Amazon Simple Storage Service

Guia de conceitos básicos

Amazon Simple Storage Service: Guia de conceitos básicos

Table of Contents

Conceitos básicos do Amazon Simple Storage Service

O Amazon Simple Storage Service (Amazon S3) é uma solução de armazenamento para a internet. Você pode utilizar o Amazon S3 para armazenar e recuperar qualquer volume de dados, a qualquer momento, de qualquer lugar na web. Você pode realizar essas tarefas usando o Console de gerenciamento da AWS, que é uma interface web simples e intuitiva.

O Amazon S3 armazena dados como objetos dentro de buckets. Um objeto é um arquivo e todos os metadados opcionais que descrevem o arquivo. Para armazenar um arquivo no Amazon S3, faça upload dele em um bucket. Ao fazer upload de um arquivo, é possível definir permissões no objeto e em todos os metadados.

Buckets são contêineres para objetos. Você pode ter um ou mais buckets. É possível controlar o acesso a cada bucket, decidindo quem pode criar, excluir e listar objetos nele. Também é possível escolher a região geográfica em que o Amazon S3 armazenará o bucket e seu conteúdo e visualizar os logs de acesso do bucket e seus objetos.

Este guia apresenta o Amazon S3 e explica como usar o Console de gerenciamento da AWS para executar as tarefas a seguir:

Para obter informações sobre os recursos, a definição de preços e as perguntas frequentes do Amazon S3, consulte a página de produto do Amazon S3.

Configurar o Amazon S3

Ao se cadastrar 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 informações sobre recursos e definição de preços do Amazon S3, consulte Amazon S3. Se você for um cliente novo do Amazon S3, poderá começar a usar Amazon S3 gratuitamente. Para obter mais informações, consulte Nível gratuito da AWS.

Para começar a o usar Amazon S3, siga estas etapas:

Tópicos

Cadastre-se no AWS

Se você ainda não tiver uma conta da AWS, use o procedimento a seguir para criar uma.

Para cadastrar-se na AWS

1. Abra https://aws.amazon.com/ e escolha Create an AWS Account.
2. Siga as instruções online.

A AWS envia um e-mail de confirmação depois que o processo de cadastramento é concluído. A qualquer momento, é possível visualizar suas atividades da conta atual e gerenciar sua conta acessando https://aws.amazon.com/ e selecionando My Account (Minha conta).

Criar um usuário do IAM

Ao criar uma conta da Amazon Web Services (AWS) pela primeira vez, comece com uma identidade de logon único. Essa identidade tem acesso completo a todos os serviços e recursos da AWS da conta. Essa identidade é chamada conta da AWS usuário raiz. Ao fazer login, insira o endereço de e-mail e a senha usados para criar a conta.

> **Important**
>
> Recomendamos que não use o usuário raiz para suas tarefas diárias, nem mesmo as administrativas. Em vez disso, siga as melhores práticas de uso do usuário raiz somente para criar seu primeiro usuário do IAM. Depois, armazene as credenciais usuário raiz com segurança e use-as para executar apenas algumas tarefas de gerenciamento de contas e de serviços. Para visualizar as tarefas que exigem que você faça login como usuário raiz, consulte Tarefas da AWS que exigem usuário raiz

Se você se inscreveu na AWS, mas não criou um usuário do IAM próprio, siga estas etapas.

Para criar um usuário administrador para você mesmo e adicionar o usuário a um grupo de administradores (console)

1. Entre no console do IAM como o proprietário da conta escolhendo usuário raiz e inserindo o endereço de e-mail de sua da conta AWS. Na próxima página, insira sua senha.

Note

Recomendamos que você siga as melhores práticas para utilizar o usuário do **`Administrator`** IAM abaixo e armazene as credenciais do usuário raiz com segurança. Cadastre-se como usuário raiz para executar somente algumas tarefas de gerenciamento de serviços e contas.

2. No painel de navegação, escolha Usuários e depois Adicionar usuário.
3. Em User name (Nome do usuário), digite **`Administrator`**.
4. Marque a caixa de seleção ao lado de Console de gerenciamento da AWS access (Acesso ao &console;). Então, selecione Custom password (Senha personalizada), e insira sua nova senha na caixa de texto.
5. (Opcional) Por padrão, a AWS exige que o novo usuário crie uma senha ao fazer login pela primeira vez. Você pode desmarcar a caixa de seleção próxima de User must create a new password at next sign-in (O usuário deve criar uma senha no próximo login) para permitir que o novo usuário redefina a senha depois de fazer login.
6. Escolha Próximo: Permissões.
7. Em Set permissions (Conceder permissões), escolha Add user to group (Adicionar usuário ao grupo).
8. Escolha Create group (Criar grupo).
9. Na caixa de diálogo Create group (Criar grupo), em Group name (Nome do grupo), digite **`Administrators`**.
10. Escolha Filter policies (Filtrar políticas) e, depois, selecione AWS managed -job function (Função de trabalho gerenciado pela &AWS;) para filtrar o conteúdo de tabelas.
11. Na lista de políticas, marque a caixa de seleção AdministratorAccess. A seguir escolha Criar grupo.

    Note

    Você deve ativar o acesso de usuário e função do IAM ao faturamento para poder usar as permissões do `AdministratorAccess` a fim de acessar o console do AWS Billing and Cost Management. Para fazer isso, siga as instruções na etapa 1 do tutorial sobre como delegar acesso ao console de faturamento.
12. Suporte a lista de grupos, selecione a caixa de seleção para seu novo grupo. Escolha Refresh (Atualizar) caso necessário, para ver o grupo na lista.
13. Escolha Next: Tags (Próximo: tags).
14. (Opcional) Adicione metadados ao usuário anexando tags como pares de chave-valor. Para obter mais informações sobre como usar tags no IAM, consulte Marcar entidades do IAM no Guia do usuário do IAM.
15. Escolha Next: Review (Próximo: Análise) para ver uma lista de associações de grupos a serem adicionadas ao novo usuário. Quando você estiver pronto para continuar, selecione Criar usuário.

Você pode usar esse mesmo processo para criar mais grupos e usuários e conceder aos seus usuários acesso aos recursos de sua conta da AWS. Para saber como usar políticas para restringir as permissões de usuário a recursos específicos da AWS, acesse Gerenciamento de acesso e Políticas de exemplo.

Faça login como usuário do IAM

Depois de criar um usuário do IAM, você pode fazer login na AWS com seu nome de usuário e senha do IAM.

Antes de fazer login como usuário do IAM, você pode verificar o link de login para usuários do IAM no console do IAM. No dashboard do IAM, no link de login de usuários do IAM, você pode ver o link de login da sua conta da AWS. O URL do link de login contém o ID da sua conta da AWS sem traços (-).

Se você não quiser que o URL do link de login contenha o ID da sua conta da AWS, crie um alias da conta. Para obter mais informações, consulte Criar, excluir e listar, e alias de conta da AWS no Guia do usuário do IAM.

Faça login como usuário da AWS.

1. Saia do Console de gerenciamento da AWS.
2. Insira link de login.

   Seu link de login inclui seu ID de conta da AWS (sem traços) ou seu alias de conta da AWS:

   ```
   https://aws_account_id_or_alias.signin.aws.amazon.com/console
   ```

3. Insira o nome e a senha de usuário do IAM que você acabou de criar.

   Quando você está conectado, a barra de navegação exibe "your_user_name @ your_aws_account_id".

Criação de um bucket

Agora que se cadastrou no AWS, você está pronto para criar um bucket usando o Console de gerenciamento da AWS. Cada objeto no Amazon S3 é armazenado em um bucket. Antes de você poder armazenar dados no Amazon S3, você deverá 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 cobranças de armazenamento, consulte Definição de preço do Amazon S3.

Para criar um bucket usando o AWS Command Line Interface, consulte create-bucket no AWS CLI Command Reference.

Para criar um bucket

1. Faça login no Console de gerenciamento da AWS e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Selecione Create bucket (Criar bucket).

   A página Create bucket (Criar bucket) é aberta.
3. Em Bucket name (Nome do bucket), insira um nome compatível com o DNS para seu bucket.

   O nome do bucket deve:

   - Ser exclusivo em todo o Amazon S3.
   - Ter entre 3 e 63 caracteres.
   - Não contém caracteres maiúsculos.
   - Começar com uma letra minúscula ou um número.

   Depois de criado o bucket, você não pode mudar seu nome. Para obter informações sobre a nomenclatura de buckets, consulte Regras para nomeação de buckets no Guia do desenvolvedor do Amazon Simple Storage Service.

   > **Important**
   >
   > Evite incluir 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.
4. Em Region (Região), escolha a região da AWS onde deseja que o bucket resida.

   Escolha uma região próxima de você para minimizar a latência e os custos e atender aos requisitos regulatórios. 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 no Referência geral do Amazon Web Services.
5. Em Bucket settings for Block Public Access (Configurações de bucket para bloquear acesso público), mantenha os valores predefinidos.

   Por padrão, o Amazon S3 bloqueia todo o acesso público ao bucket. Recomendamos deixar todas as configurações de Bloquear acesso público habilitadas. Para obter mais informações sobre o bloqueio de acesso público, consulte Uso do bloqueio de acesso público do Amazon S3 no Guia do desenvolvedor do Amazon Simple Storage Service.

6. Selecione Create bucket (Criar bucket).

Você criou um bucket no Amazon S3.

Para adicionar um objeto ao bucket, consulte Fazer upload de um objeto em um bucket (p. 7).

Fazer upload de um objeto em um bucket

Agora que você criou um bucket, você está pronto para fazer o upload de um objeto nele. 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. Na lista Bucket, escolha o nome do bucket no qual você deseja fazer upload do objeto.
2. Na guia Overview (Visão geral) do bucket, escolha Upload ou Get Started (Conceitos básicos).
3. Para escolher o arquivo para upload, na caixa de diálogo Upload (Fazer upload), escolha Add files (Adicionar arquivos) para escolher o arquivo a ser carregado.
4. Escolha um arquivo para carregar e, em seguida, escolha Open (Abrir).
5. Escolha Upload (Fazer upload).

O upload de um objeto no bucket foi realizado corretamente.

Para visualizar o objeto, consulte Acessar um objeto (p. 8).

Acessar um objeto

Agora que você fez o upload de um objeto em um bucket, pode visualizar informações sobre o objeto e fazer download do objeto em seu computador local.

Para fazer download de um objeto em um bucket

1. Na lista Buckets, escolha o nome do bucket que você criou.
2. Na lista Name (Nome), escolha o nome do objeto que você deseja bloquear.

   Para o objeto selecionado, o painel de visão geral do objeto é aberto.
3. Na guia Overview (Visão geral) revise as informações sobre seu objeto.
4. Para exibir o objeto em seu navegador, escolha Open (Abrir). Alguns tipos de objetos não podem ser visualizados no navegador. Nesse caso, será feito download do objeto no computador.
5. Para baixar o objeto em seu computador, escolha Download.

Você baixou seu objeto com êxito.

Para copiar e colar seu objeto no Amazon S3, consulte Copiar um objeto em uma pasta (p. 9).

Copiar um objeto em uma pasta

Você já adicionou um objeto a um bucket e fez download do objeto. Neste tutorial, uma pasta é criada e seu objeto é copiado nela.

Como copiar um objeto em uma pasta

1. Na lista Buckets, escolha o nome do bucket.
2. Selecione Create folder (Criar pasta) e configure a pasta:
   a. Insira um nome para a pasta (por exemplo, `favorite-pics`).
   b. Para a configuração de criptografia de pasta, selecione None (Nenhum).
   c. Escolha Save (Salvar).
3. Na guia Overview (Visão geral), marque a caixa de seleção ao lado do objeto que deseja copiar.
4. Escolha Ações e selecione Copiar.
5. Escolha a pasta de destino e selecione Choose (Selecionar).
6. Em Revisar, confirme os detalhes da cópia e escolha Copiar.

   O Amazon S3 copia o objeto na pasta de destino.
7. Para visualizar o objeto copiado na pasta de destino, selecione o nome da pasta. Na guia Overview (Visão geral) você verá o objeto copiado.

Para excluir um objeto e um bucket no Amazon S3, consulte Excluir objetos e buckets (p. 10).

Excluir objetos e buckets

Quando você não precisar mais de um objeto ou bucket, recomendamos excluí-los para evitar cobranças adicionais. Se você concluiu esse exemplo de demonstração como um exercício de aprendizagem e não planeja usar seu bucket ou objetos, recomendamos que excluir seu bucket para não acumular cobranças. Antes de excluir seu bucket, você precisa esvaziá-lo ou excluir objetos do bucket. 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 pode criar um bucket com o mesmo nome antes de você ter a chance de reutilizá-lo.

Tópicos

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), insira o nome do 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.
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 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. Na lista Name (Nome), marque a caixa de seleção do objeto que deseja excluir.
3. Escolha Actions (Ações) e escolha Delete (Excluir).
4. Na caixa de diálogo Delete objects (Excluir objetos), verifique o nome do objeto e selecione Delete (Excluir).

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 Delete (Excluir).
3. Para confirmar a exclusão, insira 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).

Para obter mais informações sobre como usar o Amazon S3, consulte Para onde ir agora? (p. 12)

Para onde ir agora?

Nos exemplos anteriores, você aprendeu a executar algumas tarefas básicas no Amazon S3. Para obter informações mais detalhadas, consulte um dos seguintes guias do Amazon S3:

- O Guia do usuário do console do Amazon Simple Storage Service para saber mais sobre como usar o console do Amazon S3.
- O Guia do desenvolvedor do Amazon Simple Storage Service para localizar informações detalhadas sobre os recursos do Amazon S3 e os exemplos de código para oferecer suporte a esses recursos.
- O Amazon Simple Storage Service API Reference para localizar detalhes sobre a API REST do Amazon S3.

Os seguintes tópicos explicam várias maneiras com as quais você obtém um entendimento mais profundo do Amazon S3 para que você possa implementá-lo em seus aplicativos.

Tópicos

Cenários de uso comuns

O site Soluções da AWS lista várias formas de utilização do Amazon S3. A lista a seguir resume algumas dessas maneiras.

- Backup e armazenamento – forneça backup de dados e serviços de armazenamento para outros.
- Hospedagem de aplicativos – forneça serviços para implantação, instalação e gerenciamento de aplicativos web.
- Hospedagem de mídia – crie uma infraestrutura redundante, dimensionável e altamente disponível para hospedar carregamentos e downloads de vídeos, fotos ou músicas.
- Entrega de software – hospede seus aplicativos de software para download pelos clientes.

Para obter informações, consulte Soluções da AWS.

Considerações daqui para frente

Esta seção apresenta tópicos que você deve considerar antes de executar seu próprio produto do Amazon S3.

Tópicos

Conta e credenciais de segurança da AWS

Quando se inscreveu no serviço, você criou uma conta da AWS usando um endereço de e-mail e uma senha. Estes são as suas credenciais de Usuário raiz da conta da AWS. Como prática recomendada, você não deve usar as credenciais de usuário raiz para acessar a AWS. Nem deve dar as credenciais para mais ninguém. Em vez disso, crie usuários individuais para quem precisar acessar sua conta da AWS. Primeiro crie um usuário administrador do AWS Identity and Access Management (IAM) para você e para seu trabalho diário. Para obter mais detalhes, consulte Criação do seu primeiro grupo e usuário administrador do IAM no Guia do usuário do IAM. A seguir, crie usuários de IAM adicionais para outras pessoas. Para obter mais detalhes, consulte Criação do seu primeiro grupo e usuário delegados doIAM no Guia do usuário do IAM.

Se você for o proprietário ou administrador da conta e quiser saber mais sobre o IAM, consulte a descrição do produto em https://aws.amazon.com/iam ou a documentação técnica no Guia do usuário do IAM.

Segurança

O Amazon S3 fornece mecanismos de autenticação para proteger os dados armazenados no Amazon S3 contra acesso não autorizado. A menos que você especifique o contrário, apenas o proprietário da conta AWS pode acessar dados carregados para o Amazon S3. Para obter mais informações sobre como gerenciar o acesso a buckets e objetos, acesse Identity and Access Management no Amazon S3 no Guia do desenvolvedor do Amazon Simple Storage Service.

No entanto, você pode criptografar seus dados antes de enviá-los para o Amazon S3.

Integração com a AWS

Você pode utilizar o Amazon S3 sozinho ou em conjunto com um ou mais outros produtos da Amazon. Veja a seguir os produtos mais comuns usados com Amazon S3:

- Amazon EC2
- Amazon EMR
- Amazon SQS
- Amazon CloudFront

Definição de preço

Conheça a estrutura de preços para armazenar e transferir dados no Amazon S3. Para obter mais informações, consulte Definição de preço do Amazon S3.

Recursos avançados do Amazon S3

Os exemplos neste guia mostram como realizar tarefas básicas como criação de um bucket, carregamento e download de dados para o bucket e movimentação e exclusão dos dados. A tabela a seguir

resume algumas das funcionalidades avançadas mais comuns oferecidas pelo Amazon S3. Algumas funcionalidades avançadas não estão disponíveis no Console de gerenciamento da AWS e requerem o uso da API do Amazon S3. Todas as funcionalidades avançadas e a forma de usá-las estão descritas no Guia do desenvolvedor do Amazon Simple Storage Service.

Link	Funcionalidade
Buckets de Pagamento pelo solicitante	Aprenda a configurar um bucket para que um cliente pague pelos downloads que ele realizar.
Usar o BitTorrent com o Amazon S3.	Use o BitTorrent, que é um protocolo aberto e peer-to-peer para distribuição de arquivos.
Versionamento	Saiba mais sobre os recursos de versionamento do Amazon S3.
Hospedar websites estáticos	Saiba como hospedar um website estático no Amazon S3.
Gerenciamento do ciclo de vida de objetos	Saiba como gerenciar o ciclo de vida de objetos no seu bucket. O gerenciamento do ciclo de vida inclui o vencimento e o arquivamento de objetos (mudança dos objetos para a classe de armazenamento do `S3 S3 Glacier`).

Melhores práticas de controle de acesso

O Amazon S3 fornece uma variedade de recursos e ferramentas de segurança. Os cenários a seguir devem servir como um guia para quais ferramentas e configurações você pode querer usar ao executar determinadas tarefas ou operar em ambientes específicos. A aplicação adequada dessas ferramentas pode ajudar a manter a integridade dos dados e ajudar a garantir que os recursos sejam acessíveis aos usuários pretendidos.

Tópicos

Criar um bucket

Ao criar um bucket, é necessário aplicar as seguintes ferramentas e configurações para ajudar a garantir que os recursos do Amazon S3 estejam protegidos.

Block Public Access

O S3 Block Public Access fornece quatro configurações para ajudar a evitar expor inadvertidamente seus recursos do S3. É possível aplicar essas configurações em qualquer combinação a pontos de acesso individuais, a buckets ou a 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. Por padrão, a configuração Block all public access (Bloquear todo o acesso público) é aplicada a novos buckets criados no console do Amazon S3.

Para obter mais informações, consulte O significado de "público" no Guia do desenvolvedor do Amazon Simple Storage Service.

Se as configurações do S3 Block Public Access forem muito restritivas, você poderá usar identidades do AWS Identity and Access Management (IAM) para conceder acesso a usuários específicos em vez de desabilitar todas as configurações do Block Public Access. Usar o Block Public Access com identidades do IAM ajuda a garantir que qualquer operação bloqueada por uma configuração do Block Public Access seja rejeitada, a menos que o usuário solicitante tenha recebido permissão específica.

Para obter mais informações, consulte Configurações do Block Public Access no Guia do desenvolvedor do Amazon Simple Storage Service.

Conceder acesso com identidades do IAM

Ao configurar contas para novos membros da equipe que exigem acesso ao S3, use usuários e funções do IAM para garantir privilégios mínimos. Também é possível implementar uma forma de autenticação multifator (MFA) do IAM para apoiar uma base de identidade sólida. Com as identidades do IAM, é possível conceder permissões exclusivas aos usuários e especificar quais recursos eles podem acessar e quais ações eles podem executar. As identidades do IAM fornecem mais recursos, incluindo a capacidade de exigir que os usuários insiram credenciais de login antes de acessar recursos compartilhados e aplicar hierarquias de permissão a diferentes objetos em um único bucket.

Para obter mais informações, consulte Exemplo 1: proprietário do bucket concedendo permissões de bucket aos usuários no Guia do desenvolvedor do Amazon Simple Storage Service.

Políticas de buckets

Com as políticas de bucket, é possível personalizar o acesso ao bucket para ajudar a garantir que somente os usuários aprovados possam acessar recursos e executar ações neles. Além das políticas de bucket, você deve usar as configurações do Block Public Access no nível do bucket para limitar ainda mais o acesso público aos dados.

Para obter mais informações, consulte Políticas e permissões no Amazon S3 no Guia do desenvolvedor do Amazon Simple Storage Service.

Ao criar políticas, evite o uso de curingas no elemento `Principal` porque ele permite efetivamente que qualquer pessoa acesse os recursos do Amazon S3. É melhor listar explicitamente usuários ou grupos que têm permissão para acessar o bucket. Em vez de incluir um curinga para as ações, conceda permissões específicas quando aplicável.

Para manter ainda mais a prática de privilégios mínimos, as instruções Deny (Negar) no elemento `Effect` devem ser tão amplas quanto possível e as instruções Allow (Permitir) devem ser tão restritas quanto possível. Negar efeitos emparelhados com a ação "`s3:*`" é outra boa maneira de implementar as melhores práticas de adesão para os usuários incluídos em instrução de condição de política.

Para obter mais informações sobre como especificar condições para quando uma política está em vigor, consulte Chaves de condição do Amazon S3 no Guia do desenvolvedor do Amazon Simple Storage Service.

Buckets em uma configuração de VPC

Ao adicionar usuários em uma configuração corporativa, você poderá usar um endpoint de nuvem privada virtual (VPC) para permitir que todos os usuários n rede virtual acessem os recursos do Amazon S3. Os VPC endpoints permitem que os desenvolvedores concedam acesso e permissões específicos a grupos de usuários com base na rede à qual o usuário está conectado. Em vez de adicionar cada usuário a uma função ou a um grupo do IAM, você poderá usar VPC endpoints para negar acesso ao bucket se a solicitação não for originada do endpoint especificado.

Para obter mais informações, consulte Exemplos de políticas de buckets para VPC endpoints do Amazon S3 no Guia do desenvolvedor do Amazon Simple Storage Service.

Armazenar e compartilhar dados

Use as seguintes ferramentas e melhores práticas para armazenar e compartilhar os dados do Amazon S3.

Versionamento e bloqueio de objetos para integridade de dados

Se você usar o console do Amazon S3 para gerenciar buckets e objetos, deverá implementar Versionamento do S3 e S3 Bloqueio de objetos. Esses recursos ajudam a evitar alterações acidentais em dados críticos e permitem reverter ações não intencionais. Esse recurso é particularmente útil quando há vários usuários com permissões completas de gravação e execução acessando o console do Amazon S3.

Para obter informações sobre Versionamento do S3, consulte Usar o versionamento no Guia do desenvolvedor do Amazon Simple Storage Service. Para obter informações sobre Bloqueio de objetos, consulte Bloquear objetos usando o S3 Object Lock no Guia do desenvolvedor do Amazon Simple Storage Service.

Gerenciamento do ciclo de vida do objeto para eficiência de custos

Para gerenciar os objetos para que eles sejam armazenados de forma econômica durante todo o ciclo de vida, você pode emparelhar políticas de ciclo de vida com o versionamento de objetos. As políticas de ciclo de vida definem as ações que você deseja que o S3 execute durante a vida útil de um objeto. Por exemplo, é possível criar uma política de ciclo de vida que fará a transição de objetos para outra classe de armazenamento, arquivá-los ou excluí-los após um período especificado. É possível definir uma política de ciclo de vida para todos os objetos ou para um subconjunto de objetos no bucket usando um prefixo ou uma tag compartilhados.

Para obter mais informações, consulte Gerenciamento do ciclo de vida de objetos no Guia do desenvolvedor do Amazon Simple Storage Service.

Replicação entre regiões para vários locais de escritório

Ao criar buckets que são acessados por diferentes locais de escritório, você deve considerar a implementação da replicação entre regiões do S3. A replicação entre regiões ajuda a garantir que todos os usuários tenham acesso aos recursos de que precisam e aumenta a eficiência operacional. A replicação entre regiões oferece maior disponibilidade copiando objetos entre buckets do S3 em diferentes regiões da AWS. No entanto, o uso dessa ferramenta aumenta os custos de armazenamento.

Para obter mais informações, consulte Replicação no Guia do desenvolvedor do Amazon Simple Storage Service.

Permissões para hospedagem segura de sites estáticos

Ao configurar um bucket para ser usado como um site estático acessado publicamente, é necessário desabilitar todas as configurações do Block Public Access. É importante fornecer apenas ações `s3:GetObject` e não permissões `ListObject` ou `PutObject` ao escrever a política de bucket para o site estático. 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 Definição de permissões: para acesso ao site no Guia do desenvolvedor do Amazon Simple Storage Service.

O Amazon CloudFront fornece os recursos necessários para configurar um site estático seguro. Os sites estáticos do Amazon S3 são compatíveis apenas com endpoints HTTP. O CloudFront usa o armazenamento durável do Amazon S3 enquanto fornece cabeçalhos de segurança adicionais, como HTTPS. HTTPS adiciona segurança criptografando uma solicitação HTTP normal e protegendo contra ataques cibernéticos comuns.

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

Compartilhar recursos

Existem várias maneiras diferentes de compartilhar recursos com um grupo específico de usuários. É possível usar as seguintes ferramentas para compartilhar um conjunto de documentos ou outros recursos com um único grupo de usuários, departamento ou escritório. Embora todos possam ser usados para atingir o mesmo objetivo, algumas ferramentas podem emparelhar melhor do que outras com as configurações existentes.

Políticas de usuário

É possível compartilhar recursos com um grupo limitado de pessoas usando políticas de grupos e de usuários do IAM. Ao criar um usuário do IAM, você será solicitado a criá-lo e adicioná-lo a um grupo. No entanto, é possível criar e adicionar usuários a grupos a qualquer momento. Se os indivíduos com os quais você pretende compartilhar esses recursos já estiverem configurados no IAM, será possível adicioná-los a um grupo comum e compartilhar o bucket com o grupo dentro da política de usuário. Também é possível usar políticas de usuário do IAM para compartilhar objetos individuais em um bucket.

Para obter mais informações, consulte Permitir a um usuário do IAM acesso a um de seus buckets no Guia do desenvolvedor do Amazon Simple Storage Service.

Listas de controle de acesso

Como regra geral, recomendamos que você use políticas de bucket do S3 ou políticas do IAM para controle de acesso. As listas de controle de acesso (ACLs) do Amazon S3 são um mecanismo de controle de acesso herdado anterior ao IAM. Se você já usa ACLs do S3 e as considera suficientes, não há necessidade de alterar. No entanto, determinados cenários de controle de acesso exigem o uso de ACLs. Por exemplo, quando um proprietário de bucket deseja conceder permissão a objetos, mas nem todos os objetos são de propriedade dele, o proprietário do objeto deve primeiro conceder permissão ao proprietário do bucket. Isso é feito usando uma ACL de objeto.

Para obter mais informações, consulte o Exemplo 3: proprietário do bucket concedendo permissões de usuários a objetos que ele não possui no Guia do desenvolvedor do Amazon Simple Storage Service.

Prefixos

Ao tentar compartilhar recursos específicos de um bucket, é possível replicar permissões no nível de pastas usando prefixos. O console do Amazon S3 é compatível com o conceito de pasta como um meio de agrupar objetos usando um prefixo de nome compartilhado para objetos. Depois, é possível especificar um prefixo dentro das condições da política de um usuário do IAM para conceder permissão explícita para que ele acesse os recursos associados a esse prefixo.

Para obter mais informações, consulte Usar pastas no Guia do usuário do console do Amazon Simple Storage Service.

Atribuição de tags (tagging)

Se usar a marcação de objetos para categorizar o armazenamento, você poderá compartilhar objetos marcados com um valor específico com usuários especificados. A marcação de recursos permite controlar o acesso a objetos com base nas tags associadas ao recurso que um usuário está tentando acessar. Para fazer isso, use a condição `ResourceTag/key-name` dentro de uma política de usuário do IAM para permitir o acesso aos recursos marcados.

Para obter mais informações, consulte Controle de acesso aos recursos da AWS usando tags de recursos no Guia do usuário do IAM.

Proteger dados

Use as seguintes ferramentas 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.

Object encryption

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 datacenters e os descriptografa ao fazer download dos objetos. Contanto que você autentique sua solicitação e tenha permissões de acesso, não há diferença na forma de acesso aos objetos criptografados ou não criptografados. Ao configurar a criptografia no lado do servidor, você tem três opções mutuamente exclusivas:

- Chaves gerenciadas do Amazon S3 (SSE-S3)
- Chaves mestres do cliente (CMK) armazenadas no AWS Key Management Service (SSE-KMS)
- Chaves fornecidas pelo cliente (SSE-C)

Para obter mais informações, consulte Proteger dados usando a criptografia no lado do servidor no Guia do desenvolvedor do Amazon Simple Storage Service.

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 no lado do servidor no Guia do desenvolvedor do Amazon Simple Storage Service.

Métodos de assinatura

O Signature versão 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 Autenticar solicitações (AWS Signature versão 4) e Processo de assinatura do Signature versão 4.

Registro em log e monitoramento

O monitoramento é uma parte importante da manutenção da confiabilidade, da disponibilidade e da performance das soluções do Amazon S3 para que você possa depurar mais facilmente uma falha de vários pontos, caso isso ocorra. O registro em log pode fornecer insight sobre os erros que os usuários estão recebendo, além de quando e quais solicitações são feitas. A AWS fornece várias ferramentas para monitorar os recursos do Amazon S3:

- Amazon CloudWatch
- AWS CloudTrail
- Logs de acesso do Amazon S3
- AWS Trusted Advisor

Para obter mais informações, consulte Registro em log e monitoramento no Amazon S3 no Guia do desenvolvedor do Amazon Simple Storage Service.

O Amazon S3 é integrado ao AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, por uma função ou por um serviço da AWS no Amazon S3. Esse recurso pode ser emparelhado com o Amazon GuardDuty, que monitora as ameaças contra os recursos do Amazon S3, analisando eventos de gerenciamento do CloudTrail e eventos de dados do S3 do CloudTrail. Essas fontes de dados monitoram diferentes tipos de atividade. Por exemplo, os eventos de gerenciamento do CloudTrail relacionados ao S3 incluem operações que listam ou configuram projetos do S3. O GuardDuty analisa eventos de dados do S3 de todos os buckets do S3 e os monitora em busca de atividades mal-intencionadas e suspeitas.

Para obter mais informações, consulte Proteção do Amazon S3 no Amazon GuardDuty no Guia do usuário do Amazon GuardDuty.

Recursos de desenvolvimento

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

- Código de exemplo e bibliotecas – o Centro do desenvolvedor da AWS tem 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. Para obter mais informações, consulte o Centro do desenvolvedor da AWS.
- Tutoriais – nosso Centro de recursos oferece mais tutoriais do Amazon S3.

  Esses tutoriais oferecem uma abordagem prática para o aprendizado das funcionalidades do Amazon S3. Para obter mais informações, consulte Artigos e tutoriais.
- Fórum de clientes – recomendamos que você examine o fórum do Amazon S3 para ter uma ideia do que outros usuários estão fazendo e se beneficiar das perguntas que eles fazem.

  O fórum pode ajudar a entender o que pode e o que não pode ser feito com o Amazon S3. O fórum também é um meio para que você faça perguntas que podem responder as dúvidas de outros usuários ou representantes da AWS. Você pode usar o fórum para relatar problemas com o serviço ou a API. Para obter mais informações, consulte os Fóruns de discussão.

Recursos de referência

A lista a seguir mostra os recursos adicionais que você pode usar para conhecer melhor o Amazon S3.

- O Guia do usuário do console do Amazon Simple Storage Service descreve todas as funções do Console de gerenciamento da AWS relacionadas ao Amazon S3.
- O Guia do desenvolvedor do Amazon Simple Storage Service oferece uma discussão detalhada do serviço.

  Esse guia inclui uma visão geral da arquitetura, descrições detalhadas de conceitos e procedimentos para usar a API.
- A Amazon Simple Storage Service API Reference fornece uma discussão detalhada sobre as ações e os parâmetros no Amazon S3.
- O Painel de status dos serviços exibe o status do serviço web do Amazon S3.

  O painel mostra se o Amazon S3 (e todos os outros produtos da AWS) estão funcionando corretamente. Para obter mais informações, consulte o Painel de status dos serviços.

Sobre este Guia

Esse é o Guia de conceitos básicos do Amazon Simple Storage Service.

O Amazon Simple Storage Service é frequentemente mencionado neste guia como "Amazon S3". Todos os direitos autorais e proteções legais ainda se aplicam.