 (por exemplo, `sample.mp4`).

   Agora, seu vídeo do S3 está acessível ao público e hospedado por meio do CloudFront em um URL personalizado semelhante a este:

   ```
   https://CloudFront distribution alternate domain name/Path to the S3 video
   ```

   Substitua *`CloudFront distribution alternate domain name`* (Nome alternativo de domínio de distribuição do CloudFront) e *`Path to the S3 video`* (Caminho para o vídeo S3) pelos valores apropriados. O URL do exemplo é: **`https://www.example.com/sample.mp4`**.

(Opcional) Etapa 8: exibir dados sobre solicitações recebidas pela distribuição do CloudFront

Para exibir dados sobre solicitações recebidas pela sua distribuição do CloudFront

1. Faça login no AWS Management Console e abra o console do CloudFront em https://console.aws.amazon.com/cloudfront/v4/home.
2. No painel de navegação esquerdo, em Reports & analytics (Relatórios e análise), escolha os relatórios no console, que incluem Cache statistics (Estatísticas de cache), Popular Objects (Objetos populares), Top Referrers (Principais indicadores), Usage (Uso) e Viewers (Espectadores).

   Você pode filtrar cada painel de relatório. Para obter mais informações, consulte Relatórios do CloudFront no console no Guia do desenvolvedor do Amazon CloudFront.
3. Para filtrar dados, escolha o ID da distribuição do CloudFront que você criou na Etapa 4.

Etapa 9: limpeza

Se você hospedou um vídeo de transmissão do S3 usando o CloudFront e o Route 53 apenas como um exercício de aprendizado, exclua os recursos da AWS alocados para que não continuar a acumular encargos.

> **Note**
>
> Ao registrar um domínio, você gasta dinheiro imediatamente e é irreversível. Você pode escolher não renovar automaticamente o domínio, mas paga antecipadamente e adquire o domínio por um ano). Para obter mais informações, consulte Registrar um novo domínio no Guia do desenvolvedor do Amazon Route 53.

Subetapas

- Exclua a distribuição do CloudFront
- Excluir o registro DNS
- Exclua a zona hospedada de seu domínio personalizado
- Exclua o nome de domínio personalizado do Route 53
- Exclua o vídeo original no bucket de origem do S3
- Exclua o bucket de origem do S3

Exclua a distribuição do CloudFront

1. Faça login no AWS Management Console e abra o console do CloudFront em https://console.aws.amazon.com/cloudfront/v4/home.
2. No painel de navegação esquerdo, escolha Distributions (Distribuições).
3. Na coluna Origins (Origens), encontre a distribuição correta do CloudFront procurando seu nome de origem, que começa com o nome do bucket do S3 que você criou na Etapa 1 (por exemplo, **`tutorial-bucket`**).
4. Para excluir a distribuição do CloudFront, você deve primeiro desabilitá-la.
   - Se o valor da coluna Status for Enabled (Habilitado) e o valor de Last modified (Última modificação) for o carimbo de data e hora em que a distribuição foi modificada pela última vez, continue para desabilitar a distribuição antes de excluí-la.
   - Se o valor de Status for Enabled (Habilitado) e o valor de Last modified (Última modificação) for Deploying (Em implantação), aguarde até que Status mude para o carimbo de data/hora em que a distribuição foi modificada pela última vez. Em seguida, continue para desabilitar a distribuição antes de excluí-la.
5. Para desabilitar a distribuição do CloudFront, faça o seguinte:

a. Na lista Distributions (Distribuições), marque a caixa de seleção ao lado do ID da distribuição que você deseja excluir.

b. Para desabilitar a distribuição, escolha Disable (Desabilitar) e depois escolha Disable (Desabilitar) para confirmar.

   Se você desabilitar uma distribuição que tenha um nome de domínio alternativo associado a ela, o CloudFront deixará de aceitar o tráfego para esse nome de domínio (como `www.example.com`), mesmo que outra distribuição tenha um nome de domínio alternativo com um caractere curinga (`**`) correspondente ao mesmo domínio (como `**.example.com`).

c. O valor da coluna Status é imediatamente alterado para Disabled (Desabilitado). Aguarde até que o valor de Last modified (Última modificação) mude de Deploying (Implantação) para o carimbo de data e hora em que a distribuição foi modificada pela última vez.

   Como o CloudFront deve propagar essa alteração para todos os locais da borda, pode levar alguns minutos para que a atualização seja concluída e a opção Delete (Excluir) esteja disponível para você excluir a distribuição.

6. Para excluir a distribuição desabilitada, faça o seguinte:

   a. Marque a caixa de seleção ao lado do ID da distribuição que você deseja excluir.

   b. Selecione Delete (Excluir) e depois escolha Delete (Excluir) para confirmar.

Excluir o registro DNS

Se você quiser excluir a zona hospedada pública para o domínio (incluindo o registro do DNS), consulte Exclua a zona hospedada de seu domínio personalizado no Guia do desenvolvedor do Amazon Route 53. Se você só deseja excluir o registro do DNS criado na Etapa 6), faça o seguinte:

1. Faça login no AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Hosted zones (Zonas hospedadas).
3. Na página Hosted zones (Zonas hospedadas), escolha o nome da zona hospedada que o Route 53 criou para você em Pré-requisitos (por exemplo, **`example.com`**).
4. Na lista de registros, marque a caixa de seleção ao lado dos registros que você deseja excluir (os registros que você criou na Etapa 6).

> **Note**
>
> Você não pode excluir registros que têm um valor Type (Tipo) de NS ou SOA.

5. Escolha Delete records (Excluir registros).
6. Para confirmar a exclusão, selecione Excluir.

   As alterações nos registros demoram para serem propagadas até os servidores de DNS do Route 53. Atualmente, a única maneira de verificar se as alterações foram propagadas é usar a ação da API GetChange. As alterações geralmente são propagadas para todos os servidores de nome do Route 53 em até 60 segundos.

Exclua a zona hospedada de seu domínio personalizado

> **Warning**
>
> Se quiser manter o registro do domínio, mas interromper o encaminhamento do tráfego da Internet para seu site ou sua aplicação Web, recomendamos excluir os registros na zona hospedada (conforme descrito na seção anterior), em vez de excluir a zona hospedada.
> Se você excluir uma zona hospedada, alguém pode usar o domínio e encaminhar o tráfego para seus próprios recursos usando seu nome de domínio.
> Além disso, se você excluir uma zona hospedada, não será possível cancelar a exclusão. É necessário criar uma nova zona hospedada e atualizar os servidores de nome para o registro do domínio, o que pode levar até 48 horas para entrar em vigor.
> Se desejar tornar o domínio indisponível na Internet, recomendamos que você transfira seu serviço de DNS para um serviço de DNS gratuito e, em seguida, elimine a zona hospedada do Route 53. Isso impede que futuras consultas DNS sejam incorretamente encaminhadas.
>
> 1. Se o domínio estiver registrado no Route 53, consulte Adição ou alteração de servidores de nome e registros cola de um domínio no Guia do desenvolvedor do Amazon Route 53 para obter informações sobre como substituir servidores de nome do Route 53 por servidores de nome do novo serviço de DNS.
> 2. Se o domínio estiver registrado com outro registrador, use o método fornecido pelo registrador para alterar os servidores de nome do domínio.

> **Note**
>
> Se você estiver excluindo uma zona hospedada de um subdomínio (`www.example.com`), não será necessário alterar os servidores de nome do domínio (`example.com`).

1. Faça login no AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Hosted zones (Zonas hospedadas).
3. Na página Hosted zones (Zonas hospedadas), escolha o nome da zona hospedada que você deseja excluir.
4. Na guia Records (Registros) de sua zona hospedada, verifique se a zona hospedada que você deseja excluir contém apenas um registro DNS e um SOA.

   Se ele contiver registros adicionais, exclua-os.

   Se você criou registros de NS para subdomínios na zona hospedada, exclua esses registros também.
5. Na guia DNSSEC signing (Assinatura de DNSSEC) para sua zona hospedada, desabilite a assinatura DNNSSEC, se ela estiver habilitada. Para obter mais informações, consulte Desabilitação de assinatura de DNSSEC no Guia do desenvolvedor do Amazon Route 53.
6. Na parte superior da página de detalhes da zona hospedada, selecioneDelete zone (Excluir zona).
7. Insira **`delete`** para confirmar a exclusão e depois escolha Delete (Excluir).

Exclua o nome de domínio personalizado do Route 53

A maioria dos domínios de nível superior (TLDs) permite a exclusão do registro quando ele não é mais necessário. Se você excluir um registro de nome de domínio do Route 53 antes de o registro ser programado para expirar, a AWS não reembolsa a taxa de registro. Para obter mais informações, consulte Exclusão de um registro de nome de domínio no Guia do desenvolvedor do Amazon Route 53.

> **Important**
>
> Se desejar transferir o domínio entre Contas da AWS ou transferir o domínio para outro registrador, não exclua um domínio esperando poder registrá-lo de novo imediatamente. Em vez disso, consulte a documentação aplicável no Guia do desenvolvedor do Amazon Route 53:
>
> - Transferência de um domínio para uma Conta da AWS diferente
> - Transferência de um domínio do Amazon Route 53 para outro registrador

Exclua o vídeo original no bucket de origem do S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets.
3. Na lista Bucket name (Nome do bucket), escolha o nome do bucket para o qual carregou o vídeo na Etapa 2 (por exemplo, **`tutorial-bucket`**).
4. Na guia Objects (Objetos), marque a caixa de seleção ao lado do nome do objeto que você deseja excluir (por exemplo, `sample.mp4`).
5. Escolha Excluir.
6. Em Permanently delete objects?, (Excluir objetos permanentemente?), insira **`permanently delete`** para confirmar que deseja excluir esse objeto.
7. Escolha Delete objects (Excluir objetos).

Exclua o bucket de origem do S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets.
3. Na lista Buckets, escolha o botão de opção ao lado do nome do bucket que você criou na Etapa 1 (por exemplo, **`tutorial-bucket`**).
4. Escolha Excluir.
5. Na página Delete bucket (Excluir bucket), confirme se deseja excluir o bucket inserindo o nome do bucket no campo de texto e escolha Delete bucket (Excluir bucket).

Próximas etapas

Depois de concluir este tutorial, você pode continuar a explorar os seguintes casos de uso relacionados:

- Transcodifique vídeos do S3 em formatos de streaming necessários para uma televisão ou dispositivo conectado específico antes de hospedar esses vídeos com uma distribuição do CloudFront.

  Para usar as Operações em Lote do Amazon S3, o AWS Lambda e o AWS Elemental MediaConvert a fim de transcodificar em lote um conjunto de vídeos para uma variedade de formatos de mídia de saída, consulte Tutorial: vídeos de transcodificação em lote com o Operações em Lote do S3.
- Hospede outros objetos armazenados no S3, como imagens, áudio, animações, folhas de estilo, HTML, JavaScript, aplicações React etc., usando o CloudFront e o Route 53.

  Por exemplo, consulte Tutorial: Configurar um site estático usando um domínio personalizado registrado no Route 53 e Acelerar seu site com o Amazon CloudFront.
- Use Amazon S3 Transfer Acceleration para configurar transferências de arquivos rápidas e seguras. O Transfer Acceleration pode acelerar o carregamento de vídeo no seu bucket do S3 para transferências de longa distância de vídeos maiores. O Transfer Acceleration melhora a performance da transferência roteando o tráfego pelos locais da borda distribuídos globalmente do CloudFront e pelas redes de estrutura da AWS. Ele também usa otimizações de protocolo de rede. Para ter mais informações, consulte Configurar transferências de arquivos rápidas e seguras usando o Amazon S3 Transfer Acceleration.

Tutorial: configurar um site estático no Amazon S3

> **Important**
>
> O Amazon S3 agora aplica criptografia do lado do servidor com chaves gerenciadas do Amazon S3 (SSE-S3) como nível básico de criptografia para cada bucket no Amazon S3. Desde 5 de janeiro de 2023, todos os novos uploads de objetos para o Amazon S3 são automaticamente criptografados sem custo adicional e sem impacto na performance. O status de criptografia automática para a configuração de criptografia padrão do bucket do S3 e para novos uploads de objetos está disponível em logs do AWS CloudTrail, no Inventário do S3, na Lente de Armazenamento do S3, no console do Amazon S3 e como cabeçalho

adicional de resposta da API do Amazon S3 na AWS Command Line Interface e em AWS SDKs. Para obter mais informações, consulte Perguntas frequentes sobre criptografia padrão.

Você pode configurar um bucket do Amazon S3 para funcionar como um site. Este exemplo conduz você pelas etapas de hospedagem de um site no Amazon S3.

Important

O tutorial a seguir exige que o Bloqueio de Acesso Público seja desabilitado. Recomendamos manter o Bloqueio de Acesso Público habilitado. Se quiser manter todas as quatro configurações do Bloqueio de Acesso Público habilitadas e hospedar um site estático, use o controle de acesso à origem (OAC) do Amazon CloudFront. O Amazon CloudFront fornece os recursos necessários para configurar um site estático seguro. Os sites estáticos do Amazon S3 só são compatíveis com endpoints HTTP. O Amazon CloudFront usa o armazenamento durável do Amazon S3 ao mesmo tempo que fornece cabeçalhos de segurança adicionais, como HTTPS. O HTTPS adiciona segurança criptografando uma solicitação HTTP normal e protegendo-a contra ataques cibernéticos comuns. Para obter mais informações, consulte Conceitos básicos de um site estático seguro no Guia do desenvolvedor do Amazon CloudFront.

Tópicos

- Etapa 1: Criar um bucket
- Etapa 2: Habilitar hospedagem de site estático
- Etapa 3: editar as configurações do Bloqueio de acesso público
- Etapa 4: Adicionar política de bucket que torna o conteúdo do bucket publicamente disponível
- Etapa 5: Configurar um documento de índice
- Etapa 6: configurar um documento de erros
- Etapa 7: testar o endpoint do site
- Etapa 8: Limpar

Etapa 1: Criar um bucket

As instruções a seguir fornecem uma visão geral de como criar seus buckets para hospedagem de sites. Para obter instruções detalhadas passo a passo sobre como criar um bucket, consulte Criar um bucket de uso geral.

Para criar um bucket

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Selecione Create bucket (Criar bucket).
3. Insira o Bucket name (Nome do bucket) (por exemplo, **`example.com`**).
4. Selecione a região onde você deseja criar o bucket.

   Escolha uma região próxima de você para minimizar a latência e os custos ou atender a requisitos normativos. A região escolhida determina o endpoint de site do Amazon S3. Para obter mais informações, consulte Endpoints de site.
5. Para aceitar as configurações padrão e criar o bucket, escolha Create (Criar).

Etapa 2: Habilitar hospedagem de site estático

Depois de criar um bucket, você pode habilitar a hospedagem de site estático para seu bucket. Você pode criar um bucket novo ou usar um existente.

Como habilitar a hospedagem de sites estáticos

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets de uso geral.
3. Na lista de buckets, escolha o nome do bucket para o qual você deseja habilitar a hospedagem de site estático.
4. Escolha Properties (Propriedades).
5. Em Static website hosting (Hospedagem estática de sites), escolha Edit (Editar).
6. Escolha Use this bucket to host a website (Usar este bucket para hospedar um site).
7. Em Static website hosting (Hospedagem estática de sites), escolha Enable (Ativar).

8. Em Index Document (Documento de índice), insira o nome do arquivo do documento de índice, que geralmente é `index.html`.

   O nome do documento de índice diferencia letras maiúsculas de minúsculas e deve corresponder exatamente ao nome do arquivo do documento de índice HTML do qual você planeja fazer upload para o bucket do S3. Quando você configura um bucket para hospedagem de site, deve especificar um documento de índice. O Amazon S3 retorna esse documento de índice quando as solicitações são feitas para o domínio raiz ou alguma subpasta. Para obter mais informações, consulte Configurar um documento de índice.

9. Para fornecer seu próprio documento de erros personalizado para erros da classe 4XX, em Error document (Documento de erros), insira o nome de arquivo do documento de erros personalizado.

   O nome do documento de erro diferencia letras maiúsculas de minúsculas e deve corresponder exatamente ao nome do arquivo do documento de erro HTML do qual você planeja fazer upload para o bucket do S3. Se você não especificar um documento de erro personalizado e ocorrer um erro, o Amazon S3 retornará um documento de erro HTML padrão. Para ter mais informações, consulte Configurar um documento de erro personalizado.

10. (Opcional) Se você quiser especificar regras avançadas de redirecionamento em Redirection rules (Regras de redirecionamento), use JSON para descrevê-las.

    Por exemplo, você pode encaminhar solicitações condicionalmente de acordo com nomes de chave de objeto ou prefixos específicos na solicitação. Para obter mais informações, consulte Configurar regras de redirecionamento para usar redirecionamentos condicionais avançados.

11. Selecione Save changes.

    O Amazon S3 permite a hospedagem estática de sites para seu bucket. Na parte inferior da página, em Static website hosting (Hospedagem estática de sites), você verá o endpoint do site do seu bucket.

12. Em Static website hosting (Hospedagem de sites estáticos), anote o Endpoint.

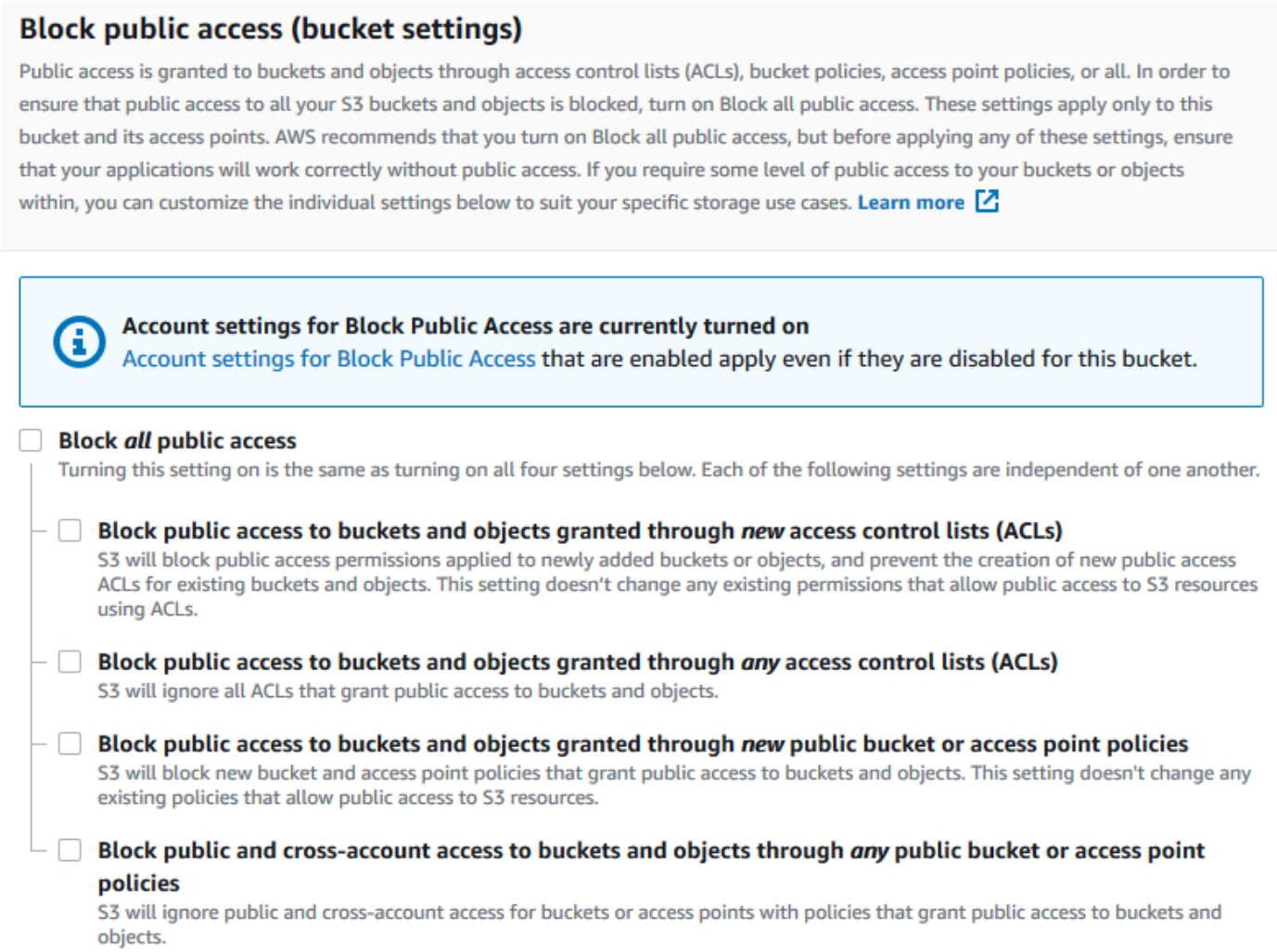
    O Endpoint é o endpoint do site do Amazon S3 para o bucket. Depois de concluir a configuração do bucket como um site estático, é possível usar esse endpoint para testar o site.

Etapa 3: editar as configurações do Bloqueio de acesso público

Por padrão, o Amazon S3 bloqueia o acesso público à sua conta e aos seus buckets. Se quiser usar um bucket para hospedar um site estático, use estas etapas para editar as configurações de bloqueio de acesso público.

> **Warning**
>
> Antes de concluir estas etapas, revise Bloquear o acesso público ao armazenamento do Amazon S3 para garantir que você entenda e aceite os riscos envolvidos em permitir o acesso público. Ao desativar as configurações de bloqueio de acesso público para tornar seu bucket público, qualquer pessoa na Internet pode acessá-lo. Recomendamos que você bloqueie todo o acesso público aos buckets.

1. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Escolha o nome do bucket configurado como um site estático.
3. Escolha Permissions (Permissões).
4. Em Block public access (bucket settings) (Bloqueio de acesso público (configurações de bucket), escolha Edit (Editar).
5. Desmarque Block all public access (Bloquear todo acesso público) e escolha Save changes (Salvar alterações).



O Amazon S3 desativa as configurações do Bloqueio de Acesso Público para o bucket. Para criar um site público estático, talvez também seja necessário editar as configurações do Bloqueio de Acesso Público para sua conta antes de adicionar uma política de bucket. Se as configurações do Bloqueio de Acesso Público da conta estiverem ativadas no momento, você verá uma observação em Bloquear acesso público (configurações de bucket).

Etapa 4: Adicionar política de bucket que torna o conteúdo do bucket publicamente disponível

Depois de editar as configurações do Bloqueio de acesso público do S3, é possível adicionar uma política de bucket para conceder acesso público de leitura ao bucket. Ao conceder um acesso público de leitura, qualquer pessoa na Internet pode acessar seu bucket.

> **Important**
>
> A política a seguir é somente um exemplo e concede acesso total aos conteúdos do bucket. Antes de prosseguir com esta etapa, revise Como posso proteger os arquivos no meu bucket do Amazon S3? para garantir que você entende as práticas recomendadas a fim de proteger os arquivos no bucket do S3 e os riscos envolvidos na concessão de acesso público.

1. Em Buckets, escolha o nome do seu bucket.
2. Escolha Permissions (Permissões).
3. Em Bucket Policy (Política de bucket), escolha Edit (Editar).
4. Para conceder acesso público de leitura ao site, copie a política de bucket a seguir e cole-a no Bucket policy editor (Editor de política de bucket).

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PublicReadGetObject",
            "Effect": "Allow",
            "Principal": "*",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::Bucket-Name/*"
            ]
        }
    ]
}
```

5. Atualize o `Resource` para o nome do bucket.

   Na política de bucket do exemplo anterior, *`Bucket-Name`* é um espaço reservado para o nome do bucket. Para usar essa política de bucket com seu próprio bucket, você deve atualizar esse nome para corresponder ao nome do seu bucket.

6. Selecione Save changes.

   Uma mensagem é exibida indicando que a política de bucket foi adicionada com sucesso.

Se você vir um erro que diz `Policy has invalid resource`, confirme se o nome do bucket na política de bucket corresponde ao nome do seu bucket. Para obter informações sobre como adicionar uma política de bucket, consulte Como adicionar uma política de bucket do S3?

Se você receber uma mensagem de erro e não puder salvar a política do bucket, verifique suas configurações de acesso público para confirmar que você permite acesso público ao bucket.

Etapa 5: Configurar um documento de índice

Quando você habilita a hospedagem de sites estáticos para seu bucket, insere o nome do documento de índice (por exemplo, **`index.html`**). Depois de habilitar a hospedagem de sites estáticos para seu bucket, faça upload de um arquivo HTML com esse nome de documento de índice para o bucket.

Como configurar o documento de índice

1. Criar um arquivo `index.html`

   Se você não tiver um arquivo `index.html`, poderá usar o HTML a seguir para criar um:

   ```
   <html xmlns="http://www.w3.org/1999/xhtml" >
   <head>
       <title>My Website Home Page</title>
   </head>
   <body>
     <h1>Welcome to my website</h1>
     <p>Now hosted on Amazon S3!</p>
   </body>
   </html>
   ```

2. Salve o arquivo de índice localmente.

   O nome do documento de índice deve corresponder exatamente ao nome do documento de índice que você inseriu na caixa de diálogo Hospedagem de site estático. O nome do documento de índice diferencia maiúsculas de minúsculas. Por exemplo, se você inserir `index.html` no nome do Documentos de índice na caixa de diálogo Hospedagem de site estático, o nome do arquivo do documento de índice também deverá ser `index.html` e não `Index.html`.

3. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.

4. No painel de navegação à esquerda, escolha Buckets de uso geral.
5. Na lista de buckets, escolha o nome do bucket que você deseja usar para hospedar um site estático.
6. Habilite a hospedagem de sites estáticos para seu bucket e insira o nome exato do documento de índice (por exemplo, `index.html`). Para obter mais informações, consulte Habilitar a hospedagem de sites.

   Depois de habilitar a hospedagem estática do site, vá para a etapa 6.
7. Para fazer upload do documento de índice para o bucket, siga um destes procedimentos:

   - Arraste e solte o arquivo de índice na listagem de buckets do console.
   - Escolha Upload (Fazer upload) e siga as instruções para escolher e fazer upload do arquivo de índice.

   Para obter instruções detalhadas, consulte Fazer upload de objetos.
8. (Opcional) Faça upload do conteúdo de outro site para o seu bucket.

Etapa 6: configurar um documento de erros

Ao habilitar a hospedagem de site estático para o bucket, insira o nome do documento de erro (por exemplo, **`404.html`**). Depois de habilitar a hospedagem de sites estáticos para seu bucket, faça upload de um arquivo HTML com esse nome de documento de erros para o bucket.

Para configurar um documento de erros

1. Crie um documento de erro, por exemplo `404.html`.
2. Salve o arquivo de documento de erros localmente.

   O nome do documento de erros diferencia maiúsculas e minúsculas e deve corresponder exatamente ao nome que você insere ao habilitar a hospedagem estática do site. Por exemplo, se você inserir `404.html` como o nome do Error document (Documento de erro) na caixa de diálogo Static website hosting (Hospedagem de site estático), o nome de arquivo do documento de erro também deve ser `404.html`.
3. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
4. No painel de navegação à esquerda, escolha Buckets de uso geral.

5. Na lista de buckets, escolha o nome do bucket que você deseja usar para hospedar um site estático.
6. Habilite a hospedagem de site estático para seu bucket e insira o nome exato do documento de erro (por exemplo, `404.html`). Para ter mais informações, consulte Habilitar a hospedagem de sites e Configurar um documento de erro personalizado.

   Depois de habilitar a hospedagem estática do site, vá para a etapa 6.
7. Para fazer upload do documento de erros para o bucket, siga um destes procedimentos:

   - Arraste e solte o arquivo de documento de erros na lista de buckets do console.
   - Escolha Upload (Fazer upload) e siga as instruções para escolher e fazer upload do arquivo de índice.

   Para obter instruções detalhadas, consulte Fazer upload de objetos.

Etapa 7: testar o endpoint do site

Depois de configurar a hospedagem de site estático para seu bucket, você pode testar o endpoint do site.

> **Note**
>
> O Amazon S3 não oferece suporte para o acesso HTTPS ao site. Se quiser usar HTTPS, você poderá usar o Amazon CloudFront para servir um site estático hospedado no Amazon S3.
> Para obter mais informações, consulte Como uso o CloudFront para veicular um site estático hospedado no Amazon S3? e Exigir HTTPS para comunicação entre visualizadores e o CloudFront.

1. Em Buckets, escolha o nome do seu bucket.
2. Escolha Properties (Propriedades).
3. Na parte inferior da página, em Static website hosting (Hospedagem estática de sites), escolha seu Bucket website endpoint (Endpoint de site do Bucket).

   Seu documento de índice é aberto em uma janela separada do navegador.

Agora você tem um site hospedado no Amazon S3. Esse site está disponível no endpoint de site do Amazon S3. No entanto, você pode ter um domínio, como `example.com`, que deseja usar para exibir o conteúdo do site que criou. Talvez você também queira usar o suporte ao domínio raiz do Amazon S3 para atender solicitações para `http://www.example.com` e `http://example.com`. Isso exige etapas adicionais. Para ver um exemplo, consulte Tutorial: Configurar um site estático usando um domínio personalizado registrado no Route 53.

Etapa 8: Limpar

Se tiver criado o site apenas como exercício de aprendizado, você poderá excluir os recursos da AWS alocados, de maneira que deixe de acumular cobranças. Depois que você excluir os recursos da AWS, o site deixará de estar disponível. Para ter mais informações, consulte Excluir um bucket de uso geral.

Tutorial: Configurar um site estático usando um domínio personalizado registrado no Route 53

Suponha que você queira hospedar um site estático no Amazon S3. Você registrou um domínio no Amazon Route 53 (por exemplo, `example.com`) e deseja que solicitações `http://www.example.com` e `http://example.com` sejam veiculadas a partir do conteúdo do Amazon S3. É possível usar essa demonstração para saber como hospedar um site estático e criar redirecionamentos no Amazon S3 para um site com um nome de domínio personalizado que é registrado com o Route 53. É possível trabalhar com um site existente que você deseja hospedar no Amazon S3 ou usar esta demonstração para começar do zero.

Depois de concluir esta demonstração, você tem a opção de usar o Amazon CloudFront para melhorar a performance do seu site. Para obter mais informações, consulte Acelerar seu site com o Amazon CloudFront.

> **Note**
>
> Os endpoints de site do Amazon S3 não oferecem suporte a HTTPS ou pontos de acesso. Se quiser usar HTTPS, você poderá usar o Amazon CloudFront para servir um site estático hospedado no Amazon S3.
>
> Consulte um tutorial sobre como hospedar seu conteúdo com segurança com o CloudFront e o Amazon S3 em Tutorial: Hospedagem de transmissão sob demanda com o Amazon S3, Amazon CloudFront e Amazon Route 53. Para obter mais informações, consulte Como uso

o CloudFront para veicular um site estático hospedado no Amazon S3? e Exigir HTTPS para comunicação entre visualizadores e CloudFront.

Automatização da configuração de site estático com um modelo do AWS CloudFormation

Você pode usar um modelo do AWS CloudFormation para automatizar a configuração do site estático. O modelo do AWS CloudFormation configura os componentes que você precisa para hospedar um site estático seguro e se concentrar mais no conteúdo do seu site e menos na configuração de componentes.

O modelo do AWS CloudFormation inclui os seguintes componentes:

- Amazon S3: cria um bucket do Amazon S3 para hospedar seu site estático.
- CloudFront: cria uma distribuição do CloudFront para acelerar seu site estático.
- Lambda@Edge: usa o Lambda@Edge para adicionar cabeçalhos de segurança a cada resposta do servidor. Os cabeçalhos de segurança são um grupo de cabeçalhos na resposta do servidor web que dizem aos navegadores da web para tomarem precauções de segurança extras. Para obter mais informações, consulte a publicação do blog: Adding HTTP security headers using Lambda@Edge and Amazon CloudFront.

Este modelo do AWS CloudFormation está disponível para download e uso. Para obter informações e instruções, consulte Conceitos básicos de um site estático seguro no Guia do desenvolvedor do Amazon CloudFront.

Tópicos

- Antes de começar
- Etapa 1: Registrar um domínio personalizado no Route 53
- Etapa 2: Criar dois buckets
- Etapa 3: Configurar o bucket de domínio raiz para hospedagem de sites
- Etapa 4: Configurar o bucket de subdomínio para redirecionamento de sites
- Etapa 5: Configurar o registro em log para o tráfego do site
- Etapa 6: Fazer upload do conteúdo do site e do índice
- Etapa 7: carregar um documento de erros
- Etapa 8: Editar configurações do S3 Block Public Access

- Etapa 9: Anexar uma política de bucket
- Etapa 10: Testar o endpoint de domínio
- Etapa 11: Adicionar registros de alias para seu domínio e subdomínio
- Etapa 12: Testar o site
- Acelerar seu site com o Amazon CloudFront
- Limpar seus recursos de exemplo

Antes de começar

Ao seguir as etapas deste exemplo, você trabalha com os seguintes serviços:

Amazon Route 53: você pode usar o Route 53 para registrar domínios e definir onde você deseja rotear o tráfego de internet para o seu domínio. O exemplo mostra como criar registros de alias do Route 53 que roteiam o tráfego para do domínio (`example.com`) e do subdomínio (`www.example.com`) para um bucket do Amazon S3 que contém um arquivo HTML.

Amazon S3: você usa o Amazon S3 para criar buckets, fazer upload de uma página de site de exemplo, configurar permissões para que todos possam visualizar conteúdo e, em seguida, configurar os buckets para hospedagem do site.

Etapa 1: Registrar um domínio personalizado no Route 53

Se você não tiver um nome de domínio registrado, como `example.com`, precisará registrar um com o Route 53. Para obter mais informações, consulte Registrar um novo domínio no Guia do desenvolvedor do Amazon Route 53. Depois de registrar seu nome de domínio, é possível criar e configurar seus buckets do Amazon S3 para hospedagem de sites.

Etapa 2: Criar dois buckets

Para oferecer suporte a solicitações no domínio raiz e no subdomínio, crie dois buckets.

- Bucket de domínio – `example.com`
- Bucket de subdomínio – `www.example.com`

Esses nomes de bucket devem corresponder exatamente ao seu nome de domínio. Neste exemplo, o nome de domínio é `example.com`. Você hospeda seu conteúdo fora do bucket de domínio

raiz (`example.com`). Crie uma solicitação de redirecionamento para o bucket de subdomínio (`www.example.com`). Em outras palavras, se uma pessoa insere `www.example.com` no navegador, ela é redirecionada para `example.com` e vê o conteúdo hospedado no bucket do Amazon S3 com esse nome.

Como criar buckets para hospedagem de sites

As instruções a seguir fornecem uma visão geral de como criar seus buckets para hospedagem de sites. Para obter instruções detalhadas passo a passo sobre como criar um bucket, consulte Criar um bucket de uso geral.

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Crie o bucket do domínio raiz:

   a. Na barra de navegação na parte superior da página, escolha o nome da Região da AWS exibida no momento. Em seguida, escolha a região na qual você deseja criar um bucket.

   > **Note**
   >
   > Para reduzir a latência e os custos e atender aos requisitos regulatórios, selecione uma região perto de você. Os objetos armazenados em uma região nunca saem dessa região, a menos que você os transfira para outra região. Para obter uma lista de Regiões da AWS do Amazon S3, consulte Endpoints de AWS service (Serviço da AWS) no Referência geral da Amazon Web Services.

   b. No painel de navegação à esquerda, escolha Buckets de uso geral.

   c. Selecione Create bucket (Criar bucket). A página Create bucket (Criar bucket) é aberta.

   d. Insira o Bucket name (Nome do bucket) (por exemplo, **`example.com`**).

   e. Selecione a região onde você deseja criar o bucket.

      Escolha uma região próxima de você para minimizar a latência e os custos ou atender a requisitos normativos. A região escolhida determina o endpoint de site do Amazon S3. Para obter mais informações, consulte Endpoints de site.

   f. Para aceitar as configurações padrão e criar o bucket, escolha Create (Criar).
3. Crie o bucket de subdomínio:

   a. Selecione Create bucket (Criar bucket).

b. Insira o Bucket name (Nome do bucket) (por exemplo, **`www.example.com`**).

c. Selecione a região onde você deseja criar o bucket.

   Escolha uma região próxima de você para minimizar a latência e os custos ou atender a requisitos normativos. A região escolhida determina o endpoint de site do Amazon S3. Para obter mais informações, consulte Endpoints de site.

d. Para aceitar as configurações padrão e criar o bucket, escolha Create (Criar).

Na próxima etapa, configure `example.com` para a hospedagem do site.

Etapa 3: Configurar o bucket de domínio raiz para hospedagem de sites

Nesta etapa, você configura o bucket de domínio raiz (`example.com`) como um site. Esse bucket terá o conteúdo do site. Ao configurar um bucket para hospedagem de sites, é possível acessar o site usando o Endpoints de site.

Como habilitar a hospedagem de sites estáticos

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets de uso geral.
3. Na lista de buckets, escolha o nome do bucket para o qual você deseja habilitar a hospedagem de site estático.
4. Escolha Properties (Propriedades).
5. Em Static website hosting (Hospedagem estática de sites), escolha Edit (Editar).
6. Escolha Use this bucket to host a website (Usar este bucket para hospedar um site).
7. Em Static website hosting (Hospedagem estática de sites), escolha Enable (Ativar).
8. Em Index Document (Documento de índice), insira o nome do arquivo do documento de índice, que geralmente é `index.html`.

   O nome do documento de índice diferencia letras maiúsculas de minúsculas e deve corresponder exatamente ao nome do arquivo do documento de índice HTML do qual você planeja fazer upload para o bucket do S3. Quando você configura um bucket para hospedagem de site, deve especificar um documento de índice. O Amazon S3 retorna esse documento de índice quando as solicitações são feitas para o domínio raiz ou alguma subpasta. Para obter mais informações, consulte Configurar um documento de índice.

9. Para fornecer seu próprio documento de erros personalizado para erros da classe 4XX, em Error document (Documento de erros), insira o nome de arquivo do documento de erros personalizado.

   O nome do documento de erro diferencia letras maiúsculas de minúsculas e deve corresponder exatamente ao nome do arquivo do documento de erro HTML do qual você planeja fazer upload para o bucket do S3. Se você não especificar um documento de erro personalizado e ocorrer um erro, o Amazon S3 retornará um documento de erro HTML padrão. Para ter mais informações, consulte Configurar um documento de erro personalizado.

10. (Opcional) Se você quiser especificar regras avançadas de redirecionamento em Redirection rules (Regras de redirecionamento), use JSON para descrevê-las.

    Por exemplo, você pode encaminhar solicitações condicionalmente de acordo com nomes de chave de objeto ou prefixos específicos na solicitação. Para obter mais informações, consulte Configurar regras de redirecionamento para usar redirecionamentos condicionais avançados.

11. Selecione Save changes.

    O Amazon S3 permite a hospedagem estática de sites para seu bucket. Na parte inferior da página, em Static website hosting (Hospedagem estática de sites), você verá o endpoint do site do seu bucket.

12. Em Static website hosting (Hospedagem de sites estáticos), anote o Endpoint.

    O Endpoint é o endpoint do site do Amazon S3 para o bucket. Depois de concluir a configuração do bucket como um site estático, é possível usar esse endpoint para testar o site.

Depois de editar as configurações de acesso público de bloqueio e adicionar uma política de bucket que permita acesso público de leitura, você pode usar o endpoint do site para acessar seu site.

Na próxima etapa, configure o subdomínio (`www.example.com`) para redirecionar solicitações para o domínio (`example.com`).

Etapa 4: Configurar o bucket de subdomínio para redirecionamento de sites

Depois de configurar o bucket de domínio raiz para a hospedagem de sites, é possível configurar o bucket do subdomínio para redirecionar todas as solicitações para o domínio. Neste exemplo, todas as solicitações para `www.example.com` são redirecionadas para `example.com`.

Para configurar uma solicitação de redirecionamento

1. No console do Amazon S3, na lista Buckets de uso geral, escolha o nome do bucket de subdomínio (`www.example.com` neste exemplo).
2. Escolha Properties (Propriedades).
3. Em Static website hosting (Hospedagem estática de sites), escolha Edit (Editar).
4. Selecione Redirect requests for an object (Redirecionar solicitações de um objeto).
5. Na caixa Target bucket (Bucket de destino), insira o domínio raiz (por exemplo, **`example.com`**).
6. Em Protocol (Protocolo), selecione http.
7. Selecione Save changes.

Etapa 5: Configurar o registro em log para o tráfego do site

Se quiser rastrear o número de visitantes que acessam seu site, opcionalmente você pode habilitar o log para seu bucket de domínio raiz. Para obter mais informações, consulte Registrar em log as solicitações com registro em log de acesso ao servidor. Se planeja usar o Amazon CloudFront para acelerar seu site, você também pode usar o registro em log do CloudFront.

Como habilitar o registro em log do acesso ao servidor para o bucket de domínio raiz

1. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Na mesma região onde você criou o bucket configurado como um site estático, crie um bucket para registro em log, por exemplo `logs.example.com`.
3. Crie uma pasta para os arquivos de log do registro em log de acesso ao servidor (por exemplo, `logs`).
4. (Opcional) Se você quiser usar o CloudFront para melhorar oa performance do seu site, crie uma pasta para os arquivos de log do CloudFront (por exemplo, `cdn`).

> **Important**
>
> Ao criar ou atualizar uma distribuição e habilitar o registro do CloudFront, o CloudFront atualiza a lista de controle de acesso (ACL) do bucket para fornecer à conta `awslogsdelivery` permissões `FULL_CONTROL` para registrar logs em seu bucket. Para obter mais informações, consulte Permissões necessárias para configurar o registro padrão e acessar seus arquivos de log no Guia do desenvolvedor do Amazon CloudFront. Se o bucket que armazena os logs usar a configuração Imposto pelo

proprietário do bucket para a Propriedade de Objetos do S3 a fim de desabilitar ACLs, o CloudFront não poderá gravar logs no bucket. Para ter mais informações, consulte Controlar a propriedade de objetos e desabilitar ACLs para seu bucket.

5. Na lista Buckets, escolha seu bucket de domínio raiz.
6. Escolha Properties (Propriedades).
7. Em Server access logging (Registro de acesso ao servidor), selecione Edit (Editar).
8. Escolha Habilitar.
9. No Target bucket (Bucket de destino), escolha o destino do bucket e da pasta para os logs de acesso ao servidor:
   - Navegue até o local da pasta e do bucket:
     1. Escolha Browse S3 (Navegar no S3).
     2. Escolha o nome do bucket e, depois, escolha a pasta de logs.
     3. Selecione Choose path (Escolher caminho).
   - Insira o caminho do bucket do S3, por exemplo, `s3://logs.example.com/logs/`.
10. Selecione Save changes.

    No bucket de log, agora você pode acessar seus logs. O Amazon S3 grava os logs de acesso ao site no bucket de log a cada duas horas.

Etapa 6: Fazer upload do conteúdo do site e do índice

Nesta etapa, faça upload do documento de índice e do conteúdo opcional do site no bucket de domínio raiz.

Quando você habilita a hospedagem de sites estáticos para seu bucket, insere o nome do documento de índice (por exemplo, **`index.html`**). Depois de habilitar a hospedagem de sites estáticos para seu bucket, faça upload de um arquivo HTML com esse nome de documento de índice para o bucket.

Como configurar o documento de índice

1. Criar um arquivo `index.html`

   Se você não tiver um arquivo `index.html`, poderá usar o HTML a seguir para criar um:

```
<html xmlns="http://www.w3.org/1999/xhtml" >
<head>
    <title>My Website Home Page</title>
</head>
<body>
  <h1>Welcome to my website</h1>
  <p>Now hosted on Amazon S3!</p>
</body>
</html>
```

2. Salve o arquivo de índice localmente.

   O nome do documento de índice deve corresponder exatamente ao nome do documento de índice que você inseriu na caixa de diálogo Hospedagem de site estático. O nome do documento de índice diferencia maiúsculas de minúsculas. Por exemplo, se você inserir `index.html` no nome do Documentos de índice na caixa de diálogo Hospedagem de site estático, o nome do arquivo do documento de índice também deverá ser `index.html` e não `Index.html`.

3. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.

4. No painel de navegação à esquerda, escolha Buckets de uso geral.

5. Na lista de buckets, escolha o nome do bucket que você deseja usar para hospedar um site estático.

6. Habilite a hospedagem de sites estáticos para seu bucket e insira o nome exato do documento de índice (por exemplo, `index.html`). Para obter mais informações, consulte Habilitar a hospedagem de sites.

   Depois de habilitar a hospedagem estática do site, vá para a etapa 6.

7. Para fazer upload do documento de índice para o bucket, siga um destes procedimentos:

   - Arraste e solte o arquivo de índice na listagem de buckets do console.
   - Escolha Upload (Fazer upload) e siga as instruções para escolher e fazer upload do arquivo de índice.

   Para obter instruções detalhadas, consulte Fazer upload de objetos.

8. (Opcional) Faça upload do conteúdo de outro site para o seu bucket.

Etapa 7: carregar um documento de erros

Ao habilitar a hospedagem de site estático para o bucket, insira o nome do documento de erro (por exemplo, **`404.html`**). Depois de habilitar a hospedagem de sites estáticos para seu bucket, faça upload de um arquivo HTML com esse nome de documento de erros para o bucket.

Para configurar um documento de erros

1. Crie um documento de erro, por exemplo `404.html`.
2. Salve o arquivo de documento de erros localmente.

   O nome do documento de erros diferencia maiúsculas e minúsculas e deve corresponder exatamente ao nome que você insere ao habilitar a hospedagem estática do site. Por exemplo, se você inserir `404.html` como o nome do Error document (Documento de erro) na caixa de diálogo Static website hosting (Hospedagem de site estático), o nome de arquivo do documento de erro também deve ser `404.html`.
3. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
4. No painel de navegação à esquerda, escolha Buckets de uso geral.
5. Na lista de buckets, escolha o nome do bucket que você deseja usar para hospedar um site estático.
6. Habilite a hospedagem de site estático para seu bucket e insira o nome exato do documento de erro (por exemplo, `404.html`). Para ter mais informações, consulte Habilitar a hospedagem de sites e Configurar um documento de erro personalizado.

   Depois de habilitar a hospedagem estática do site, vá para a etapa 6.
7. Para fazer upload do documento de erros para o bucket, siga um destes procedimentos:

   - Arraste e solte o arquivo de documento de erros na lista de buckets do console.
   - Escolha Upload (Fazer upload) e siga as instruções para escolher e fazer upload do arquivo de índice.

   Para obter instruções detalhadas, consulte Fazer upload de objetos.

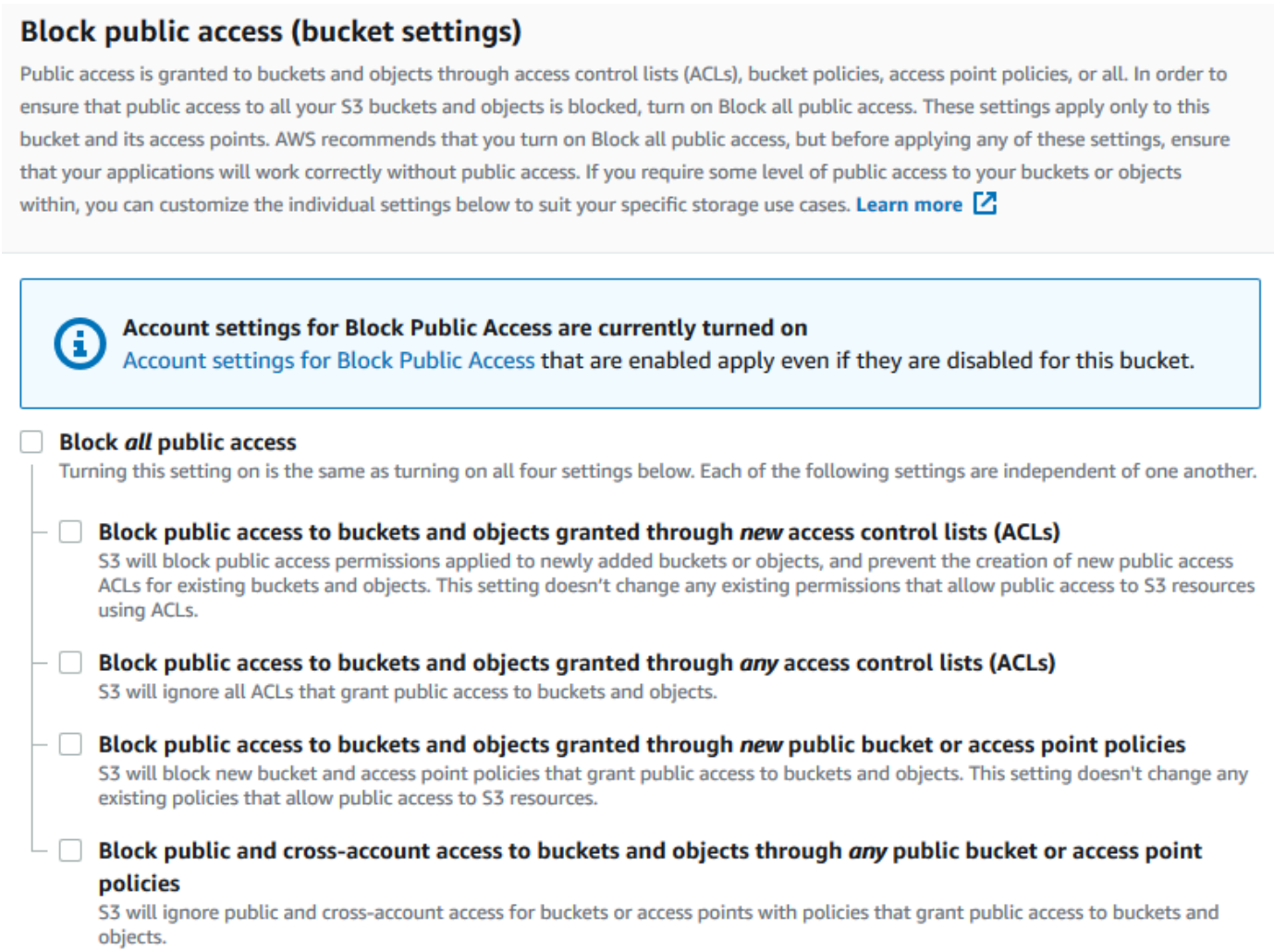
Etapa 8: Editar configurações do S3 Block Public Access

Neste exemplo, você edita configurações de bloqueio de acesso público para o bucket de domínio (`example.com`) para permitir acesso público.

Por padrão, o Amazon S3 bloqueia o acesso público à sua conta e aos seus buckets. Se quiser usar um bucket para hospedar um site estático, use estas etapas para editar as configurações de bloqueio de acesso público.

> **Warning**
>
> Antes de concluir estas etapas, revise Bloquear o acesso público ao armazenamento do Amazon S3 para garantir que você entenda e aceite os riscos envolvidos em permitir o acesso público. Ao desativar as configurações de bloqueio de acesso público para tornar seu bucket público, qualquer pessoa na Internet pode acessá-lo. Recomendamos que você bloqueie todo o acesso público aos buckets.

1. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Escolha o nome do bucket configurado como um site estático.
3. Escolha Permissions (Permissões).
4. Em Block public access (bucket settings) (Bloqueio de acesso público (configurações de bucket), escolha Edit (Editar).
5. Desmarque Block all public access (Bloquear todo acesso público) e escolha Save changes (Salvar alterações).



O Amazon S3 desativa as configurações do Bloqueio de Acesso Público para o bucket. Para criar um site público estático, talvez também seja necessário editar as configurações do Bloqueio de Acesso Público para sua conta antes de adicionar uma política de bucket. Se as configurações do Bloqueio de Acesso Público da conta estiverem ativadas no momento, você verá uma observação em Bloquear acesso público (configurações de bucket).

Etapa 9: Anexar uma política de bucket

Neste exemplo, você anexa uma política de bucket ao bucket de domínio (`example.com`) para permitir acesso de leitura pública. Você substitui o *`Bucket-Name`* na política de bucket de exemplo pelo nome do bucket de domínio, por exemplo, `example.com`.

Depois de editar as configurações do Bloqueio de acesso público do S3, é possível adicionar uma política de bucket para conceder acesso público de leitura ao bucket. Ao conceder um acesso público de leitura, qualquer pessoa na Internet pode acessar seu bucket.

> **Important**
>
> A política a seguir é somente um exemplo e concede acesso total aos conteúdos do bucket. Antes de prosseguir com esta etapa, revise Como posso proteger os arquivos no meu bucket do Amazon S3? para garantir que você entende as práticas recomendadas a fim de proteger os arquivos no bucket do S3 e os riscos envolvidos na concessão de acesso público.

1. Em Buckets, escolha o nome do seu bucket.
2. Escolha Permissions (Permissões).
3. Em Bucket Policy (Política de bucket), escolha Edit (Editar).
4. Para conceder acesso público de leitura ao site, copie a política de bucket a seguir e cole-a no Bucket policy editor (Editor de política de bucket).

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PublicReadGetObject",
            "Effect": "Allow",
            "Principal": "*",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::Bucket-Name/*"
            ]
        }
    ]
}
```

5. Atualize o `Resource` para o nome do bucket.

   Na política de bucket do exemplo anterior, *`Bucket-Name`* é um espaço reservado para o nome do bucket. Para usar essa política de bucket com seu próprio bucket, você deve atualizar esse nome para corresponder ao nome do seu bucket.

6. Selecione Save changes.

   Uma mensagem é exibida indicando que a política de bucket foi adicionada com sucesso.

   Se você vir um erro que diz `Policy has invalid resource`, confirme se o nome do bucket na política de bucket corresponde ao nome do seu bucket. Para obter informações sobre como adicionar uma política de bucket, consulte Como adicionar uma política de bucket do S3?

   Se você receber uma mensagem de erro e não puder salvar a política do bucket, verifique suas configurações de acesso público para confirmar que você permite acesso público ao bucket.

Na próxima etapa, é possível descobrir os endpoints do site e testar o endpoint do domínio.

Etapa 10: Testar o endpoint de domínio

Depois de configurar seu bucket de domínio para hospedar um site público, você pode testar seu endpoint. Para obter mais informações, consulte Endpoints de site. Somente será possível testar o endpoint de seu bucket de domínio porque ele está configurado para redirecionamento de site e não para hospedagem de site estático.

> **Note**
>
> O Amazon S3 não oferece suporte para o acesso HTTPS ao site. Se quiser usar HTTPS, você poderá usar o Amazon CloudFront para servir um site estático hospedado no Amazon S3.
> Para obter mais informações, consulte Como uso o CloudFront para veicular um site estático hospedado no Amazon S3? e Exigir HTTPS para comunicação entre visualizadores e o CloudFront.

1. Em Buckets, escolha o nome do seu bucket.
2. Escolha Properties (Propriedades).
3. Na parte inferior da página, em Static website hosting (Hospedagem estática de sites), escolha seu Bucket website endpoint (Endpoint de site do Bucket).

   Seu documento de índice é aberto em uma janela separada do navegador.

Na próxima etapa, você usa o Amazon Route 53 para permitir que os clientes usem ambos os URLs personalizados para navegar até o site.

Etapa 11: Adicionar registros de alias para seu domínio e subdomínio

Nesta etapa, você cria os registros de alias adicionados à zona hospedada dos mapas de domínio `example.com` e `www.example.com`. Em vez de usar endereços IP, os registros de alias usam os endpoints de site do Amazon S3. O Amazon Route 53 mantém um mapeamento entre os registros de alias e os endereços IP onde os buckets do Amazon S3 residem. Crie dois registros de alias, um para o domínio raiz e um para o subdomínio.

Adicionar um registro de alias para seu domínio raiz e subdomínio

Como adicionar um registro de alias ao domínio raiz (**`example.com`**)

1. Abra o console do Route 53 em https://console.aws.amazon.com/route53/.

   > **Note**
   >
   > Se você ainda não usa o Route 53, consulte Etapa 1: registrar um domínio no Guia do desenvolvedor do Amazon Route 53. Após concluir a configuração, é possível retomar as instruções.

2. Selecione Hosted zones (Zonas hospedadas).
3. Na lista de zonas hospedadas, escolha o nome da zona hospedada que corresponde ao nome de domínio.
4. Escolha Create record (Criar registro).
5. Escolha Switch to wizard (Alternar para assistente).

   > **Note**
   >
   > Se você quiser usar a criação rápida para criar seus registros de alias, consulte Configurar o Route 53 para rotear o tráfego para um bucket do S3.

6. Escolha Simple routing (Roteamento simples) e Next (Próximo).
7. Escolha Define simple record (Definir registro simples).
8. Em Record name (Nome do registro), aceite o valor padrão, que é o nome da zona hospedada e do domínio.

9. Em Value/Route traffic to (Valor/Encaminhar tráfego para), escolha Alias to S3 website endpoint (Alias para o endpoint do site do S3).
10. Escolha a região .
11. Escolha o bucket do S3.

    O nome do bucket deve corresponder ao nome que aparece na caixa Name (Nome). Na lista Choose S3 bucket (Escolher bucket do S3), o nome do bucket aparece com o endpoint do site do Amazon S3 para a região onde o bucket foi criado, por exemplo, `s3-website-us-west-1.amazonaws.com (example.com)`.

    Choose S3 bucket (Escolher bucket do S3) lista um bucket se:

    - Você configurou o bucket como um site estático.
    - O nome do bucket é o mesmo que o nome do registro que você está criando.
    - A Conta da AWS atual criou o bucket.

    Se o bucket não aparecer na lista Choose S3 bucket (Escolher bucket do S3), insira o endpoint de site do Amazon S3 da região em que o bucket foi criado, por exemplo, **`s3-website-us-west-2.amazonaws.com`**. Para obter uma lista completa dos endpoints do site do Amazon S3, consulte Endpoints de site do Amazon S3. Para obter mais informações sobre o destino de alias, consulte Valor/rotear tráfego para no Guia do desenvolvedor do Amazon Route 53.
12. Em Record type (Tipo de registro), escolha A - Routes traffic to an IPv4 address and some AWS resources (Encaminha o tráfego para um endereço IPv4 e alguns recursos da AWS).
13. Em Evaluate target health (Avaliar integridade do destino), escolha No (Não).
14. Escolha Define simple record (Definir registro simples).

Como adicionar um registro de alias ao subdomínio (**`www.example.com`**)

1. Em Configure records (Configurar registros), escolha Define simple record (Definir registro simples).
2. Em Record name (Nome do registro) para seu subdomínio, digite `www`.
3. Em Value/Route traffic to (Valor/Encaminhar tráfego para), escolha Alias to S3 website endpoint (Alias para o endpoint do site do S3).
4. Escolha a região .

5. Escolha o bucket do S3, por exemplo, `s3-website-us-west-2.amazonaws.com (www.example.com)`.

   Se o bucket não aparecer na lista Choose S3 bucket (Escolher bucket do S3), insira o endpoint de site do Amazon S3 da região em que o bucket foi criado, por exemplo, **`s3-website-us-west-2.amazonaws.com`**. Para obter uma lista completa dos endpoints do site do Amazon S3, consulte Endpoints de site do Amazon S3. Para obter mais informações sobre o destino de alias, consulte Valor/rotear tráfego para no Guia do desenvolvedor do Amazon Route 53.
6. Em Record type (Tipo de registro), escolha A - Routes traffic to an IPv4 address and some AWS resources (Encaminha o tráfego para um endereço IPv4 e alguns recursos da AWS).
7. Em Evaluate target health (Avaliar integridade do destino), escolha No (Não).
8. Escolha Define simple record (Definir registro simples).
9. Na página Configure records (Configurar registros), escolha Create records (Criar registros).

> **Note**
>
> As alterações são geralmente propagadas para todos os servidores do Route 53 dentro de 53 segundos. Quando a propagação for concluída, será possível rotear o tráfego para o bucket do Amazon S3 usando os nomes de registros de alias criados nesse procedimento.

Adicionar um registro de alias para seu domínio raiz e subdomínio (antigo console do Route 53)

Como adicionar um registro de alias ao domínio raiz (**`example.com`**)

O console do Route 53 foi reprojetado. No console do Route 53, você pode usar temporariamente o console antigo. Se você optar por trabalhar com o console do Route 53 antigo, use o procedimento abaixo.

1. Abra o console do Route 53 em https://console.aws.amazon.com/route53/.

   > **Note**
   >
   > Se você ainda não usa o Route 53, consulte Etapa 1: registrar um domínio no Guia do desenvolvedor do Amazon Route 53. Após concluir a configuração, é possível retomar as instruções.

2. Selecione Hosted Zones (Zonas hospedadas).
3. Na lista de zonas hospedadas, escolha o nome da zona hospedada que corresponde ao nome de domínio.
4. Escolha Create Record Set (Criar conjunto de registros).
5. Especifique os seguintes valores:

   Nome

   Aceite o valor padrão, que é o nome da zona hospedada e do domínio.

   Para o domínio raiz, não é necessário inserir nenhuma informação adicional no campo Name (Nome).

   Tipo

   Escolha A - IPv4 address (A – Endereço IPv4).

   Alias

   Escolha Sim.

   Alvo do alias

   Na seção S3 website endpoints (Endpoints de site do S3) da lista, escolha o nome do bucket.

   O nome do bucket deve corresponder ao nome que aparece na caixa Name (Nome). Na listagem Alias Target (Destino do alias), o nome do bucket é seguido pelo endpoint de site do Amazon S3 para a região onde o bucket foi criado, por exemplo, `example.com (s3-website-us-west-2.amazonaws.com)`. Alias Target (Alvo do alias) lista um bucket se:

   - Você configurou o bucket como um site estático.
   - O nome do bucket é o mesmo que o nome do registro que você está criando.
   - A Conta da AWS atual criou o bucket.

   Se o bucket não aparecer na listagem Alias Target (Destino do alias), insira o endpoint de site do Amazon S3 da região em que o bucket foi criado, por exemplo, `s3-website-us-west-2`. Para obter uma lista completa dos endpoints do site do Amazon S3, consulte Endpoints de site do Amazon S3. Para obter mais informações sobre o destino de alias, consulte Valor/rotear tráfego para no Guia do desenvolvedor do Amazon Route 53.

Política de roteamento

Aceite o valor padrão de Simple (Simples).

Avaliar status do alvo

Aceite o valor padrão de No (Não).

6. Escolha Create (Criar).

Como adicionar um registro de alias ao subdomínio (**`www.example.com`**)

1. Na zona hospedada do domínio raiz (`example.com`), selecione Create Record Set (Criar conjunto de registros).
2. Especifique os seguintes valores:

   Nome

   Para o subdomínio, insira `www` na caixa.

   Tipo

   Escolha A - IPv4 address (A – Endereço IPv4).

   Alias

   Escolha Sim.

   Alvo do alias

   Na seção S3 website endpoints (Endpoints de site do S3) da lista, escolha o mesmo nome de bucket que é exibido no campo Name (Nome), por exemplo, `www.example.com (s3-website-us-west-2.amazonaws.com)`.

   Política de roteamento

   Aceite o valor padrão de Simple (Simples).

   Avaliar status do alvo

   Aceite o valor padrão de No (Não).

3. Escolha Create (Criar).

> **Note**
>
> As alterações geralmente são propagadas para todos os servidores do Route 53 dentro de 53 segundos. Quando a propagação for concluída, será possível rotear o tráfego para o bucket do Amazon S3 usando os nomes de registros de alias criados nesse procedimento.

Etapa 12: Testar o site

Verifique se o site e o redirecionamento funcionam corretamente. No navegador, insira os URLs. Neste exemplo, é possível tentar os seguintes URLs:

- Domínio (`http://example.com`): exibe o documento de índice no bucket `example.com`.
- Subdomínio (`http://www.example.com`): redireciona sua solicitação para `http://example.com`. Veja o documento de índice no bucket `example.com`.

Se o seu site ou links de redirecionamento não funcionarem, tente o seguinte:

- Limpar cache: limpe o cache do seu navegador da Web.
- Verificar servidores de nomes: se a página da Web e os links de redirecionamento não funcionarem depois de limpar o cache, você poderá comparar os servidores de nome do seu domínio e os servidores de nome da sua zona hospedada. Se os servidores de nome não corresponderem, talvez seja necessário atualizar seus servidores de nome de domínio para corresponder aos listados na zona hospedada. Para obter mais informações, consulte Adicionar ou alterar servidores de nomes e registros cola para um domínio.

Depois de testar com êxito o domínio raiz e o subdomínio, você pode configurar uma distribuição do Amazon CloudFront para melhorar a performance do seu site e fornecer logs que você possa usar para revisar o tráfego do site. Para ter mais informações, consulte Acelerar seu site com o Amazon CloudFront.

Acelerar seu site com o Amazon CloudFront

Você pode usar o Amazon CloudFront para melhorar a performance do seu site do Amazon S3. O CloudFront disponibiliza os arquivos do site (como HTML, imagens e vídeos) por meio de datacenters em todo o mundo (conhecidos como pontos de presença). Quando um visitante solicita um arquivo em seu site, o CloudFront redireciona automaticamente a solicitação para uma cópia do

arquivo no ponto de presença mais próximo. Isso resulta em tempos de download mais rápidos se o visitante tiver solicitado o conteúdo em um datacenter localizado mais longe.

O CloudFront armazena em cache o conteúdo em pontos de presença por um período especificado por você. Se um visitante solicitar conteúdo que foi armazenado em cache por mais tempo que a data de expiração, o CloudFront verificará o servidor de origem para saber se há uma versão mais nova do conteúdo disponível. Se houver uma versão mais nova à disposição, o CloudFront copiará a nova versão para o ponto de presença. As alterações feitas no conteúdo original são replicadas para pontos de presença à medida que os visitantes solicitam o conteúdo.

Usar o CloudFront sem o Route 53

Os tutoriais nesta página usam o Route 53 para apontar para sua distribuição do CloudFront. No entanto, se você quiser servir conteúdo hospedado em um bucket do Amazon S3 usando o CloudFront sem usar o Route 53, consulte Tutoriais do Amazon CloudFront: configurar uma distribuição dinâmica de conteúdo para o Amazon S3. Ao servir conteúdo hospedado em um bucket do Amazon S3 usando o CloudFront, você pode usar qualquer nome de bucket, e tanto HTTP quanto HTTPS são compatíveis.

Automatizar a configuração com um modelo do AWS CloudFormation

Para obter mais informações sobre como usar um modelo do AWS CloudFormation para configurar um site estático seguro que cria uma distribuição do CloudFront para veicular seu site, consulte Introdução a um site estático seguro no Guia do desenvolvedor do Amazon CloudFront.

Tópicos

- Etapa 1: Criar uma distribuição do CloudFront
- Etapa 2: Atualizar os conjuntos de registros do domínio e do subdomínio
- (Opcional) Etapa 3: verificar os arquivos de log

Etapa 1: Criar uma distribuição do CloudFront

Primeiro, você cria uma distribuição do CloudFront. Isso torna seu site disponível em datacenters em todo o mundo.

Como criar uma distribuição com uma origem do Amazon S3

1. Abra o console do CloudFront em https://console.aws.amazon.com/cloudfront/v4/home.

2. Escolha Criar distribuição.
3. Na página Create Distribution (Criar distribuição), na seção Origin Settings (Configurações de origem), em Origin Domain Name (Nome do domínio de origem), digite o endpoint do site do Amazon S3 para seu bucket, por exemplo, **`example.com.s3-website.us-west-1.amazonaws.com`**.

   O CloudFront preenche o Origin ID (ID de origem) para você.
4. Em Default Cache Behavior Settings (Configurações do comportamento de cache padrão), mantenha os valores padrão definidos.

   Com as configurações padrão do Viewer Protocol Policy (Política de protocolo de visualizador), é possível usar HTTPS para o site estático. Para obter mais informações sobre essas opções de configuração, consulte Valores que você especifica quando cria ou atualiza uma distribuição na Web no Guia do desenvolvedor do Amazon CloudFront.
5. Para Distribution Settings (Configurações de distribuição), faça o seguinte:

   a. Deixe Price Class (Classe de preço) definida como Use All Edge Locations (Best Performance) (Usar todos os pontos de presença [melhor performance]).

   b. Defina Alternate Domain Names (CNAMEs) Nomes de domínio alternativos (CNAMEs) para o domínio raiz e para o subdomínio `www`. Neste tutorial, são `example.com` e `www.example.com`.

      > **Important**
      >
      > Antes de executar essa etapa, veja os requisitos para o uso de nomes de domínio alternativos, principalmente a necessidade de um certificado SSL/TLS válido.

   c. Em SSL Certificate (Certificado SSL), selecione Custom SSL Certificate (example.com) (Certificado SSL personalizado (exemplo.com)) e escolha o certificado personalizado que contém os nomes de domínio e subdomínio.

      Para obter mais informações, consulte Certificado SSL no Guia do desenvolvedor do Amazon CloudFront.

   d. Em Default Root Object (Objeto raiz padrão), insira o nome do documento de índice, por exemplo, `index.html`.

      Se o URL usado para acessar a distribuição não contiver um nome de arquivo, a distribuição do CloudFront retornará o documento de índice. O Default Root Object (Objeto

raiz padrão) deve corresponder exatamente ao nome do documento de índice do seu site estático. Para ter mais informações, consulte Configurar um documento de índice.

e. Defina Logging (Registro em log) como On (Ligado).

> **Important**
>
> Ao criar ou atualizar uma distribuição e habilitar o registro do CloudFront, o CloudFront atualiza a lista de controle de acesso (ACL) do bucket para fornecer à conta `awslogsdelivery` permissões `FULL_CONTROL` para registrar logs em seu bucket. Para obter mais informações, consulte Permissões necessárias para configurar o registro padrão e acessar seus arquivos de log no Guia do desenvolvedor do Amazon CloudFront. Se o bucket que armazena os logs usar a configuração Imposto pelo proprietário do bucket para a Propriedade de Objetos do S3 a fim de desabilitar ACLs, o CloudFront não poderá gravar logs no bucket. Para ter mais informações, consulte Controlar a propriedade de objetos e desabilitar ACLs para seu bucket.

f. Em Bucket for Logs (Bucket para logs), escolha o bucket para o registro em log que você criou.

   Para obter mais informações sobre como configurar um bucket de log, consulte (Opcional) Registrar em log o tráfego da web.

g. Se quiser armazenar os logs gerados pelo tráfego para a distribuição do CloudFront em uma pasta, em Log Prefix (Prefixo de log), insira o nome da pasta.

h. Mantenha todas as outras configurações segundo seus valores predefinidos.

6. Escolha Criar distribuição.
7. Para ver o status atual da distribuição, localize a distribuição no console e verifique a coluna Status.

   Um status `InProgress` indica que a distribuição ainda não foi totalmente implantada.

   Depois que a distribuição estiver implantada, você pode fazer referência ao conteúdo com o novo nome do domínio do CloudFront.
8. Registre o valor de Domain Name (Nome do domínio) mostrado no console do CloudFront, por exemplo, `dj4p1rv6mvubz.cloudfront.net`.
9. Para verificar se a distribuição do CloudFront está funcionando, insira o nome de domínio da distribuição em um navegador da Web.

Se o seu site estiver visível, a distribuição do CloudFront funciona. Se o seu site tiver um domínio personalizado registrado no Amazon Route 53, você precisará do nome de domínio do CloudFront para atualizar o conjunto de registros na próxima etapa.

Etapa 2: Atualizar os conjuntos de registros do domínio e do subdomínio

Agora que você criou com sucesso uma distribuição do CloudFront, atualize o registro de alias no Route 53 para apontar para a nova distribuição do CloudFront.

Para atualizar o registro de alias para apontar para uma distribuição do CloudFront

1. Abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Hosted zones (Zonas hospedadas).
3. Na página Hosted Zones (Zonas hospedadas), escolha a zona hospedada criada por você para o subdomínio, por exemplo, `www.example.com`.
4. Em Records (Registros), selecione o registro A que você criou para seu subdomínio.
5. Em Record details (Detalhes do registro), escolha Edit record (Editar registro).
6. Em Route traffic to (Rotear tráfego para), escolha Alias to CloudFront distribution (Alias para distribuição do CloudFront).
7. Em Choose distribution (Escolher distribuição), escolha a distribuição do CloudFront.
8. Escolha Save (Salvar).
9. Para redirecionar o registro A do domínio raiz para a distribuição do CloudFront, repita esse procedimento do domínio raiz, por exemplo, `example.com`.

   A atualização dos conjuntos de registros entra em vigor dentro de 2 a 48 horas.
10. Para ver se os novos registros A entraram em vigor, em um navegador da Web, digite o URL do subdomínio, por exemplo, `http://www.example.com`.

    Se o navegador não o redirecionar para o domínio raiz (por exemplo, `http://example.com`), os novos registros A estarão no lugar. Quando o novo registro A entra em vigor, o tráfego roteado pelo novo registro A para a distribuição do CloudFront não é redirecionado para o domínio raiz. Qualquer visitante que faça referência ao site usando `http://example.com` ou `http://www.example.com` é redirecionado para o ponto de presença do CloudFront mais próximo, onde ele aproveita tempos de download menores.

> **Tip**
>
> Os navegadores podem armazenar em cache configurações de redirecionamento. Se você acreditar que as novas configurações do registro A devem ter entrado em vigor, mas o navegador ainda redirecionar `http://www.example.com` para `http://example.com`, tente limpar o histórico e limpar o cache do navegador, fechando e reabrindo a aplicação do navegador ou usando outro navegador da Web.

(Opcional) Etapa 3: verificar os arquivos de log

Os logs de acesso informam quantas pessoas estão visitando o site. Eles também contêm dados comerciais valiosos que você pode analisar com outros serviços, como o Amazon EMR.

Os logs do CloudFront são armazenados no bucket e na pasta escolhidos ao criar uma distribuição do CloudFront e habilitar o registro em log. O CloudFront grava logs em seu bucket de log dentro de 24 horas a partir do momento em que as solicitações correspondentes são feitas.

Para ver os arquivos de log do site

1. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Escolha o nome do bucket de registro em log do site.
3. Escolha a pasta de logs do CloudFront.
4. Baixe os arquivos `.gzip` escritos pelo CloudFront antes de abri-los.

Se tiver criado o site apenas como um exercício de aprendizado, você poderá excluir os recursos alocados, para não acumular mais cobranças. Para fazer isto, consulte Limpar seus recursos de exemplo. Depois que você excluir os recursos da AWS, o site deixará de estar disponível.

Limpar seus recursos de exemplo

Se você tiver criado o site estático apenas como um exercício de aprendizado, exclua os recursos da AWS alocados, para deixar de acumular cobranças. Depois que você excluir os recursos da AWS, o site deixará de estar disponível.

Tarefas

- Etapa 1: exclua a distribuição do Amazon CloudFront
- Etapa 2: exclua a zona hospedada do Route 53
- Etapa 3: Desabilitar o registro em log e excluir o bucket do S3

Etapa 1: exclua a distribuição do Amazon CloudFront

Antes de excluir uma distribuição do Amazon CloudFront, você deve desabilitá-la. Uma distribuição desabilitada deixa de ser funcional e não acumula encargos. É possível habilitar uma distribuição desabilitada a qualquer momento. Depois que você excluir uma distribuição desabilitada, ela deixará de estar disponível.

Como desabilitar e excluir uma distribuição do CloudFront

1. Abra o console do CloudFront em https://console.aws.amazon.com/cloudfront/v4/home.
2. Selecione a distribuição que você deseja desabilitar e escolha Disable (Desabilitar).
3. Quando a confirmação for solicitada, escolha Yes, Disable (Sim, desabilitar).
4. Selecione a distribuição desabilitada e escolha Delete (Excluir).
5. Quando a confirmação for solicitada, escolha Yes, Delete (Sim, excluir).

Etapa 2: exclua a zona hospedada do Route 53

Para excluir a zona hospedada, você deve excluir os conjuntos de registros criados. Você não precisa excluir os registros de Start of Authority (SOA – Início da autoridade) e Name Server (NS – Servidor de nomes); eles são excluídos automaticamente quando se exclui a zona hospedada.

Para excluir os conjuntos de registros

1. Abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. Na lista de nomes de domínio, selecione o nome do seu domínio e escolha Go to Record Sets (Ir para conjuntos de registros).
3. Na lista de conjuntos de registros, selecione os registros A que você criou.

   O tipo de cada conjunto de registros está listado na coluna Type (Tipo).
4. Escolha Delete Record Set (Excluir conjunto de registros).
5. Quando a confirmação for solicitada, escolha Confirm (Confirmar).

Como excluir uma zona hospedada do Route 53

1. Continuando o procedimento anterior, escolha Back to Hosted Zones (Voltar para zonas hospedadas).
2. Selecione o nome do seu domínio e escolha Delete Hosted Zone (Excluir zona hospedada).
3. Quando a confirmação for solicitada, escolha Confirm (Confirmar).

Etapa 3: Desabilitar o registro em log e excluir o bucket do S3

Antes de excluir o bucket do S3, verifique se o registro está desativado para o bucket. Caso contrário, a AWS continuará gravando logs para o bucket à medida que você o excluir.

Para desabilitar o registro em log para um bucket

1. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Em Buckets, escolha o nome do bucket e, em seguida, escolha Properties (Propriedades).
3. Em Properties (Propriedades), escolha Logging (Registro).
4. Desmarque a caixa de seleção Enabled (Habilitado).
5. Escolha Save (Salvar).

Agora, você pode excluir seu bucket. Para ter mais informações, consulte Excluir um bucket de uso geral.

Implantar um site estático no AWS Amplify Hosting diretamente de um bucket do S3 de uso geral

Recomendamos que você use o AWS Amplify Hosting para hospedar conteúdo de site estático armazenado no S3. O Amplify Hosting é um serviço totalmente gerenciado que facilita a implantação de seus sites em uma rede de entrega de conteúdo (CDN) disponível globalmente, desenvolvida pelo Amazon CloudFront, permitindo hospedagem segura de sites estáticos sem configuração extensiva. Com o AWS Amplify Hosting, você pode selecionar a localização de seus objetos no bucket de uso geral, implantar seu conteúdo em uma CDN gerenciada e gerar um URL HTTPS público para que seu site possa ser acessado em qualquer lugar. Implantar um site estático usando o Amplify Hosting fornece os seguintes benefícios e recursos:

- Implantação na rede de entrega de conteúdo (CDN) da AWS desenvolvida pelo Amazon CloudFront: o CloudFront é um serviço da Web que acelera a distribuição do conteúdo estático e

dinâmico da Web para os usuários. O CloudFront distribui o conteúdo por meio de uma rede global de data centers denominados locais da borda. Quando um usuário solicita um conteúdo que você está disponibilizando com o CloudFront, a solicitação é roteada para o local da borda que fornece a menor latência (atraso), assim o conteúdo é entregue com o melhor desempenho possível, maior confiabilidade e disponibilidade. Consulte mais informações em Como o CloudFront entrega conteúdo no Guia do desenvolvedor do Amazon CloudFront.

- Suporte HTTPS: fornece comunicação segura e transferência de dados entre seu site e o navegador do usuário.
- Domínios personalizados: conecte facilmente seu site a um URL personalizado comprado de um registrador de domínios, como o Amazon Route 53.
- Certificados SSL personalizados: ao configurar seu domínio personalizado, é possível usar o certificado gerenciado padrão que o Amplify fornece para você ou usar seu próprio certificado personalizado adquirido da autoridade de certificação de terceiros de sua escolha.
- Métricas incorporadas e monitoramento do CloudWatch: monitore tráfego, erros, transferência de dados e latência do site.
- Proteção por senha: restrinja o acesso ao site, configurando um requisito de nome de usuário e senha no console do Amplify.
- Redirecionamentos e regravações: crie regras de redirecionamento e regravação no console do Amplify para permitir que um servidor web redirecione a navegação de um URL para outro.

Quando você implanta sua aplicação a partir de um bucket de uso geral do Amazon S3 no Amplify Hosting, as cobranças da AWS são baseadas no modelo de preços do Amplify. Para obter mais informações, consulte Preços do AWS Amplify.

> **Important**
>
> O Amplify Hosting não está disponível em todos as Regiões da AWS onde o Amazon S3 está disponível. Para implantar um site estático no Amplify Hosting, o bucket de uso geral do Amazon S3 contendo seu site deve estar localizado em uma região em que o Amplify esteja disponível. Para obter uma lista das regiões onde o Amplify está disponível, consulte Endpoints do Amplify no Referência geral da Amazon Web Services.

É possível iniciar o processo de implantação no console do Amazon S3, no console do Amplify na AWS CLI e em AWS SDKs. Você só pode implantar no Amplify por meio de um bucket de uso geral localizado em sua própria conta. O Amplify não oferece suporte ao acesso a buckets do entre contas.

Use as instruções a seguir para implantar um site estático por meio de um bucket de uso geral do Amazon S3 no Amplify Hosting iniciando pelo console do Amazon S3.

Implantar um site estático no Amplify pelo console do S3

Como implantar um site estático pelo console do Amazon S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação à esquerda, escolha Buckets.
3. Na lista Buckets, escolha o bucket de uso geral que contém o site que você deseja implantar no Amplify Hosting.
4. Escolha a guia Properties (Propriedades).
5. Em Hospedagem de site estático, escolha Criar aplicação do Amplify. Nessa etapa, o processo de implantação será transferido para o console do Amplify.
6. Na página Implantar com o S3, siga as etapas a seguir.
   a. Em Nome da aplicação, insira o nome da aplicação ou do site.
   b. Em Nome da ramificação, insira o nome do backend da aplicação.
   c. Em Localização dos objetos do S3 a hospedar, insira o caminho do diretório do bucket de uso geral ou escolha Procurar no S3 para localizá-lo e selecioná-lo.
7. Escolha Salvar e implantar.

> **Note**
>
> Se atualizar qualquer um dos objetos de um site estático em um bucket de uso geral hospedado no Amplify, você deverá reimplantar a aplicação no Amplify Hosting para que as alterações entrem em vigor. O Amplify Hosting não detecta automaticamente as alterações no bucket. Para obter mais informações, consulte Atualização de um site estático implantado no Amplify a partir de um bucket do S3 no Guia do usuário do AWS Amplify Hosting.

Para iniciar diretamente do console do Amplify, consulte Deploying a static website from S3 using the Amplify console no Guia do usuário do AWS Amplify Hosting.

Para começar a usar os AWS SDKs, consulte Creating a bucket policy to deploy a static website from S3 using the AWS SDKs no Guia do usuário do AWS Amplify Hosting.

Cotas

Sua Conta da AWS tem cotas padrão para cada serviço da AWS, que anteriormente eram chamadas de limites. As cotas do Amazon S3 incluem o número de buckets de uso geral, buckets de diretório, pontos de acesso e muito mais. É possível solicitar um aumento de algumas cotas, mas nem todas elas podem ser aumentadas. Esses aumentos não são concedidos imediatamente, de forma que pode levar alguns dias para que seu aumento entre em vigor.

Consulte uma lista de cotas do Amazon S3 e seus valores padrão em Amazon S3 quotas na Referência geral da AWS.

Aumentos de cota

Para solicitar um aumento da cota

É possível solicitar o aumento da cota usando uma das seguintes opções:

- No AWS Management Console, abra o console do Service Quotas. No painel de navegação, selecione serviços da AWS. Selecione Amazon S3, escolha uma cota e siga as instruções para solicitar um aumento de cota. Para obter mais informações, consulte Solicitar um aumento de cota no Manual do usuário do Service Quotas.
- Na AWS CLI: use o comando request-service-quota-increase da AWS CLI. Para obter mais informações, consulte Solicitar um aumento de cota no Manual do usuário do Service Quotas.

Referência

Além do console do Amazon S3, você pode trabalhar com o Amazon S3 de forma programática usando as APIs REST, os SDKs da AWS ou a AWS Command Line Interface (AWS CLI) do Amazon S3.

- Referência de APIs do Amazon Simple Storage Service
- Exemplos de código na Referência de API do Amazon Simple Storage Service
- AWS Command Line Interface no Guia do usuário do AWS Command Line Interface.
- SDKs da AWS

Documentação do SDK	Exemplos de código
AWS SDK para C++	Exemplos de código do AWS SDK para C++
AWS CLI	Exemplos de código da AWS CLI.
AWS SDK para Go	Exemplos de código do AWS SDK para Go
AWS SDK para Java	Exemplos de código do AWS SDK para Java
AWS SDK para JavaScript	Exemplos de código do AWS SDK para JavaScript
AWS SDK para Kotlin	Exemplos de código do AWS SDK para Kotlin
AWS SDK para .NET	Exemplos de código do AWS SDK para .NET
AWS SDK para PHP	Exemplos de código do AWS SDK para PHP
Ferramentas da AWS para PowerShell	Tools for PowerShell code examples
AWS SDK para Python (Boto3)	Exemplos de código do AWS SDK para Python (Boto3)
AWS SDK para Ruby	Exemplos de código do AWS SDK para Ruby
AWS SDK para Rust	Exemplos de código do AWS SDK para Rust

Documentação do SDK	Exemplos de código
SDK da AWS para SAP ABAP	Exemplos de código do SDK da AWS para SAP ABAP
AWS SDK for Swift	Exemplos de código do AWS SDK for Swift

Histórico do documento

- Versão atual da API: 2006-03-01

A tabela a seguir descreve as alterações importantes em cada versão da Referência da API do Amazon Simple Storage Service e do Guia do usuário do Amazon S3. Para receber notificações sobre atualizações dessa documentação, você pode se inscrever em um feed RSS.

Alteração	Descrição	Data
O Amazon S3 Express One Zone agora permite o uso de tags para alocação de custos e controle de acesso por atributo	O Amazon S3 Express One Zone, uma classe de armazenamento de alto desempenho do S3, agora permite tags para alocação de custos e controle de acesso por atributo (ABAC). Você pode adicionar tags aos buckets de diretório do S3 para rastrear e organizar custos da AWS usando o Gerenciamento de Faturamento e Custos da AWS. Além disso, com o suporte ao ABAC, você pode escalar o controle de acesso aos seus buckets de diretório usando tags. O S3 Express One Zone permite o uso de tags em buckets de diretório em qualquer Região da AWS em que essa classe de armazenamento está disponível. Você pode começar a usar tags por meio do Console de Gerenciamento	2 de julho de 2025

	da AWS, da API REST do S3, da AWS CLI ou do SDK da AWS. Para saber mais sobre o uso de tags para simplific ar a alocação de custos ou o ABAC, consulte Usar tags com buckets de diretório do S3.	
Agora é possível anexar pontos de acesso a um volume do FSx para OpenZFS	Você pode criar e anexar um ponto de acesso a um volume do FSx para OpenZFS usando o console do Amazon FSx, a AWS CLI ou a API. Depois de anexado, você pode usar as APIs de objeto do S3 para acessar seus dados de arquivo. Seus dados continuam residindo no sistema de arquivos do Amazon FSx e continuam diretamente acessíveis para suas workloads existentes. Para ter mais informações, consulte Gerenciar o acesso a conjuntos de dados compartil hados com pontos de acesso.	25 de junho de 2025

O serviço Tabelas do S3 agora permite novas estratégias de compactação para tabelas	O serviço Tabelas do S3 agora permite várias estratégias de compactação para otimizar o desempenho de consulta com base em diferentes padrões de acesso aos dados. As novas estratégias incluem sort e Z-order. Para ter mais informações, consulte as estratégias de compactação para tabelas.	18 de junho de 2025
O serviço Tabelas do S3 adiciona nova política gerenciada pela para tabelas do S3	O serviço Tabelas do S3 adicionou uma nova política gerenciada pela AWS chamada `AmazonS3TablesLakeFormationServiceRole`. Essa política concede permissões que autorizam que o perfil de serviço do Lake Formation acesse tabelas e buckets do serviço Tabelas do Amazon S3. Para ter mais informações, consulte Políticas gerenciadas pela AWS para o serviço Tabelas do S3.	19 de maio de 2025

O serviço Tabelas do S3 agora é compatível com SSE-KMS usando chaves gerenciadas pelo cliente	A funcionalidade Tabelas do S3 agora comporta a criptografia do lado do servidor com chaves do AWS Key Management Service (AWS KMS) (SSE-KMS) usando chaves gerenciadas pelo cliente. É possível aplicar a criptografia SSE-KMS em nível de bucket e de tabela. Para ter mais informações, consulte Usar a criptografia do lado do servidor com chaves do AWS KMS (SSE-KMS) em buckets de tabela.	16 de abril de 2025
Pontos de acesso para buckets de diretório estão disponíveis em zonas locais da AWS	Os buckets de diretório agora permitem pontos de acesso para simplificar o gerenciam ento do acesso a dados em escala de conjuntos de dados compartilhados no Amazon S3. Com esse novo recurso, você pode criar centenas de pontos de acesso por bucket, cada um com um nome distinto e permissões personali zadas para cada aplicação. Para obter mais informações, consulte Gerenciar o acesso a conjuntos de dados compartil hados em buckets de diretório por meio de pontos de acesso.	31 de março de 2025

A integração de bucket de tabelas do S3 com o Amazon SageMaker Lakehouse agora está disponível ao público	É possível integrar buckets de tabela do S3 ao Amazon SageMaker Lakehouse para acessar tabelas de serviços de analytics da AWS, como o Amazon Athena, o Amazon Redshift e o QuickSigh t. O Amazon SageMaker Lakehouse unifica todos os dados nos data lakes do Amazon S3 e nos data warehouses do Amazon Redshift, para que seja possível criar aplicações de analytics, machine learning (ML) e IA generativa em uma única cópia dos dados. A integração preenche o AWS Glue Data Catalog com os recursos da tabela e federa o acesso a esses recursos com o AWS Lake Formation. A integração permite o controle de acesso refinado por meio do Lake Formation para oferecer segurança adicional. Para ter mais informações, consulte Usar tabelas do Amazon S3 com serviços de analytics da AWS. Se você configuro u a integração com a versão prévia, pode continuar usando sua integração atual. No entanto, como o processo de integração atualizado oferece	13 de março de 2025

	melhorias de desempenho, recomendamos a migração. Para migrar para a integraçã o atualizada, consulte Migrar para o processo de integração atualizado.	
Suporte adicionado para criar e consultar tabelas do serviço Tabelas do S3 no console do Amazon S3	O serviço Tabelas do S3 agora permite realizar operações de criação de tabelas e consulta a tabelas diretamente no console do Amazon S3 usando o Amazon Athena. Com esse novo recurso, agora você pode criar uma tabela, preenchê-la com dados e consultá-la com apenas algumas etapas no console do Amazon S3. Para ter mais informações, consulte Criar uma tabela do Amazon S3 e Consultar tabelas do Amazon S3 com o Amazon Athena.	13 de março de 2025
A funcionalidade Tabelas do S3 adiciona suporte à adição de esquemas ao criar tabelas	Agora você pode usar a operação de API `CreateTable` da funcionalidade Tabelas do S3 para criar tabelas com esquemas ao adicionar um sinalizador de metadados opcional. Para ter mais informações, consulte Criar uma tabela.	30 de janeiro de 2025

A funcionalidade Tabelas do S3 adiciona suporte à adição de esquemas ao criar tabelas	Agora você pode usar a operação de API `CreateTable` da funcionalidade Tabelas do S3 para criar tabelas com esquemas ao adicionar um sinalizador de metadados opcional. Para ter mais informações, consulte Criar uma tabela.	30 de janeiro de 2025

O S3 Metadata agora está disponível ao público	O Amazon S3 Metadata agora está disponível ao público. O S3 Metadata ajuda você a descobrir e entender facilmente os dados do S3 com metadados automatizados e consultáveis que são atualizados quase em tempo real. Com o S3 Metadata, você pode fazer a curadoria, identificar e usar os dados do S3 para analytics de negócios, treinamento de modelos de inteligência artificial e de machine learning (IA/ML) e muito mais. O S3 Metadata oferece suporte a metadados de objetos, que incluem informações definidas pelo sistema, como o tamanho e a origem do objeto, e metadados personalizados, como tags com informações que incluem SKUs de produtos, IDs de transações ou classificações de conteúdo. Para ter mais informações, consulte Accelerating data discovery with S3 Metadata.	27 de janeiro de 2025
Políticas gerenciadas pela AWS: novas políticas	A funcionalidade Tabelas do S3 adicionou duas novas políticas gerenciadas pela AWS.	06 de dezembro de 2024

Tabelas do S3	A funcionalidade Tabelas do Amazon S3 fornece armazenamento do S3 otimizado para workloads de analytics, com recursos que melhoram a performance das consultas, reduzem os custos de armazenamento de tabelas e simplificam a operação de data lakes em grande escala. A funcionalidade Tabelas do S3 apresenta um novo tipo de bucket: buckets de tabela, que têm o propósito específico de armazenar tabelas Apache Iceberg como sub-recursos. Os buckets de tabela fornecem quantidades mais altas de transações por segundo (TPS) e melhor throughput de consultas em comparação com as tabelas autogerenciadas em buckets de uso geral do S3. Você pode integrar automaticamente os buckets de tabela aos serviços de analytics da AWS, como Athena, Amazon Redshift, QuickSight e outros. Para ter mais informações, consulte Working with Amazon S3 Tables and table buckets.	3 de dezembro de 2024

Prévia do S3 Metadata	O Amazon S3 Metadata ajuda você a descobrir e entender facilmente os dados do S3 com metadados automatizados e consultáveis que são atualizados quase em tempo real. Com o S3 Metadata, você pode fazer a curadoria, identificar e usar os dados do S3 para analytics de negócios, treinamento de modelos de inteligência artificial e de machine learning (IA/ML) e muito mais. O S3 Metadata oferece suporte a metadados de objetos, que incluem informações definidas pelo sistema, como o tamanho e a origem do objeto, e metadados personalizados, como tags com informações que incluem SKUs de produtos, IDs de transações ou classificações de conteúdo. Para ter mais informações, consulte Accelerating data discovery with S3 Metadata.	3 de dezembro de 2024

Navegador de Armazenamento para S3	O Navegador de Armazenamento para S3 é um componente de código aberto que você pode adicionar a aplicativos web para fornecer aos usuários finais uma interface simples para dados armazenados no S3. Para ter mais informações, consulte Storage Browser para Amazon S3.	1.º de dezembro de 2024
Novo algoritmo de soma de verificação do Amazon S3 e melhoria dos recursos de integridade da soma de verificação	O Amazon S3 adiciona o algoritmo de soma de verificação `CRC-64NVME` e recursos de integridade da soma de verificação aprimorados. Para ter mais informações, consulte Verificar a integridade do objeto no Amazon S3.	1.º de dezembro de 2024
Workloads de residência de dados	Nas zonas locais dedicadas, você pode criar buckets de diretório do S3 a fim de armazenar dados para casos de uso de isolamento e residência de dados. Para ter mais informações, consulte Data residency workloads.	1.º de dezembro de 2024

Novas chaves de condição para impor gravações condicionais	O Amazon S3 adiciona novas chaves de condição `s3:if-match` e `s3:if-none-match` para uso em políticas de bucket a fim de forçar os clientes a usar os cabeçalhos HTTP `If-None-Match` ou `If-Match`. Para ter mais informações, consulte Enforce conditional writes on Amazon S3 buckets.	25 de novembro de 2024
Novo cabeçalho HTTP para gravações condicionais a fim de verificar se o objeto foi alterado	O Amazon S3 adiciona o cabeçalho HTTP `If-Match` para verificar a tag de entidade (ETag) de um objeto antes de gravá-lo para algumas operações de API. Com esse cabeçalho, o Amazon S3 compara o valor da ETag fornecido com o valor da ETag do objeto no S3. Se esses valores de ETag não forem correspondentes, a operação vai falhar. Para ter mais informações, consulte Como evitar substituições de objeto com gravações condicionais.	25 de novembro de 2024

Amazon Redshift agora se integra à funcionalidade Concessões de Acesso do S3	Os clientes do Amazon Redshift agora podem usar a funcionalidade Concessões de Acesso do S3 para escalar e gerenciar permissões para dados do S3. Isso permite que os clientes do Amazon Redshift escalem as permissões do S3 para identidades corporativas usando o AWS IAM Identity Center, bem como para grupos e usuários do IAM. Consulte mais informações em Amazon Redshift integration with Amazon S3 Access Grants.	15 de novembro de 2024
As contas-membro do AWS Organizations agora podem recuperar o acesso aos buckets do Amazon S3 bloqueados acidentalmente	As contas-membro do AWS Organizations agora podem usar um processo simples por meio do AWS Identity and Access Management (IAM) para recuperar acesso a buckets do Amazon S3 bloqueados acidentalmente. Consulte mais informações em Perform a privileged task on an AWS Organizations member account no Guia do usuário do AWS Identity and Access Management.	14 de novembro de 2024

Políticas de controle de recursos (RCPs), um novo tipo de política de autorização no AWS Organizations, também está disponível para buckets do Amazon S3	Políticas de controle de recursos (RCPs), uma nova política de autorização gerenciada no AWS Organizations, podem ser usadas para definir o máximo de permissões disponíveis nos buckets do Amazon S3 em toda a sua organização. Consulte mais informações em Resource control policies (RCPs) no Guia do usuário do AWS Organizations.	13 de novembro de 2024
O Amazon S3 agora aprova automaticamente aumentos de cota de bucket para até 1.000 buckets	O Amazon S3 agora aprova automaticamente aumentos de cota de bucket para até 1.000 buckets. Para visualizar a utilização do bucket ou solicitar um aumento, acesse o console do Service Quotas.	30 de setembro de 2024
Novo comportamento padrão de transição de tamanho mínimo de objeto para configurações do Ciclo de Vida do Amazon S3	Agora o Amazon S3 aplica um comportamento padrão às configurações do ciclo de vida do S3 que não permite a transferência de objetos menores que 128 KB para nenhuma classe de armazenamento. Para saber como mudar esse comportamento, consulte Allowing objects smaller than 128 KB to be transitioned.	24 de setembro de 2024

Os buckets de diretório agora são compatíveis com SSE-KMS usando chaves gerenciadas pelo cliente.	Os buckets de diretório agora comportam a criptografia do lado do servidor com chaves do AWS Key Management Service (AWS KMS) (SSE-KMS) usando chaves gerenciadas pelo cliente. Você tem mais opções para criptografar e gerenciar a segurança dos seus dados nos buckets de diretório. Para ter mais informações, consulte Data protection and encryption in directory buckets.	17 de setembro de 2024
O recurso Concessão de Acesso do S3 permite uma ação de API que lista as concessões de acesso do chamador	As identidades do IAM e de diretório corporativo do Centro de Identidade do IAM podem usar a API `ListCallerAccessGrants` para listar todos os buckets, prefixos e objetos do Amazon S3 que elas podem acessar, conforme definido pelo recurso Concessão de Acesso do S3. Use essa API para descobrir todos os dados do S3 que uma entidade do IAM ou uma identidade de diretório corporativo pode acessar por meio do recurso Concessão de Acesso do S3, em uma Conta da AWS específica. Para ter mais informações, consulte Listar as concessões de acesso do chamador.	5 de setembro de 2024

As mensagens aprimoradas de acesso negado são exibidas para solicitações da mesma conta	O Amazon S3 agora inclui contexto adicional em erros de acesso negado (HTTP `403 Forbidden`) para solicitações feitas a recursos dentro da mesma Conta da AWS. Esse novo contexto inclui o tipo de política que negou o acesso, o motivo da negação e informações sobre o usuário ou o perfil do AWS Identity and Access Management (IAM) que solicitou acesso ao recurso. Esse contexto ajuda você a solucionar problemas de acesso, identificar a causa-raiz dos erros de acesso negado e corrigir controles de acesso incorretos por meio da atualização das políticas pertinentes. Esse contexto adicional também está disponível nos logs do AWS CloudTrail. As mensagens de erro aprimoradas de acesso negado para solicitações da mesma conta agora estão disponíveis em todas as Regiões da AWS, incluindo as AWS GovCloud (US) Regions e as da China. Consulte mais informações em Solucionar erros de acesso negado (403 Forbidden) no Amazon S3.	21 de agosto de 2024

O Amazon S3 comporta o uso de gravações condicionais para `PutObject` e `CompleteMultipartUpload`.	É possível conferir a existência de um objeto no bucket antes de criá-lo usando uma gravação condicional nas operações de upload. Isso pode evitar a substituição de dados existentes. As gravações condicionais confirmarão que não há nenhum objeto com o mesmo nome de chave no bucket. Para ter mais informações, consulte Solicitações condicionais.	20 de agosto de 2024
Vários códigos de erro HTTP não são mais cobrados pelo Amazon S3	Houve uma alteração Amazon S3 que permite que as solicitações não autorizadas que os clientes não iniciaram sejam gratuitas. Para ter mais informações, consulte Cobrança pelas respostas de erro do Amazon S3.	19 de agosto de 2024
O Amazon S3 Select não está mais disponível para novos clientes.	O Amazon S3 Select não está mais disponível para novos clientes. Os clientes existentes do Amazon S3 Select podem continuar usando o atributo normalmente. Saiba mais.	25 de julho de 2024

O Inventário Amazon S3 é compatível com a chave de condição s3:InventoryAccessibleOptionalFields	O Inventário Amazon S3 é compatível com a chave de condição s3:InventoryAccessibleOptionalFields para controlar se os usuários podem incluir campos de metadados opcionais em seus relatórios. Consulte mais informações em Control S3 Inventory report configuration creation.	20 de fevereiro de 2024
Suporte a IPv6 para o S3 no Outposts	Agora é possível acessar buckets do S3 no Outposts usando IPv6 via endpoints de pilha dupla do S3 no Outposts. O suporte a IPv6 para S3 no Outposts permite que você gerencie buckets do S3 no Outposts e controle os recursos do ambiente de gerenciamento em redes IPv6.	16 de janeiro de 2024

Nova classe de armazenamento de zona única e alta performance do Amazon S3: S3 Express One Zone	A classe Amazon S3 Express One Zone é uma classe de armazenamento de zona única e alto desempenho do Amazon S3 desenvolvida com o propósito específico de fornecer acesso consistente aos dados e com latência inferior a dez milissegundos para as aplicações mais sensíveis à latência. Para obter mais informações, consulte S3 Express One Zone.	28 de novembro de 2023
O Mountpoint para Amazon S3 adiciona suporte à classe S3 Express One Zone	Agora você pode montar buckets de diretório da classe S3 Express One Zone com o Mountpoint.	28 de novembro de 2023
Versão do esquema de invocação do Lambda	A funcionalidade Operações em Lote do Amazon S3 apresenta uma nova versão do esquema de invocação do Lambda para uso com trabalhos da funcionalidade Operações em Lote que atuam em buckets de diretório. Para obter mais informações, consulte Usar o Lambda e a funcionalidade Operações em Lote do Amazon S3 com buckets de diretório.	28 de novembro de 2023

Ação de importação para buckets de diretório	Lançamento da ação de importação no Amazon S3. A importação é um método simplificado para criar trabalhos da funcional idade Operações em Lote do Amazon S3 a fim de copiar objetos de buckets de uso geral para buckets de diretório . Para obter mais informações, consulte Importing objects into a directory bucket.	28 de novembro de 2023
Gerenciar o acesso ao S3 com a funcionalidade Concessões de Acesso do S3	A funcionalidade Concessõe s de Acesso do Amazon S3 permite que você gerencie permissões de dados em grande escala para entidades principais do AWS Identity and Access Management (IAM), além de identidades de diretórios corporativos, como Azure AD. Agora você pode aplicar permissões do S3 de privilégio mínimo e escalar facilmente essas permissões com base nas necessidades da sua empresa. Para obter mais informações, consulte Gerenciar o acesso com a funcionalidade Concessões de Acesso do S3.	26 de novembro de 2023

O Mountpoint para Amazon S3 adiciona o recurso de armazenamento em cache	Com o Mountpoint, agora é possível configurar o armazenamento em cache para dados acessados repetidamente.	22 de novembro de 2023
Melhoria da geração de manifestos da funcionalidade Operações em Lote do Amazon S3	Agora você pode instruir a funcionalidade Operações em Lote do Amazon S3 a gerar um manifesto automaticamente com base nos critérios de filtro de objetos especificados ao criar um trabalho. Essa opção está disponível para trabalhos de replicação em lote criados no console do Amazon S3 ou para qualquer tipo de trabalho criado usando a AWS CLI, SDKs da AWS ou a API REST do Amazon S3. Para obter mais informações, consulte Criar um trabalho de operações em lote do S3.	22 de novembro de 2023
Buckets do Amazon S3 existentes agora podem adicionar configurações da funcionalidade Bloqueio de Objetos	Agora é possível habilitar a funcionalidade Bloqueio de Objetos em um bucket do Amazon S3 existente. Você pode definir retenções jurídicas e períodos de retenção para buckets novos ou existentes. Para obter mais informações, consulte Usar o bloqueio de objetos do S3.	20 de novembro de 2023

Métricas de solicitação da Lente de Armazenamento do S3 para prefixos	A Lente de Armazenamento do S3 apresenta métricas de solicitação para prefixos em um bucket do Amazon S3. Para obter mais informaçõ es, consulte Categorias de métricas.	17 de novembro de 2023
Grupos de Lente de Armazenamento do Amazon S3	A Lente de Armazenamento do S3 apresenta grupos da Lente de Armazenamento, um filtro personalizado definido para objetos com base em metadados de objetos. Para obter mais informaçõ es, consulte Trabalhar com grupos de Lente de Armazenamento do Amazon S3.	15 de novembro de 2023
Nova política do IAM	O S3 no Outposts agora conta com o `AWSServic eRoleForS3OnOutpos ts` , um perfil vinculado a serviços para ajudar a gerenciar recursos de rede para você. Para obter mais informações, consulte Usar perfis vinculados a serviços para o S3 no Outposts.	3 de outubro de 2023

O Amazon S3 fornece a hora da `Last-Modified` para marcadores de exclusão.	O Amazon S3 fornece a hora da `Last-Modified` dos marcadores de exclusão nos cabeçalhos de resposta das operações de API `Head` e `Get` do S3. Para obter mais informações, consulte Trabalhar com marcadores de exclusão.	27 de setembro de 2023
Atualização do Amazon S3 para políticas gerenciadas pela AWS	O Amazon S3 adicionou permissões `s3:Describe*` a `AmazonS3ReadOnlyAccess`. Para receber mais informações, consulte Políticas gerenciadas da AWS para o Amazon S3.	11 de agosto de 2023
Horários de início aprimorados para solicitações de restauração padrão feitas por meio do Operações em Lote do S3	As recuperações padrão para solicitações de restauração feitas por meio do Operações em Lote do S3 agora podem começar em minutos. Para receber mais informações, consulte Opções de recuperação de arquivo.	9 de agosto de 2023
Foi adicionado o Mountpoint, um cliente com alta taxa de throughput para montar um bucket Amazon S3 como um sistema de arquivos local.	Com o Mountpoint, as aplicações podem acessar objetos armazenados no Amazon S3 por meio de operações de arquivo, oferecendo às aplicações acesso ao armazenamento elástico e ao throughput do Amazon S3 por meio de uma interface de arquivo.	9 de agosto de 2023

Criptografia de camada dupla do lado do servidor com chaves do AWS Key Management Service (DSSE-KMS)	A criptografia de camada dupla do lado do servidor com chaves do AWS Key Management Service (AWS KMS) (DSSE-KMS) aplica duas camadas de criptografia aos objetos quando eles são carregados no Amazon S3. Para ter mais informações, consulte Utilização da criptografia de camada dupla do lado do servidor com chaves do AWS KMS.	13 de junho de 2023
O Amazon S3 habilita o Bloqueio de Acesso Público do S3 e desabilita as listas de controle de acesso (ACLs) do S3 para todos os novos buckets.	Agora o Amazon S3 automaticamente habilita o Bloqueio de Acesso Público do S3 e desabilita as listas de controle de acesso (ACLs) do S3 para todos os novos buckets em todas as Regiões AWS . Para ter mais informações, consulte Bloquear o acesso público ao armazenamento do Amazon S3 e Controlar a propriedade de objetos e desabilitar ACLs para seu bucket.	27 de abril de 2023

Métrica de falha de operações de replicação do S3	O Amazon S3 adiciona uma nova métrica do Amazon CloudWatch para monitorar falhas de replicação do S3. Para obter mais informações, consulte Monitoramento do progresso com métricas de replicação.	5 de abril de 2023
DNS privado	O AWS PrivateLink para Amazon S3 agora é compatível com o DNS privado. Para ter mais informações, consulte DNS privado.	14 de março de 2023
Suporte aos pontos de acesso entre contas no console do Amazon S3	O Amazon S3 agora é compatível com a criação de pontos de acesso entre contas com o console do Amazon S3. Para obter mais informações, consulte Criar pontos de acesso.	14 de março de 2023
O Amazon S3 no Outposts é compatível com a replicação do S3 no Outposts	Com a replicação do S3 local, você pode replicar automaticamente objetos para um único bucket de destino do Outposts ou para vários buckets de destino. Os buckets de destino podem estar em um AWS Outposts diferente ou no mesmo Outposts que o bucket de origem. Para ter mais informações, consulte Replicar objetos para o S3 no Outposts.	14 de março de 2023

Alias de pontos de acesso do Amazon S3 Object Lambda	Quando você cria um ponto de acesso do Object Lambda, o Amazon S3 gera automaticamente um alias exclusivo para seu ponto de acesso do Object Lambda. É possível usar esse alias em vez de um nome de bucket do Amazon S3 ou o nome do recurso da Amazon (ARN) do ponto de acesso do Object Lambda em uma solicitação para operações de plano de dados do ponto de acesso. Para ter mais informações, consulte Como usar um alias em estilo de bucket para seu ponto de acesso do Object Lambda.	14 de março de 2023
Suporte entre contas a pontos de acesso multirregião do Amazon S3	O Amazon S3 agora é compatível com a criação de pontos de acesso multirregionais entre contas com o console do Amazon S3. Para ter mais informações, consulte Criar pontos de acesso multirregionais.	14 de março de 2023

Pontos de acesso entre contas	O Amazon S3 oferece suporte à criação de pontos de acesso entre contas. Você pode criar um ponto de acesso entre contas usando a AWS Command Line Interface (AWS CLI) ou a operação `CreateAccessPoint` da API REST. Para obter mais informações, consulte Criar pontos de acesso.	30 de novembro de 2022
Amazon S3 oferece suporte a controles de failover para pontos de acesso multirregionais do Amazon S3	O Amazon S3 adicionou controles de failover para pontos de acesso multirregionais do Amazon S3. Esses controles permitem que você transfira o tráfego de solicitações de acesso a dados do S3 que passam por um ponto de acesso multirregional do Amazon S3 para outra Região da AWS em questão de minutos para testar e criar aplicações altamente disponíveis. Para obter mais informações, consulte Controles de failover para pontos de acesso multirregionais do Amazon S3.	28 de novembro de 2022

Lente de Armazenamento do Amazon S3 aumenta a visibilidade em toda a organização com 34 novas métricas	A Lente de Armazenamento do S3 adicionou 34 novas métricas para revelar oportunidades de otimização de custos mais profundas, identificar práticas recomendadas de proteção de dados e melhorar a performance das workloads de aplicações. Para obter mais informações, consulte Métricas da Lente de Armazenamento do S3.	17 de novembro de 2022
Amazon S3 oferece suporte a taxas de solicitações de restauração mais altas para S3 Glacier Flexible Retrieval e S3 Glacier Deep Archive	O Amazon S3 oferece suporte a solicitações de restauração a uma taxa de até 1.000 transações por segundo, por Conta da AWS, para as classes de armazenamento S3 Glacier Flexible Retrieval e S3 Glacier Deep Archive.	15 de novembro de 2022

Amazon S3 no Outposts oferece suporte a ações e filtros adicionais para o Ciclo de Vida do S3	O S3 no Outposts oferece suporte a regras adicionais do Ciclo de Vida do S3 para otimizar o gerenciamento da capacidade. Você pode expirar objetos à medida que envelhecem ou quando são substituídos por versões mais recentes. Você pode criar uma regra de ciclo de vida para um bucket inteiro ou um subconjunto de objetos dentro de um bucket ao filtrar por prefixos, etiquetas de objeto ou tamanho de objeto. Para obter mais informações, consulte Criar e gerenciar uma configuração de ciclo de vida.	2 de novembro de 2022
Suporte à Replicação do S3 para objetos SSE-C	Você pode replicar objetos criados com criptografia do lado do servidor usando chaves de criptografia fornecidas pelo cliente. Para obter mais informações sobre como replicar objetos criptografados, consulte Replicar objetos criados com criptografia do lado do servidor (SSE-C, SSE-S3, SSE-KMS).	24 de outubro de 2022

Amazon S3 no Outposts oferece suporte a alias de pontos de acesso	Com o S3 on Outposts, você deve usar pontos de acesso para acessar qualquer objeto em um bucket do Outposts. Toda vez que você cria um ponto de acesso para um bucket, o S3 no Outposts gera automaticamente um alias de ponto de acesso. É possível usar esse alias de ponto de acesso em vez de um ARN de ponto de acesso para qualquer operação de plano de dados. Para obter mais informações, consulte Usar um alias em estilo de bucket para um ponto de acesso de bucket do S3 no Outposts.	21 de outubro de 2022
S3 Object Lambda oferece suporte às operações `HeadObject` , `ListObjects` e `ListObjectsV2`	Você pode usar código personalizado para modificar os dados retornados por solicitações `GET`, `LIST` e `HEAD` padrão do S3 para filtrar linhas, redimensionar imagens dinamicamente, editar dados confidenciais e muito mais. Para obter mais informações, consulte Transformar objetos com o S3 Object Lambda.	04 de outubro de 2022

Amazon S3 no Outposts oferece suporte ao versionamento do S3	Quando habilitado, o versionamento do S3 salva várias cópias distintas de um objeto no mesmo bucket. O versionamento do S3 pode ser usado para preservar, recuperar e restaurar todas as versões de cada objeto armazenado em buckets do Outposts. O versionamento do S3 ajuda você a se recuperar de ações não intencionais de usuários e de falhas da aplicação. Para obter mais informações, consulte Gerenciar o versionamento do S3 para um bucket do S3 no Outposts.	21 de setembro de 2022
AWS Backup for Amazon S3	O AWS Backup é um serviço totalmente gerenciado e baseado em políticas que você pode usar para definir uma política de backup central para proteger seus dados do Amazon S3. Para obter mais informações, consulte Usar o AWS Backup para o Amazon S3.	18 de fevereiro de 2022

Usar a replicação em lote do S3 para replicar objetos existentes	Com a replicação em lote do S3, você pode replicar objetos que existiam antes que uma configuração de replicação estivesse em vigor. A replicação de objetos existentes é feita por meio do uso de um trabalho de operações em lote. A replicação em lote do S3 é diferente da replicação em tempo real, que copia contínua e automaticamente novos objetos nos buckets do Amazon S3. Para obter mais informações, consulte Replicating existing objects with S3 Batch Replication (Replicar objetos existentes com o S3 Batch Replication).	8 de fevereiro de 2022
Novo nome: S3 Glacier Flexible Retrieval	A classe de armazenamento Glacier foi renomeada para S3 Glacier Flexible Retrieval. Essa alteração não afeta a API.	30 de novembro de 2021

Nova configuração do S3 Object Ownership para desabilitar ACLs	Você pode aplicar a configuração imposta pelo proprietário do bucket em Object Ownership para desabilitar ACLs para o bucket e os objetos contidos nele, e assumir a propriedade de cada objeto de seu bucket. A configuração imposta pelo proprietário do bucket simplifica o gerenciamento de acesso aos dados armazenados no Amazon S3. Para obter mais informações, consulte Controlar a propriedade de objetos e desabilitar ACLs para seu bucket.	30 de novembro de 2021
Nova classe de armazenamento S3 Intelligent-Tiering	O S3 Intelligent-Tiering Archive Instant Access é uma classe de armazenamento adicional do S3 Intelligent-Tiering. Para obter mais informações, consulte Como o S3 Intelligent-Tiering funciona.	30 de novembro de 2021
Nova classe de armazenamento S3 Glacier Instant Retrieval	Agora é possível colocar objetos na classe de armazenamento do S3 Glacier Instant Retrieval. Para obter mais informações sobre essa classe de armazenamento, consulte Usar as classes de armazenamento do Amazon S3.	30 de novembro de 2021

Pré-visualização do AWS Backup para o Amazon S3	O AWS Backup é um serviço totalmente gerenciado e baseado em políticas que você pode usar para definir uma política de backup central para proteger seus dados do Amazon S3. Para obter mais informações, consulte Usar o AWS Backup para o Amazon S3.	30 de novembro de 2021
AWS Identity and Access Management Access Analyzer for Amazon S3	O IAM Access Analyzer executa verificações de política para validar sua política em relação à gramática das políticas e às práticas recomendadas e do IAM. Para saber mais sobre a validação de políticas usando o IAM Access Analyzer, consulte Validação de políticas do IAM Access Analyzer no Guia do usuário IAM.	30 de novembro de 2021
Novos tipos de evento	Para ver os novos tipos de evento adicionados às notificações de eventos do Amazon S3, consulte Notificações de eventos do Amazon S3.	29 de novembro de 2021
Habilitar o Amazon EventBridge em buckets	Você pode habilitar o EventBridge em buckets do Amazon S3 para enviar eventos ao Amazon EventBridge. Consulte Usar o EventBridge.	29 de novembro de 2021

Novos filtros do S3 Lifecycle	É possível criar regras de ciclo de vida com base no tamanho do objeto ou especificar quantas versões de objeto desatualizadas deverão ser mantidas. Para obter mais informações, consulte Exemplos de configuração do Ciclo de Vida do S3.	23 de novembro de 2021
Publicar métricas do Amazon S3 Storage Lens no Amazon CloudWatch	É possível publicar métricas de uso e atividade do S3 Storage Lens no Amazon CloudWatch para criar uma visão unificada de sua integridade operacional nos painéis do CloudWatch. Também é possível usar os recursos do CloudWatch, como alarmes e ações acionadas, matemática métrica e detecção de anomalias, para monitorar e realizar ações sobre as métricas do S3 Storage Lens. Além disso, as APIs do CloudWatch permitem que aplicações, inclusive provedores de terceiros, acessem as métricas do S3 Storage Lens. Para obter mais informações, consulte Monitorar métricas do S3 Storage Lens no CloudWatch.	22 de novembro de 2021

Pontos de acesso multirregionais	Você pode usar pontos de acesso multirregionais para criar um endpoint global que as aplicações podem usar para atender a solicitações de buckets do Amazon S3, localizados em várias Regiões da AWS. Você pode usar esse ponto de acesso multirregional para rotear dados para o bucket de menor latência. Para obter mais informações sobre os pontos de acesso multirregionais e como usá-los, consulte Pontos de acesso multirregionais no Amazon S3.	2 de setembro de 2021
O Amazon S3 no Outposts adiciona acesso local direto às aplicações	Execute suas aplicações fora da nuvem privada virtual (VPC) do AWS Outposts e acesse seus dados do S3 on Outposts. Também é possível acessar objetos do S3 on Outposts diretamente da rede local. Para obter mais informações sobre como configurar endpoints do S3 on Outposts usando endereços IP de propriedade do cliente (CoIP) e acessar seus objetos criando um gateway local na rede local, consulte Como acessar o Amazon S3 on Outposts usando pontos de acesso somente para VPC.	29 de julho de 2021

Alias de ponto de acesso do Amazon S3	Quando você cria um ponto de acesso, o Amazon S3 gera automaticamente um alias que poderá ser usado no lugar de um nome de bucket para acesso a dados. É possível usar esse alias de ponto de acesso em vez de um nome do recurso da Amazon (ARN) para qualquer operação de plano de dados do ponto de acesso. Para obter mais informações, consulte Usar um alias em estilo de bucket para seu ponto de acesso.	26 de julho de 2021
O Amazon S3 Inventory e o recurso de operações em lote do S3 são compatíveis com o status de chave de bucket do S3	O Amazon S3 Inventory e o Batch Operations oferecem suporte à identificação e à cópia de objetos existente s com chaves de bucket do S3. As chaves de Bucket do S3 aceleram a redução dos custos de criptografia no lado do servidor para objetos existentes. Para obter mais informações, consulte Amazon S3 Inventory e Objeto Copy do Batch Operations.	3 de junho de 2021

Snapshot da conta de métricas do Amazon S3 Storage Lens	O snapshot da conta do S3 Storage Lens exibe o armazenamento total, a contagem de objetos e o tamanho médio do objeto na página inicial (Buckets) resumindo as métricas do painel padrão. Para obter mais informações, consulte Snapshot da conta de métricas do S3 Storage Lens.	5 de maio de 2021
Aumento do suporte ao endpoint do Amazon S3 no Outposts	O S3 on Outposts agora suporta até 100 endpoints por Outpost. Para obter mais informações, consulte Restrições de rede do S3 no Outposts.	29 de abril de 2021
Notificações de eventos do Amazon S3 no Outposts usando Amazon CloudWatch Events	Você pode usar o CloudWatch Events para criar uma regra para capturar qualquer evento da API do S3 no Outposts e ser notificado por meio de todos os destinos compatíveis do CloudWatch. Para obter mais informações, consulte Como receber notificações de eventos do S3 no Outposts usando o CloudWatch Events.	19 de abril de 2021

S3 Object Lambda	Com o S3 Object Lambda, você pode adicionar seu próprio código às solicitações GET do Amazon S3 para modificar e processar dados, conforme eles são retornados para uma aplicação. Você pode usar o código personalizado para modificar os dados retornados por solicitações GET padrão do S3 para filtrar linhas, redimensionar imagens dinamicamente, editar dados confidenciais e muito mais. Para obter mais informações, consulte Transformar objetos.	18 de março de 2021
AWS PrivateLink	Com o AWS PrivateLink para Amazon S3, você pode se conectar diretamente ao S3 usando um endpoint de interface em sua nuvem privada virtual (VPC) em vez de se conectar pela Internet. Os endpoints de interface são diretamente acessíveis a partir de aplicações on-premises ou em uma Região da AWS diferente. Para obter mais informações, consulte AWS PrivateLink para Amazon S3.	2 de fevereiro de 2021

Gerenciar a capacidade do Amazon S3 em Outposts com AWS CloudTrail	Os eventos de gerenciamento do S3 no Outposts estão disponíveis por meio de logs do CloudTrail. Para obter mais informações, consulte Como gerenciar a capacidade do S3 no Outposts com o CloudTrail.	21 de dezembro de 2020
Forte consistência	O Amazon S3 oferece uma forte consistência de leitura após gravação para solicitações PUT e DELETE de objetos no bucket do S3 em todas as Regiões da AWS. Além disso, as operações de leitura no Amazon S3 Select, listas de controle de acesso do Amazon S3, etiquetas de objeto do Amazon S3 e metadados de objeto (por exemplo, objeto HEAD) são fortemente consistentes. Para obter mais informações, consulte Modelo de consistência de dados do Amazon S3.	1º de dezembro de 2020

Sincronização de modificação de réplica do Amazon S3	A sincronização de modificação de réplica do Amazon S3 mantém metadados de objeto, como etiquetas, ACLs e configurações de bloqueio de objetos, em sincronia entre objetos de origem e réplicas. Quando esse recurso está habilitado, o Amazon S3 replica as alterações de metadados feitas no objeto de origem ou nas cópias da réplica. Para obter mais informações, consulte Replicar alterações de metadados com sincronização de modificação de réplica.	1º de dezembro de 2020
Amazon S3 Bucket Keys	As chaves de bucket do Amazon S3 reduzem o custo da criptografia do lado do servidor do Amazon S3 com o AWS Key Management Service (SSE-KMS). Essa nova chave no nível de bucket para criptografia no lado do servidor pode reduzir os custos de solicitações do AWS KMS em até 99%, diminuindo o tráfego de solicitações do Amazon S3 para o AWS KMS. Para obter mais informações, consulte Reduzir o custo do SSE-KMS usando chaves de bucket do S3.	1º de dezembro de 2020

Amazon S3 Storage Lens	A Lente de Armazenamento do S3 agrega suas métricas e exibe as informações na seção Account snapshot (Snapshot da conta) na página Buckets do console do Amazon S3. A Lente de Armazenamento do S3 também oferece um painel interativo para visualizar insights e tendências, sinalizar discrepâncias e receber recomendações para otimizar os custos de armazenam ento e aplicar as práticas recomendadas de proteção de dados. O painel tem opções de detalhamento para gerar e visualizar insights no nível da organização, conta, Região da AWS, classe de armazenam ento, bucket, prefixo ou grupo de Lente de Armazenam ento. Você também pode enviar uma exportação diária de métricas em CSV ou no formato Parquet para um bucket do S3. Para obter mais informações, consulte Avaliar a atividade e o uso do armazenamento com o S3 Storage Lens.	18 de novembro de 2020

Rastrear solicitações do S3 usando o AWS X-Ray	O Amazon S3 integra-se ao X-Ray para propagar o contexto de rastreamento e fornecer uma cadeia de solicitações com nós upstream e downstream. Para obter mais informações, consulte Rastrear solicitações usando o X-Ray.	16 de novembro de 2020
Métricas de replicação do S3	As métricas de replicação do S3 fornecem métricas detalhadas para as regras de replicação na configuração de replicação. Para obter mais informações, consulte Métricas de replicação e notificações de eventos do Amazon S3.	9 de novembro de 2020
Acesso ao arquivo em S3 Intelligent-Tiering S3 e acesso ao arquivo profundo	O acesso ao arquivamento e o acesso ao arquivamento profundo do S3 Intelligent-Tiering são camadas de armazenamento adicionais sob o S3 Intelligent-Tiering. Para obter mais informações, consulte Classe de armazenamento para otimizar automaticamente objetos acessados com frequência e pouca frequência.	9 de novembro de 2020

Replicação de marcadores de exclusão	Com a replicação de marcadores de exclusão, você pode garantir que os marcadores de exclusão sejam copiados para seus buckets de destino para suas regras de replicação. Para obter mais informações, consulte Usando replicação de marcadores de exclusão.	9 de novembro de 2020
Propriedade de objeto do S3	Propriedade de objetos é uma configuração de bucket do S3 que pode ser usada para controlar a proprieda de de novos objetos que são carregados nos buckets. Para obter mais informaçõ es, consulte Usar o S3 Object Ownership.	2 de outubro de 2020

Amazon S3 on Outposts	Com o Amazon S3 no Outposts, é possível criar buckets do S3 em seus recursos do AWS Outposts, além de armazenar e recuperar facilmente objetos no ambiente on-premises para aplicações que exigem acesso a dados locais, processamento de dados local e residência de dados. Você pode usar o S3 on Outposts por meio do AWS Managemen t Console, da AWS CLI, de AWS SDKs ou da API REST. Para obter mais informações, consulte Uso do Amazon S3 no Outposts.	30 de setembro de 2020
Condição do proprietário do bucket	É possível usar a condição de proprietário do bucket do Amazon S3 para garantir que os buckets usados nas operações do S3 pertençam às Contas da AWS esperadas . Para obter mais informaçõ es, consulte Condição do proprietário do bucket.	11 de setembro de 2020

Suporte a operações em lote do S3 para retenção de bloqueio de objetos	Agora você pode usar operações em lote com bloqueio de objeto do S3 para aplicar configurações de retenção a muitos objetos do Amazon S3 de uma só vez. Para obter mais informaçõ es, consulte Definir datas de retenção do bloqueio de objetos do S3 com operações em lote do S3.	4 de maio de 2020
Suporte a operações em lote do S3 para retenção legal de bloqueio de objetos	Agora você pode usar operações em lote com bloqueio de objetos do S3 para adicionar uma retenção legal a muitos objetos do Amazon S3 de uma só vez. Para obter mais informaçõ es, consulte Usar o S3 Batch Operations para definir a retenção legal do bloqueio de objeto do S3.	4 de maio de 2020
Etiquetas de trabalho para operações em lote do S3	Você pode adicionar tags aos trabalhos de operações em lote do S3 para controlar e rotular esses trabalhos. Para obter mais informaçõ es, consulte Etiquetas para trabalhos de operações em lote do S3.	16 de março de 2020

Pontos de acesso do Amazon S3	Os pontos de acesso do Amazon S3 simplificam o gerenciamento do acesso a dados em escala para conjuntos de dados compartilhados no S3. Os pontos de acesso são nomeados endpoints de rede anexados a buckets que podem ser usados para executar operações de objeto do S3. Para obter mais informações, consulte Gerenciar o acesso a dados com pontos de acesso do Amazon S3.	2 de dezembro de 2019
Analisador de acesso para Amazon S3	O Access Analyzer para Amazon S3 alerta sobre buckets do S3 configurados para permitir o acesso a qualquer pessoa na Internet ou a outras Contas da AWS, incluindo contas fora da organização. Para obter mais informações, consulte Usar o Access Analyzer para Amazon S3.	2 de dezembro de 2019

Controle do tempo de replicação do S3 (S3 RTC)	O recurso Controle do tempo de replicação do S3 (S3 RTC) replica a maioria dos objetos que você carrega para o Amazon S3 em segundos, bem como 99,99% desses objetos em 15 minutos. Para obter mais informações, consulte Replicating objects using S3 Replication Time Control (S3 RTC) [“Replicar objetos usando o Controle de Tempo de Replicação do S3 (S3 RTC)”].	20 de novembro de 2019
Replicação para a mesma região	Você pode usar a replicação para a mesma região (SRR) a fim de copiar objetos entre buckets do Amazon S3 na mesma Região da AWS. Para obter informações sobre replicação entre regiões (CRR) e replicação para a mesma região, consulte Replicação.	18 de setembro de 2019
Suporte da replicação entre regiões ao bloqueio de objetos do S3	A replicação entre regiões agora oferece suporte ao bloqueio de objetos. Para obter mais informações, consulte What does Amazon replicate? (“O que o Amazon S3 replica?”).	28 de maio de 2019

Operações em lote do S3	Usando o recurso de operações em lote do S3, você pode executar operações em lote de grande escala em objetos do Amazon S3. O recurso Operações em lote do S3 pode executar uma única operação em listas de objetos que você especific ar. Uma única tarefa pode realizar a operação especific ada em bilhões de objetos contendo exabytes de dados. Para obter mais informações, consulte Executar o S3 Batch Operations.	30 de abril de 2019
Região Ásia-Pacífico (Hong Kong)	Agora o Amazon S3 está disponível na região Ásia-Pacífico (Hong Kong). Para obter mais informações sobre regiões e endpoints do Amazon S3, consulte Regiões e endpoints na Referência geral da AWS.	24 de abril de 2019
Adição de um novo campo aos logs de acesso ao servidor	O Amazon S3 adicionou o seguinte campo aos logs de acesso ao servidor: Transport Layer Security (TLS) version (Versão do Transport Layer Security [TLS]). Para obter mais informações, consulte Formato do log de acesso ao servidor.	28 de março de 2019

Nova classe de armazenamento de arquivos	Agora o Amazon S3 oferece uma nova classe de armazenamento de arquivos, a Deep Archive (`DEEP_ARCHIVE`) do S3 Glacier, para armazenar objetos raramente acessados. Para obter mais informações, consulte Classes de armazenamento	27 de março de 2019
Adição de novos campos aos logs de acesso ao servidor	O Amazon S3 adicionou os seguintes novos campos aos logs de acesso ao servidor: Host Id (ID do host), Signature Version (Versão do Signature), Cipher Suite (Pacote de criptografia), Authentication Type (Tipo de autenticação) e Host Header (Cabeçalho de host). Para obter mais informações, consulte Formato do log de acesso ao servidor.	5 de março de 2019
Suporte para arquivos do Amazon S3 Inventory no formato Parquet	O Amazon S3 agora dá suporte ao formato Apache Parquet (Parquet) além dos formatos de arquivo Apache optimized row columnar (ORC) e Comma-Separated Values (CSV – Valores separados por vírgulas) para arquivos de saída de inventário. Para obter mais informações, consulte Inventário.	4 de dezembro de 2018

Bloqueio de objetos do S3	O Amazon S3 agora oferece a funcionalidade de bloqueio de objetos que fornece proteções de gravação única e leitura múltipla (WORM) para objetos do Amazon S3. Para obter mais informações, consulte Bloquear objetos.	26 de novembro de 2018
Restaurar atualização rápida	Usando a atualização rápida de restauração do Amazon S3, altere a velocidade de uma restauração da classe de armazenamento S3 Glacier Flexible Retrieval para mais rapidez durante o andamento da restauração. Para obter mais informações, consulte Restaurar objetos arquivados.	26 de novembro de 2018
Restaurar Notificações de Eventos	As Notificações de Eventos do Amazon S3 agora oferecem suporte a eventos de início e conclusão durante a restauração de objetos na classe de armazenamento S3 Glacier Flexible Retrieval. Para obter mais informações, consulte Notificações de eventos.	26 de novembro de 2018

PUT diretamente na classe de armazenamento Flexible Retrieval do S3 Glacier	A operação PUT do Amazon S3 agora oferece suporte à especificação de Flexible Retrieval do S3 Glacier como classe de armazenamento durante a criação de objetos. Anteriormente, era necessário fazer a transição de objetos para a classe de armazenamento S3 Glacier Flexible Retrieval de outra classe de armazenamento do Amazon S3. Além disso, ao usar a replicação entre regiões (CRR) do S3, você já especifica S3 Glacier Flexible Retrieval como a classe de armazenamento para objetos replicados. Para obter mais informações sobre a classe de armazenamento S3 Glacier Flexible Retrieval, consulte Classes de armazenamento. Para obter mais informações sobre como especificar a classe de armazenamento para objetos replicados, consulte Visão geral da configuração de replicação. Para obter mais informações sobre as alterações de API REST de PUT diretamente para Flexible Retrieval do S3 Glacier, consulte Histórico do documento: PUT diretamente	26 de novembro de 2018

	em Flexible Retrieval do S3 Glacier.	
Nova classe de armazenamento	O Amazon S3 agora oferece uma nova classe de armazenamento chamada S3 Intelligent-Tiering (`INTELLIGENT_TIERING`) projetada para dados duradouros com padrões de acesso alternados ou desconhecidos. Para obter mais informações, consulte Classes de armazenamento	26 de novembro de 2018
Bloqueio de acesso público do Amazon S3	O Amazon S3 agora inclui a possibilidade de bloquear acesso público a buckets e objetos por bucket ou conta. Para obter mais informações, consulte Usar o Amazon S3 Block Public Access.	15 de novembro de 2018

Filtrar melhorias nas regras de replicação entre regiões (CRR)	Na configuração da regra de CRR, você pode especific ar o filtro de um objeto para escolher um subgrupo de objetos aos quais a regra deve ser aplicada. Antes, você poderia filtrar somente por um prefixo de chaves de objeto. Nesta versão, você pode filtrar usando um prefixo de chaves de objeto, uma ou mais tags de objeto ou ambos. Para obter mais informaçõ es, consulte Configuração da CRR: visão geral da configura ção da replicação.	19 de setembro de 2018
Novos recursos do Amazon S3 Select	O Amazon S3 Select agora é compatível com entradas do Apache Parquet, consultas em objetos JSON aninhados e duas novas métricas de monitoramento do Amazon CloudWatch (`SelectSca nnedBytes` e `SelectRet urnedBytes`).	5 de setembro de 2018
Atualizações agora disponíve is em RSS	Agora você pode assinar um RSS Feed para receber notificações sobre atualizaç ões no Guia do usuário do Amazon S3.	19 de junho de 2018

Atualizações anteriores

A tabela a seguir descreve as alterações importantes em cada versão do Guia do usuário do Amazon S3 antes de 19 de junho de 2018.

Alteração	Descrição	Data
Atualização de exemplos de código	Exemplos de código atualizados: • C#: atualizamos todos os exemplos para usar o padrão assíncrono baseado em tarefas. Para obter mais informações, consulte APIs assíncronas de Amazon Web Services para .NET no Guia do desenvolvedor do AWS SDK para .NET. Agora os exemplos de código são compatíveis com a versão 3 do AWS SDK para .NET. • Java: atualizamos todos os exemplos a fim de usar o modelo de criador do cliente. Para obter mais informaçõ es sobre o modelo de criador do cliente, consulte Criar clientes de serviço. • PHP: atualização de todos os exemplos para usar o AWS SDK para PHP 3.0. Para obter mais informações sobre o AWS SDK para PHP 3.0, consulte AWS SDK para PHP. • Ruby: atualização do código de exemplo para que os exemplos funcionem com o AWS SDK para Ruby versão 3.	30 de abril de 2018
O Amazon S3 agora relata classes de armazenam ento S3 Glacier Flexible Retrieval e `ONEZONE_IA` para métricas de	Além de relatar bytes reais, essas métricas de armazenam ento incluem sobrecarga de bytes por objeto para classes de armazenamento aplicáveis (`ONEZONE_IA` , `STANDARD_IA` e S3 Glacier Flexible Retrieval): •	30 de abril de 2018

Alteração	Descrição	Data

armazenamento do Amazon CloudWatch Logs	Para objetos das classes de armazenamento `ONEZONE_IA` e `STANDARD_IA`, o Amazon S3 relata objetos com menos de 128 KB como tendo 128 KB. Para obter mais informações, consulte Compreender e gerenciar classes de armazenamento do Amazon S3.
	• Para objetos da classe de armazenamento S3 Glacier Flexible Retrieval, as métricas de armazenamento relatam as seguintes sobrecargas:
	  • Uma sobrecarga de 32 KB por objeto, cobrada de acordo com o preço da classe de armazenamento S3 Glacier Flexible Retrieval
	  • Uma sobrecarga de 8 KB por objeto, cobrada de acordo com os preços da classe de armazenamento `STANDARD`
	  Para obter mais informações, consulte Transição de objetos usando o Amazon S3 Lifecycle.
	
	Para obter mais informações sobre métricas de armazenamento, consulte Monitoramento de métricas com o Amazon CloudWatch.	

Nova classe de armazenamento	O Amazon S3 agora oferece uma nova classe de armazenamento, `STANDARD_IA` (IA significa “infrequent access”, inglês para “acesso com pouca frequência”), para armazenar objetos. Essa classe de armazenamento é otimizada para dados armazenados por longo tempo e acessados com menos frequência. Para obter mais informações, consulte Compreender e gerenciar classes de armazenamento do Amazon S3.	4 de abril de 2018

Alteração	Descrição	Data
Amazon S3 Select	O Amazon S3 agora oferece suporte à recuperação de conteúdo de objetos com base em uma expressão SQL. Para obter mais informações, consulte Consultar dados no local com o Amazon S3 Select.	4 de abril de 2018
Região Ásia-Pacífico (Osaka-Local)	O Amazon S3 agora está disponível na região Ásia-Pacífico (Osaka-Local). Para obter mais informações sobre regiões e endpoints do Amazon S3, consulte Regiões e endpoints na Referência geral da AWS. **Important** Você pode usar a região Ásia-Pacífico (Osaka-Local) apenas em conjunto com a região Ásia-Pacífico (Tóquio). Para solicitar acesso à região Ásia-Pacífico (Osaka-Local), entre em contato com seu representante de vendas.	12 de fevereiro de 2018
Carimbo de data e hora da criação do Amazon S3 Inventory	O Amazon S3 Inventory agora conta com um carimbo de data e hora com a data e a hora de início da criação do relatório do Amazon S3 Inventory. Você pode usar o timestamp para determinar alterações no armazenamento do Amazon S3 a partir da hora de início em que o relatório de inventário foi gerado.	16 de janeiro de 2018
Região Europa (Paris)	O Amazon S3 já está disponível na região Europa (Paris). Para obter mais informações sobre regiões e endpoints do Amazon S3, consulte Regiões e endpoints na Referência geral da AWS.	18 de dezembro de 2017
Região da China (Ningxia)	Agora o Amazon S3 está disponível na região da China (Ningxia). Para obter mais informações sobre regiões e endpoints do Amazon S3, consulte Regiões e endpoints na Referência geral da AWS.	29 de novembro de 2017

Alteração	Descrição	Data
Suporte para arquivos do Amazon S3 Inventory no formato ORC	Agora, o Amazon S3 é compatível com arquivos de saída de inventário no formato colunar de linhas otimizado do Apache (ORC) e no formato de valores separados por vírgulas (CSV). Além disso, agora você pode consultar o inventário do Amazon S3 usando o SQL padrão usando o Amazon Athena, o Amazon Redshift Spectrum e outras ferramentas como Presto, Apache Hive e Apache Spark. Para obter mais informações, consulte Catalogar e analisar seus dados com o Inventário S3.	17 de novembro de 2017
Criptografia padrão para buckets do S3	A criptografia padrão do Amazon S3 fornece uma forma de configurar o comportamento de criptografia padrão para um bucket do S3. Você pode configurar a criptografia padrão em um bucket para que todos os objetos sejam criptografados quando forem armazenados nele. Os objetos são criptografados usando a criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3) ou chaves gerenciadas pela AWS (SSE-KMS). Para obter mais informações, consulte Definir o comportamento padrão da criptografia para os buckets do Amazon S3.	06 de novembro de 2017
Status de criptografia no Amazon S3 Inventory	Agora, o Amazon S3 é compatível e inclui o status da criptografia no Amazon S3 Inventory para que você possa ver como seus objetos são criptografados em repouso para a auditoria de conformidade e outras finalidades. Você também pode configurar para criptografar o Amazon S3 Inventory com a criptografia do lado do servidor (SSE) ou o SSE-KMS para que todos os arquivos do inventário sejam criptografados apropriadamente. Para obter mais informações, consulte Catalogar e analisar seus dados com o Inventário S3.	06 de novembro de 2017

Alteração	Descrição	Data
Melhorias da replicação entre regiões (CRR)	Agora, a replicação entre regiões oferece suporte ao seguinte: • Em um cenário entre contas, você pode adicionar uma configuração de CRR a fim de alterar a propriedade da réplica para a Conta da AWS que tem o bucket de destino. Para obter mais informações, consulte Alterar o proprietário da réplica. • Por padrão, o Amazon S3 não replica objetos no seu bucket de origem que foram criados usando a criptografia no lado do servidor usando chaves armazenadas no AWS KMS. Mas, na sua configuração de CRR, você pode orientar o Amazon S3 a replicar esses objetos. Para obter mais informações, consulte Replicar objetos criptografados (SSE-S3, SSE-KMS, DSSE-KMS, SSE-C).	06 de novembro de 2017
Região Europa (Londres)	O Amazon S3 já está disponível na região Europa (Londres). Para obter mais informações sobre regiões e endpoints do Amazon S3, consulte Regiões e endpoints na Referência geral da AWS.	13 de dezembro de 2016
Região do Canadá (Central)	O Amazon S3 já está disponível na região Canadá (Central). Para obter mais informações sobre regiões e endpoints do Amazon S3, consulte Regiões e endpoints na Referência geral da AWS.	8 de dezembro de 2016

Alteração	Descrição	Data
Marcação de objetos	O Amazon S3 agora oferece suporte para marcação de objetos. Ela permite classificar o armazenamento. Os prefixos de nome de chave de objeto também permitem classificar o armazenamento, mas a marcação de objetos adiciona outra dimensão a isso. Há benefícios adicionados oferecidos pela marcação. Dentre elas estão: • As tags de objeto permitem um controle de acesso rigoroso das permissões (por exemplo, você pode conceder permissões de usuário do IAM a objetos somente leitura com tags específicas). • Controle fino para especificar a configuração de ciclo de vida. Você pode especificar tags para selecionar um subconjunto de objetos aos quais a regra de ciclo de vida se aplica. • Se você tiver a replicação entre regiões (CRR) configura da, o Amazon S3 poderá replicar as tags. Você deve conceder a permissão necessária para a função do IAM criada para o Amazon S3 assumir que é preciso replicar objetos em seu nome. • Você também pode personalizar métricas do CloudWatc h e eventos do CloudTrail para exibir informações por filtros de tags específicos. Para obter mais informações, consulte Categorizar seu armazenamento usando tags.	29 de novembro de 2016

Alteração	Descrição	Data
Agora, o Amazon S3 Lifecycle oferece suporte a filtros baseados em etiquetas	Agora, o Amazon S3 oferece suporte para filtragem com base em tag na configuração de ciclo de vida. Você já pode especificar regras do ciclo de vida nas quais é possível determinar um prefixo de chave, uma ou mais tags de objeto ou uma combinação das duas para selecionar um subconjunto de objetos ao qual a regra do ciclo de vida se aplica. Para obter mais informações, consulte Gerenciar o ciclo de vida dos objetos.	29 de novembro de 2016
Métricas de solicitação do CloudWatch para buckets	O Amazon S3 agora oferece suporte a métricas do CloudWatch para solicitações feitas em buckets. Quando você habilita essas métricas para um bucket, elas são registradas em intervalos de 1 minuto. Você também pode configurar quais objetos em um bucket registrarão essas métricas de solicitação. Para obter mais informaçõ es, consulte Monitoramento de métricas com o Amazon CloudWatch.	29 de novembro de 2016
Inventário do Amazon S3	O Amazon S3 agora oferece suporte para inventário de armazenamento. O Amazon S3 Inventory fornece uma saída de arquivo sem formatação de seus objetos e dos metadados correspondentes diária ou semanalmente para um bucket do S3 ou um prefixo compartilhado (ou seja, objetos que têm nomes que começam com uma string comum). Para obter mais informações, consulte Catalogar e analisar seus dados com o Inventário S3.	29 de novembro de 2016

Alteração	Descrição	Data
Análise do Amazon S3: análise de classe de armazenamento	O novo recurso de análise de classe de armazenamento do Amazon S3 observa padrões de acesso de dados para ajudar você a determinar quando fazer a transição do armazenamento `STANDARD` acessado menos frequente mente para a classe de armazenamento `STANDARD_IA` IA significa “infrequent access”, inglês para “acesso com pouca frequência”). Depois que a análise de classe de armazenamento observa os padrões incomuns de acesso a um conjunto filtrado de dados em um período, você pode usar os resultados da análise para ajudar a a melhorar suas configurações de ciclo de vida. Esse recurso também inclui uma análise diária detalhada do uso de armazenam ento no nível de bucket, prefixo ou tag especificado que você pode exportar para um bucket do S3.	29 de novembro de 2016
Novas recuperações de dados expressas e em massa ao restaurar objetos arquivados no S3 Glacier	O Amazon S3 agora oferece suporte para recuperações de dados expressas e em massa, além de recuperações padrão ao restaurar objetos arquivados no S3 Glacier. Para obter mais informações, consulte Restaurar um objeto arquivado.	21 de novembro de 2016
Registro de objetos do CloudTrail	O CloudTrail oferece suporte ao registro em log de operações de API no nível do objeto do Amazon S3, como `GetObject` , `PutObject` e `DeleteObject` . Você pode configurar seletores de eventos para registrar operações de API no nível do objeto. Para obter mais informações, consulte Registrar chamadas de API do Amazon S3 em log usando AWS CloudTrail.	21 de novembro de 2016
US East (Ohio) Region	O Amazon S3 já está disponível na região Leste dos EUA (Ohio). Para obter mais informações sobre regiões e endpoints do Amazon S3, consulte Regiões e endpoints na Referência geral da AWS.	17 de outubro de 2016

Alteração	Descrição	Data
Suporte a IPv6 para o Amazon S3 Transfer Acceleration	O Amazon S3 agora oferece suporte ao Protocolo de Internet versão 6 (IPv6) para o Amazon S3 Transfer Acceleration. Você pode se conectar ao Amazon S3 por IPv6 usando o novo endpoint de pilha dupla para Transfer Acceleration. Para obter mais informações, consulte Conceitos básicos do Amazon S3 Transfer Acceleration.	6 de outubro de 2016
Suporte a IPv6	O Amazon S3 agora oferece suporte ao Protocolo de Internet versão 6 (IPv6). Você pode acessar o Amazon S3 por IPv6 usando endpoints de pilha dupla. Consulte mais informações em Making requests to Amazon S3 over IPv6 na Referência de API do Amazon S3.	11 de agosto de 2016
Asia Pacific (Mumbai) Region	O Amazon S3 já está disponível na região da Ásia-Pacífico (Mumbai). Para obter mais informações sobre regiões e endpoints do Amazon S3, consulte Regiões e endpoints na Referência geral da AWS.	27 de junho de 2016
Amazon S3 Transfer Acceleration	O Amazon S3 Transfer Acceleration possibilita transferências de arquivos rápidas, fáceis e seguras em longas distâncias entre o seu cliente e um bucket do S3. O Transfer Acceleration aproveita os locais da borda do Amazon CloudFront distribuídos globalmente. Para obter mais informações, consulte Configurar transferências de arquivos rápidas e seguras usando o Amazon S3 Transfer Acceleration.	19 de abril de 2016
Suporte de ciclo de vida para remover os marcadores de exclusão de objeto expirado	A ação `Expiration` de configuração do ciclo de vida agora permite que você instrua o Amazon S3 a remover os marcadores de exclusão de objeto expirado em um bucket com versionamento. Para obter mais informações, consulte Elementos para descrever ações de ciclo de vida.	16 de março de 2016

Alteração	Descrição	Data
A configuração de ciclo de vida de bucket agora oferece suporte para parar multipart uploads incompletos	A configuração de ciclo de vida de bucket agora oferece suporte para a ação `AbortIncompleteMultipartUpload`, que você pode usar para instruir o Amazon S3 a parar os multipart uploads não concluídos em um número específico de dias após serem iniciados. Quando um multipart upload torna-se qualificado para uma operação de interrupção, o Amazon S3 exclui todas as partes carregadas e para o multipart upload. Para obter informações conceituais, consulte os seguintes tópicos no Guia do usuário do Amazon S3: • Abortar um multipart upload • Elementos para descrever ações de ciclo de vida As seguintes operações de API foram atualizadas para oferecer suporte à nova ação: • Ciclo de vida de PUT Bucket: a configuração de XML agora permite que você especifique a ação `AbortIncompleteMultipartUpload` em uma regra de configuração de ciclo de vida. • Listar partes e Iniciar o multipart upload: essas duas operações de API agora retornarão dois cabeçalhos de resposta adicionais (`x-amz-abort-date` e `x-amz-abort-rule-id`) se o bucket tiver uma regra de ciclo de vida que especifique a ação `AbortIncompleteMultipartUpload`. Esses cabeçalhos de resposta indicam quando o multipart upload iniciado se tornará qualificado para a operação de interrupção e qual regra de ciclo de vida é aplicável.	16 de março de 2016

Alteração	Descrição	Data
Asia Pacific (Seoul) Region	O Amazon S3 já está disponível na região Ásia-Pacífico (Seul). Para obter mais informações sobre regiões e endpoints do Amazon S3, consulte Regiões e endpoints na Referência geral da AWS.	6 de janeiro de 2016
Nova chave de condição e uma alteração para carregamentos fracionados	As políticas do IAM agora oferecem suporte para a chave de condição `s3:x-amz-storage-class` do Amazon S3. Para obter mais informações, consulte Exemplos de políticas de bucket usando chaves de condição. Você não precisa mais ser o iniciador de um multipart upload para fazer upload de partes e terminar o upload. Para obter mais informações, consulte API de multipart upload e permissões.	14 de dezembro de 2015
Região Padrão dos EUA renomeada	A string de nome de região mudou de "Padrão dos EUA" para "Leste dos EUA (Norte da Virgínia)". Essa é só uma atualização de nome de região, não há nenhuma alteração na funcionalidade.	11 de dezembro de 2015

Alteração	Descrição	Data
Nova classe de armazenamento	O Amazon S3 agora oferece uma nova classe de armazenamento, STANDARD_IA (IA, para acesso raro), para armazenar objetos. Essa classe de armazenamento é otimizada para dados armazenados por longo tempo e acessados com menos frequência. Para obter mais informações, consulte Compreender e gerenciar classes de armazenamento do Amazon S3. As atualizações de recurso de configuração de ciclo de vida agora permitem fazer a transição de objetos para a classe de armazenamento STANDARD_IA. Para obter mais informações, consulte Gerenciar o ciclo de vida dos objetos. Anteriormente, o recurso de replicação entre regiões usava a classe de armazenamento do objeto de origem para réplicas de objeto. Agora, ao configurar a replicação entre regiões, você pode especificar uma classe de armazenam ento para a réplica de objeto criada no bucket de destino. Para obter mais informações, consulte Replicar objetos dentro de uma região e entre regiões.	16 de setembro de 2015
Integração do AWS CloudTrail	A nova integração do AWS CloudTrail permite que você registre a atividade da API do Amazon S3 no bucket do S3. Você pode usar o CloudTrail para acompanhar criações ou exclusões de buckets do S3, modificações de controle de acesso ou alterações de configuração de ciclo de vida. Para obter mais informações, consulte Registrar chamadas de API do Amazon S3 em log usando AWS CloudTrail.	1 de setembro de 2015

Alteração	Descrição	Data
Aumento do limite do bucket	O Amazon S3 agora oferece suporte para aumentos de limite de bucket. Por padrão, os clientes podem criar até 100 buckets na respectiva Conta da AWS. Os clientes que precisarem de buckets adicionais poderão aumentar esse limite enviando um aumento de limite de serviço. Para ter informações sobre como aumentar o limite do bucket, consulte Cotas do AWS service (Serviço da AWS) na Referência geral da AWS. Para obter mais informaçõ es, consulte Uso dos SDKs da AWS e Cotas, limitações e restrições de buckets de uso geral.	4 de agosto de 2015
Atualização do modelo de consistência	O Amazon S3 agora oferece suporte para consistência de leitura após gravação para novos objetos adicionad os ao Amazon S3 na região Leste dos EUA (Norte da Virgínia). Antes dessa atualização, todas as regiões menos a região Leste dos EUA (Norte da Virgínia) permitiam a consistência de leitura após gravação para novos objetos carregados no Amazon S3. Com esse aprimoramento, o Amazon S3 agora oferece suporte para consistência de leitura após gravação em todas as regiões para novos objetos adicionados ao Amazon S3. A consistência de leitura após gravação permite que você recupere objetos imediatamente após a criação no Amazon S3. Para obter mais informações, consulte Regiões.	4 de agosto de 2015
Notificações de eventos	As Notificações de Eventos do Amazon S3 foram atualizad as para adicionar notificações quando objetos são excluídos e para adicionar a filtragem em nomes de objeto com correspondência de prefixo e sufixo. Para obter mais informações, consulte Notificações de eventos do Amazon S3.	28 de julho de 2015

Alteração	Descrição	Data
Integração do Amazon CloudWatch	A nova integração do Amazon CloudWatch permite monitorar e definir alarmes de uso do Amazon S3 por meio de métricas do CloudWatch para o Amazon S3. As métricas compatíveis incluem total de bytes para armazenamento Standard, total de bytes para Reduced Redundancy Storage e número total de objetos para determinado bucket do S3. Para obter mais informaçõ es, consulte Monitoramento de métricas com o Amazon CloudWatch.	28 de julho de 2015
Suporte para excluir e esvaziar buckets não vazios	O Amazon S3 agora oferece suporte para excluir e esvaziar buckets não vazios. Para obter mais informações, consulte Esvaziar um bucket de uso geral.	16 de julho de 2015
Políticas de bucket para endpoints da Amazon VPC	O Amazon S3 adicionou suporte para políticas de bucket para VPC endpoints. Você pode usar políticas de bucket do S3 para controlar o acesso a buckets de VPC endpoints específicos ou VPCs específicas. Os VPC endpoints são fáceis de configurar, são extremamente confiáveis e fornecem uma conexão segura com o Amazon S3 sem exigir um gateway ou uma instância NAT. Para obter mais informações, consulte Controlar o acesso a partir de VPC endpoints com políticas de bucket.	29 de abril de 2015
Notificações de eventos	As Notificações de Eventos do Amazon S3 foram atualizad as para oferecer suporte à alternância para permissões com base em recursos para funções do AWS Lambda. Para obter mais informações, consulte Notificações de eventos do Amazon S3.	9 de abril de 2015
Replicação entre regiões	O Amazon S3 já oferece suporte à replicação entre regiões. A replicação entre regiões é a cópia assíncrona automática de objetos em buckets em diferentes Regiões da AWS. Para obter mais informações, consulte Replicar objetos dentro de uma região e entre regiões.	24 de março de 2015

Alteração	Descrição	Data
Notificações de eventos	O Amazon S3 agora oferece suporte para novos tipos e destinos de evento em uma configuração de notificação de bucket. Antes dessa versão, o Amazon S3 era compatível somente com o tipo de evento s3:ReducedRedundancyLostObject e um tópico do Amazon SNS como o destino. Para obter mais informações sobre os novos tipos de evento, consulte Notificações de eventos do Amazon S3.	13 de novembro de 2014
Criptografia do lado do servidor com chaves fornecidas pelo cliente	Criptografia no lado do servidor com chaves do AWS Key Management Service (AWS KMS) (SSE-KMS) O Amazon S3 agora oferece suporte para criptografia do lado do servidor usando o AWS KMS. Esse recurso permite que você gerencie a chave de envelope por meio do AWS KMS, e o Amazon S3 chama o AWS KMS para acessar a chave de envelope nas permissões definidas. Para obter mais informações sobre criptografia no lado do servidor com AWS KMS, consulte Proteção de dados usando criptografia no lado do servidor com o AWS Key Management Service.	12 de novembro de 2014
Europe (Frankfurt) Region	O Amazon S3 já está disponível na região Europa (Frankfurt).	23 de outubro de 2014

Alteração	Descrição	Data
Criptografia do lado do servidor com chaves fornecidas pelo cliente	O Amazon S3 agora oferece suporte para criptografia de servidor com chaves de criptografia fornecidas pelo cliente (SSE-C). A criptografia do lado do servidor permite que você solicite ao Amazon S3 para criptografar seus dados em repouso. Ao usar SSE-C, o Amazon S3 criptografa os objetos com chaves de criptografia personalizadas que você fornece. Como o Amazon S3 executa a criptografia, você obtém os benefícios de usar suas próprias chaves de criptografia sem o custo de gravação ou execução de seu próprio código de criptografia. Para obter mais informações sobre SSE-C, consulte Criptografia do servidor (com chaves de criptografia fornecidas pelo cliente).	12 de junho de 2014
Suporte de ciclo de vida para versionamento	Antes dessa versão, a configuração de ciclo de vida era permitida somente em buckets sem versões. Agora você pode configurar o ciclo de vida em buckets sem versões e com o versionamento ativado. Para obter mais informações, consulte Gerenciar o ciclo de vida dos objetos.	20 de maio de 2014
Tópicos de controle de acesso revisados	Documentação revisada de controle de acesso do Amazon S3. Para obter mais informações, consulte Gerenciamento de identidade e acesso para o Amazon S3.	15 de abril de 2014
Tópico de registro de acesso de servidor revisado	Documentação revisada de registro de acesso de servidor. Para obter mais informações, consulte Registrar em log as solicitações com registro em log de acesso ao servidor.	26 de novembro de 2013
Exemplos de SDK do .NET atualizados para a versão 2.0	Os exemplos de SDK do .NET neste guia agora são compatíveis com a versão 2.0.	26 de novembro de 2013

Alteração	Descrição	Data
Suporte a SOAP via HTTP descontinuado	O suporte de SOAP via HTTP está obsoleto, mas continua disponível via HTTPS. Novos recursos do Amazon S3 não serão compatíveis com o SOAP. Recomendamos usar a API REST ou os AWS SDKs.	20 de setembro de 2013
Suporte para variáveis de política do IAM	Agora, a linguagem de política do IAM oferece suporte a variáveis. Quando uma política é avaliada, todas as variáveis de política são substituídas por valores fornecidos por informações baseadas no contexto da sessão do usuário autenticado. Você pode usar variáveis de política para definir políticas de uso geral sem, explicitamente, listar todos os componentes da política. Para obter mais informações sobre variáveis de política, consulte Visão geral das variáveis de política do IAM no Guia do usuário do IAM. Para obter exemplos de variáveis de políticas no Amazon S3, consulte Exemplos de políticas baseadas em identidade para o Amazon S3.	3 de abril de 2013
Suporte do console para Pagamento pelo solicitante	Agora você pode configurar seu bucket para pagamentos pelo solicitante usando o console do Amazon S3. Para obter mais informações, consulte Utilizar buckets de uso geral com pagamento pelo solicitante para transferência e uso de armazenamento.	31 de dezembro de 2012

Alteração	Descrição	Data
Suporte de domínio raiz para hospedagem de sites	O Amazon S3 agora oferece suporte a hospedagem de sites estáticos no domínio raiz. Os visitantes podem acessar seu site do navegador sem especificar www no endereço da Web (por exemplo, eles podem usar example.com em vez de www.example.com). Muitos clientes já hospedam sites estáticos no Amazon S3 que podem ser acessados de um subdomínio www (por exemplo, www.example.com). Anteriormente, para oferecer suporte para acesso de domínio raiz, você precisava executar seu próprio servidor da web para as solicitações de domínio raiz de proxy de navegadores para seu site no Amazon S3. Executar um servidor da web para solicitações de proxy introduz custos adicionais, carga operacional e outro ponto de falha em potencial. Agora, você pode aproveitar a alta disponibilidade e a durabilidade do Amazon S3 para endereços www e de domínio raiz. Para obter mais informações, consulte Hospedagem de um site estático usando o Amazon S3.	27 de dezembro de 2012
Revisão do console	O console do Amazon S3 foi atualizado. Os tópicos de documentação que se referem ao console foram revisados conforme necessário.	14 de dezembro de 2012

Alteração	Descrição	Data
Suporte para arquivamento de dados no S3 Glacier	Agora, o Amazon S3 oferece suporte a uma opção de armazenamento que permite utilizar o serviço de armazenamento de baixo custo do S3 Glacier para arquivamento de dados. Para arquivar objetos, defina regras de arquivamento identificando objetos e um cronograma quando deseja que o Amazon S3 arquive esses objetos no S3 Glacier. Você pode definir regras facilmente em um bucket usando o console do Amazon S3 ou usando programaticamente a API do Amazon S3 ou AWS SDKs. Para obter mais informações, consulte Gerenciar o ciclo de vida dos objetos.	13 de novembro de 2012
Suporte para redirecionamentos de página de site	Para um bucket que é configurado como um site, o Amazon S3 agora oferece suporte ao redirecionamento de uma solicitação de um objeto para outro objeto no mesmo bucket ou um URL externo. Para obter mais informações, consulte (Opcional) Configurar um redirecionamento de uma página da Web. Para obter informações sobre a hospedagem de sites, consulte Hospedagem de um site estático usando o Amazon S3.	4 de outubro de 2012
Suporte para compartilhamento de recursos de origem cruzada (CORS)	O Amazon S3 oferece suporte para compartilhamento de recursos de origem cruzada (CORS). O CORS define uma maneira de os aplicativos web clientes carregados em um domínio poderem interagir com ou acessar recursos em outro domínio. Com suporte a CORS no Amazon S3, você pode criar aplicações Web cliente avançados no Amazon S3 e permitir seletivamente o acesso de domínio cruzado aos recursos do Amazon S3. Para obter mais informações, consulte Usar o compartilhamento de recursos de origem cruzada (CORS).	31 de agosto de 2012

Alteração	Descrição	Data
Suporte para tags de alocação de custos	O Amazon S3 agora oferece suporte para tags de alocação de custos, o que permite identificar buckets do S3 para facilitar o acompanhamento de custos de projetos ou outros critérios. Para obter mais informações sobre o uso de tags para buckets, consulte Usar tags de alocação de custos para buckets do S3.	21 de agosto de 2012
Suporte para acesso à API protegido por MFA nas políticas de bucket	O Amazon S3 agora oferece suporte para acesso à API protegido por MFA, um recurso que pode impor a AWS Multi-Factor Authentication para um nível de segurança extra ao acessar os recursos do Amazon S3. É um recurso de segurança que exige que os usuários comprovem a posse física de um dispositivo MFA fornecendo um código válido de MFA. Para obter mais informações, consulte AWS Multi-Factor Authentication. Agora você pode exigir a autenticação de MFA para todas as solicitações de acesso aos recursos do Amazon S3. Para aplicar a autenticação de MFA, o Amazon S3 agora oferece suporte para a chave `aws:MultiFactorAuthAge` em uma política de bucket. Para ver um exemplo de política de bucket, consulte Exigir MFA.	10 de julho de 2012
Suporte para expiração de objeto	Você pode usar a expiração de objeto para programar a remoção automática de dados após um período configurado. Para definir a expiração de objeto, adicione a configuração de ciclo de vida a um bucket.	27 de dezembro de 2011
Nova região compatível	O Amazon S3 agora oferece suporte à região da América do Sul (São Paulo). Para obter mais informações, consulte Acessar um bucket de uso geral do Amazon S3.	14 de dezembro de 2011

Alteração	Descrição	Data
Exclusão de vários objetos	O Amazon S3 agora oferece suporte para a API de exclusão de vários objetos que permite excluir vários objetos em uma única solicitação. Com esse recurso, você pode remover um grande número de objetos do Amazon S3 mais rapidamente do que usando várias solicitaç ões DELETE individuais. Para obter mais informações, consulte Excluir objetos do Amazon S3.	7 de dezembro de 2011
Nova região compatível	O Amazon S3 agora oferece suporte à região do Oeste dos EUA (Oregon). Para obter mais informações, consulte Buckets e regiões.	8 de novembro de 2011
Atualização da documentação	Correções de erros de documentação.	8 de novembro de 2011
Atualização da documentação	Além de correções de erros de documentação, esta versão inclui os seguintes aprimoramentos: • Novas seções de criptografia do lado do servidor usando o AWS SDK para PHP e o AWS SDK para Ruby (consulte Especificar a criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3)).	17 de outubro de 2011

Alteração	Descrição	Data
Suporte para criptografia do lado do servidor	O Amazon S3 agora oferece suporte para criptografia do lado do servidor. Ela permite solicitar ao Amazon S3 para criptografar seus dados em repouso, ou seja, criptografar seus dados de objeto quando o Amazon S3 grava seus dados em discos nos datacenters. Além das atualizações de API REST, o AWS SDK para Java e o .NET oferecem a funcionalidade necessária para solicitar criptografia do lado do servidor. Você também pode solicitar a criptografia de servidor ao fazer upload de objetos usando o Console de Gerenciamento da AWS Management Console. Para saber mais sobre a criptografia de dados, acesse Usar criptografia de dados.	4 de outubro de 2011
Atualização da documentação	Além de correções de erros de documentação, esta versão inclui os seguintes aprimoramentos: • Amostras de Ruby e PHP adicionadas à seção Making requests na Referência de API do Amazon S3. • Adição de seções que descrevem como gerar e usar pre-signed URLs. Para obter mais informações, consulte Compartilhar objetos com URLs pré-assinados e Compartilhar objetos com URLs pré-assinados. • Atualização de uma seção existente para apresentar o AWS Explorer para Eclipse e Visual Studio. Consulte mais informações em Developing with Amazon S3 using the AWS SDKs na Referência de API do Amazon S3.	22 de setembro de 2011

Alteração	Descrição	Data
Suporte para enviar solicitações usando credenciais de segurança temporárias	Além de usar suas credenciais de segurança de Conta da AWS e de usuário do IAM para enviar solicitações autenticadas ao Amazon S3, agora você pode enviar solicitações usando credenciais de segurança temporárias obtidas no AWS Identity and Access Management (IAM). Você pode usar a API do AWS Security Token Service ou bibliotecas de wrapper de AWS SDK para solicitar essas credenciais temporárias no IAM. Você pode solicitar essas credenciais de segurança temporárias para seu próprio uso ou para enviá-las para usuários federados e aplicativos. Esse recurso permite que você gerencie usuários fora da AWS e forneça a eles as credenciais de segurança temporárias para acessar os recursos da AWS. Consulte mais informações em Making requests na Referência da API do Amazon S3. Para obter mais informações sobre o suporte do IAM para credenciais de segurança temporárias, consulte Credenciais de segurança temporárias no Guia do usuário do IAM.	3 de agosto de 2011
API de multipart upload estendida para permitir a cópia de objetos de até 5 TB	Antes dessa versão, a API do Amazon S3 permitia a cópia de objetos de até 5 GB. Para permitir a cópia de objetos com mais de 5 GB, o Amazon S3 agora estende a API de multipart upload com uma nova operação, `Upload Part (Copy)`. Você pode usar essa operação do multipart upload para copiar objetos com até 5 TB. Para obter mais informações, consulte Copiar, mover e renomear objetos. Para obter informações conceituais sobre a API do multipart upload, consulte Carregar e copiar objetos usando upload fracionado no Amazon S3.	21 de junho de 2011

Alteração	Descrição	Data
Chamadas de API SOAP via HTTP desativadas	Para aumentar a segurança, as chamadas de API SOAP via HTTP são desativadas. As solicitações SOAP autenticadas e anônimas devem ser enviadas para o Amazon S3 usando SSL.	6 de junho de 2011
O IAM habilita a delegação entre contas	Anteriormente, para acessar um recurso do Amazon S3, um usuário do IAM precisava de permissões da Conta da AWS pai e do proprietário do recurso do Amazon S3. Com o acesso entre contas, o usuário do IAM agora só precisa da permissão da conta do proprietário. Ou seja, se o proprietário de um recurso conceder acesso a uma Conta da AWS, a Conta da AWS agora poderá conceder aos usuários do IAM acesso a esses recursos. Para ter mais informações, consulte Criar um perfil para delegar permissões a um usuário do IAM no Guia do usuário do IAM. Para obter mais informações sobre como especificar principais em uma política de bucket, consulte Entidades principais para políticas de bucket.	6 de junho de 2011
Novo link	As informações de endpoint deste serviço agora estão localizadas na Referência geral da AWS. Para ter mais informações, consulte Regiões e endpoints na Referência geral da AWS.	1 de março de 2011

Alteração	Descrição	Data
Suporte para a hospedagem de sites estáticos no Amazon S3	O Amazon S3 introduz o suporte aprimorado para hospedagem de sites estáticos. Isso inclui suporte para documentos de índice e documentos de erros personalizados. Ao usar esses recursos, as solicitações para a raiz de seu bucket ou uma subpasta (por exemplo, `http://mywebsite.com/subfolder`) retornam o documento de índice em vez da lista de objetos em seu bucket. Se um erro for encontrado, o Amazon S3 retornará sua mensagem de erro personalizada em vez de uma mensagem de erro do Amazon S3. Para obter mais informações, consulte Hospedagem de um site estático usando o Amazon S3.	6 de junho de 2011
As informações de endpoint deste serviço agora estão localizadas na Referência geral da AWS. Para ter mais informações, consulte Regiões e endpoints na Referência geral da AWS.	1 de março de 2011	

Alteração	Descrição	Data
Suporte para a hospedagem de sites estáticos no Amazon S3	O Amazon S3 introduz o suporte aprimorado para hospedagem de sites estáticos. Isso inclui suporte para documentos de índice e documentos de erros personalizados. Ao usar esses recursos, as solicitações para a raiz de seu bucket ou uma subpasta (por exemplo, `http://mywebsite.com/subfolder`) retornam o documento de índice em vez da lista de objetos em seu bucket. Se um erro for encontrado, o Amazon S3 retornará sua mensagem de erro personalizada em vez de uma mensagem de erro do Amazon S3. Para obter mais informações, consulte Hospedagem de um site estático usando o Amazon S3.	17 de fevereiro de 2011
Suporte para API do cabeçalho de resposta	A API REST do objeto GET agora permite alterar os cabeçalhos de resposta da solicitação REST do objeto GET para cada solicitação. Isto é, você pode alterar metadados de objeto na resposta, sem modificar o objeto em si. Para obter mais informações, consulte Baixar objetos.	14 de janeiro de 2011
Suporte para objetos grandes	O Amazon S3 aumentou o tamanho máximo de um objeto que você pode armazenar em um bucket do S3 de 5 GB para 5 TB. Se estiver usando a API REST, você poderá fazer upload de objetos de até 5 GB em uma única operação PUT. Para objetos maiores, você deve usar a API REST do multipart upload para fazer upload de objetos em partes. Para obter mais informações, consulte Carregar e copiar objetos usando upload fracionado no Amazon S3.	9 de dezembro de 2010
Multipart upload	O multipart upload permite fazer uploads mais flexíveis mais rapidamente no Amazon S3. Ele permite carregar um único objeto como um conjunto de partes. Para obter mais informações, consulte Carregar e copiar objetos usando upload fracionado no Amazon S3.	10 de novembro de 2010

Alteração	Descrição	Data
Suporte de ID canônico em políticas de bucket	Agora você pode especificar IDs canônicos em políticas de bucket. Para obter mais informações, consulte Entidades principais para políticas de bucket.	17 de setembro de 2010
O Amazon S3 funciona com o IAM	Esse serviço agora é integrado ao AWS Identity and Access Management (IAM). Para ter mais informações, acesse Serviços da AWS que funcionam com o IAM no Guia do usuário do IAM.	2 de setembro de 2010
Notificações	O recurso de notificações do Amazon S3 permite configura r um bucket para que o Amazon S3 publique uma mensagem em um tópico do Amazon Simple Notification Service (Amazon SNS) quando o Amazon S3 detecta um evento-chave em um bucket. Para obter mais informaçõ es, consulte Configuração de notificação de eventos de bucket.	14 de julho de 2010
Políticas de buckets	As políticas de bucket são um sistema de gerenciamento de acesso usado para definir permissões de acesso em buckets, objetos e conjuntos de objetos. Essa funcional idade suplementa e, em muitos casos, substitui as listas de controle de acesso. Para obter mais informações, consulte Políticas de bucket para o Amazon S3.	6 de julho de 2010
Sintaxe de estilo de caminho disponível em todas as regiões	O Amazon S3 agora oferece suporte para a sintaxe de caminho para qualquer bucket na região clássica dos EUA ou se o bucket estiver na mesma região do endpoint da solicitação. Para obter mais informações, consulte Hospedagem virtual.	9 de junho de 2010
Novo endpoint para a Europa (Irlanda)	O Amazon S3 agora fornece um endpoint para a Europa (Irlanda): `http://s3-eu-west-1.amazonaws.com` .	9 de junho de 2010

Alteração	Descrição	Data
Console	Agora você pode usar o Amazon S3 por meio do AWS Management Console. Você pode ler sobre toda a funcionalidade do Amazon S3 no console no Manual do usuário do Amazon Simple Storage Service.	9 de junho de 2010
Redundância reduzida	O Amazon S3 agora permite reduzir seus custos de armazenamento armazenando objetos no Amazon S3 com redundância reduzida. Para obter mais informações, consulte Reduced Redundancy Storage (RRS).	12 de maio de 2010
Nova região compatível	O Amazon S3 agora oferece suporte à região Ásia-Pací fico (Cingapura). Para obter mais informações, consulte Buckets e regiões.	28 de abril de 2010
Versionamento de objeto	Essa versão apresenta o versionamento de objeto. Todos os objetos agora podem ter uma chave e uma versão. Se você habilitar o versionamento para um bucket, o Amazon S3 fornecerá a todos os objetos adicionados a um bucket um ID exclusivo de versão. Esse recurso permite que você se recupere de substituições e exclusões indesejadas. Para obter mais informações, consulte Versionamento e Usar versionamento.	8 de fevereiro de 2010
Nova região compatível	O Amazon S3 agora oferece suporte à região Oeste dos EUA (Norte da Califórnia). O novo endpoint para solicitações para essa região é `s3-us-west-1.amazonaws.com` . Para obter mais informações, consulte Buckets e regiões.	2 de dezembro de 2009

Alteração	Descrição	Data
AWS SDK para .NET	A AWS agora fornece bibliotecas, códigos de exemplo, tutoriais e outros recursos para os desenvolvedores de software que preferem criar aplicativos usando operações de API específicas da linguagem .NET em vez de REST ou SOAP. Essas bibliotecas oferecem as funções básicas (não incluídas nas APIs REST ou SOAP), como autenticação de solicitação, novas tentativas de solicitação e processamento de erros, para que você possa começar a usar com mais facilidade. Consulte mais informações sobre recursos e bibliotecas de linguagem específica em Developing with Amazon S3 using the AWS SDKs na Referência de API do Amazon S3.	11 de novembro de 2009