Guia do usuário

AWS Support

Versão da API 2013-04-15

AWS Support: Guia do usuário

Table of Contents

Conceitos básicos do AWS Support 1
Criar casos de suporte e gerenciamento de casos 1
Criar um caso de suporte 2
Descrever o problema 5
Escolher uma gravidade 5
Exemplo: criar um caso de suporte para conta e faturamento 8
Criar um aumento de cota de serviço 14
Atualizar, resolver e reabrir casos 15
Atualizar um caso de suporte existente 16
Resolver um caso de suporte 17
Reabrir um caso resolvido 19
Abrir um caso relacionado 20
Histórico de caso 22
Solução de problemas 22
Quero reabrir um chat ao vivo para o meu caso 23
Não consigo me conectar ao chat ao vivo 23
Como trabalhar com AWS SDKs 23
Sobre a API do AWS Support 25
Gerenciamento de casos de suporte 25
AWS Trusted Advisor 26
Endpoints 26
Suporte nos SDKs da AWS 27
AWS Support Planos 28
Características dos AWS Support planos 28
Mudando AWS Support os planos 30
Informações relacionadas 31
AWS Trusted Advisor 32
Conceitos básicos das recomendações do Trusted Advisor 33
Fazer login no console do Trusted Advisor 33
Visualizar categorias de verificação 35
Visualizar verificações específicas 36
Filtrar as verificações 38
Atualizar resultados da verificação 39
Baixar dos resultados 40

Visualização organizacional 41
Preferences 41
Comece a usar a Trusted Advisor API 43
Usar o Trusted Advisor como um web service 44
Obter a lista de verificações disponíveis do Trusted Advisor 45
Atualizar a lista de verificações disponíveis do Trusted Advisor 45
Sondar uma verificação de alterações de status do Trusted Advisor 46
Solicitar um resultado de verificação do Trusted Advisor 48
Imprimir detalhes de uma verificação do Trusted Advisor 49
Visualização organizacional para AWS Trusted Advisor 49
Pré-requisitos 50
Habilitar a visualização organizacional 50
Atualizar verificações do Trusted Advisor 51
Criar relatórios da visualização organizacional 52
Visualize o resumo do relatório. 56
Baixar um relatório da visualização organizacional 57
Desabilitar a visualização organizacional 62
Utilização de políticas do IAM para permitir acesso à visualização organizacional 64
Usar outros serviços da AWS para visualizar relatórios do Trusted Advisor 67
Exibir as verificações do Trusted Advisor fornecidas pelo AWS Config 77
Solução de problemas 78
Visualizar os controles do Security Hub no Trusted Advisor 79
Pré-requisitos 80
Para visualizar os resultados do Security Hub 81
Atualizar os resultados do Security Hub 83
Desabilitar o Security Hub do Trusted Advisor 84
Solução de problemas 84
Optar por verificações do Trusted Advisor para o AWS Compute Optimizer 88
Informações relacionadas 89
Conceitos básicos do AWS Trusted Advisor Priority 89
Pré-requisitos 90
Habilitar o Trusted Advisor Priority 91
Visualizar recomendações priorizadas 91
Reconhecer uma recomendação 94
Ignorar uma recomendação 97
Resolver uma recomendação 99

Reabrir uma recomendação ... 101
Baixar os detalhes da recomendação ... 103
Registrar administradores delegados ... 103
Cancelar o registro dos administradores delegados ... 104
Gerenciar as notificações do Trusted Advisor Priority ... 104
Desabilitar o Trusted Advisor Priority ... 106
Comece a usar o AWS Trusted Advisor Engage (versão pré-visualização) ... 106
Pré-requisitos ... 107
Visualize o painel de interações ... 107
Visualize o catálogo de tipos de interação ... 108
Solicitar uma interação ... 109
Editar uma interação ... 111
Enviar anexos e notas ... 113
Alterar o status da interação ... 114
Diferencie entre as interações recomendadas e solicitadas ... 115
Pesquisar interações ... 116
Referência de verificação do Trusted Advisor ... 117
Otimização de custo ... 118
Performance ... 156
Segurança ... 210
Tolerância a falhas ... 250
Limites do serviço ... 362
Excelência operacional ... 382
Registro de alterações para AWS Trusted Advisor ... 425
Nova verificação de tolerância a falhas ... 425
Tolerância a falhas e verificações de segurança atualizadas ... 425
Nova verificação de tolerância a falhas ... 425
Verificação atualizada de tolerância a falhas ... 426
Verificação de segurança atualizada ... 426
Novas verificações de segurança e desempenho ... 426
Nova verificação de segurança ... 426
Novas verificações de tolerância a falhas e otimização de custos ... 427
Novas verificações de tolerância a falhas ... 427
Novas verificações para o Amazon RDS ... 427
Nova AWS Trusted Advisor API ... 427
Trusted Advisor verifique a remoção ... 428

Integração de AWS Config cheques em Trusted Advisor 428
Novas verificações de tolerância a falhas 428
Verificação de novos limites de serviço 429
Nova verificação de tolerância a falhas 429
Novas verificações de tolerância a falhas e performance 429
Novas verificações de tolerância a falhas 430
Novas verificações de tolerância a falhas 430
Expansão regional das verificações de tolerância a falhas do Amazon ECS 430
Novas verificações de tolerância a falhas 430
Novas verificações de tolerância a falhas 426
Atualizações na Trusted Advisor integração com AWS Security Hub 431
Novas verificações de tolerância a falhas para o AWS Resilience Hub 427
Atualização para o Trusted Advisor console 432
Novas verificações para o Amazon EC2 433
Verificações do Security Hub adicionadas ao Trusted Advisor 433
Cheques adicionados de AWS Compute Optimizer 433
Atualizações para a verificação de chaves de acesso expostas 434
Verificações atualizadas para AWS Direct Connect 435
AWS Security Hub controles adicionados ao AWS Trusted Advisor console 435
Novas verificações para o Amazon EC2 e o AWS Well-Architected 436
Nome do cheque atualizado para o Amazon OpenSearch Service 436
Verificações adicionadas para o armazenamento de volumes do Amazon Elastic Block Store 437
Verificações adicionadas para AWS Lambda 437
Trusted Advisor verifique a remoção 438
Verificações atualizadas para o Amazon Elastic Block Store 438
Trusted Advisor verifique a remoção 439
Trusted Advisor verifique a remoção 440
Aplicativo AWS Support no Slack 441
Pré-requisitos 442
Gerenciar o acesso ao widget do aplicativo AWS Support 443
Gerenciar o acesso ao aplicativo AWS Support 444
Autorizar um espaço de trabalho do Slack 451
Autorizar várias contas 453
Configurar um canal do Slack 454
Atualizar a configuração do seu canal do Slack 459

Criar casos de suporte no Slack ... 460
Responder a casos de suporte no Slack ... 466
Entrar em uma sessão de chat ao vivo com o AWS Support ... 468
Procurar casos de suporte no Slack ... 474
Usar os resultados da pesquisa ... 476
Resolver casos de suporte no Slack ... 478
Reabrir casos de suporte no Slack ... 478
Solicitar aumentos de cota de serviço ... 479
Excluir uma configuração de canal do Slack do aplicativo AWS Support ... 482
Excluir uma configuração de espaço de trabalho do Slack no aplicativo AWS Support ... 482
Aplicativo AWS Support nos comandos do Slack ... 484
Comandos do canal do Slack ... 484
Comandos do canal de chat ao vivo ... 484
Visualizar correspondências do aplicativo AWS Support no AWS Support Center Console ... 485
Crie recursos do AWS CloudFormation para o AWS Support App no Slack ... 486
Aplicativo AWS Support e modelos do AWS CloudFormation ... 486
Criar recursos de configuração do Slack para a organização ... 486
Saiba mais sobre o CloudFormation ... 492
Criar recursos do AWS Support App ao usar o Terraform ... 492
Segurança ... 494
Proteção de dados ... 495
Segurança para casos de suporte ... 496
Gerenciamento de identidade e acesso ... 497
Público ... 497
Autenticando com identidades ... 498
Gerenciamento do acesso usando políticas ... 501
Como AWS Support funciona com o IAM ... 503
Exemplos de políticas baseadas em identidade ... 506
Usar funções vinculadas a serviços ... 508
AWS políticas gerenciadas ... 516
Gerencie o acesso ao AWS Support Centro ... 572
Gerencie o acesso aos AWS Support planos ... 576
Gerencie o acesso ao AWS Trusted Advisor ... 581
Políticas de controle de serviço de exemplo para o AWS Trusted Advisor ... 594
Solução de problemas ... 595
Resposta a incidentes ... 598

Registro e monitoramento em AWS Support e AWS Trusted Advisor 598
Validação de conformidade 599
Resiliência 600
Segurança da infraestrutura 601
Análise de configuração e vulnerabilidade 601
Exemplos de código 602
Ações 610
AddAttachmentsToSet 611
AddCommunicationToCase 617
CreateCase 623
DescribeAttachment 630
DescribeCases 636
DescribeCommunications 644
DescribeServices 652
DescribeSeverityLevels 660
DescribeTrustedAdvisorCheckRefreshStatuses 667
DescribeTrustedAdvisorCheckResult 668
DescribeTrustedAdvisorCheckSummaries 670
DescribeTrustedAdvisorChecks 672
RefreshTrustedAdvisorCheck 673
ResolveCase 675
Cenários 680
Conceitos básicos de casos 681
Monitorar e registrar em log para o AWS Support 739
Monitorando AWS Support casos com EventBridge 739
Criar uma regra do EventBridge para casos do AWS Support 740
Eventos de exemplo do AWS Support 742
Consulte também 744
Registrar em log chamadas de API do AWS Support com o AWS CloudTrail 744
Informações do AWS Support no CloudTrail 745
Informações do AWS Trusted Advisor no registro do CloudTrail 746
Noções básicas sobre entradas de arquivos de log do AWS Support 746
Registro em log de chamadas de API do aplicativo AWS Support com o CloudTrail 748
Informações do aplicativo AWS Support no CloudTrail 749
Noções básicas sobre entradas de arquivos de log do aplicativo AWS Support 750
Como monitorar e registrar planos de suporte 754

Como registrar as chamadas de API dos planos do AWS Support com o AWS CloudTrail 754
Informações dos planos do AWS Support no CloudTrail 755
Noções básicas sobre as entradas de arquivos de log dos planos do AWS Support 756
Registrar ações do console para alterações em seu plano AWS Support 761
Monitorar e registrar em log para o Trusted Advisor 765
Monitorando Trusted Advisor os resultados da verificação com EventBridge 766
Criar alarmes do CloudWatch para monitorar métricas do Trusted Advisor 768
Pré-requisitos 769
Métricas do CloudWatch para Trusted Advisor 773
Métricas e dimensões do Trusted Advisor 779
Registro de ações do console do AWS Trusted Advisor com AWS CloudTrail 782
Trusted Advisorinformações em CloudTrail 782
Exemplo: entradas do arquivo de log do Trusted Advisor 785
Recursos de solução de problemas 790
Solução de problemas de erros específicos do serviço 790
Histórico do documento 795
Atualizações anteriores 824
AWS Glossário 828
..... dcccxxix

Conceitos básicos do AWS Support

O AWS Support oferece uma variedade de planos que permitem conceder acesso a ferramentas e conhecimentos que oferecem suporte ao sucesso e à integridade operacional das soluções da AWS. Todos os planos de suporte oferecem acesso 24 horas por dia, 7 dias por semana ao atendimento ao cliente, à documentação da AWS, aos whitepapers e aos fóruns de suporte. Para obter suporte técnico e mais recursos para planejar, implantar e aprimorar o ambiente da AWS, você pode selecionar um plano de suporte para seu caso de uso da AWS.

Observações

- Para abrir um caso de suporte no AWS Management Console, consulte Criar um caso de suporte.
- Para obter mais informações sobre os diferentes planos do AWS Support, consulte Comparar planos do AWS Support e Mudando AWS Support os planos.
- Os planos de suporte oferecem tempos de resposta diferentes para seus casos de suporte. Consulte Escolher uma gravidade e Tempos de resposta.

Tópicos

- Criar casos de suporte e gerenciamento de casos
- Criar um aumento de cota de serviço
- Atualizar, resolver e reabrir um caso
- Solução de problemas
- Usar o AWS Support com um SDK da AWS

Criar casos de suporte e gerenciamento de casos

No AWS Management Console, você pode criar três tipos de casos de cliente no AWS Support:

- Casos de suporte a contas e cobrança estão disponíveis para todos os clientes da AWS. É possível obter ajuda com perguntas sobre cobranças e contas.

- Solicitações de Service limit increase (Aumento de limite do serviço) também estão disponíveis para todos os clientes da AWS. Para obter mais informações sobre as cotas de serviço padrão, anteriormente chamadas de limites, consulte AWS Service Quotas na Referência geral da AWS.
- Casos de Technical support (Suporte técnico) conectam você ao suporte técnico para obter ajuda com problemas técnicos relacionados aos serviços e, em alguns casos, aplicativos de terceiros. Se você tiver o suporte Básico, não poderá criar um caso de suporte técnico.

> Observações
>
> - Para alterar o plano de suporte, consulte Mudando AWS Support os planos.
> - Para fechar a conta, consulte, Fechar uma conta no Manual do usuário do AWS Billing.
> - Para encontrar tópicos comuns de solução de problemas para Serviços da AWS, consulte Recursos de solução de problemas.
> - Se você for cliente de uma AWS Partner que seja parte da AWS Partner Network, e você usa o suporte de revenda, entre em contato diretamente com a sua AWS Partner para quaisquer problemas relacionados ao faturamento. O AWS Support não pode ajudar com problemas não técnicos do suporte de revenda, como faturamento e gerenciamento de contas. Para obter mais informações, consulte os tópicos a seguir:
>   - Como os parceiros da AWS podem determinar planos do AWS Support em uma organização
>   - Suporte prestado pelo AWS Partner

Criar um caso de suporte

É possível abrir um caso de suporte na Central de Suporte do AWS Management Console.

> Observações
>
> - É possível entrar na Central de Suporte como o usuário raiz de sua conta da AWS ou como um usuário do AWS Identity and Access Management (IAM). Para obter mais informações, consulte Gerencie o acesso ao AWS Support Centro.
> - Se você não conseguir entrar na Central de Suporte e criar um caso de suporte, use a página Entre em contato conosco. É possível usar esta página para obter ajuda com problemas de cobrança e conta.

Como criar um caso de suporte

1. Faça login no AWS Support Center Console.

> **Tip**
>
> No AWS Management Console, você também pode escolher o ícone de ponto de interrogação
> ()
> e escolher Support Center.

2. Escolha Criar caso.
3. Escolha uma das seguintes opções:
   - Conta e faturamento
   - Técnico
   - Para aumentos de cota de serviço, escolha Looking for service limit increases? (Deseja aumentar o limite de serviço?) e siga as instruções para o Criar um aumento de cota de serviço.
4. Selecione o Service (Serviço), a Category (Categoria) e a Severity (Severidade).

> **Tip**
>
> Você pode usar as soluções recomendadas que aparecem para verificar as perguntas mais frequentes.

5. Selecione Next step: Additional information (Próxima etapa: Informações adicionais).
6. Na página Additional information (Informações adicionais), em Subject (Assunto), insira um título sobre o problema.
7. Em Description (Descrição), siga as instruções para descrever seu caso, como segue:
   - Mensagens de erro recebidas
   - Etapas de resolução de problemas que você seguiu
   - Como você está acessando o serviço:
     - AWS Management Console
     - AWS Command Line Interface (AWS CLI)

- Operações de API

8. (Opcional) Escolha Attach files (Anexar arquivos) para adicionar arquivos relevantes ao seu caso, como registros de erros ou capturas de tela. É possível anexar até três arquivos. Cada arquivo pode ter até 5 MB.
9. Escolha Next step: Solve now or contact us (Próximo passo: solucionar agora ou entrar em contato conosco).
10. Na página Contact us (Fale conosco), escolha seu idioma preferencial.
11. Escolha seu método de contato preferido. Você pode escolher uma das seguintes opções:

    a. Web: receba uma resposta no Support Center.

    b. Chat (Bate-papo): inicie um bate-papo ao vivo com um agente de suporte. Se você não conseguir se conectar a um chat, consulte Solução de problemas.

    c. Phone (Telefone) - Recebe uma chamada telefônica de um agente de suporte. Se você escolher essa opção, insira as seguintes informações:

    - Country or region (País ou região)
    - Número de telefone
    - (Optional) Extension ([Opcional] Ramal)

    > **Observações**
    >
    > - As opções de contato exibidas dependem do tipo de caso e do plano de suporte.
    > - É possível escolher Discard draft (Descartar rascunho) para limpar o rascunho do caso de suporte.

12. (Opcional) Se você tiver um plano de Support Business, Enterprise On-Ramp ou Enterprise, a opção Additional contacts (Contatos adicionais) será exibida. Você pode inserir os endereços de e-mail das pessoas a serem notificadas quando o status do caso mudar. Se você estiver conectado como um usuário do IAM, inclua seu próprio endereço de e-mail. Se você estiver conectado com seu endereço de e-mail e sua senha da conta root, não será necessário incluir seu endereço de e-mail.

> **Note**
>
> Se tiver o plano de suporte Basic, a opção Additional contacts (Contatos adicionais) não ficará visível. No entanto, o contato Operations (Operações) especificado na seção Alternate Contacts (Contatos alternativos) da página My Account (Minha conta) recebe cópias da correspondência de caso, mas somente para os tipos de caso específicos de conta e faturamento e técnico.

13. Revise os detalhes do seu caso e escolha Submit (Enviar). O número do ID do caso e o resumo são exibidos.

Descrever o problema

Faça a descrição com o máximo de detalhes possível. Inclua informações de recursos relevantes com outras informações que possam nos ajudar a entender o problema. Por exemplo, para solucionar problemas de performance, inclua time stamps e logs. Para solicitações de recursos ou perguntas de orientação geral, inclua uma descrição do seu ambiente e a finalidade. Em todos os casos, siga a Orientação da descrição que aparece no formulário de envio de caso.

Ao fornecer o máximo de detalhes possível, você aumenta as chances de que seu caso seja resolvido rapidamente.

Escolher uma gravidade

É possível que você tenda a sempre criar um caso de suporte com a mais elevada gravidade permitida pelo seu plano de suporte. No entanto, recomendamos escolher as gravidades mais elevadas para casos que não possam ser evitados ou que afetam diretamente aplicativos de produção. Para obter informações sobre como criar seus serviços de modo que a perda de recursos únicos não afete suas aplicações, consulte o whitepaper Desenvolvimento de aplicações tolerantes a falhas na AWS.

A tabela a seguir lista os níveis de gravidade, tempos de resposta e exemplos de problemas.

> **Observações**
>
> - Não é possível alterar o código de gravidade de um caso de suporte após criá-lo. Se a sua situação mudar, trabalhe com o atendente do AWS Support para o seu caso de suporte.

- Para obter mais informações sobre o nível de severidade, consulte a Referência de API do AWS Support.

Severidade	Código de nível de severidade	Tempo da primeira resposta	Descrição e plano de suporte
Orientações gerais	`low`	24 horas	Você tem uma pergunta de desenvolvimento geral ou quer solicitar um recurso. (Plano de suporte *Developer, Business, Enterprise On-Ramp ou Enterprise)
Sistema prejudicado	`normal`	12 horas	Funções não críticas de seu aplicativo estão se comportando de forma anormal ou você tem uma pergunta sobre desenvolvimento urgente. (Plano de suporte *Developer, Business, Enterprise On-Ramp ou Enterprise)
Sistema de produção prejudicado	`high`	4 horas	Funções importantes de seu aplicativo estão prejudicadas ou reduzidas. (Plano de suporte Business, Enterprise On-Ramp ou Enterprise)
Sistema de produção desativado	`urgent`	1 hora	Sua empresa está sendo afetada de forma significativa. Funções importantes de seu aplicativo não estão disponíveis. (Plano de suporte Business, Enterprise On-Ramp ou Enterprise)
Sistema crítico para os negócios inativo	`critical`	15 minutos	Sua empresa está em risco. Funções essenciais de sua aplicação não estão disponíveis (plano de suporte Enterprise) Observe que esse tempo é de 30 minutos para o plano de suporte Enterprise On-Ramp.

Tempos de resposta

Fazemos todos os esforços razoáveis para responder à sua solicitação inicial no prazo indicado. Para obter informações sobre o escopo do suporte para cada plano do AWS Support, consulte Recursos do AWS Support.

Se você tiver um plano de suporte Business, Enterprise On-Ramp ou Enterprise, terá acesso 24 horas por dia, 7 dias por semana, ao suporte técnico. *Para o plano de suporte Developer, as metas de resposta são calculadas com base no horário comercial. O horário comercial é geralmente definido como das 8h às 18h no país do cliente, exceto feriados e fins de semana. Esses horários podem variar em países com vários fusos horários. Essas informações são exibidas na seção Contact Information (Informações de contato) da página My Account (Minha conta) no AWS Management Console.

Note

Se você escolher o japonês como seu idioma de contato preferencial para casos de suporte, o suporte em japonês poderá estar disponível da seguinte forma:

- Se você precisar de atendimento ao cliente para casos de suporte não técnico ou se tiver um plano Developer Support e precisar de suporte técnico, o suporte em japonês estará disponível durante o horário comercial no Japão, definido como das 9h às 18h, horário padrão do Japão (GMT+9), exceto feriados e fins de semana.
- Se você tiver um plano de suporte Business, Enterprise On-Ramp ou Enterprise, terá acesso ao suporte técnico 24 horas por dia, 7 dias por semana, em japonês

Se você escolher o chinês como seu idioma de contato preferencial para casos de suporte, o suporte em chinês poderá estar disponível da seguinte forma:

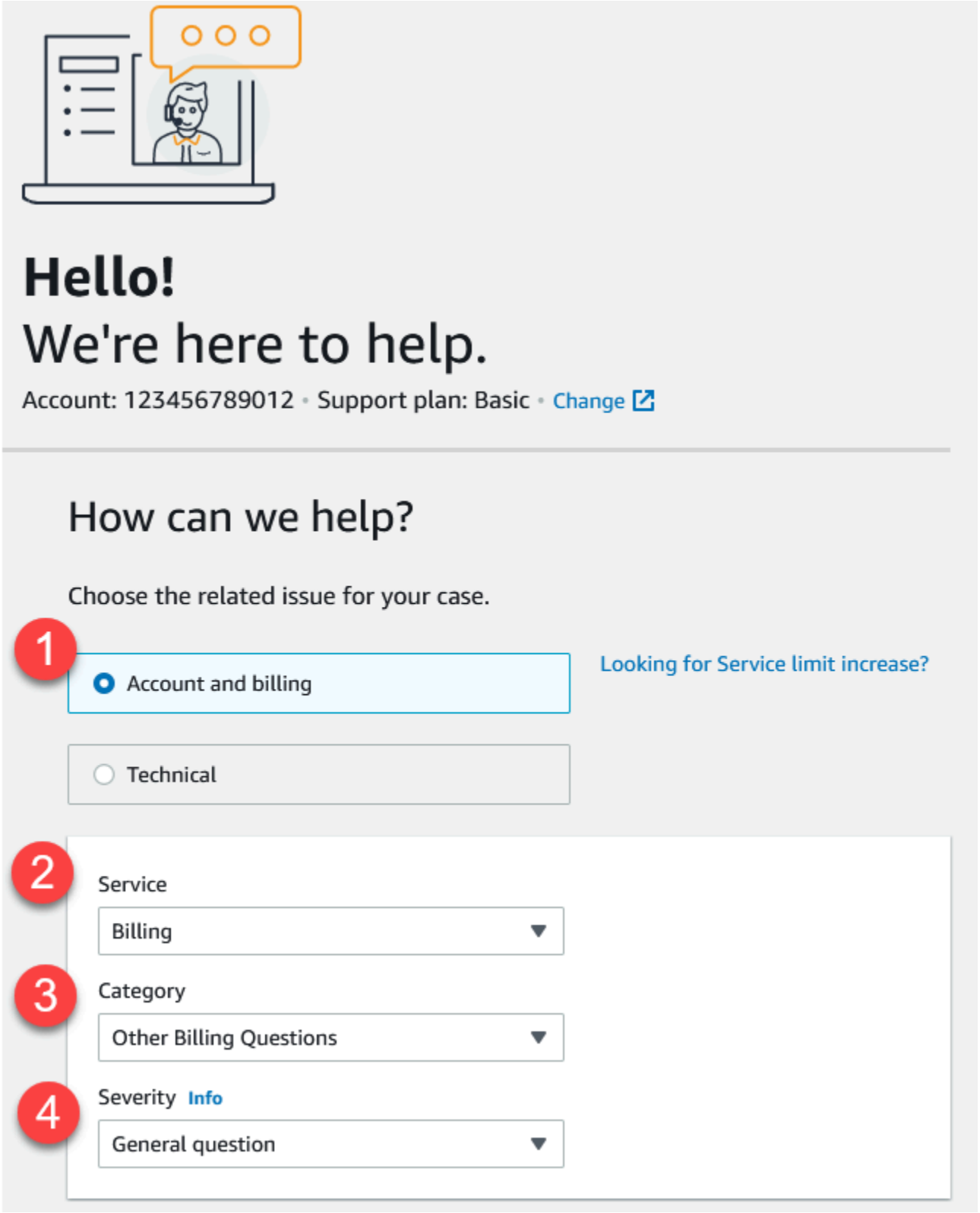
- Se você precisar de atendimento ao cliente para casos de suporte não técnico, o suporte em chinês estará disponível das 9h às 18h (GMT+8), exceto feriados e fins de semana.
- Se você tiver um plano Developer Support, o suporte técnico em chinês estará disponível durante o horário comercial, geralmente definido das 8h às 18h em seu país, conforme definido em Minha conta, exceto feriados e fins de semana. Esses horários podem variar em países com vários fusos horários.
- Se você tiver um plano de suporte Business, Enterprise On-Ramp ou Enterprise Support, terá acesso ao suporte técnico 24 horas por dia, 7 dias por semana, em chinês.

Se você escolher o coreano como seu idioma de contato preferencial para casos de suporte, o suporte em coreano poderá estar disponível da seguinte forma:

- Se você precisar de atendimento ao cliente para casos de suporte não técnico, o suporte em coreano estará disponível durante o horário comercial na Coreia, definido como das 9h às 18h, horário padrão da Coreia (GMT+9), exceto feriados e fins de semana.
- Se você tiver um plano Developer Support, o suporte técnico em coreano estará disponível durante o horário comercial, geralmente definido das 8h às 18h em seu país, conforme definido em Minha conta, exceto feriados e fins de semana. Esses horários podem variar em países com vários fusos horários.
- Se você tiver um plano de suporte Business, Enterprise On-Ramp ou Enterprise Support, terá acesso ao suporte técnico 24 horas por dia, 7 dias por semana, em coreano.

Exemplo: criar um caso de suporte para conta e faturamento

O exemplo a seguir é um caso de suporte para um problema de faturamento e conta.



1. Create case (Criar caso): escolha o tipo de caso a ser criado. Neste exemplo, o tipo de caso é Account and billing (Conta e faturamento).

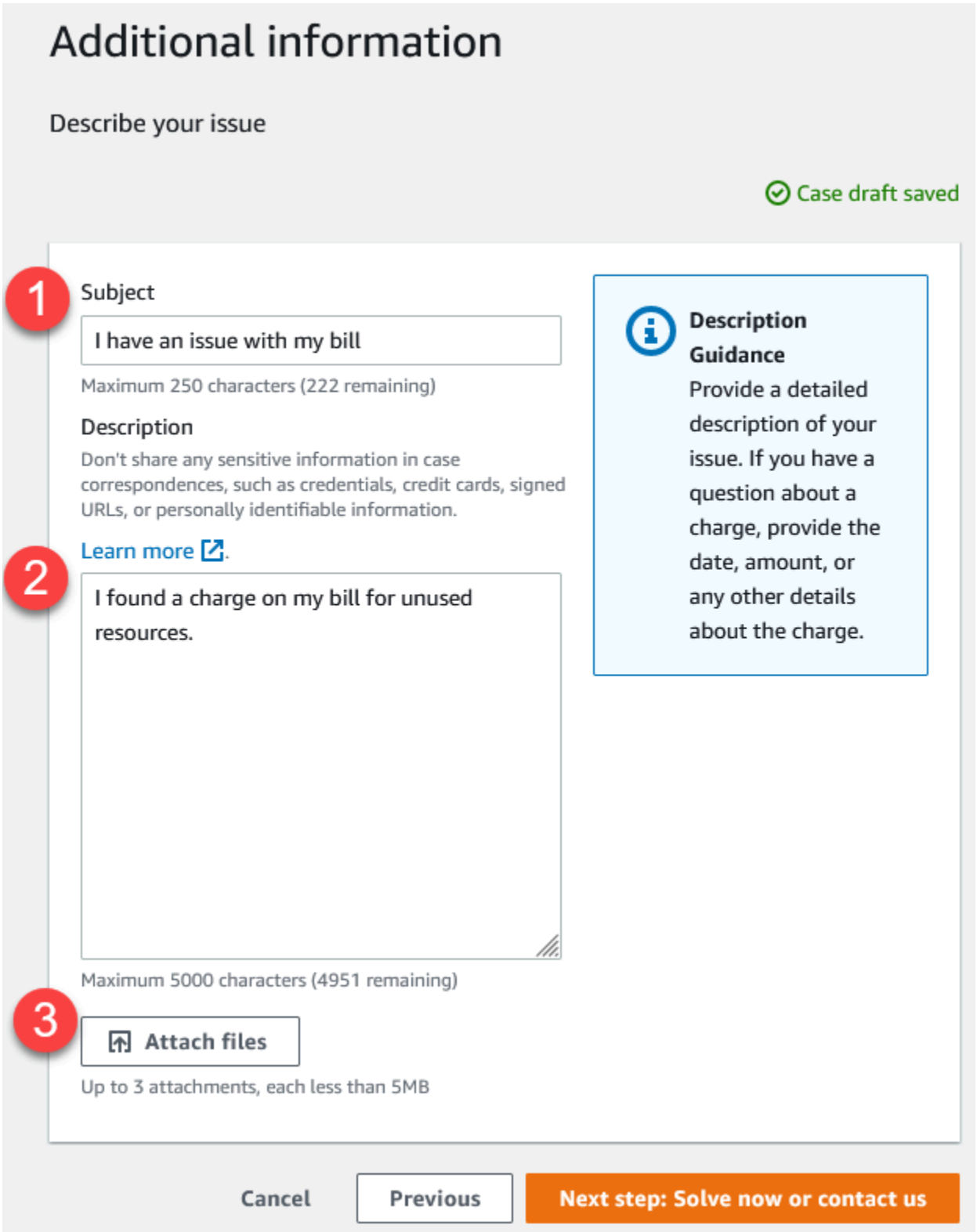
> **Note**
>
> Se você tiver o plano de suporte Básico, não poderá criar um caso de suporte técnico.

2. Service (Serviço) - Se a sua dúvida afetar vários serviços, selecione o serviço mais aplicável.
3. Category (Categoria) - Selecione a categoria que seja mais adequada ao caso de uso. Quando você escolher uma categoria, os links para informações que podem resolver o problema aparecerão abaixo.
4. Severity (Gravidade) - Os clientes com um plano de suporte pago podem escolher o nível de gravidade General guidance (Orientação geral) (tempo de resposta de 1 dia) ou System impaired (Sistema prejudicado) (tempo de resposta de 12 horas). Os clientes com um plano de suporte Business também podem escolher Production system impaired (Sistema de produção prejudicado) (resposta em 4 horas) ou Production system down (Sistema de produção desabilitado) (resposta em 1 hora). Os clientes com um plano Enterprise On-Ramp ou Enterprise Support podem escolher Business-critical system down (Sistema crítico para os negócios inativo) (resposta de 15 minutos para o Enterprise Support e resposta de 30 minutos para o Enterprise On-Ramp).

   Os tempos de resposta são para a primeira resposta do AWS Support. Esses tempos de resposta não se aplicam a respostas subsequentes. Para problemas de terceiros, os tempos de resposta podem ser mais longos, dependendo da disponibilidade de funcionários qualificados. Para obter mais informações, consulte Escolher uma gravidade.

   > **Note**
   >
   > Com base na sua seleção de categoria, você pode ser solicitado a fornecer mais informações.

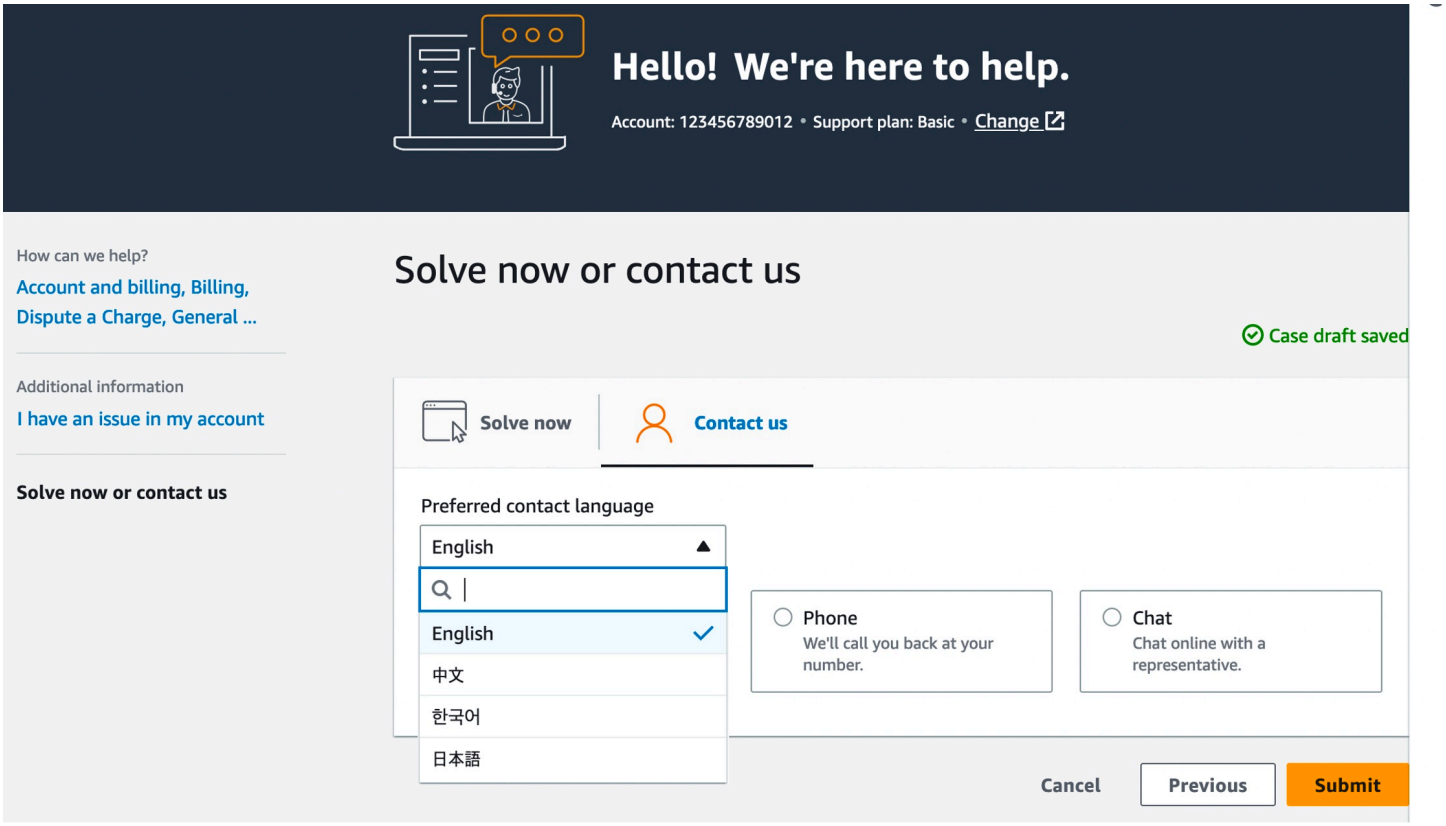
Depois de especificar o tipo de ocorrência e a classificação, você pode especificar a descrição e como deseja ser contatado.



1. Subject (Assunto) - Insira um título que descreva brevemente o problema.

2. Description (Descrição) — Descreva seu caso de suporte. Essa é a informação mais importante fornecida ao AWS Support. Para algumas combinações de serviço e categoria, um aviso é exibido com informações relacionadas. Use esses links para ajudar a resolver seu problema. Para obter mais informações, consulte Descrever o problema.
3. Attachments (Anexos): capturas de tela e outros arquivos podem ajudar os agentes de suporte a solucionar seu caso mais rapidamente. É possível anexar até três arquivos. Cada arquivo pode ter até 5 MB.

Após adicionar os detalhes do caso, você pode escolher como deseja ser contatado.



1. Idioma de contato preferencial: escolha o idioma de sua preferência. Atualmente, você pode escolher chinês, inglês, japonês ou coreano. As opções de contato personalizadas em seu idioma preferencial serão mostradas pelo seu plano de suporte.
2. Escolha um método de contato. As opções de contato exibidas dependem do tipo de caso e do plano de suporte.
   - Se você escolher Web, poderá ler e responder ao andamento do caso na Central de Suporte.

- Selecione Chat (Bate-papo) ou Phone (Telefone). Se você selecionar Phone (Telefone), será solicitado a fornecer um número para retorno de chamada.

3. Selecione Submit (Enviar) quando suas informações forem preenchidas e você estiver pronto para criar o caso.

> **Note**
>
> Se você escolher o japonês como seu idioma de contato preferencial para casos de suporte, o suporte em japonês poderá estar disponível da seguinte forma:
>
> - Se você precisar de atendimento ao cliente para casos de suporte não técnico ou se tiver um plano Developer Support e precisar de suporte técnico, o suporte em japonês estará disponível durante o horário comercial no Japão, definido como das 9h às 18h, horário padrão do Japão (GMT+9), exceto feriados e fins de semana.
> - Se você tiver um plano de suporte Business, Enterprise On-Ramp ou Enterprise, terá acesso ao suporte técnico 24 horas por dia, 7 dias por semana, em japonês
>
> Se você escolher o chinês como seu idioma de contato preferencial para casos de suporte, o suporte em chinês poderá estar disponível da seguinte forma:
>
> - Se você precisar de atendimento ao cliente para casos de suporte não técnico, o suporte em chinês estará disponível das 9h às 18h (GMT+8), exceto feriados e fins de semana.
> - Se você tiver um plano Developer Support, o suporte técnico em chinês estará disponível durante o horário comercial, geralmente definido das 8h às 18h em seu país, conforme definido em Minha conta, exceto feriados e fins de semana. Esses horários podem variar em países com vários fusos horários.
> - Se você tiver um plano de suporte Business, Enterprise On-Ramp ou Enterprise Support, terá acesso ao suporte técnico 24 horas por dia, 7 dias por semana, em chinês.
>
> Se você escolher o coreano como seu idioma de contato preferencial para casos de suporte, o suporte em coreano poderá estar disponível da seguinte forma:
>
> - Se você precisar de atendimento ao cliente para casos de suporte não técnico, o suporte em coreano estará disponível durante o horário comercial na Coreia, definido como das 9h às 18h, horário padrão da Coreia (GMT+9), exceto feriados e fins de semana.

- Se você tiver um plano Developer Support, o suporte técnico em coreano estará disponível durante o horário comercial, geralmente definido das 8h às 18h em seu país, conforme definido em Minha conta, exceto feriados e fins de semana. Esses horários podem variar em países com vários fusos horários.
- Se você tiver um plano de suporte Business, Enterprise On-Ramp ou Enterprise Support, terá acesso ao suporte técnico 24 horas por dia, 7 dias por semana, em coreano.

Criar um aumento de cota de serviço

Para melhorar o desempenho do seu serviço, solicite aumentos de suas cotas de serviço (anteriormente chamadas de limites).

> **Note**
>
> É possível usar o serviço Service Quotas para solicitar aumentos diretamente para seus serviços. No momento, as Service Quotas não são compatíveis com cotas de serviço para todos os serviços. Para obter mais informações, consulte O que são cotas de serviço? no Guia do usuário do Service Quotas.

Criar um caso de suporte para aumentos de cota de serviço

1. Faça login no AWS Support Center Console.

   > **Tip**
   >
   > No AWS Management Console, você também pode escolher o ícone de ponto de interrogação
   > ()
   > e escolher Support Center.

2. Escolha Criar caso.
3. Escolha Looking for service limit increases? (Deseja aumentar o limite de serviço?).
4. Para solicitar um aumento, siga as instruções. As opções incluem o seguinte:

   - Limit Type (Tipo de limite)

- Gravidade

> **Note**
>
> Com base na sua seleção de categoria, os avisos podem solicitar mais informações.

5. Em Requests (Solicitações), escolha a Region (Região).
6. Em Limit (Limite), escolha o tipo de limites de serviço.
7. Em New limit value (Novo valor do limite), insira o valor que deseja.
8. (Opcional) Para solicitar outro aumento, escolha Add another request (Adicionar outra solicitação).
9. Em Case description (Descrição do caso), descreva seu caso de suporte.
10. Na página Contact options (Opções de contato), escolha seu idioma preferencial e como deseja ser contatado. Você pode escolher uma das seguintes opções:

    - Web: receba uma resposta no Support Center.
    - Chat (Bate-papo): inicie um bate-papo ao vivo com um agente de suporte. Se você não conseguir se conectar a um chat, consulte Solução de problemas.
    - Phone (Telefone) - Recebe uma chamada telefônica de um agente de suporte. Se você escolher essa opção, insira as seguintes informações:
        - Country/Region (País/região)
        - Número de telefone
        - (Optional) Extension ([Opcional] Ramal)
11. Selecione Submit (Enviar). O número do ID do caso e o resumo são exibidos.

Atualizar, resolver e reabrir um caso

Depois de criar seu caso de suporte, é possível monitorar o status do caso na Central de Suporte. Um novo caso começa com o estado Unassigned (Não atribuído). Quando um agente de suporte começar a trabalhar em um caso, o status será alterado para Work in Progress (Trabalho em andamento). O agente de suporte responderá ao seu caso, para solicitar mais informações, consulte (Pending Customer Action (Ação pendente do cliente)) ou para saber se o caso está sendo investigado (Pending Amazon Action) (Ação pendente da Amazon)).

Quando o seu caso é atualizado, você recebe e-mail com a correspondência e um link para o caso na Central de Suporte. Use o link no e-mail para navegar até o caso de suporte. No entanto, não é possível responder a correspondência do caso por e-mail.

Observações

- É necessário fazer login na Conta da AWS que enviou o caso de suporte. Se você fizer login como um usuário do AWS Identity and Access Management (IAM), precisará ter as permissões necessárias para visualizar casos de suporte. Para obter mais informações, consulte Gerencie o acesso ao AWS Support Centro.
- Se você não responder ao caso em alguns dias, o AWS Support resolverá o caso automaticamente.
- Casos de Support que estiveram no estado resolvido há mais de 14 dias não podem ser reabertos. Se você tiver um problema semelhante relacionado ao caso resolvido, será possível criar um caso relacionado. Para obter mais informações, consulte Abrir um caso relacionado.

Tópicos

- Atualizar um caso de suporte existente
- Resolver um caso de suporte
- Reabrir um caso resolvido
- Abrir um caso relacionado
- Histórico de caso

Atualizar um caso de suporte existente

Você pode atualizar seu caso para fornecer mais informações para o atendente de suporte. Por exemplo, é possível responder a correspondências, iniciar outro chat ao vivo, adicionar destinatários de e-mail extras e assim por diante. Contudo, não é possível atualizar a gravidade de um caso após criá-lo. Para obter mais informações, consulte Escolher uma gravidade.

Para atualizar um caso de suporte existente

1. Faça login no AWS Support Center Console.

> **Tip**
>
> No AWS Management Console, você também pode escolher o ícone de ponto de interrogação
> ()
> e escolher Support Center.

2. Em Open support cases (Abrir casos de suporte), escolha a opção Subject (Assunto) do caso de suporte.
3. Selecione Reply (Responder). Na seção Correspondence (Correspondência), você também pode fazer uma ou todas as alterações a seguir:
   - Forneça as informações solicitadas pelo atendente de suporte
   - Fazer upload de anexos de arquivos
   - Alterar seu método de contato preferido
   - Adicionar endereços de e-mail para receber atualizações de casos
4. Selecione Submit (Enviar).

> **Tip**
>
> Se você fechar a janela de chat e quiser iniciar outro chat ao vivo, poderá adicionar uma Reply (Resposta) ao seu caso de suporte, escolher Chat e Submit (Enviar). Uma nova janela pop-up de chat é aberta.

Resolver um caso de suporte

Quando estiver satisfeito com a resposta ou quando o problema for resolvido, será possível resolver o caso na Central de Suporte.

Para resolver um caso de suporte

1. Faça login no AWS Support Center Console.

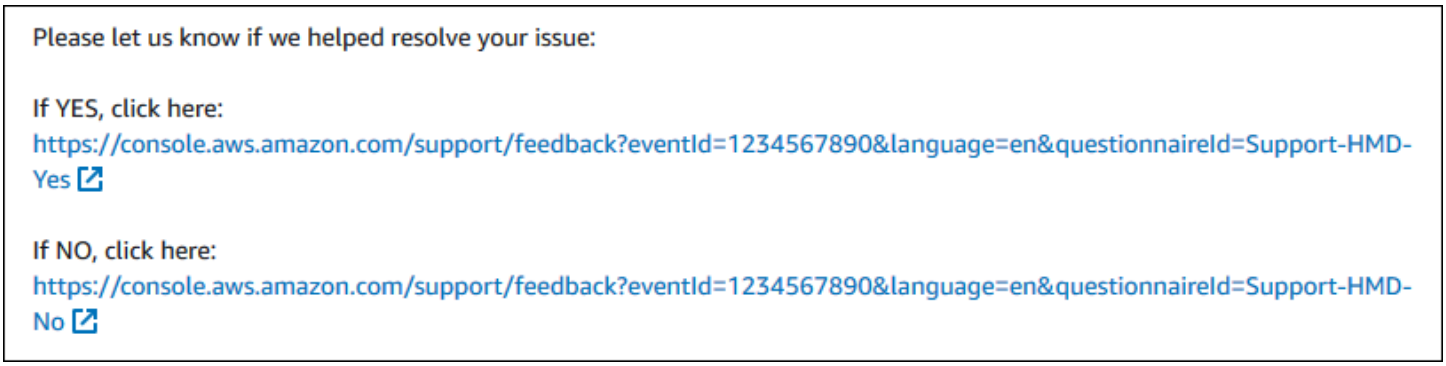
> **Tip**
>
> No AWS Management Console, você também pode escolher o ícone de ponto de interrogação
> ()
> e escolher Support Center.

2. Em Open support cases (Abrir casos de suporte), escolha a opção Subject (Assunto) do caso de suporte que você deseja resolver.
3. (Opcional) Escolha Reply (Responder) e em Correspondence (Correspondência), insira por que você está resolvendo o caso e escolha Submit (Enviar. Por exemplo, é possível inserir informações sobre como você mesmo corrigiu o problema caso precise dessas informações para referência futura.
4. Escolha Resolve case (Resolver caso).
5. Na caixa de diálogo, escolha OK para resolver o caso.

> **Note**
>
> Se o AWS Support tiver resolvido o caso para você, será possível usar o link de comentários para fornecer mais informações sobre a sua experiência com o AWS Support.

Example : Links de comentários

A captura de tela a seguir mostra os links de comentários na correspondência de um caso na Central de Suporte.



Reabrir um caso resolvido

Se você estiver enfrentando o mesmo problema novamente, será possível reabrir o caso original. Forneça detalhes sobre quando o problema ocorreu novamente e quais etapas de solução de problemas você tentou. Inclua todos os números de caso relacionados para que o atendente de suporte possa consultar as correspondências anteriores.

> **Observações**
>
> - É possível reabrir seu caso de suporte até 14 dias a partir do momento em que o problema foi resolvido. No entanto, não é possível reabrir um caso que esteja inativo há mais de 14 dias. É possível criar um novo caso ou um caso relacionado. Para obter mais informações, consulte Abrir um caso relacionado.
> - Se você reabrir um caso existente que tenha informações diferentes do problema atual, o atendente do suporte poderá solicitar que você crie um novo caso.

Como reabrir um caso resolvido

1. Faça login no AWS Support Center Console.

   > **Tip**
   >
   > No AWS Management Console, você também pode escolher o ícone de ponto de interrogação
   > ()
   > e escolher Support Center.

2. Escolha View all cases (Visualizar todos os casos) e, em seguida, escolha Subject (Assunto) ou Case ID (ID do Caso) do caso de suporte que você deseja reabrir.
3. Selecione Reopen case (Reabrir caso).
4. Em Correspondence (Correspondência), em Reply (Responder), insira os detalhes do caso.
5. (Opcional) Escolha Choose files (Escolher arquivos) para anexar arquivos ao seu caso. É possível anexar até 3 arquivos.
6. Em Select methods (Selecionar métodos), escolha uma das seguintes opções:
   - Web - Seja notificado por e-mail e pela Central de Suporte.

- Chat (Bate–papo) - Converse online com um agente de suporte.
- Phone (Telefone) - Recebe uma chamada telefônica de um agente de suporte.

7. (Opcional) Em Additional contacts (Contatos adicionais), insira endereços de e-mail de outras pessoas que você deseja que recebam correspondências sobre o caso.
8. Revise os detalhes do seu caso e escolha Submit (Enviar).

Abrir um caso relacionado

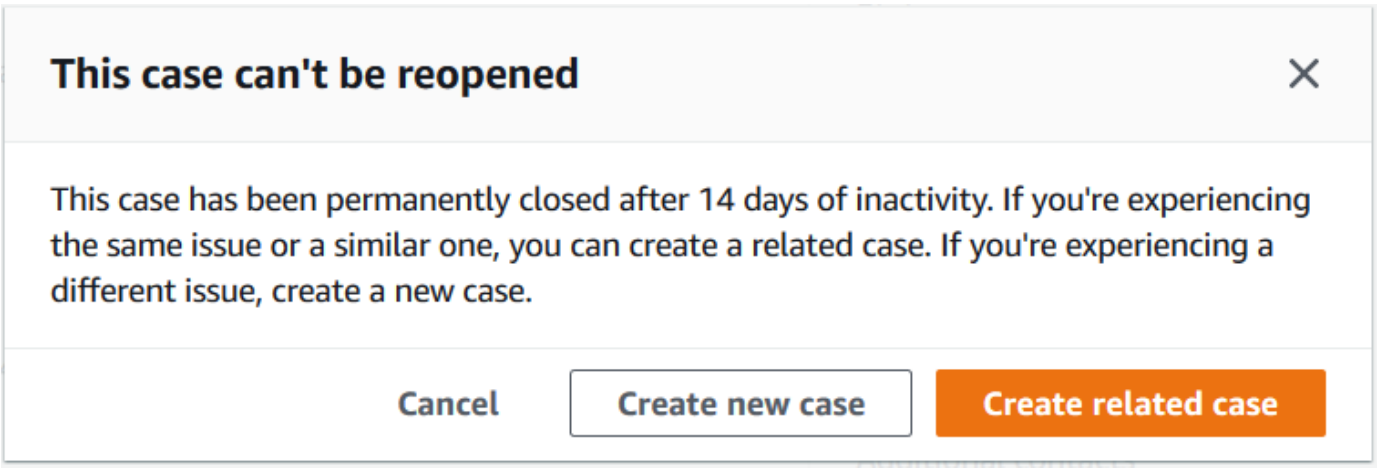
Após 14 dias de inatividade, você não poderá reabrir um caso resolvido. Se você tiver um problema semelhante relacionado ao caso resolvido, será possível criar um caso relacionado. Esse caso relacionado incluirá um link para o caso resolvido anteriormente para que o atendente do suporte possa analisar os detalhes do caso anterior e as correspondências. Se você estiver enfrentando um problema diferente, recomendamos que abra um novo caso.

Como abrir um caso relacionado

1. Faça login no AWS Support Center Console.

> **Tip**
>
> No AWS Management Console, você também pode escolher o ícone de ponto de interrogação
> ()
> e escolher Support Center.

2. Escolha View all cases (Visualizar todos os casos) e, em seguida, escolha Subject (Assunto) ou Case ID (ID do Caso) do caso de suporte que você deseja reabrir.
3. Selecione Reopen case (Reabrir caso).
4. Na caixa de diálogo, escolha Create related case (Criar caso relacionado). As informações do caso anterior serão adicionadas automaticamente ao seu caso relacionado. Se você tiver um problema diferente, escolha Create new case (Criar novo caso).

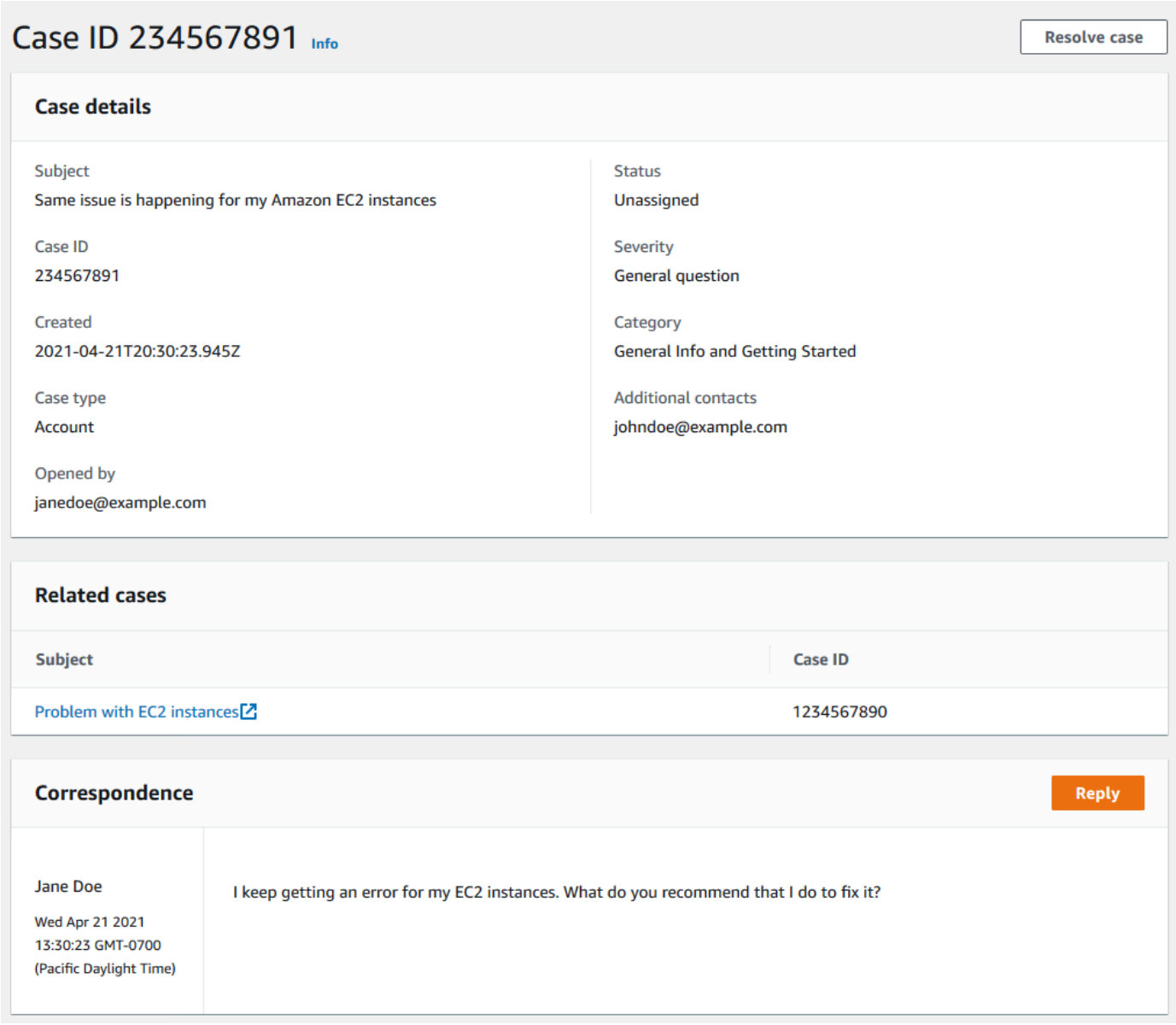


5. Siga estas etapas para criar o seu caso. Consulte Criar um caso de suporte.

> **Note**
>
> Por padrão, seu caso relacionado tem Type (Tipo), Category (Categoria) e Severity (Gravidade) iguais ao caso anterior. É possível atualizar os detalhes do caso conforme necessário.

6. Revise os detalhes do seu caso e escolha Submit (Enviar).

   Depois de criar o caso, o caso anterior aparecerá na seção Related cases (Casos relacionados), como no exemplo a seguir.



Histórico de caso

Você pode visualizar as informações do histórico do caso até 24 meses após a criação dele.

Solução de problemas

Se estiver enfrentando dificuldades ao criar ou gerenciar seu caso de suporte, consulte as informações de solução de problemas a seguir.

Quero reabrir um chat ao vivo para o meu caso

Você pode responder ao seu caso de suporte existente para abrir outra janela de chat. Para obter mais informações, consulte Atualizar um caso de suporte existente.

Não consigo me conectar ao chat ao vivo

Se você escolheu a opção Chat, mas não consegue se conectar à janela de chat, execute primeiro as verificações a seguir:

- Verifique se você configurou seu navegador para permitir janelas pop-up na Central de Suporte.

> **Note**
>
> Revise as configurações do seu navegador. Para obter mais informações, consulte os sites de Ajuda do Chrome e Suporte do Firefox.

- Verifique se você configurou sua rede para poder usar o AWS Support:
  - Sua rede pode acessar o endpoint `*.connect.us-east-1.amazonaws.com`.

> **Note**
>
> Para AWS GovCloud (US), o endpoint é `*.connect-fips.us-east-1.amazonaws.com`.

  - Seu firewall oferece suporte a conexões de soquete da Web.

Se, mesmo assim, você não conseguir se conectar à janela de chat, entre em contato com o AWS Support usando as opções de contato por e-mail ou telefone.

Usar o AWS Support com um SDK da AWS

Os kits de desenvolvimento de software (SDKs) da AWS estão disponíveis para muitas linguagens de programação populares. Cada SDK fornece uma API, exemplos de código e documentação que facilitam a criação de aplicações em seu idioma preferido pelos desenvolvedores.

Documentação do SDK	Exemplos de código
AWS SDK for C++	Exemplos de código do AWS SDK for C++
AWS SDK for Go	Exemplos de código do AWS SDK for Go
AWS SDK for Java	Exemplos de código do AWS SDK for Java
AWS SDK for JavaScript	Exemplos de código do AWS SDK for JavaScript
AWS SDK para Kotlin	Exemplos de código do AWS SDK para Kotlin
AWS SDK for .NET	Exemplos de código do AWS SDK for .NET
AWS SDK for PHP	Exemplos de código do AWS SDK for PHP
AWS SDK for Python (Boto3)	Exemplos de código do AWS SDK for Python (Boto3)
AWS SDK for Ruby	Exemplos de código do AWS SDK for Ruby
AWS SDK para Rust	Exemplos de código do AWS SDK para Rust
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

Exemplo de disponibilidade

Você não consegue encontrar o que precisa? Solicite um código de exemplo no link Fornecer feedback na parte inferior desta página.

Sobre a API do AWS Support

A API do AWS Support fornece acesso a alguns dos recursos da Central de Suporte da AWS.

A API fornece dois grupos de operações diferentes:

- Operações Gerenciamento de casos de suporte para gerenciar todo o ciclo de vida de seus casos de suporte da AWS, desde a abertura de um caso à sua resolução
- Operações AWS Trusted Advisor para acessar verificações do AWS Trusted Advisor

> **Note**
>
> É necessário ter um plano de suporte Business, Enterprise On-Ramp ou Enterprise para usar a API do AWS Support. Para obter mais informações, consulte AWS Support.

Para obter mais informações sobre as operações e os tipos de dados fornecidos peloAWS Support, consulte a Referência de API do AWS Support.

Tópicos

- Gerenciamento de casos de suporte
- AWS Trusted Advisor
- Endpoints
- Suporte nos SDKs da AWS

Gerenciamento de casos de suporte

É possível usar a API para realizar as seguintes tarefas:

- Abrir um caso de suporte
- Obter uma lista e informações detalhadas sobre os casos de suporte recentes
- Filtrar a pesquisa de casos de suporte por datas e identificadores de caso, incluindo os casos resolvidos

- Adicione comunicações e anexos de arquivo aos seus casos e adicione os destinatários do e-mail para correspondências de casos. É possível anexar até três arquivos. Cada arquivo pode ter até 5 MB
- Resolver seus casos

A AWS Support API oferece suporte ao CloudTrail registro para operações de gerenciamento de casos de suporte. Para obter mais informações, consulte Registrar em log chamadas de API do AWS Support com o AWS CloudTrail.

Para obter exemplos de código que demonstram como gerenciar todo o ciclo de vida de um caso de suporte, consulte Code examples for AWS Support using AWS SDKs.

AWS Trusted Advisor

É possível usar as operações do Trusted Advisor para executar as seguintes tarefas:

- Obtenha nomes e identificadores para as verificações do Trusted Advisor.
- Solicitar que uma verificação do Trusted Advisor seja realizada na conta e recursos da AWS
- Obter resumos e informações detalhadas para suas verificações do Trusted Advisor
- Atualizar as verificações do Trusted Advisor
- Obter o status de cada verificação do Trusted Advisor

A AWS Support API oferece suporte CloudTrail ao registro de Trusted Advisor operações. Para obter mais informações, consulte Informações do AWS Trusted Advisor no registro do CloudTrail.

Você pode usar o Amazon CloudWatch Events para monitorar as alterações nos resultados da sua verificação paraTrusted Advisor. Para obter mais informações, consulte Monitorando resultados de AWS Trusted Advisor cheques com a Amazon EventBridge.

Por ver um exemplo do código Java que demonstra como usar as operações Trusted Advisor, consulte Usar o Trusted Advisor como um web service.

Endpoints

O AWS Support é um serviço global. Isso significa que qualquer endpoint que você usar atualizará seus casos de suporte no console da Central de suporte.

Por exemplo, se você usar o endpoint Leste dos EUA (Norte da Virgínia) para criar um caso, poderá usar o endpoint Oeste dos EUA (Oregon) ou Europa (Irlanda) para adicionar uma correspondência ao mesmo caso.

É possível usar os seguintes endpoints com a API do AWS Support:

- Leste dos EUA (Norte da Virgínia): https://support.us-east-1.amazonaws.com
- Oeste dos EUA (Oregon): https://support.us-west-2.amazonaws.com
- Europa (Irlanda): https://support.eu-west-1.amazonaws.com

> **Important**
>
> - Se você chamar a CreateCaseoperação para criar casos de suporte de teste, recomendamos que você inclua uma linha de assunto, como TEST CASE-Ignore. Depois de concluir seu caso de suporte de teste, chame a ResolveCaseoperação para resolvê-lo.
> - Para chamar as operações do AWS Trusted Advisor na API do AWS Support, é necessário usar o endpoint Leste dos EUA (Norte da Virgínia). Atualmente, os endpoints Oeste dos EUA (Oregon) e Europa (Irlanda) não oferecem suporte às operações do Trusted Advisor.

Para obter mais informações sobre endpoints da AWS, consulte AWS Support endpoints and quotas, na Referência geral da Amazon Web Services.

Suporte nos SDKs da AWS

A AWS Command Line Interface (AWS CLI) e os Kits de desenvolvimento de software (SDKs) da AWS incluem suporte para a API do AWS Support.

Para obter uma lista de linguagens compatíveis com a AWS Support API, escolha um nome de operação CreateCase, como, e na seção Consulte também, escolha seu idioma preferido.

AWS Support Planos

Você pode alterar AWS Support os planos da sua conta com base nas necessidades da sua empresa.

Tópicos

- Características dos AWS Support planos
- Mudando AWS Support os planos

Características dos AWS Support planos

AWS Support oferece cinco planos de suporte:

- Basic
- Desenvolvedor
- Business
- Enterprise On-Ramp
- Enterprise

O plano Básico é gratuito e oferece suporte para dúvidas sobre contas e faturamento e aumentos de cotas de serviços. Os outros planos oferecem vários casos de suporte técnico com pay-by-the-month preços e sem contratos de longo prazo.

Todos os AWS clientes têm acesso automático 24 horas por dia, 7 dias por semana, a esses recursos do Basic Support:

- O ne-on-one respostas às perguntas sobre contas e faturamento
- Fóruns de suporte
- Verificações de integridade de serviços
- Documentação, whitepapers e guias sobre práticas recomendadas

Os clientes com um plano de suporte Desenvolvedor têm acesso a estes recursos adicionais:

- Orientação sobre as melhores práticas
- Ferramentas de diagnóstico do lado do cliente

- Suporte de arquitetura básica: orientação sobre como usar AWS produtos, recursos e serviços juntos
- Oferece suporte a um número ilimitado de casos de suporte que podem ser abertos por qualquer usuário com permissões.

Além disso, os clientes com um plano de suporte Business, Enterprise On-Ramp ou Enterprise têm acesso a estes recursos:

- Orientação de caso de uso — quais AWS produtos, recursos e serviços usar para melhor atender às suas necessidades específicas.
- AWS Trusted Advisor— Um recurso do AWS Support, que inspeciona os ambientes dos clientes e identifica oportunidades de economizar dinheiro, fechar lacunas de segurança e melhorar a confiabilidade e o desempenho do sistema. Você pode acessar todos os Trusted Advisor cheques.
- A AWS Support API para interagir com o Support Center Trusted Advisor e. É possível usar a API do AWS Support para automatizar o gerenciamento do caso de suporte e as operações do Trusted Advisor .
- Suporte a software de terceiros - Ajuda com sistemas operacionais e a configuração de instâncias do Amazon Elastic Compute Cloud (Amazon EC2). Além disso, ajude com o desempenho dos componentes de software de terceiros mais populares do AWS. O suporte a software de terceiros não está disponível para clientes dos planos de suporte Basic ou Developer.
- Oferece suporte a um número ilimitado de usuários AWS Identity and Access Management (IAM) que podem abrir casos de suporte técnico.

Além disso, os clientes com um plano de suporte Enterprise On-Ramp ou Enterprise têm acesso a estes recursos:

- Orientação sobre arquitetura de aplicação - Orientações consultivas sobre como os serviços operam em conjunto para atender a casos de uso, workloads ou aplicações específicos.
- Gerenciamento de eventos de infraestrutura- Engajamento de curto prazo com o AWS Support para obter uma compreensão profunda do caso de uso. Após a análise, forneça orientações sobre arquitetura e escalabilidade para um evento.
- Gerente de conta técnico - Trabalhe com um gerente de conta técnico (TAM) para seus casos de uso e aplicações específicas.
- Roteamento de casos "white-glove"
- Análises empresariais de gerenciamento.

Para obter mais informações sobre os recursos e preços de cada plano de suporte, consulte AWS Supporte compare AWS Support os planos. Alguns recursos, como suporte por telefone e chat 24 horas por dia, 7 dias por semana, não estão disponíveis em todos os idiomas.

Mudando AWS Support os planos

Você pode usar o console AWS Support Planos para alterar seu plano de suporte para o seu Conta da AWS. Para alterar seu plano de suporte, você precisa ter permissões AWS Identity and Access Management (IAM) ou entrar na sua conta como usuário root. Para obter mais informações, consulte Gerencie o acesso aos AWS Support planos e AWS políticas gerenciadas para AWS Support planos.

Como alterar o plano de suporte

1. Faça login no console AWS Support Planos em https://console.aws.amazon.com/support/plans/home.
2. (Opcional) Na página Planos do AWS Support , compare os planos de suporte. Para obter mais informações sobre a definição de preço, consulte a página pricing detail (detalhe de definição de preço).
3. (Opcional) Em Exemplo de preço do AWS Support , escolha Ver exemplos e escolha uma das opções do plano de suporte para ver o custo estimado.
4. Ao decidir sobre um plano, escolha Review downgrade (Revisar o downgrade) ou Review upgrade (Revisar upgrade) para o plano que você deseja.

   Observações

   - Caso se inscreva em um plano de suporte pago, você é responsável por uma assinatura mínima de um mês do AWS Support. Para obter mais informações, consulte as Perguntas frequentes do AWS Support.
   - Se você tiver um plano de suporte Enterprise On-Ramp ou Enterprise, na caixa de diálogo Change plan confirmation (Alterar confirmação de plano), entre em contato com o AWS Support para alterar o plano de suporte.

5. Na caixa de diálogo Change plan confirmation (Alterar a confirmação de plano), você pode expandir os itens de suporte para ver os recursos que deseja adicionar ou remover da sua conta.

Em Pricing (Definição de preços), você pode visualizar as cobranças únicas projetadas para o novo plano de suporte.

6. Escolha Accept and agree (Aceitar e concordar).

Informações relacionadas

Para obter mais informações sobre AWS Support os planos, consulte as AWS Support perguntas frequentes. Você também pode escolher Contact us (Fale conosco) no console dos planos de suporte.

Para fechar a conta, consulte, Fechar uma conta no Manual do usuário do AWS Billing .

AWS Trusted Advisor

Trusted Advisor baseia-se nas melhores práticas aprendidas ao atender centenas de milhares de AWS clientes. Trusted Advisor inspeciona seu AWS ambiente e, em seguida, faz recomendações quando existem oportunidades para economizar dinheiro, melhorar a disponibilidade e o desempenho do sistema ou ajudar a fechar lacunas de segurança.

Se você tiver um plano Basic ou Developer Support, poderá usar o Trusted Advisor console para acessar todas as verificações na categoria Limites de Serviço e seis verificações na categoria Segurança.

Se você tiver um plano Business, Enterprise On-Ramp ou Enterprise Support, poderá usar o Trusted Advisor console e a AWS Trusted Advisor API para acessar todas as Trusted Advisor verificações. Você também pode usar o Amazon CloudWatch Events para monitorar o status dos Trusted Advisor cheques. Para ter mais informações, consulte Monitorando resultados de AWS Trusted Advisor cheques com a Amazon EventBridge.

Você pode acessar Trusted Advisor no AWS Management Console. Para obter mais informações sobre como controlar o acesso ao Trusted Advisor console, consulteGerencie o acesso ao AWS Trusted Advisor.

Para ter mais informações, consulte Trusted Advisor.

Tópicos

- Conceitos básicos das recomendações do Trusted Advisor
- Comece a usar a Trusted Advisor API
- Usar o Trusted Advisor como um web service
- Visualização organizacional para AWS Trusted Advisor
- Exibir as verificações do AWS Trusted Advisor fornecidas pelo AWS Config
- Visualizar os controles do AWS Security Hub no AWS Trusted Advisor
- Optar por verificações do Trusted Advisor para o AWS Compute Optimizer
- Conceitos básicos do AWS Trusted Advisor Priority
- Comece a usar o AWS Trusted Advisor Engage (versão pré-visualização)
- Referência de verificação do AWS Trusted Advisor
- Registro de alterações para AWS Trusted Advisor

Conceitos básicos das recomendações do Trusted Advisor

Você pode usar a página Recomendações do Trusted Advisor do console do Trusted Advisor para revisar os resultados da verificação da sua Conta da AWS e seguir as etapas recomendadas para corrigir qualquer problema. Por exemplo, o Trusted Advisor pode recomendar que você exclua recursos não utilizados para reduzir sua fatura mensal, como uma instância do Amazon Elastic Compute Cloud (Amazon EC2).

Também é possível usar a API do AWS Trusted Advisor para executar operações nas verificações Trusted Advisor. Para obter mais informações, consulte a Referência de APIs do AWS Trusted Advisor

Tópicos

- Fazer login no console do Trusted Advisor
- Visualizar categorias de verificação
- Visualizar verificações específicas
- Filtrar as verificações
- Atualizar resultados da verificação
- Baixar dos resultados
- Visualização organizacional
- Preferences

Fazer login no console do Trusted Advisor

É possível visualizar as verificações e o status de cada verificação no console do Trusted Advisor.

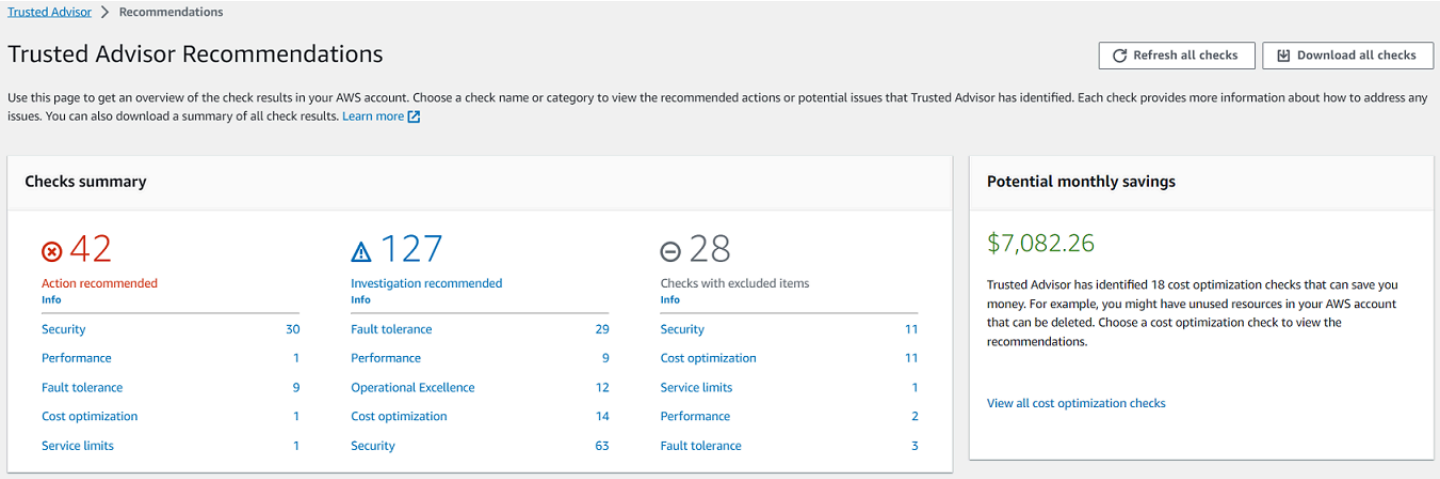
> **Note**
>
> É necessário ter um conjunto mínimo de permissões do AWS Identity and Access Management (IAM) para acessar o console do Trusted Advisor. Para obter mais informações, consulte Gerencie o acesso ao AWS Trusted Advisor.

Como fazer login no console do Trusted Advisor

1. Faça login no console do Trusted Advisor em https://console.aws.amazon.com/trustedadvisor/home.
2. Na página Recomendações do Trusted Advisor, visualize o resumo de cada categoria de verificação:
   - Ação recomendada (vermelho) - O Trusted Advisor recomenda uma ação para a verificação. Por exemplo, uma verificação que detecta um problema de segurança para seus recursos do IAM pode recomendar etapas urgentes.
   - Investigação recomendada (amarelo) - Trusted Advisordetecta um possível problema para a verificação. Por exemplo, uma verificação que atinge uma cota para um recurso pode recomendar maneiras de excluir recursos não utilizados.
   - Verificações com itens excluídos (cinza): o número de verificações que excluíram itens, como recursos que você deseja que uma verificação ignore. Por exemplo, isso pode ser instâncias do Amazon EC2 que você não deseja que a verificação avalie.
3. Na página Recomendações do Trusted Advisor, você pode fazer o seguinte:
   - Para atualizar todas as verificações na conta, escolha Refresh all checks (Atualizar todas as verificações).
   - Para criar um arquivo .xls que inclua todos os resultados da verificação, escolha Download all checks (Baixar todas as verificações).
   - Em Checks summary (Resumo de verificações), escolha uma categoria de verificação, como Security (Segurança), para visualizar os resultados.
   - Em Potential monthly savings (Possíveis economias mensais), você pode ver o quanto é possível economizar em sua conta e as obter recomendações nas verificações de otimização de custos.
   - Em Recent changes (Alterações recentes), é possível exibir alterações para verificar status dos últimos 30 dias. Escolha um nome de verificação para exibir os seus resultados mais recentes ou escolha o ícone de seta para exibir a próxima página.

Example : recomendações do Trusted Advisor

O exemplo a seguir mostra um resumo dos resultados da verificação para uma Conta da AWS.



Visualizar categorias de verificação

É possível exibir as descrições da verificação e os resultados das seguintes categorias de verificação:

- Otimização de custos - Recomendações que podem economizar dinheiro. Essas verificações destacam recursos não utilizados e oportunidades para reduzir sua fatura.
- Performance - Recomendações que podem melhorar a velocidade e a capacidade de resposta de suas aplicações.
- Segurança - Recomendações para configurações de segurança que podem tornar a solução da AWS mais segura.
- Tolerância a falhas - Recomendações que ajudam a aumentar a resiliência da sua solução da AWS. Essas verificações destacam deficiências de redundância e recursos usados em excesso.
- Limites de serviço - Verifica o uso de sua conta e se sua conta se aproxima ou excede o limite (também conhecido como cotas) para serviços e recursos da AWS.
- Excelência operacional: recomendações para ajudar você a operar seu ambiente da AWS de forma eficaz e em grande escala.

Para visualizar categorias de verificação

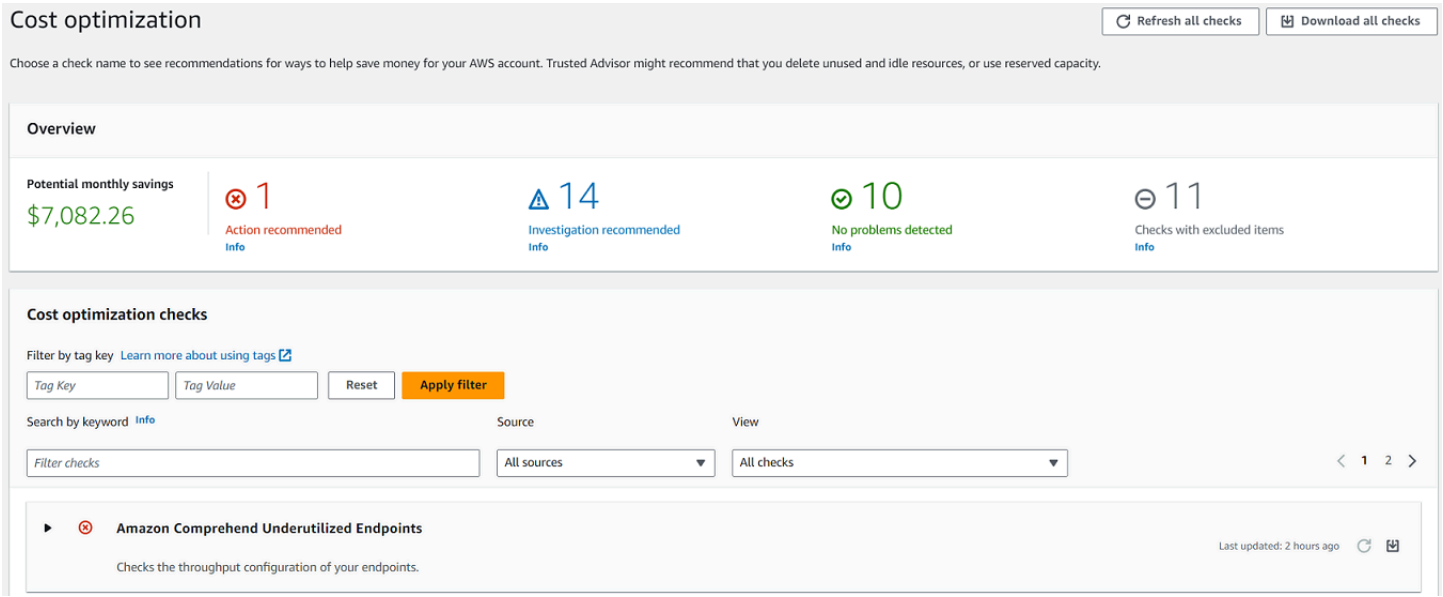
1. Faça login no console do Trusted Advisor em https://console.aws.amazon.com/trustedadvisor/home.
2. No painel de navegação, escolha a categoria de custo.
3. Na página de categoria, exiba o resumo de cada categoria de verificação:

- Ação recomendada (vermelho) - O Trusted Advisor recomenda uma ação para a verificação.
- Investigação recomendada (amarelo) - Trusted Advisordetecta um possível problema para a verificação.
- Nenhum problema detectado (verde) - o Trusted Advisor não detecta um problema para a verificação.
- Itens excluídos (cinza) - O número de verificações que excluíram itens, como recursos que você deseja que uma verificação ignore.

4. Para cada seleção, escolha o ícone de atualização
   ( )
   para atualizar esta verificação.
5. Escolha o ícone de download
   ( )
   para criar um arquivo .xls que inclua os resultados dessa verificação.

Example : Categoria de otimização de custos

O exemplo a seguir mostra 16 verificações (verdes) que não apresentam problemas.



Visualizar verificações específicas

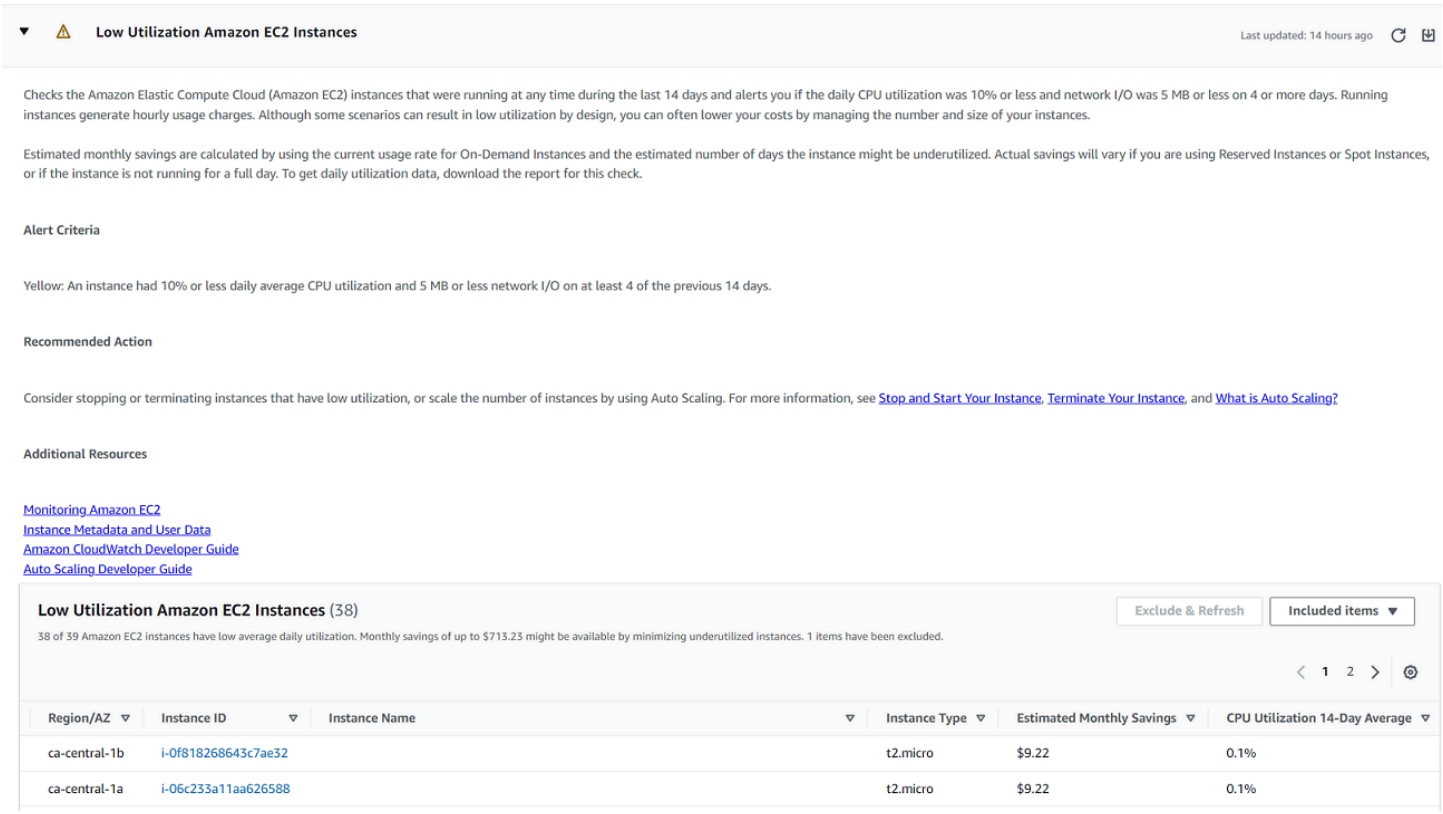
Expanda uma verificação para visualizar a sua descrição completa, os recursos afetados, quaisquer etapas recomendadas e links para mais informações.

Para exibir uma verificação específica

1. Faça login no console do Trusted Advisor em https://console.aws.amazon.com/trustedadvisor/home.
2. No painel de navegação, escolha uma categoria de verificação.
3. Escolha o nome da verificação para exibir a descrição e os seguintes detalhes:
   - Alert Criteria (Critérios de alerta) - Descreve o limite quando uma verificação mudará o status.
   - Recommended Action (Ação recomendada) - Descreve as ações recomendadas para esta verificação.
   - Additional Resources (Recursos adicionais) - Lista a documentação do AWS relacionada.
   - Uma tabela que lista os itens afetados na sua conta. É possível incluir ou excluir esses itens dos resultados da verificação.
4. (Opcional) Para excluir itens para que eles não apareçam nos resultados da verificação:
   a. Selecione um item e escolha Exclude & Refresh (Excluir e atualizar).
   b. Para exibir todos os itens excluídos, escolha Excluded items (Itens excluídos).
5. (Opcional) Para incluir itens para que a verificação os avalie novamente:
   a. Selecione Excluded items (Itens excluídos), selecione um item e, em seguida, selecione Include & Refresh (Incluir e atualizar).
   b. Para exibir todos os itens incluídos, escolha Included items (Itens incluídos).
6. Escolha o ícone de configurações
   ().
   Na caixa de diálogo Preferences (Preferências), especifique o número de itens ou as propriedades a serem exibidas e escolha Confirm (Confirmar).

Example : Verificação de otimização de custos

Os seguintes exemplos de Low Utilization Amazon EC2 Instances (Instâncias do Amazon EC2 com pouca utilização) lista as instâncias afetadas na conta. Essa verificação identifica 38 instâncias do Amazon EC2 que têm baixo uso e recomenda interromper ou encerrar os recursos.



Filtrar as verificações

Nas páginas de categoria de verificação, é possível especificar quais resultados de verificação você deseja exibir. Por exemplo, é possível filtrar por verificações que detectaram erros na conta, de modo que você possa investigar problemas urgentes primeiro.

Se você tiver verificações que avaliam itens na conta, como recursos do AWS, será possível usar filtros de tag para mostrar somente os itens que têm a tag especificada.

Para filtrar as verificações

1. Faça login no console do Trusted Advisor em https://console.aws.amazon.com/trustedadvisor/home.
2. No painel de navegação ou na página Recomendações do Trusted Advisor, escolha a categoria de verificação.
3. Para Search by keyword (Pesquisar por palavra-chave), insira uma palavra-chave do nome ou da descrição da verificação para filtrar os resultados.
4. Na lista View (Exibir), especifique quais verificações devem ser exibidas:

   - All checks (Todas as verificações): lista todas as verificações para esta categoria.

- Action recommended (Ação recomendada - Lista verificações que recomendam que você execute uma ação. Essas verificações são destacadas em vermelho.
- Investigation recommended (Investigação recomendada - Lista verificações que recomendam que você execute uma possível ação. Essas verificações são destacadas em amarelo.
- No problems detected (Nenhum problema detectado) - Lista verificações que não têm problemas. Essas verificações são destacadas em verde.
- Checks with excluded items (Verificações com itens excluídos) - Lista verificações que você especificou para excluir itens dos resultados da verificação.

5. Se você adicionou tags aos recursos do AWS, como instâncias do Amazon EC2 ou trilhas do AWS CloudTrail, é possível filtrar seus resultados para que as verificações só mostrem itens com a tag especificada.

   Em Filter by tag (Filtrar por tag), insira uma chave e um valor de tag e, em seguida, escolha Apply filter (Aplicar filtro).
6. Na tabela de verificação, os resultados da verificação mostram apenas itens que têm a chave e o valor especificados.
7. Para limpar o filtro de tags, escolha Reset (Redefinir).

Informações relacionadas

Para obter mais informações sobre a marcação de objetos para Trusted Advisor, consulte os seguintes tópicos:

- O AWS Support habilita recursos de marcação para o Trusted Advisor
- Tagging AWS resources na Referência geral da AWS

Atualizar resultados da verificação

É possível atualizar as verificações para obter os resultados mais recentes da sua conta. Se tiver um plano Developer ou Basic Support, você poderá fazer login no console do Trusted Advisor para atualizar as verificações. Se você tiver um plano de suporte Business, Enterprise On-Ramp ou Enterprise, o Trusted Advisor atualizará automaticamente as verificações em sua conta semanalmente.

Para atualizar as verificações do Trusted Advisor

1. Navegue até o console do AWS Trusted Advisor em https://console.aws.amazon.com/trustedadvisor.
2. Na página Recomendações do Trusted Advisor ou em uma página de categoria de verificação, escolha Atualizar todas as verificações.

Também é possível atualizar verificações específicas das seguintes maneiras:

- Escolha o ícone de atualização
  ()
  para fazer uma verificação individual.
- Use a RefreshTrustedAdvisorCheck operação de API.

> Observações
>
> - O Trusted Advisor atualiza automaticamente algumas verificações várias vezes ao dia, como a verificação de problemas de alto risco para a confiabilidade do AWS Well-Architected. Pode levar algumas horas para as alterações aparecerem na conta. Para essas verificações atualizadas automaticamente, não é possível escolher o ícone de atualização
>   ()
>   para atualizar manualmente os resultados.
> - Se você habilitou AWS Security Hub para sua conta, não poderá usar o console do Trusted Advisor para atualizar os controles do Security Hub. Para obter mais informações, consulte Atualizar os resultados do Security Hub.

Baixar dos resultados

É possível baixar os resultados da verificação para obter uma visão geral do Trusted Advisor em sua conta. É possível baixar os resultados de todas as verificações ou de uma verificação específica.

Baixar os resultados de verificações das recomendações do Trusted Advisor

1. Navegue até o console do AWS Trusted Advisor em https://console.aws.amazon.com/trustedadvisor.
   - Para baixar todos os resultados da verificação, na página Recomendações do Trusted Advisor ou em uma página de categoria de verificação, escolha Baixar todas as verificações.
   - Para baixar um resultado de verificação para uma verificação específica, escolha o nome da verificação e escolha o ícone de baixar ( ).
2. Salve ou abra o arquivo .xls. O arquivo contém as mesmas informações de resumo do console do Trusted Advisor, como o nome da verificação, a descrição, o status, os recursos afetados e assim por diante.

Visualização organizacional

É possível configurar o recurso de visualização organizacional para criar um relatório para todas as contas de membro da sua organização da AWS. Para obter mais informações, consulte Visualização organizacional para AWS Trusted Advisor.

Preferences

Na página Gerenciar Trusted Advisor, você pode desativar o Trusted Advisor.

Na página Notifications (Notificações), você pode configurar suas mensagens de e-mail semanais para o resumo da verificação. Consulte Configurar as preferências de notificação.

Na página Sua organização, você pode ativar ou desativar o acesso confiável com o AWS Organizations. Isso é necessário para o recurso Visualização organizacional para AWS Trusted Advisor, o Trusted Advisor Priority e o Trusted Advisor Engage.

Configurar as preferências de notificação

Especifique quem pode receber mensagens de e-mail do Trusted Advisor com resultados de verificação e o idioma. Você recebe uma notificação por e-mail sobre seu resumo de verificação para recomendações do Trusted Advisor uma vez por semana.

As notificações por e-mail para as recomendações do Trusted Advisor não incluem resultados para o Trusted Advisor Priority. Para obter mais informações, consulte Gerenciar as notificações do Trusted Advisor Priority.

Para configurar preferências de notificação

1. Faça login no console do Trusted Advisor em https://console.aws.amazon.com/trustedadvisor/home.
2. No painel de navegação, em Preferences (Preferências), escolha Notifications (Notificações).
3. Em Recommendations (Recomendações), selecione a quem notificar os resultados da verificação. É possível adicionar e remover contatos da página Account Settings (Configurações da conta) no console do AWS Billing and Cost Management.
4. Em Language (Idioma), escolha o idioma da mensagem de e-mail.
5. Escolha Save your preferences (Salvar suas preferências).

Configurar a visualização organizacional

Se você configurar a conta do com o AWS Organizations, será possível criar relatórios para todas as contas-membro de sua organização. Para obter mais informações, consulte Visualização organizacional para AWS Trusted Advisor.

Desabilitar Trusted Advisor

Quando você desabilitar esse serviço, o Trusted Advisor não efetuará nenhuma verificação na sua conta. Qualquer pessoa que tentar acessar o console do Trusted Advisor ou usar as operações da API receberá uma mensagem de acesso negado.

Para desabilitar o Trusted Advisor

1. Faça login no console do Trusted Advisor em https://console.aws.amazon.com/trustedadvisor/home.
2. No painel de navegação, em Preferências, escolha Gerenciar o Trusted Advisor.
3. Em Trusted Advisor, desative Enabled (Habilitado). Essa ação desabilita o Trusted Advisor para todas as verificações na conta.
4. Em seguida, você pode excluir manualmente a da sua conta. Para obter mais informações, consulte Excluir uma função vinculada ao serviço para o Trusted Advisor.

Informações relacionadas

Para obter mais informações sobre o Trusted Advisor, consulte os seguintes tópicos:

- Como começo a usar o Trusted Advisor?
- Referência de verificação do AWS Trusted Advisor

Comece a usar a Trusted Advisor API

A Referência da AWS Trusted Advisor API é destinada a programadores que precisam de informações detalhadas sobre as operações da Trusted Advisor API e os tipos de dados. Essa API fornece acesso às Trusted Advisor recomendações para sua conta ou para todas as contas da sua AWS organização. A Trusted Advisor API usa métodos HTTP que retornam resultados no formato JSON.

> **Note**
>
> - Você deve ter um plano Business, Enterprise On-Ramp ou Enterprise Support para usar a API Trusted Advisor
> - Se você chamar a AWS Trusted Advisor API de uma conta que não tem um plano Business, Enterprise On-Ramp ou Enterprise Support, receberá uma exceção de Access Denied. Para obter mais informações sobre como alterar seu plano de suporte, consulte AWS Support.

Você pode usar a AWS Trusted Advisor API para obter uma lista de verificações e suas descrições, recomendações e recursos para recomendações. Você também pode atualizar o ciclo de vida das recomendações. Para gerenciar recomendações, use as seguintes operações de API:

- Use as operações ListChecksListRecommendations, GetRecommendation, e ListRecommendationResourcesda API para ver recomendações e contas e recursos correspondentes.
- Use a operação da UpdateRecommendationLifecycleAPI para atualizar o ciclo de vida de uma recomendação gerenciada pela Trusted Advisor Priority.
- As chamadas ListOrganizationRecommendationsGetOrganizationRecommendation, ListOrganizationRecommendationResources, ListOrganizationRecommendationAccounts, e de

UpdateOrganizationRecommendationLifecycleAPI oferecem suporte somente às recomendações gerenciadas pela Trusted Advisor Priority. Essas recomendações também são chamadas de recomendações priorizadas. Você pode visualizar e gerenciar suas recomendações priorizadas em uma conta administrativa ou de administrador delegado se tiver ativado o Trusted Advisor Priority. Se a Prioridade não estiver ativada, você receberá uma exceção de Acesso Negado ao fazer solicitações.

Para obter mais informações, consulte AWS Trusted Advisor o AWS Support User Guide.

Para autenticação de solicitações, consulte o Processo de assinatura da versão 4 do Signature.

Usar o Trusted Advisor como um web service

> **Note**
>
> Trusted Advisoras operações não serão suportadas pela Support API em 2024. Use a nova AWS Trusted AdvisorAPI para acessar programaticamente as verificações e recomendações de melhores práticas

O serviço AWS Support permite que você crie aplicativos que interajam com o AWS Trusted Advisor. Este tópico mostra como obter uma lista de verificações do Trusted Advisor, atualizar uma delas e, em seguida, obter os resultados detalhados da verificação. Estas tarefas são demonstradas em Java. Para obter informações sobre suporte a outros idiomas, consulte Ferramentas para Amazon Web Services.

Tópicos

- Obter a lista de verificações disponíveis do Trusted Advisor
- Atualizar a lista de verificações disponíveis do Trusted Advisor
- Sondar uma verificação de alterações de status do Trusted Advisor
- Solicitar um resultado de verificação do Trusted Advisor
- Imprimir detalhes de uma verificação do Trusted Advisor

Obter a lista de verificações disponíveis do Trusted Advisor

O seguinte trecho de código Java cria uma instância de um cliente AWS Support que é possível usar para chamar todas as operações de API do Trusted Advisor. Em seguida, o código obtém a lista de Trusted Advisor verificações e seus `CheckId` valores correspondentes chamando a operação da DescribeTrustedAdvisorChecksAPI. Você pode usar essas informações para criar interfaces de usuário que permitem aos usuários selecionar a verificação que desejam executar ou atualizar.

```
private static AWSSupport createClient()
{
    return AWSSupportClientBuilder.defaultClient();
}
// Get the List of Available Trusted Advisor Checks
public static void getTAChecks() {
    // Possible language parameters: "en" (English), "ja" (Japanese), "fr" (French),
 "zh" (Chinese)
    DescribeTrustedAdvisorChecksRequest request = new
 DescribeTrustedAdvisorChecksRequest().withLanguage("en");
    DescribeTrustedAdvisorChecksResult result =
 createClient().describeTrustedAdvisorChecks(request);
    for (TrustedAdvisorCheckDescription description : result.getChecks()) {
        // Do something with check description.
        System.out.println(description.getId());
        System.out.println(description.getName());
    }
}
```

Atualizar a lista de verificações disponíveis do Trusted Advisor

O seguinte trecho de código Java cria uma instância de um cliente AWS Support que você pode usar para atualizar os dados do Trusted Advisor.

```
// Refresh a Trusted Advisor Check
// Note: Some checks are refreshed automatically, and they cannot be refreshed by using
 this operation.
// Specifying the check ID of a check that is automatically refreshed causes an
 InvalidParameterValue error.
public static void refreshTACheck(final String checkId) {
    RefreshTrustedAdvisorCheckRequest request = new
 RefreshTrustedAdvisorCheckRequest().withCheckId(checkId);
    RefreshTrustedAdvisorCheckResult result =
 createClient().refreshTrustedAdvisorCheck(request);
```

```
    System.out.println("CheckId: " + result.getStatus().getCheckId());
    System.out.println("Milliseconds until refreshable: " +
 result.getStatus().getMillisUntilNextRefreshable());
    System.out.println("Refresh Status: " + result.getStatus().getStatus());
}
```

Sondar uma verificação de alterações de status do Trusted Advisor

Depois de enviar a solicitação para executar uma Trusted Advisor verificação para gerar os dados de status mais recentes, você usa a operação da DescribeTrustedAdvisorCheckRefreshStatusesAPI para solicitar o progresso da execução da verificação e quando novos dados estiverem prontos para a verificação.

O seguinte trecho de código Java é o status da verificação solicitada na seção a seguir, usando o valor correspondente na variável `CheckId`. Além disso, o código demonstra vários outros usos do serviço Trusted Advisor:

1. Você pode chamar `getMillisUntilNextRefreshable` percorrendo os objetos contidos na instância `DescribeTrustedAdvisorCheckRefreshStatusesResult`. Você pode usar o valor retornado para testar se você deseja que seu código prossiga com a renovação da verificação.
2. Se `timeUntilRefreshable` equivaler a zero, vocÊ poderá solicitar uma atualização da verificação.
3. Usando o status retornado, você pode continuar a pesquisa de alterações de status; o trecho de código define o intervalo de pesquisa como o valor recomendado de dez segundos. Se o status for `enqueued` ou `in_progress`, o loop retornará e solicitará outro status. Se a chamada retornar `successful`, o loop será encerrado.
4. Por fim, o código retorna uma instância de um tipo de dados `DescribeTrustedAdvisorCheckResultResult` que você pode usar para percorrer as informações produzidas pela verificação.

Observação: use uma única solicitação de atualização antes da sondagem para o status da solicitação.

```
// Retrieves TA refresh statuses. Multiple checkId's can be submitted.
public static List<TrustedAdvisorCheckRefreshStatus> getTARefreshStatus(final String...
 checkIds) {
    DescribeTrustedAdvisorCheckRefreshStatusesRequest request =
```

```
            new
 DescribeTrustedAdvisorCheckRefreshStatusesRequest().withCheckIds(checkIds);
    DescribeTrustedAdvisorCheckRefreshStatusesResult result =
            createClient().describeTrustedAdvisorCheckRefreshStatuses(request);
    return result.getStatuses();
}
// Retrieves a TA check status, and checks to see if it has finished processing.
public static boolean isTACheckStatusInTerminalState(final String checkId) {
    // Since we only submitted one checkId to getTARefreshStatus, just retrieve the
 only element in the list.
    TrustedAdvisorCheckRefreshStatus status = getTARefreshStatus(checkId).get(0);
    // Valid statuses are:
    // 1. "none", the check has never been refreshed before.
    // 2. "enqueued", the check is waiting to be processed.
    // 3. "processing", the check is in the midst of being processed.
    // 4. "success", the check has succeeded and finished processing - refresh data is
 available.
    // 5. "abandoned", the check has failed to process.
    return status.getStatus().equals("abandoned") ||
 status.getStatus().equals("success");
}
// Enqueues a Trusted Advisor check refresh. Periodically polls the check refresh
 status for completion.
public static TrustedAdvisorCheckResult getFreshTACheckResult(final String checkId)
 throws InterruptedException {
    refreshTACheck(checkId);
    while(!isTACheckStatusInTerminalState(checkId)) {
        Thread.sleep(10000);
    }
    return getTACheckResult(checkId);
}
// Retrieves fresh TA check data whenever possible.
// Note: Some checks are refreshed automatically, and they cannot be refreshed by using
 this operation. This method
// is only functional for checks that can be refreshed using the
 RefreshTrustedAdvisorCheck operation.
public static void pollForTACheckResultChanges(final String checkId) throws
 InterruptedException {
    String checkResultStatus = null;
    do {
        TrustedAdvisorCheckResult result = getFreshTACheckResult(checkId);
        if (checkResultStatus != null && !checkResultStatus.equals(result.getStatus()))
 {
            break;
```

```
        }
        checkResultStatus = result.getStatus();
        // The rule refresh has completed, but due to throttling rules the checks may
 not be refreshed again
        // for a short period of time.
        // Since we only submitted one checkId to getTARefreshStatus, just retrieve the
 only element in the list.
        TrustedAdvisorCheckRefreshStatus refreshStatus =
 getTARefreshStatus(checkId).get(0);
        Thread.sleep(refreshStatus.getMillisUntilNextRefreshable());
    } while(true);
    // Signal that a TA check has changed check result status here.
}
```

Solicitar um resultado de verificação do Trusted Advisor

Depois de selecionar a verificação dos resultados detalhados que você deseja, você envia uma solicitação usando a operação da DescribeTrustedAdvisorCheckResultAPI.

> **Tip**
>
> Os nomes e descrições das verificações do Trusted Advisor estão sujeitos a alterações. Recomendamos que você especifique o ID de verificação do código para identificar exclusivamente um verificação. Você pode usar a operação da DescribeTrustedAdvisorChecksAPI para obter o ID do cheque.

O seguinte trecho de código Java usa a instância `DescribeTrustedAdvisorChecksResult` referenciada pela variável `result`, que foi obtida no trecho de código anterior. Em vez de definir uma verificação interativamente por meio de uma interface de usuário, depois que enviar a solicitação para executar o trecho, envie uma solicitação para a primeira verificação na lista a ser executada especificando um valor de índice de 0 em cada chamada `result.getChecks().get(0)`. Em seguida, o código define uma instância de `DescribeTrustedAdvisorCheckResultRequest`, e passa-a para uma instância de `DescribeTrustedAdvisorCheckResultResult` chamada `checkResult`. Você pode usar as estruturas de membro desse tipo de dados para visualizar os resultados da verificação.

```
// Request a Trusted Advisor Check Result
public static TrustedAdvisorCheckResult getTACheckResult(final String checkId) {
```

```
    DescribeTrustedAdvisorCheckResultRequest request = new
 DescribeTrustedAdvisorCheckResultRequest()
            // Possible language parameters: "en" (English), "ja" (Japanese),
 "fr" (French), "zh" (Chinese)
            .withLanguage("en")
            .withCheckId(checkId);
    DescribeTrustedAdvisorCheckResultResult requestResult =
 createClient().describeTrustedAdvisorCheckResult(request);
    return requestResult.getResult();
}
```

Observação: solicitar um resultado de verificação do Trusted Advisor não gerará dados de resultados atualizados.

Imprimir detalhes de uma verificação do Trusted Advisor

O seguinte trecho de código Java faz a iteração sobre a instância `DescribeTrustedAdvisorCheckResultResult` retornada na seção anterior para obter uma lista de recursos sinalizados pela verificação do Trusted Advisor.

```
// Print ResourceIds for flagged resources.
for (TrustedAdvisorResourceDetail flaggedResource :
    result1.getResult().getFlaggedResources())
{
    System.out.println(
        "The resource for this ResourceID has been flagged: " +
        flaggedResource.getResourceId());
}
```

Visualização organizacional para AWS Trusted Advisor

A visualização organizacional permite ver as verificações do Trusted Advisorde todas as contas do AWS Organizations. Depois de habilitar esse recurso, você poderá criar relatórios para agregar os resultados da verificação de todas as contas de membro em sua organização. O relatório inclui um resumo dos resultados da verificação e informações sobre os recursos afetados para cada conta. Por exemplo, é possível usar os relatórios para identificar quais contas da sua organização estão usando o AWS Identity and Access Management (IAM) com a verificação de Uso do IAM ou se você tiver ações recomendadas para buckets do Amazon Simple Storage Service (Amazon S3) com a verificação de Permissões de bucket do Amazon S3.

Tópicos

- Pré-requisitos
- Habilitar a visualização organizacional
- Atualizar verificações do Trusted Advisor
- Criar relatórios da visualização organizacional
- Visualize o resumo do relatório.
- Baixar um relatório da visualização organizacional
- Desabilitar a visualização organizacional
- Utilização de políticas do IAM para permitir acesso à visualização organizacional
- Usar outros serviços da AWS para visualizar relatórios do Trusted Advisor

Pré-requisitos

Você deve atender aos seguintes requisitos para habilitar a visualização organizacional:

- As suas contas devem ser membro de uma Organização AWS.
- A sua organização deve ter todos os recursos habilitados para o Organizations. Para obter mais informações, consulte Habilitar todos os recursos na sua organização no Manual do usuário do AWS Organizations.
- A conta de gerenciamento da em sua organização deve ter um plano de suporte Business, Enterprise On-Ramp ou Enterprise. É possível encontrar seu plano de suporte na Central do AWS Support ou na página Planos de suporte. Consulte Comparar planos do AWS Support.
- É necessário estar conectado como usuário na conta mestra (ou com uma função equivalente assumida). Independentemente de fazer login como um usuário do IAM ou uma função do IAM, você deverá ter uma política com as permissões necessárias. Consulte Utilização de políticas do IAM para permitir acesso à visualização organizacional.

Habilitar a visualização organizacional

Depois de atender aos pré-requisitos, siga estas etapas para habilitar o modo de visualização organizacional. Depois que você habilitar esse recurso, acontecerá o seguinte:

- O Trusted Advisor está habilitado como um serviço confiável em sua organização. Para obter mais informações sobre como habilitar o acesso confiável, consulte Habilitar acesso confiável com serviços da AWS no Manual do usuário do AWS Organizations.
- A função `AWSServiceRoleForTrustedAdvisorReporting` vinculada ao serviço é criada para você na conta de gerenciamento em sua organização. Essa função inclui as permissões que o Trusted Advisor precisa para chamar o Organizations em seu nome. Essa função vinculada ao serviço está bloqueada e não é possível excluí-la manualmente. Para obter mais informações, consulte Usar perfis vinculados ao serviço do Trusted Advisor.

É possível habilitar o modo de visualização organizacional no console do Trusted Advisor.

Para habilitar a visualização organizacional

1. Faça login como administrador na conta de gerenciamento da organização e abra o console do AWS Trusted Advisor em https://console.aws.amazon.com/trustedadvisor.
2. No painel de navegação, em Preferences (Preferências), escolha Your organization (Sua organização).
3. Em Habilitar acesso confiável com o AWS Organizations, ative a opção Habilitado.

> **Note**
>
> Habilitar a visualização organizacional para a conta de gerenciamento não fornece as mesmas verificações para todas as contas de membro. Por exemplo, se suas contas de membro tiverem suporte Básico, essas contas não terão as mesmas verificações disponíveis da sua conta de gerenciamento. O plano AWS Support determina qual verificação da Trusted Advisor está disponível para uma conta.

Atualizar verificações do Trusted Advisor

Antes de criar um relatório para sua organização, recomendamos que você atualize os status das verificações do Trusted Advisor. É possível baixar um relatório sem atualizar as verificações do Trusted Advisor, mas o relatório pode não ter as informações mais recentes.

Se você tiver um plano de suporte Business, Enterprise On-Ramp ou Enterprise, o Trusted Advisor atualizará automaticamente as verificações em sua conta semanalmente.

> **Note**
>
> Se você tiver contas em sua organização que tenham um plano de suporte Developer ou Basic, os usuários dessas contas deverão entrar no console do Trusted Advisor para atualizar as verificações. Não é possível atualizar verificações para todas as contas a partir da conta de gerenciamento da organização.

Para atualizar as verificações do Trusted Advisor

1. Navegue até o console do AWS Trusted Advisor em https://console.aws.amazon.com/trustedadvisor.
2. Na página Recomendações do Trusted Advisor, escolha Atualizar todas as verificações. Isso atualizará todas as verificações da conta.

Também é possível atualizar verificações específicas das seguintes maneiras:

- Use a operação de API RefreshTrustedAdvisorCheck.
- Escolha o ícone de atualização
  ()
  para fazer uma verificação individual.

Criar relatórios da visualização organizacional

Depois de habilitar o modo de visualização organizacional, é possível criar relatórios para exibir os resultados da verificação do Trusted Advisor para a sua organização.

É possível criar até 50 relatórios. Se você criar relatórios além dessa cota, o Trusted Advisor excluirá o relatório mais antigo. Não é possível recuperar as chaves excluídas.

Para criar relatórios da visualização organizacional

1. Faça login na conta de gerenciamento da organização e abra o console do AWS Trusted Advisor em https://console.aws.amazon.com/trustedadvisor.
2. No painel de navegação, selecione Organizational View (Visualização organizacional).
3. Escolha Create report (Criar relatório).

4. Por padrão, o relatório inclui todas as regiões da AWS, categorias de verificação, verificações e status de recursos. Na página Create report (Criar relatório), é possível usar as opções de filtro para personalizar o relatório. Por exemplo, é possível desmarcar a caixa de seleção All (Tudo) de Region (Região) e especificar as regiões individuais a serem incluídas no relatório.

   a. Insira um Name (Nome) para o relatório.

   b. Em Format, escolha JSON ou CSV.

   c. Em Region (Região), especifique as regiões da AWS ou escolha All (Tudo).

   d. Em Check category (Categoria de verificação), escolha a categoria a ser verificada ou escolha All (Tudo).

   e. Em Checks (Verificações), escolha as verificações específicas para essa categoria ou escolha All (Tudo).

      > **Note**
      >
      > O filtro Check category (Categoria de verificação) substitui o filtro Checks (Verificações). Por exemplo, se você escolher a opção Security (Segurança) e, em seguida, escolher um nome de verificação específico, o relatório incluirá todos os resultados de verificação para essa categoria. Para criar um relatório somente para verificações específicas, mantenha o valor padrão All (Tudo) para Check category (Categoria de verificação) e, em seguida, escolha os nomes de verificação.

   f. Em Resource status (Status do recurso), escolha o status a ser filtrado, como Warning (Aviso) ou escolhaAll (Tudo).

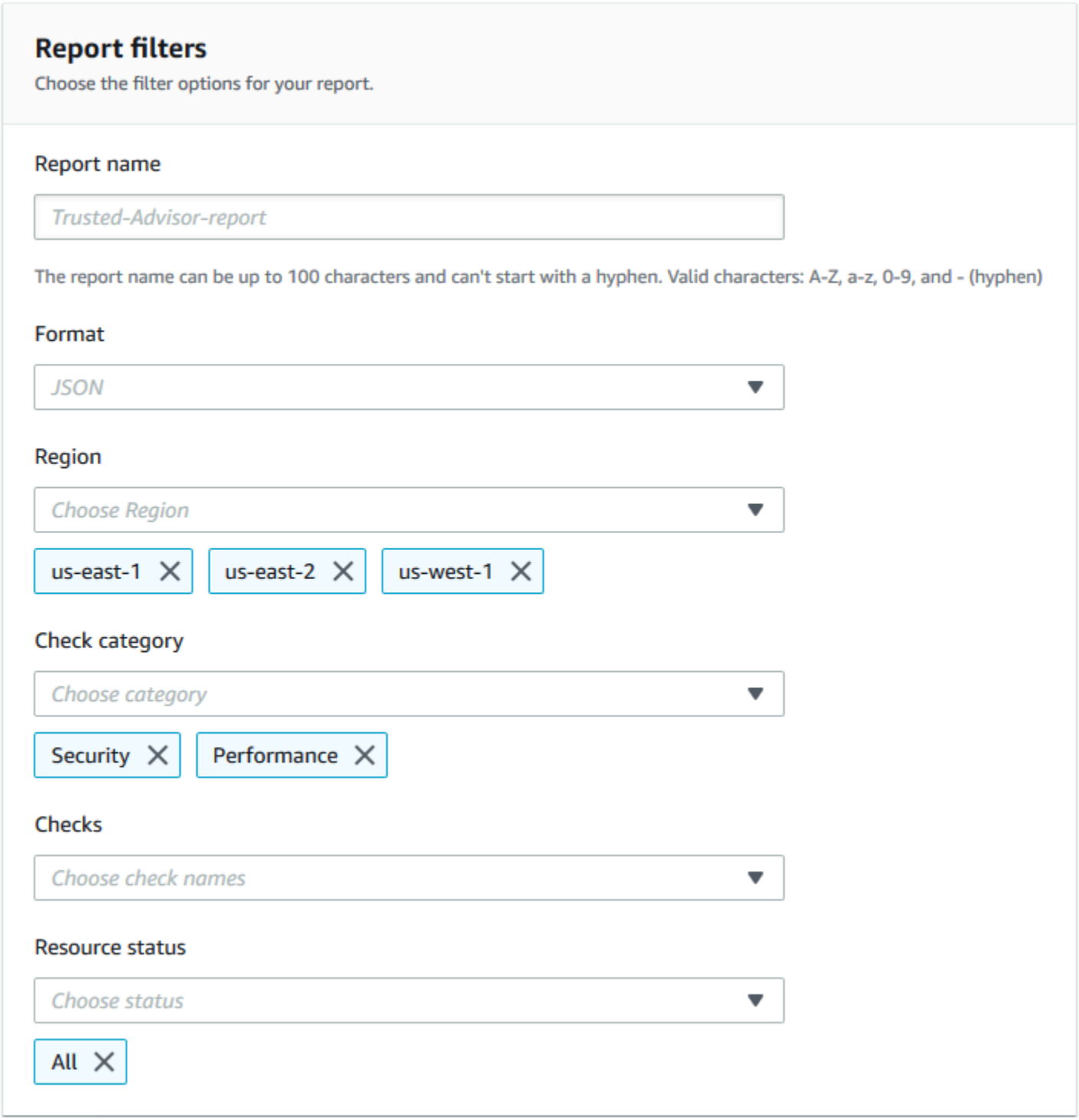
5. Em AWS Organization (Organização da AWS), selecione as unidades organizacionais (UOs) a serem incluídas no relatório. Para obter mais informações sobre as UOs, consulte Gerenciamento de unidades organizacionais no Manual do usuário do AWS Organizations.

6. Escolha Create report (Criar relatório).

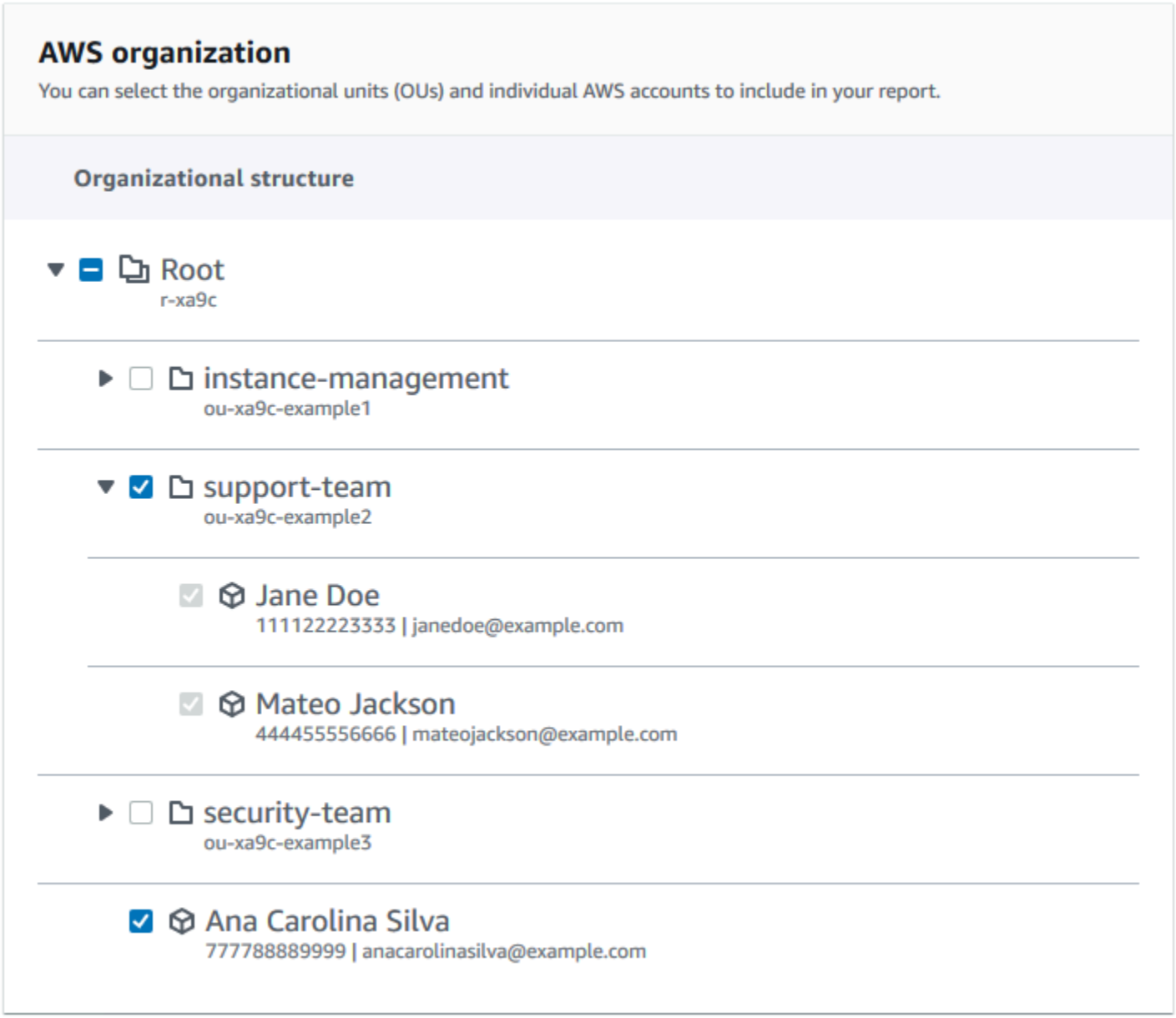
Example : Criar opções de filtro de relatório

O exemplo a seguir cria um relatório JSON para o seguinte:

- Três regiões da AWS
- Todas as verificações de Warning (Segurança) e Performance



No exemplo a seguir, o relatório inclui a UO support-team e uma conta da AWS que fazem parte da organização.



Observações

- O tempo necessário para criar o relatório dependerá do número de contas na organização e do número de recursos em cada conta.
- Não é possível criar mais de um relatório simultaneamente, a menos que o relatório atual esteja em execução há mais de 6 horas.
- Atualize a página se o relatório não for exibido na página.

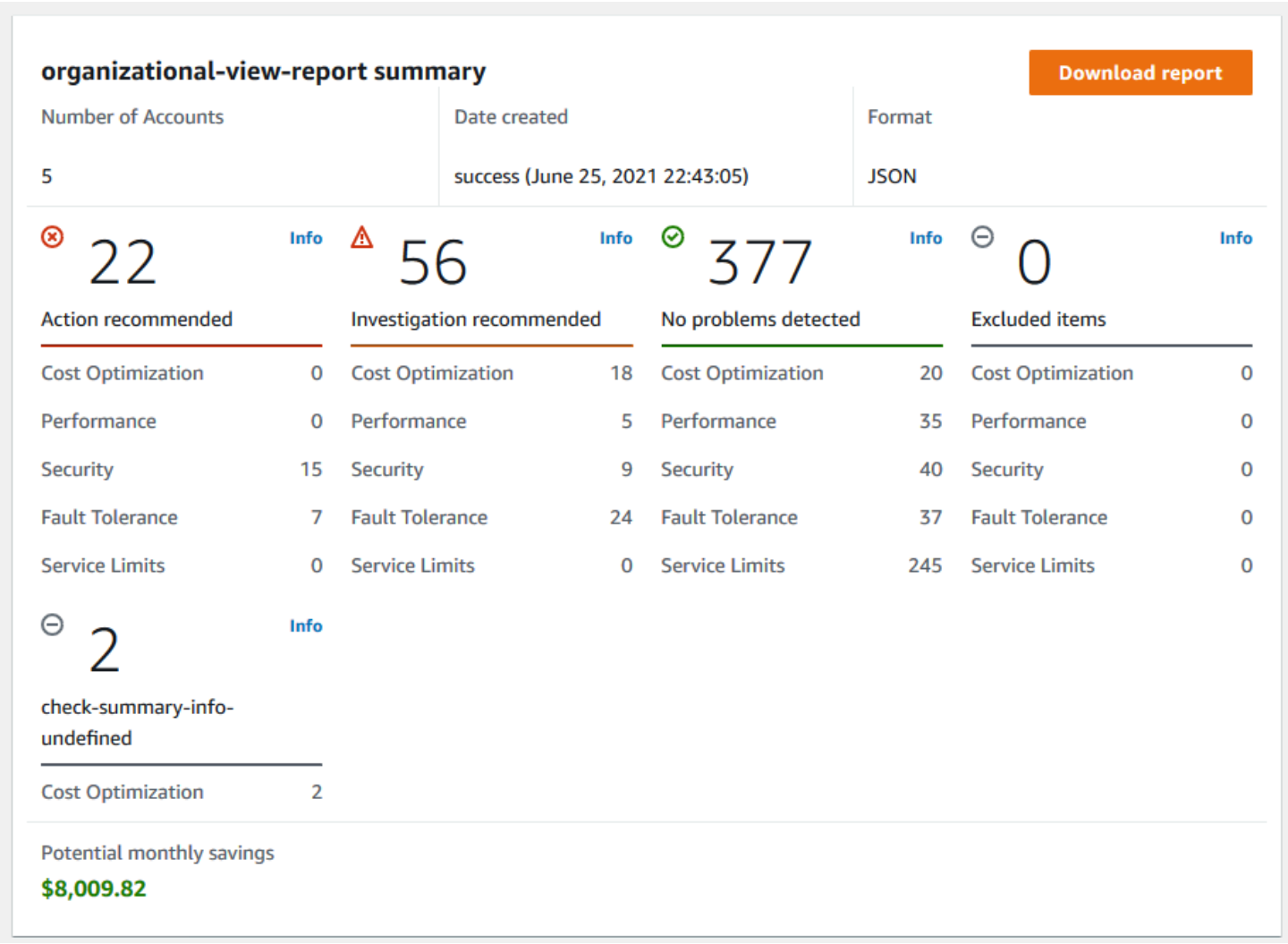
Visualize o resumo do relatório.

Depois que o relatório estiver pronto, será possível exibir o resumo do relatório no console do Trusted Advisor. Isso permitirá que você visualize rapidamente o resumo dos resultados da verificação em toda a organização.

Para visualizar o resumo do relatório.

1. Faça login na conta de gerenciamento da organização e abra o console do AWS Trusted Advisor em https://console.aws.amazon.com/trustedadvisor.
2. No painel de navegação, selecione Organizational View (Visualização organizacional).
3. Escolha o nome do relatório.
4. Na página Summary (Resumo), exiba os status de verificação de cada categoria. Também é possível escolher Download report (Baixar relatório).

Example : Resumo do relatório para uma organização



Baixar um relatório da visualização organizacional

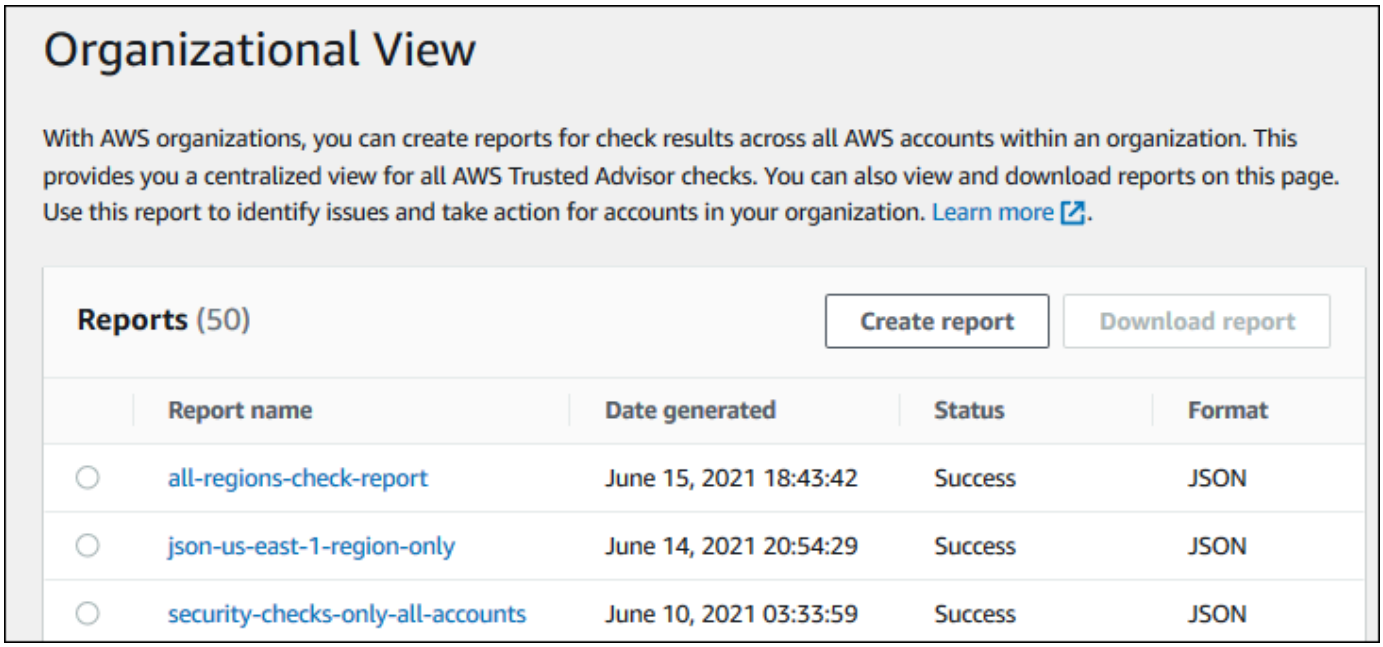
Depois que o relatório estiver pronto, baixe o console do Trusted Advisor. O relatório é um arquivo .zip que contém três arquivos:

- `summary.json` - Contém um resumo dos resultados da verificação para cada categoria de verificação.
- `schema.json` - Contém o esquema das verificações especificadas no relatório.
- Um arquivo de recursos (.json ou .csv) - Contém informações detalhadas sobre os status de verificação de recursos na organização.

Para baixar um relatório da visualização organizacional

1. Faça login na conta de gerenciamento da organização e abra o console do AWS Trusted Advisor em https://console.aws.amazon.com/trustedadvisor.
2. No painel de navegação, selecione Organizational View (Visualização organizacional).

   A página Organizational View (Visualização organizacional) exibe os relatórios disponíveis para baixar.
3. Selecione um relatório, escolha Download report (Baixar relatório) e salve o arquivo. Apenas um relatório pode ser obtido por download de cada vez.



4. Descompacte o arquivo.
5. Use um editor de texto para abrir o arquivo `.json` ou uma aplicação de planilha para abrir o arquivo `.csv`.

> **Note**
>
> Você poderá receber vários arquivos se o seu relatório tiver 5 MB ou mais.

Example : arquivo summary.json

O arquivo `summary.json` exibe o número de contas na organização e os status das verificações em cada categoria.

O Trusted Advisor usa o seguinte código de cores nos resultados de verificação:

- `Green` - Trusted Advisor não detecta um problema para a verificação.
- `Yellow` - Trusted Advisor detecta um possível problema para a verificação.
- `Red` - Trusted Advisor detecta um erro e recomenda uma ação para a verificação.
- `Blue` - Trusted Advisor não consegue determinar o status da verificação.

No exemplo a seguir, duas verificações são `Red`, uma é `Green` e uma é `Yellow`.


```
{
    "numAccounts": 3,
    "filtersApplied": {
        "accountIds": ["123456789012","111122223333","111111111111"],
        "checkIds": "All",
        "categories": [
            "security",
            "performance"
        ],
        "statuses": "All",
        "regions": [
            "us-west-1",
            "us-west-2",
            "us-east-1"
        ],
        "organizationalUnitIds": [
            "ou-xa9c-EXAMPLE1",
            "ou-xa9c-EXAMPLE2"
        ]
    },
    "categoryStatusMap": {
        "security": {
            "statusMap": {
                "ERROR": {
                    "name": "Red",
                    "count": 2
                },
                "OK": {
                    "name": "Green",
                    "count": 1
                },
                "WARN": {
```

```
                    "name": "Yellow",
                    "count": 1
                }
            },
            "name": "Security"
        }
    },
    "accountStatusMap": {
        "123456789012": {
            "security": {
                "statusMap": {
                    "ERROR": {
                        "name": "Red",
                        "count": 2
                    },
                    "OK": {
                        "name": "Green",
                        "count": 1
                    },
                    "WARN": {
                        "name": "Yellow",
                        "count": 1
                    }
                },
                "name": "Security"
            }
        }
    }
}
```

Example : arquivo schema.json

O arquivo `schema.json` inclui o esquema para as verificações no relatório. O exemplo a seguir inclui os IDs e as propriedades para as verificações da Política de senha do IAM (Yw2K9puPzl) e de Rotação de chaves do IAM (DqdJqYeRm5).

```
{
    "Yw2K9puPzl": [
        "Password Policy",
        "Uppercase",
        "Lowercase",
        "Number",
        "Non-alphanumeric",
```

```
        "Status",
        "Reason"
    ],
    "DqdJqYeRm5": [
        "Status",
        "IAM User",
        "Access Key",
        "Key Last Rotated",
        "Reason"
    ],
    ...
}
```

Example : arquivo resources.csv

O arquivo `resources.csv` inclui informações sobre recursos na organização. Este exemplo mostra algumas das colunas de dados que são exibidas no relatório, como as seguintes:

- ID da conta afetada
- O ID de verificação do Trusted Advisor
- O ID do recurso.
- Carimbo de data/hora do relatório
- O nome completo da verificação do Trusted Advisor
- A categoria de verificação do Trusted Advisor
- O ID da conta da unidade organizacional (UO) pai ou raiz

AccountId	CheckId	ResourceId	TimeStamp	CheckName	Category
1.11122E+11	Qch7DwouX1	LnW14f1M40NMjmMLvY5(	1.58983E+12	Low Utilization Amazon EC2 Instances	Cost Optimizing
1.11122E+11	HCP4007jGY	dJrQZXw36ZdswBeo9WUl.	1.58983E+12	Security Groups - Specific Ports Unrestricted	Security
1.11122E+11	HCP4007jGY	1hzakmTbWd5UmAM_a0L	1.58983E+12	Security Groups - Specific Ports Unrestricted	Security
4.44456E+11	1iG5NDGVre	dJrQZXw36ZdswBeo9WUl.	1.58983E+12	Security Groups - Unrestricted Access	Security
4.44456E+11	1iG5NDGVre	1hzakmTbWd5UmAM_a0L	1.58983E+12	Security Groups - Unrestricted Access	Security
4.44456E+11	Pfx0RwqBli	vioZmlba45kf2JWIe_W0j5	1.58983E+12	Amazon S3 Bucket Permissions	Security
4.44456E+11	Pfx0RwqBli	wAvASS3YOwy6WWxlBHf	1.58983E+12	Amazon S3 Bucket Permissions	Security
1.23457E+11	Pfx0RwqBli	LIc4zRaUSiIGRSlmqaMa5V	1.58983E+12	Amazon S3 Bucket Permissions	Security
1.23457E+11	Pfx0RwqBli	gWB27TMXof2evYzMSYBg	1.58983E+12	Amazon S3 Bucket Permissions	Security
7.77789E+11	Pfx0RwqBli	M3LBsF0e15Cl9Mxppapcx	1.58983E+12	Amazon S3 Bucket Permissions	Security
7.77789E+11	Yw2K9puPzl	47DEQpj8HBSa-_TImW-5J(	1.58983E+12	IAM Password Policy	Security
7.77789E+11	H7lgTzjTYb	1xHQ5ovV8bS0H1Z-t7Kbib	1.58983E+12	Amazon EBS Snapshots	Fault Tolerance
7.77789E+11	wuy7G1zxql	10F6p6VAF0F-MuL6Dc-dl1	1.58983E+12	Amazon EC2 Availability Zone Balance	Fault Tolerance

O arquivo de recursos só conterá entradas se houver um resultado de verificação no nível do recurso. Talvez você não veja as verificações no relatório pelos seguintes motivos:

- Algumas verificações, como o MFA on Root Account (MFA na conta raiz) não têm recursos e não aparecerão no relatório. As verificações sem recursos aparecem no `summary.json` em vez disso.
- Algumas verificações mostrarão apenas os recursos se forem `Red` ou `Yellow`. Se todos os recursos forem `Green`, eles poderão não aparecer no relatório.
- Se uma conta não estiver habilitada para um serviço que requer a verificação, a verificação poderá não aparecer no relatório. Por exemplo, se você não estiver usando as instâncias reservadas do Amazon Elastic Compute Cloud na organização, a verificação de expiração de leasing da instância reservada do Amazon EC2 não aparecerá no relatório.
- A conta não atualizou os resultados da verificação. Isso pode acontecer quando os usuários com um plano de suporte Básico ou Desenvolvedor entrarem no console do Trusted Advisor do pela primeira vez. Se você tiver um plano de suporte Business, Enterprise On-Ramp ou Enterprise, poderá levar até uma semana a partir do cadastro da conta para que os usuários vejam os resultados da verificação. Para obter mais informações, consulte Atualizar verificações do Trusted Advisor.
- Se apenas a conta de gerenciamento da organização tiver habilitado recomendações para verificações, o relatório não incluirá recursos para outras contas da organização.

Para o arquivo de recursos, é possível usar software comum, como o Microsoft Excel, para abrir o formato de arquivo .csv. É possível usar o arquivo .csv para uma análise única de todas as verificações em todas as contas da organização. Se você quiser usar o relatório com uma aplicação, é possível baixar o relatório como um arquivo.json.

O formato de arquivo .json oferece mais flexibilidade do que o formato de arquivo .csv para casos de uso avançados, como agregação e análise avançada com vários conjuntos de dados. Por exemplo, é possível usar uma interface SQL com umserviço da AWS, como o Amazon Athena, para executar consultas nos relatórios. Também é possível usar o Amazon QuickSight para criar painéis e visualizar dados. Para obter mais informações, consulte Usar outros serviços da AWS para visualizar relatórios do Trusted Advisor.

Desabilitar a visualização organizacional

Siga este procedimento para desabilitar o modo de visualização organizacional. Você deve fazer login na conta de gerenciamento da organização ou assumir uma função com as permissões

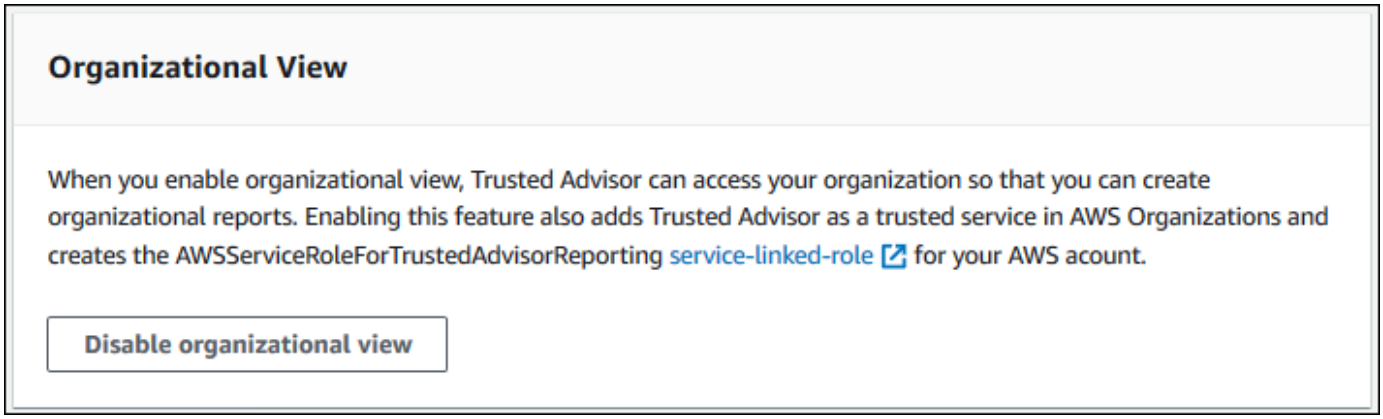
necessárias para desabilitar esse recurso. Não é possível desabilitar esse recurso usando outra conta da organização.

Depois que você desabilitar esse recurso, acontecerá o seguinte:

- O Trusted Advisor será removido como um serviço confiável do Organizations.
- A função vinculada ao serviço `AWSServiceRoleForTrustedAdvisorReporting` será criada para você na conta de gerenciamento em sua organização. Isso significa que é possível excluí-lo manualmente, se necessário.
- Não é possível criar, exibir ou baixar relatórios para sua organização. Para acessar relatórios criados anteriormente, você deve reativar o modo de visualização organizacional do console do Trusted Advisor. Consulte Habilitar a visualização organizacional.

Para desabilitar a visualização organizacional para Trusted Advisor

1. Faça login na conta de gerenciamento da organização e abra o console do AWS Trusted Advisor em https://console.aws.amazon.com/trustedadvisor.
2. No painel de navegação, escolha Preferences.
3. Em Organizational View (Visualização organizacional), escolha Disable organizational view (Desabilitar o modo organizacional).



Depois de desabilitar o modo de visualização organizacional, o Trusted Advisor não agregará mais verificações de outras contas da AWS na organização. No entanto, a função vinculada ao serviço `AWSServiceRoleForTrustedAdvisorReporting` permanecerá na conta de gerenciamento da organização até que você a remova por meio do console do IAM, da API do IAM do ou da AWS Command Line Interface (AWS CLI). Para obter mais informações, consulte Excluir uma função vinculada ao serviço no Guia do usuário do IAM.

> **Note**
>
> É possível usar outros serviços da AWS para consultar e visualizar dados para relatórios de visualização organizacional. Para mais informações, consulte os seguintes recursos do :
>
> - Exibir recomendações do AWS Trusted Advisor em escala com AWS Organizations noBlog de gerenciamento e governança da AWS
> - Usar outros serviços da AWS para visualizar relatórios do Trusted Advisor

Utilização de políticas do IAM para permitir acesso à visualização organizacional

É possível usar as seguintes políticas de AWS Identity and Access Management (IAM) para permitir que usuários ou funções na conta acessem a visualização organizacional no AWS Trusted Advisor.

Example : Acesso total à visualização organizacional

A política a seguir permite acesso total ao recurso de visualização organizacional. Um usuário com essas permissões pode fazer o seguinte:

- Habilitar e desabilitar visualização organizacional
- Criar, exibir e baixar relatórios

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReadStatement",
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccountsForParent",
                "organizations:ListAccounts",
                "organizations:ListRoots",
                "organizations:DescribeOrganization",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListAWSServiceAccessForOrganization",
                "trustedadvisor:DescribeAccount",
                "trustedadvisor:DescribeChecks",
```

```
                "trustedadvisor:DescribeCheckSummaries",
                "trustedadvisor:DescribeAccountAccess",
                "trustedadvisor:DescribeOrganization",
                "trustedadvisor:DescribeReports",
                "trustedadvisor:DescribeServiceMetadata",
                "trustedadvisor:DescribeOrganizationAccounts",
                "trustedadvisor:ListAccountsForParent",
                "trustedadvisor:ListRoots",
                "trustedadvisor:ListOrganizationalUnitsForParent"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CreateReportStatement",
            "Effect": "Allow",
            "Action": [
                "trustedadvisor:GenerateReport"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ManageOrganizationalViewStatement",
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:DisableAWSServiceAccess",
                "trustedadvisor:SetOrganizationAccess"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CreateServiceLinkedRoleStatement",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/
reporting.trustedadvisor.amazonaws.com/AWSServiceRoleForTrustedAdvisorReporting"
        }
    ]
}
```

Example : Acesso de leitura à visualização organizacional

A política a seguir permite acesso somente leitura à visualização organizacional do Trusted Advisor. Um usuário com essas permissões só pode exibir e baixar relatórios existentes.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReadStatement",
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccountsForParent",
                "organizations:ListAccounts",
                "organizations:ListRoots",
                "organizations:DescribeOrganization",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListAWSServiceAccessForOrganization",
                "trustedadvisor:DescribeAccount",
                "trustedadvisor:DescribeChecks",
                "trustedadvisor:DescribeCheckSummaries",
                "trustedadvisor:DescribeAccountAccess",
                "trustedadvisor:DescribeOrganization",
                "trustedadvisor:DescribeReports",
                "trustedadvisor:ListAccountsForParent",
                "trustedadvisor:ListRoots",
                "trustedadvisor:ListOrganizationalUnitsForParent"
            ],
            "Resource": "*"
        }
    ]
}
```

Também é possível criar a sua própria política personalizada do IAM. Para obter mais informações, consulte Criar políticas do IAM no Manual do usuário do IAM.

> **Note**
>
> Se você habilitou o AWS CloudTrail na sua conta, as funções a seguir poderão aparecer nas entradas de log:

- `AWSServiceRoleForTrustedAdvisorReporting` - A função vinculada ao serviço do que o Trusted Advisor usa para acessar contas da organização.
- `AWSServiceRoleForTrustedAdvisor` - A função vinculada ao serviço do que o Trusted Advisor usa para acessar serviços na organização.

Para obter mais informações sobre funções vinculadas ao serviço, consulte Usar perfis vinculados ao serviço do Trusted Advisor.

Usar outros serviços da AWS para visualizar relatórios do Trusted Advisor

Siga este tutorial para carregar e visualizar seus dados usando outros serviços da AWS. Neste tópico, você cria um bucket do Amazon Simple Storage Service (Amazon S3) para armazenar seu relatório e um modelo do AWS CloudFormation para criar recursos na conta. Em seguida, é possível usar o Amazon Athena para analisar ou executar consultas para seu relatório ou o Amazon QuickSight para visualizar esses dados em um painel.

Para obter informações e exemplos de visualização dos dados do relatório, consulte View AWS Trusted Advisor recommendations at scale with AWS Organizations no Blog de Gestão e Governança da AWS.

Pré-requisitos

Antes de usar esse tutorial, verifique se ele atende aos requisitos a seguir.

- Faça login no AWS Identity and Access Management (IAM) com um usuário que tenha permissões de administrador.
- Use a região da AWS Leste dos EUA (Norte da Virgínia) para configurar rapidamente os serviços e recursos da AWS.
- Crie uma conta do Amazon QuickSight. Para obter mais informações, consulte Conceitos básicos sobre análise de dados no Amazon QuickSight no Manual do usuário do Amazon QuickSight.

Carregue o relatório no Amazon S3.

Depois de baixar o relatório `resources.json`, carregue o arquivo no Amazon S3. Você deve usar um bucket na região Leste dos EUA (Norte da Virgínia).

Para carregar o relatório para um bucket do Amazon S3

1. Faça login no AWS Management Console em https://console.aws.amazon.com/.
2. Use o Region selector (Seletor de regiões) e selecione a região Leste dos EUA (Norte da Virgínia).
3. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
4. Na lista de buckets, escolha um bucket do S3 e, em seguida, copie o nome. Você usará o nome no próximo procedimento.
5. Na página *bucket-name*, escolha Creata folder (Criar pasta), digite o nome **folder1** e, depois, escolha Save (Salvar).
6. Selecione folder1 (pasta1).
7. Em folder1 (pasta1), escolha Upload (Carregar) e escolha a opção do arquivo `resources.json`.
8. Selecione Next (Próximo), mantenha as opções padrão e selecione Upload (Carregar).

> **Note**
>
> Se você carregar um novo relatório neste bucket, renomeie os arquivos `.json` cada vez que você carregá-los para que eles não substituam os relatórios existentes. Por exemplo, é possível adicionar o carimbo de data/hora a cada arquivo, como `resources-timestamp.json`, `resources-timestamp2.json` e assim por diante.

Criar recursos usando o AWS CloudFormation

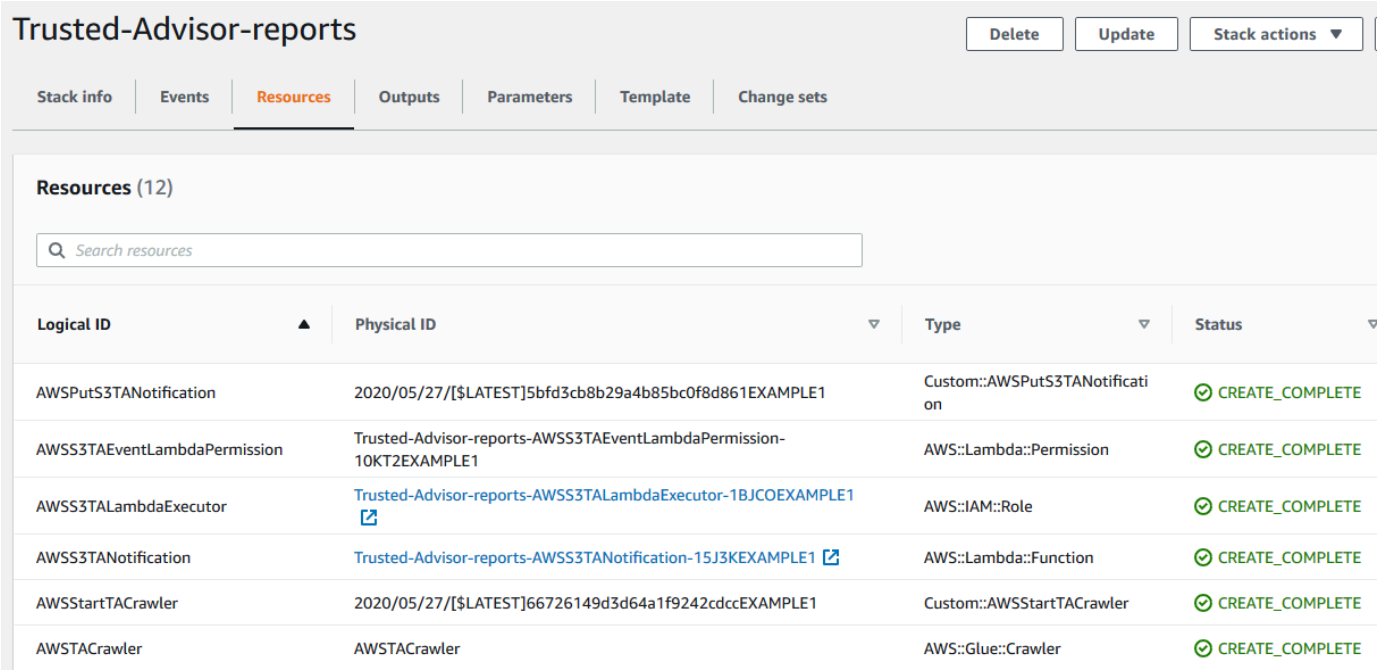
Depois de carregar o relatório no Amazon S3, carregue o seguinte modelo YAML no AWS CloudFormation. Este modelo diz ao AWS CloudFormation quais recursos criar para sua conta para que outros serviços possam usar os dados do relatório no bucket do S3. O modelo cria recursos para o IAM ,AWS Lambda e AWS Glue.

Para criar recursos com o AWS CloudFormation

1. Baixe o arquivo trusted-advisor-reports-template.zip.
2. Descompacte o arquivo.
3. Abra o arquivo de modelo em um editor de texto.

4. Para os parâmetros `BucketName` e `FolderName`, substitua os valores para *`your-bucket-name-here`* e *`folder1`* com o nome do bucket e o nome da pasta na conta.
5. Salve o arquivo.
6. Abra o console do AWS CloudFormation em https://console.aws.amazon.com/cloudformation.
7. Se você ainda não tiver feito isso, no Region selector (Seletor de regiões), escolha a região Leste dos EUA (Norte da Virgínia).
8. No painel de navegação, escolha Stacks (Pilhas).
9. Selecione Create stack (Criar pilha) e With new resources (standard) (Com novos recursos (padrão)).
10. Na página Create stack (Criar pilha), em Specify template (Especificar modelo), escolha Upload a template file (Fazer upload de um arquivo de modelo) e escolha Choose file (Escolher arquivo).
11. Escolha seu arquivo YAML e escolha Next (Próximo).
12. Na página Specify stack details (Especificar detalhes da pilha), digite o nome da pilha, como **`Organizational-view-Trusted-Advisor-reports`** e escolha Next (Próximo).
13. Na página Configure stack options (Configurar as opções da pilha), mantenha os padrões e selecione Next (Próximo).
14. Na página Review **`Organizational-view-Trusted-Advisor-reports`** (Analisar), examine suas escolhas. Na parte inferior da página, marque a caixa de seleção que indica Reconheço que o AWS CloudFormation pode criar recursos do IAM.
15. Selecione Criar pilha.

    A pilha leva cerca de 5 minutos para ser criada.
16. Depois que a pilha for criada com êxito, a guia Resources (Recursos) será exibida com o exemplo a seguir.



Consulte os dados no Amazon Athena

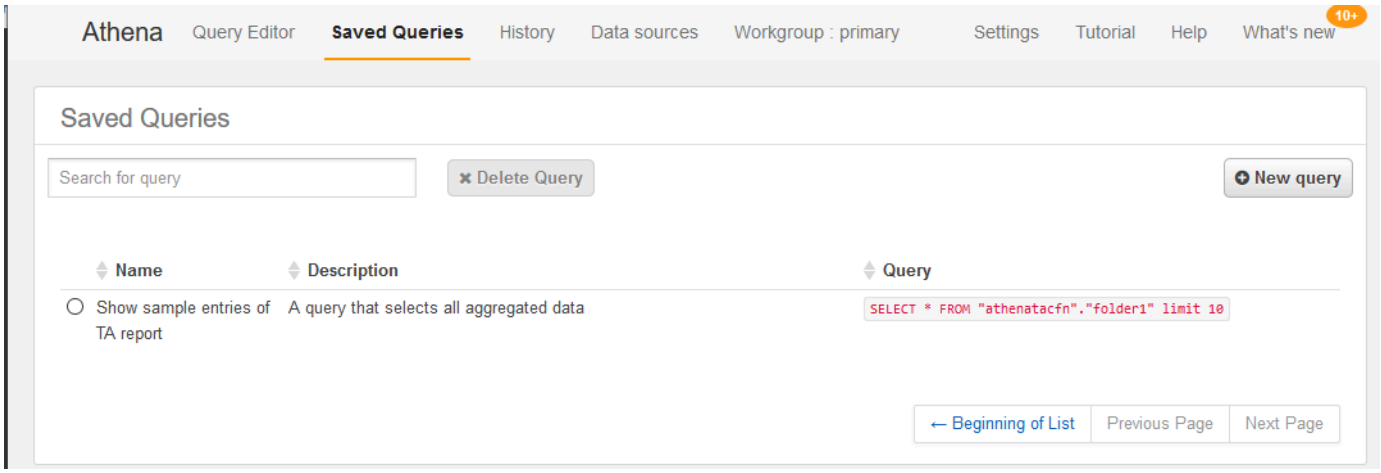
Depois de obter seus recursos, será possível visualizar os dados no Athena. Use o Athena para criar consultas e analisar os resultados do relatório, como pesquisar resultados de verificação específicos para contas na organização.

> **Observações**
>
> - Escolha a região Leste dos EUA (Norte da Virgínia).
> - Se você for novo no Athena, deverá especificar um local de resultado de consulta antes de executar uma consulta para seu relatório. Recomendamos que você especifique um bucket do S3 diferente para esse local. Para obter mais informações, consulte Especificar um local de resultados da consulta no Manual do usuário do Amazon Athena.

Para consultar os dados no Athena

1. Abra o console do Athena em https://console.aws.amazon.com/athena/.
2. Se você ainda não tiver feito isso, no Region selector (Seletor de regiões), escolha a região Leste dos EUA (Norte da Virgínia).
3. Selecione Saved Queries (Consultas salvas) e, no campo de pesquisa, insira **`Show sample`**.

4. Escolha a consulta que aparece, como Show sample entries of TA report (Mostrar entradas de exemplo do relatório do TA).



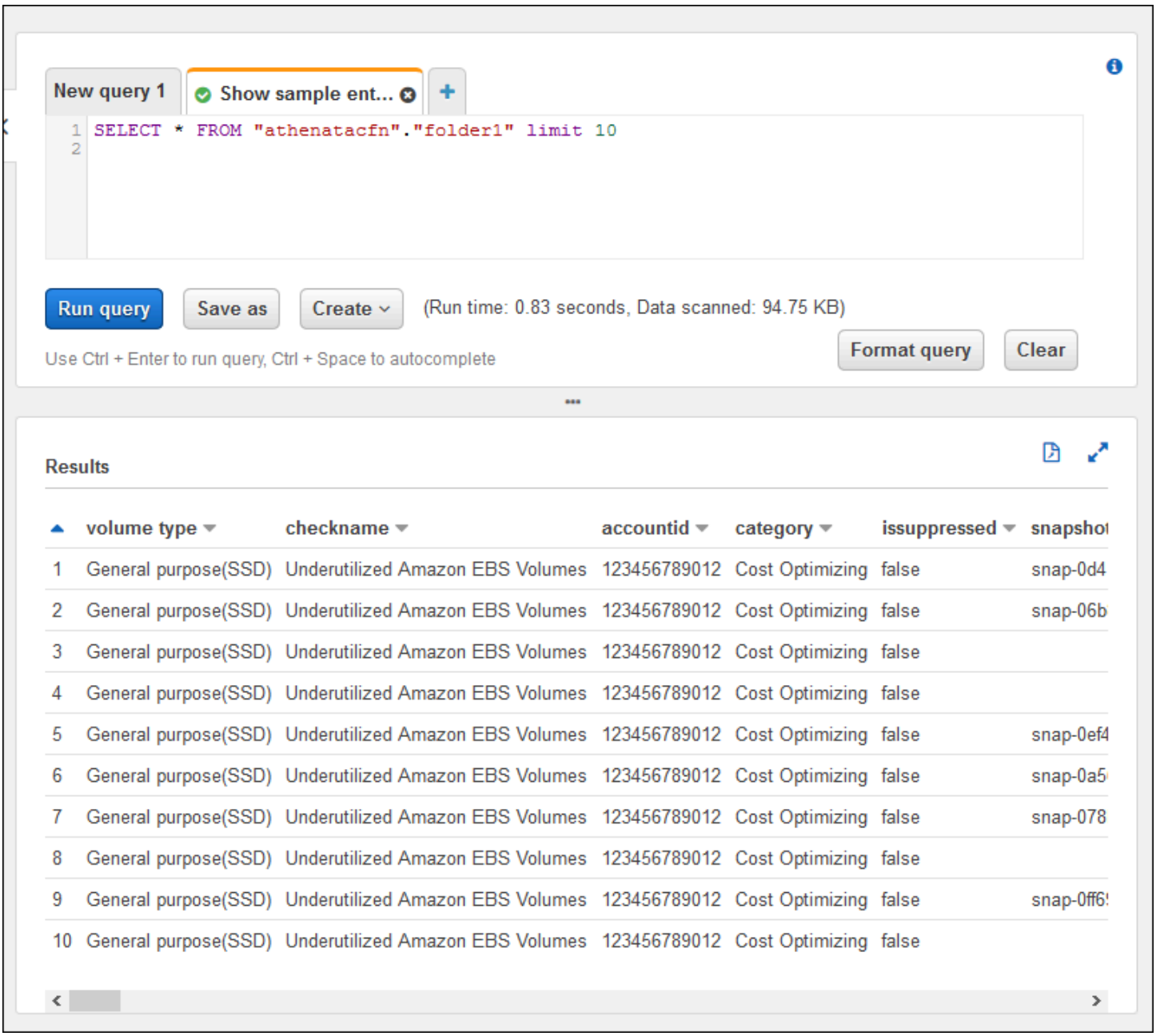
A consulta deve ter a aparência a seguir.

```
SELECT * FROM "athenatacfn"."folder1" limit 10
```

5. Selecione Run query (Executar consulta). Os resultados da consulta são exibidos.

Example : Consulta do Athena

O exemplo a seguir mostra 10 entradas de amostra do relatório.



Para obter mais informações, consulte Executar consultas SQL usando o Amazon Athena no Manual do usuário do Amazon Athena.

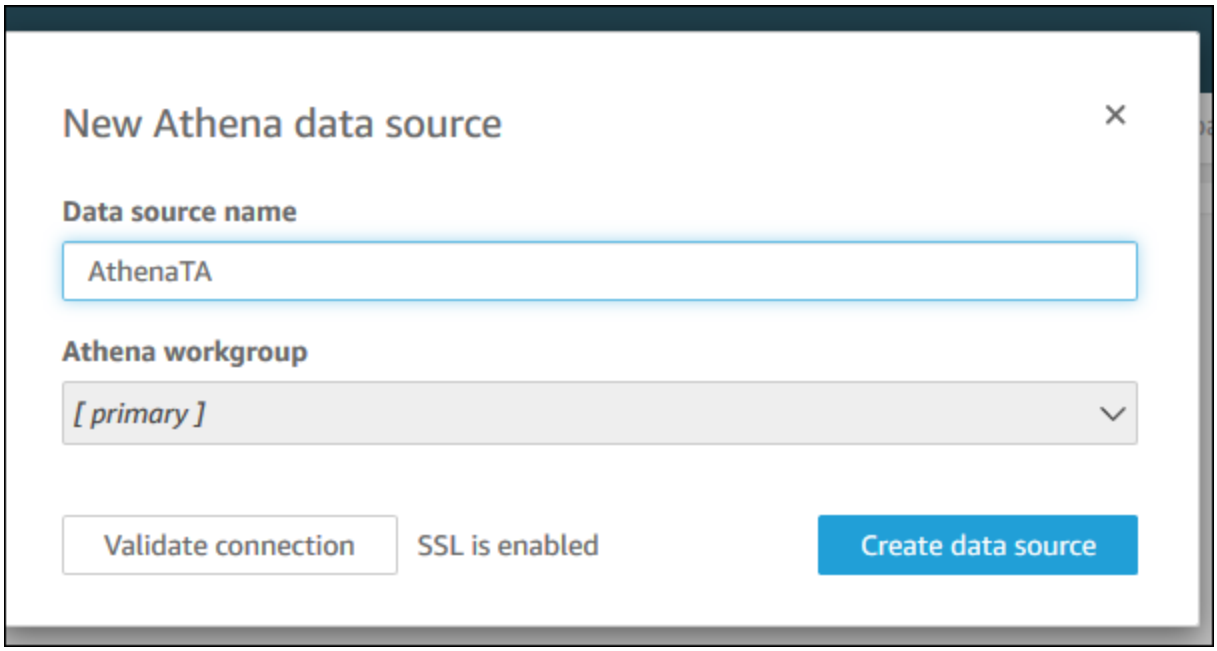
Criar um painel no Amazon QuickSight

Também é possível configurar o Amazon QuickSight para visualizar seus dados em um painel e visualizar suas informações de relatório.

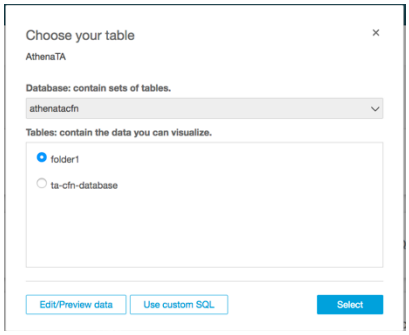
> **Note**
>
> Você deve usar a região Leste dos EUA (Norte da Virgínia).

Para criar um painel no Amazon QuickSight

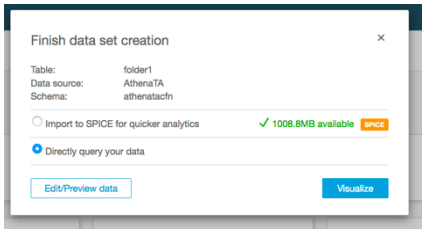
1. Navegue até o console do Amazon QuickSight e faça login na sua conta.
2. Selecione New analysis (Nova análise), New dataset (Novo conjunto de dados) e, em seguida, escolha Athena.
3. Em New Athena data source (Nova fonte de dados do Athena), insira um nome de fonte de dados, como AtenaTA e, em seguida, escolha Create data source (Criar fonte de dados).



4. Na caixa de seleção Choose your table (Escolher sua tabela), escolha a tabela athenatacfn, escolha folder1 (pasta1) e, depois, escolha Select (Selecionar).



5. Na caixa de seleção Finish data set creation (Finalizar criação do conjunto de dados), escolha Directly query your data (Consulte seus dados diretamente) e, depois, escolha Visualize (Visualizar).

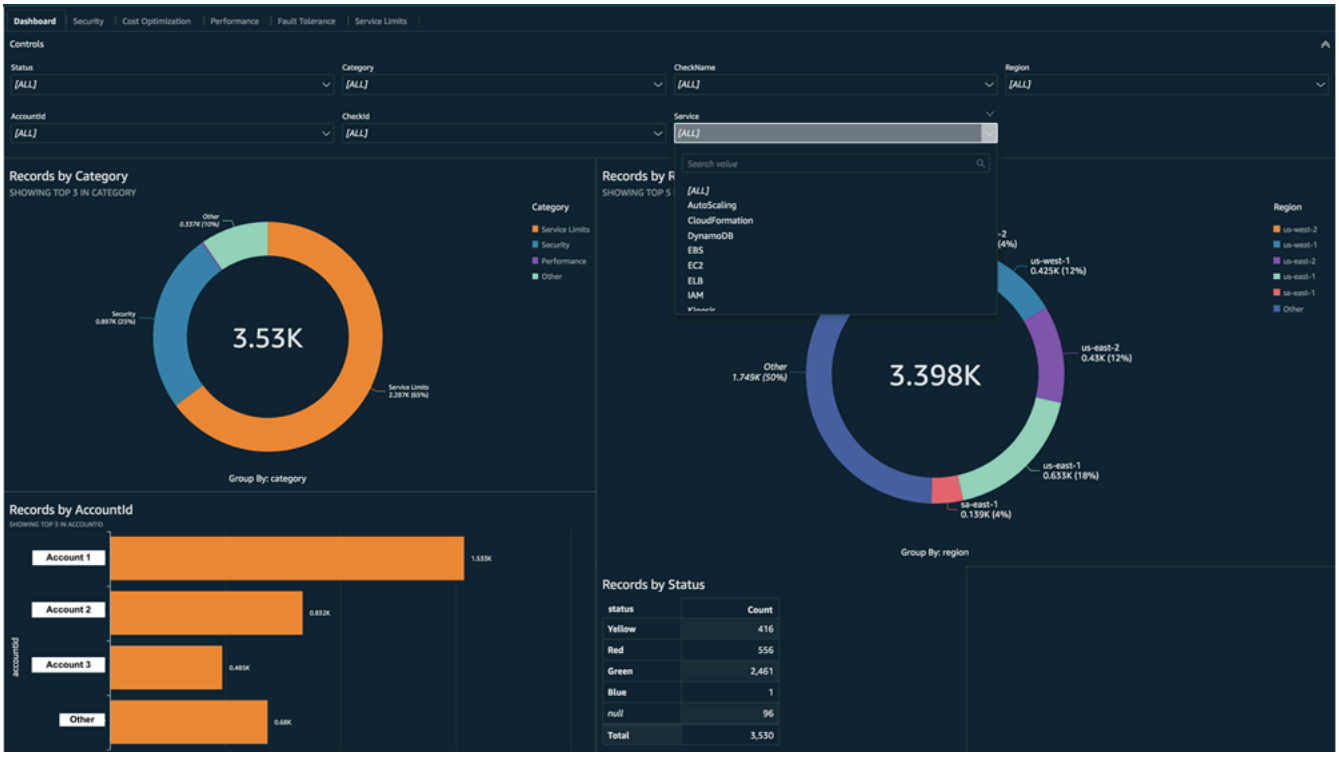


Agora é possível criar um painel no Amazon QuickSight. Para obter mais informações, consulte Working with Dashboards (Trabalhar com painéis) no Manual do usuário do Amazon QuickSight.

Example : Painel do Amazon QuickSight

O exemplo de painel a seguir mostra informações sobre as verificações do Trusted Advisor, como as seguintes:

- IDs da conta afetada
- Resumo por regiões da AWS
- Categorias de verificação
- Status de verificação
- Número de entradas no relatório para cada conta



> **Note**
>
> Se você tiver erros de permissão ao criar seu painel, certifique-se de que o Amazon QuickSight possa usar o Athena. Para obter mais informações, consulte Não consigo me conectar ao Amazon Athena no Manual do usuário do Amazon QuickSight.

Para obter mais informações e exemplos de visualização dos dados do relatório, consulte View AWS Trusted Advisor recommendations at scale with AWS Organizations no Blog de Gestão e Governança da AWS.

Solução de problemas

Se você tiver problemas com este tutorial, consulte as dicas de solução de problemas a seguir.

Não vejo os dados mais recentes no meu relatório

Quando você cria um relatório, o recurso de visualização organizacional não atualiza automaticamente o Trusted Advisor na organização. Para obter os resultados de verificação mais recentes, atualize as verificações da conta de gerenciamento e da cada conta de membro na organização. Para obter mais informações, consulte Atualizar verificações do Trusted Advisor.

Tenho colunas duplicadas no relatório

O console do Athena pode mostrar o erro a seguir na tabela se o relatório tiver colunas duplicadas.

```
HIVE_INVALID_METADATA: Hive metadata for table folder1 is invalid: Table descriptor contains duplicate columns
```

Por exemplo, se você adicionou uma coluna no relatório que já existe, isso pode causar problemas ao tentar exibir os dados do relatório no console do Athena. É possível seguir estas etapas para corrigir esse problema.

Localizar colunas duplicadas

É possível usar o console do AWS Glue para exibir o esquema e identificar rapidamente se há colunas duplicadas no relatório.

Para localizar colunas duplicadas

1. Abra o console do AWS Glue em https://console.aws.amazon.com/glue/.
2. Se você ainda não tiver feito isso, no Region selector (Seletor de regiões), escolha a região Leste dos EUA (Norte da Virgínia).
3. No painel de navegação, selecione Tables (Tabelas).
4. Escolha o nome da pasta, como ***folder1*** (pasta1) e, depois, em Schema (Esquema), visualize os valores para Column name (Nome da coluna).

   Se alguma coluna estiver duplicada, você deverá carregar um novo relatório no bucket do Amazon S3. Consulte as seções de Carregar um novo relatório a seguir.

Carregar um novo relatório

Depois de identificar a coluna duplicada, recomendamos substituir o relatório existente por um novo. Isso garantirá que os recursos criados a partir deste tutorial usem os dados de relatório mais recentes da sua organização.

Para carregar um novo relatório

1. Se ainda não tiver feito isso, atualize as verificações do Trusted Advisor para as contas da organização. Consulte Atualizar verificações do Trusted Advisor.
2. Crie e baixe outro relatório JSON no console do Trusted Advisor. Consulte Criar relatórios da visualização organizacional. Você deve usar um arquivo JSON para este tutorial.

3. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
4. Escolha o bucket do Amazon S3 e selecione a pasta *folder1*.
5. Selecione os relatórios *resources*.json anteriores e escolha Delete (Excluir).
6. Na página Delete objects (Excluir objetos), em Permanently delete objects? (Excluir objetos permanentemente?), insira **permanently delete** e, depois, escolha Delete objects (Excluir objetos).
7. No bucket do S3, escolha Upload (Carregar) e, em seguida, especifique o novo relatório. Esta ação atualiza automaticamente a tabela do Athena e os recursos do crawler do AWS Glue com os dados de relatório mais recentes. Pode demorar alguns minutos para atualizar os recursos.
8. Digite uma nova consulta no console do Athena. Consulte Consulte os dados no Amazon Athena.

> **Note**
>
> Se você ainda tiver problemas com este tutorial, poderá abrir um caso de suporte técnico na Central de AWS Support.

Exibir as verificações do AWS Trusted Advisor fornecidas pelo AWS Config

O AWS Config é um serviço que avalia, audita e analisa continuamente suas configurações de recursos de acordo com as configurações desejadas. O AWS Config fornece as regras gerenciadas, que são verificações de conformidade predefinidas e personalizáveis usadas pelo AWS Config para avaliar se seus recursos da AWS estão em conformidade com as práticas recomendadas comuns.

O console do AWS Config orienta você na configuração e ativação das regras gerenciadas. Você também pode usar a AWS Command Line Interface (AWS CLI) ou a API do AWS Config para transmitir o código JSON que define a configuração de uma regra gerenciada. Você pode personalizar o comportamento de uma regra gerenciada para atender às suas necessidades. Você pode personalizar os parâmetros da regra para definir atributos que seus recursos devem ter para ser compatíveis com a regra. Para saber mais sobre como habilitar o AWS Config, consulte o Guia do desenvolvedor do AWS Config.

As regras gerenciadas do AWS Config acionam um conjunto de verificações do Trusted Advisor em todas as categorias. Quando você habilita determinadas regras gerenciadas, as verificações correspondentes do Trusted Advisor são habilitadas automaticamente. Para ver quais verificações do Trusted Advisor são acionadas por regras específicas gerenciadas do AWS Config, consulte Referência de verificação do AWS Trusted Advisor.

As verificações avançadas do AWS Config estão disponíveis para clientes com os planos AWS Business Support, AWS Enterprise On-Ramp e AWS Enterprise Support. Caso habilite o AWS Config e tenha um desses planos do AWS Support, você verá automaticamente as recomendações baseadas nas regras gerenciadas e implantadas correspondentes do AWS Config.

> **Note**
>
> Os resultados dessas verificações são atualizados automaticamente com base em atualizações acionadas por alterações nas regras gerenciadas do AWS Config. Não é permitido fazer solicitações de atualização. No momento, não é possível excluir recursos dessas verificações.

Solução de problemas

Se tiver problemas com essa integração, consulte as informações de solução de problemas a seguir.

Sumário

- Acabei de habilitar a gravação e as regras gerenciadas para o AWS Config, mas não vejo as verificações correspondentes do Trusted Advisor.
- Eu implantei a mesma regra gerenciada do AWS Config duas vezes, o que verei no Trusted Advisor?
- Desativei a gravação para o AWS Config em uma região da AWS. O que verei no Trusted Advisor?

Acabei de habilitar a gravação e as regras gerenciadas para o AWS Config, mas não vejo as verificações correspondentes do Trusted Advisor.

Depois que a regra do AWS Config gera os resultados da avaliação, você vê os resultados no Trusted Advisor quase em tempo real. Se você tiver problemas com esse recurso, crie um caso de suporte técnico no AWS Support Center.

Eu implantei a mesma regra gerenciada do AWS Config duas vezes, o que verei no Trusted Advisor?

Você vê entradas separadas nos resultados da verificação do Trusted Advisor para cada regra gerenciada que instala.

Desativei a gravação para o AWS Config em uma região da AWS. O que verei no Trusted Advisor?

Se você desativou o registro de recursos para o AWS Config em uma região da AWS, o Trusted Advisor não receberá mais dados para as regras e verificações gerenciadas correspondentes nessa região. Os resultados das regras gerenciadas existentes permanecem no AWS Config e no Trusted Advisor até que o AWS Config expire, com base na política de retenção de gravadores. Se você excluir uma regra gerenciada, os dados de verificação do Trusted Advisor geralmente serão excluídos quase em tempo real.

Visualizar os controles do AWS Security Hub no AWS Trusted Advisor

Após habilitar o AWS Security Hub para o Conta da AWS, você pode visualizar os controles de segurança e seus resultados no console do Trusted Advisor. Você pode usar os controles do Security Hub para identificar as vulnerabilidades de segurança na conta da mesma maneira que pode usar as verificações do Trusted Advisor. Você pode visualizar o status da verificação e a lista dos recursos afetados, e depois seguir as recomendações do Security Hub para resolver os problemas de segurança. Você pode usar esse recurso para encontrar as recomendações de segurança do Trusted Advisor e do Security Hub em um único local conveniente.

Observações

- No Trusted Advisor, é possível visualizar os controles do padrão de segurança AWS Foundational Security Best Practices, exceto os controles que apresentam Category: Recover > Resilience (Categoria: Recuperar > Resiliência). Para obter uma lista dos controles, consulte AWS Foundational Security Best Practices controls no Guia do usuário do AWS Security Hub.

  Para obter mais informações sobre as categorias do Security Hub, consulte Control categories (Categorias de controle).

- No momento, quando o Security Hub adiciona novos controles ao padrão de segurança AWS Foundational Security Best Practices, pode haver um atraso de duas a quatro semanas antes que você possa visualizá-las no Trusted Advisor. Esse período é o melhor esforço e não é uma garantia.

Tópicos

- Pré-requisitos
- Para visualizar os resultados do Security Hub
- Atualizar os resultados do Security Hub
- Desabilitar o Security Hub do Trusted Advisor
- Solução de problemas

Pré-requisitos

Você deve atender aos seguintes requisitos para habilitar a integração do Security Hub com o Trusted Advisor:

- É necessário ter um plano de suporte Business, Enterprise On-Ramp ou Enterprise para esse recurso. Você pode encontrar o plano de suporte na Central do AWS Support ou na página Planos de suporte. Para obter mais informações, consulte Comparar os planos do AWS Support.
- Você deve habilitar o registro de recursos no AWS Config para as Regiões da AWS que desejar para os controles do Security Hub. Para obter mais informações, consulte Habilitar e configurar a AWS Config.
- Você deve habilitar o Security Hub e selecionar o padrão de segurança AWS Foundational Security Best Practices v1.0.0. Se você ainda não o fez, consulte Configurar o AWS Security Hub no Guia do usuário do AWS Security Hub.

> **Note**
>
> Se você já tiver concluído os pré-requisitos, pode ir para Para visualizar os resultados do Security Hub.

Sobre as contas do AWS Organizations

Se você já concluiu os pré-requisitos para uma conta de gerenciamento, essa integração é habilitada automaticamente para todas as contas-membro da organização. As contas-membro individuais não precisam entrar em contato com o AWS Support para habilitar esse recurso. Porém, as contas-membro de sua organização devem habilitar o Security Hub se quiserem ver os resultados no Trusted Advisor.

Se você quiser desabilitar essa integração para uma conta-membro específica, consulte Desabilitar esse recurso para contas do AWS Organizations.

Para visualizar os resultados do Security Hub

Depois que você habilita o Security Hub para a conta, pode levar até 24 horas para os resultados do Security Hub aparecerem na página Security (Segurança) console do Trusted Advisor.

Para visualizar os resultados do Security Hub no Trusted Advisor

1. Navegue até o console do Trusted Advisor e escolha a categoria Security (Segurança).
2. No campo Search by keyword (Pesquisar por palavra-chave), insira o nome ou a descrição do controle no campo.

   > **Tip**
   >
   > Para Source (Fonte), você pode escolher AWS Security Hub para filtrar para controles do Security Hub.

3. Escolha o nome do controle do Security Hub para visualizar as seguintes informações:

   - Description (Descrição): descreve como esse controle confere as vulnerabilidades de segurança da conta.
   - Source (Fonte): se a verificação vem do AWS Trusted Advisor ou do AWS Security Hub. Para os controles do Security Hub, você pode encontrar o ID de controle.
   - Alert Criteria (Critérios de alerta): o status do controle. Por exemplo, se o Security Hub detectar um problema importante, o status pode ser Red: Critical or High (Vermelho: crítico ou alto).
   - Recommended Action (Ação recomendada): use o link da documentação do Security Hub para encontrar as etapas recomendadas para corrigir o problema.

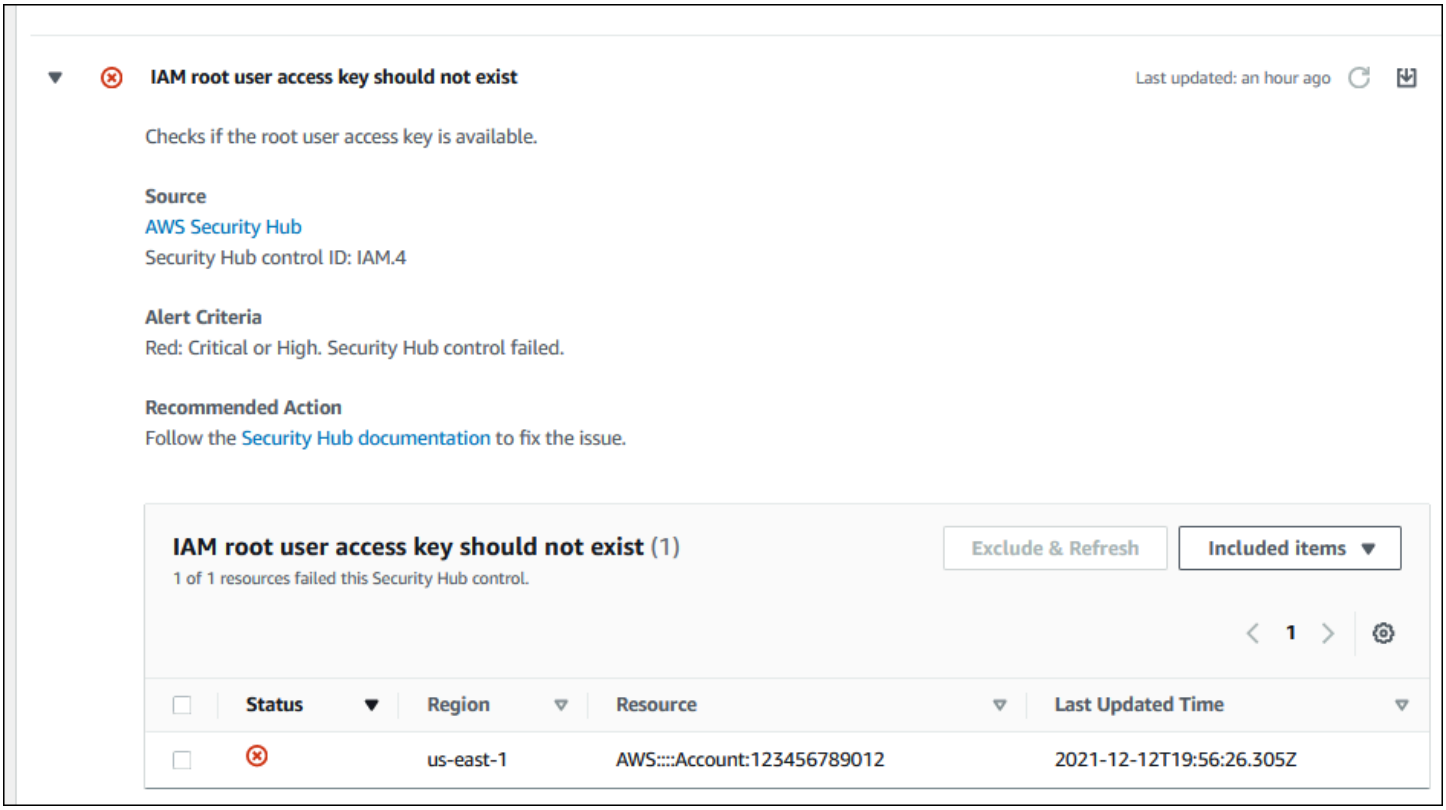
- Security Hub resources (Recursos do Security Hub): você pode encontrar os recursos da conta em que o Security Hub detectou um problema.

Observações

- Você deve usar o Security Hub para excluir recursos dos resultados. No momento, não é possível usar o console do Trusted Advisor para excluir itens dos controles do Security Hub. Para obter mais informações, consulte Setting the workflow status for findings (Definir o status do fluxo de trabalho para os resultados).
- O recurso de visualização organizacional oferece suporte a essa integração com o Security Hub. Você pode visualizar os resultados para os controles do Security Hub em toda a organização e, depois, criar e baixar relatórios. Para obter mais informações, consulte Visualização organizacional para AWS Trusted Advisor.

Example Exemplo: o controle do Security Hub para chave de acesso de usuário do IAM não deve existir

Veja a seguir um exemplo de resultado para um controle do Security Hub no console do Trusted Advisor.



Atualizar os resultados do Security Hub

Depois que você habilita um padrão de segurança, pode levar até duas horas para o Security Hub ter os resultados para os recursos. Pode levar até 24 horas para os dados aparecerem no console do Trusted Advisor. Se você habilitou recentemente o padrão de segurança AWS Foundational Security Best Practices v1.0.0, verifique o console do Trusted Advisor novamente mais tarde.

> **Note**
>
> - A programação de atualização para cada controle do Security Hub é periódica ou é acionada por alteração. No momento, você não é possível usar o console do Trusted Advisor nem a API do AWS Support para atualizar os controles do Security Hub. Para obter mais informações, consulte Schedule for running security checks (Programar a execução de verificações de segurança).
> - Você deve usar o Security Hub para excluir recursos das suas descobertas. No momento, não é possível usar o console do Trusted Advisor para excluir itens dos controles do Security Hub. Para obter mais informações, consulte Setting the workflow status for findings (Definir o status do fluxo de trabalho para os resultados).

Desabilitar o Security Hub do Trusted Advisor

Siga este procedimento se não quiser que as informações do Security Hub apareçam no console do Trusted Advisor. Este procedimento desabilita apenas a integração do Security Hub com o Trusted Advisor. Ele não afetará as configurações com o Security Hub. Você pode continuar usando o console do Security Hub para visualizar controles de segurança, recursos e recomendações.

Para desabilitar a integração do Security Hub

1. Entre em contato com o AWS Support e solicite que a integração do Security Hub com o Trusted Advisor seja desabilitada.

   Após o AWS Support desativar esse recurso, o Security Hub não enviará mais dados para o Trusted Advisor. Os dados do Security Hub serão removidos do Trusted Advisor.
2. Se desejar habilitar essa integração novamente, entre em contato com o AWS Support.

Desabilitar esse recurso para contas do AWS Organizations

Se você já concluiu o procedimento anterior para uma conta de gerenciamento, a integração do Security Hub é removida automaticamente para todas as contas-membro de organização. As contas-membro individuais da organização não precisam entrar em contato com o AWS Support separadamente.

Se você for uma conta-membro de uma organização, entre em contato com o AWS Support para remover esse recurso somente da sua conta.

Solução de problemas

Se estiver tendo problemas com essa integração, consulte as informações de solução de problemas a seguir.

Sumário

- Não vejo os resultados do Security Hub no console do Trusted Advisor
- Configurei o Security Hub e o AWS Config corretamente, mas os resultados continuam não aparecendo
- Desejo desabilitar controles específicos do Security Hub
- Quero encontrar recursos excluídos do Security Hub

- Quero habilitar ou desabilitar esse recurso para uma conta-membro que pertence a uma organização da AWS
- Eu vejo vários Regiões da AWS para o mesmo recurso afetado para uma verificação do Security Hub
- Desativei o Security Hub ou o AWS Config em uma região
- Meu controle está arquivado no Security Hub, mas ainda vejo as descobertas no Trusted Advisor
- Continuo não conseguindo visualizar os resultados do Security Hub

Não vejo os resultados do Security Hub no console do Trusted Advisor

Verifique se você concluiu as seguintes etapas:

- Você tem um plano de suporte Business, Enterprise On-Ramp ou Enterprise.
- Você habilitou a gravação de recursos no AWS Config na mesma região do Security Hub.
- Você habilitou o Security Hub e selecionou o padrão de segurança AWS Foundational Security Best Practices v1.0.0.
- Novos controles do Security Hub são adicionados como verificações ao Trusted Advisor em duas a quatro semanas. Consulte a observação.

Para obter mais informações, consulte Pré-requisitos.

Configurei o Security Hub e o AWS Config corretamente, mas os resultados continuam não aparecendo

Pode levar até duas horas para o Security Hub ter os resultados para os recursos. Pode levar até 24 horas para os dados aparecerem no console do Trusted Advisor. Confira o console do Trusted Advisor novamente mais tarde.

> **Observações**
>
> - Somente suas descobertas para os controles do padrão de segurança AWS Foundational Security Best Practices aparecerão no Trusted Advisor, exceto os controles que apresentam Category: Recover > Resilience (Categoria: Recuperar > Resiliência).

- Se houver algum problema de serviço com o Security Hub ou se o Security Hub não estiver disponível, pode levar até 24 horas para os resultados aparecerem no Trusted Advisor. Confira o console do Trusted Advisor novamente mais tarde.

Desejo desabilitar controles específicos do Security Hub

O Security Hub envia os dados para o Trusted Advisor automaticamente. Se você desabilitar um controle do Security Hub ou não tiver mais recursos para esse controle, os resultados não aparecerão no Trusted Advisor.

Você pode entrar no console do Security Hub e verificar se o controle está habilitado ou desabilitado.

Se você desabilitar um controle do Security Hub ou desabilitar todos os controles do padrão de segurança AWS Foundational Security Best Practices, suas descobertas serão arquivadas em até cinco dias. Esse período de cinco dias para arquivamento é aproximado e é apenas um melhor esforço, não sendo garantido. Quando as descobertas forem arquivadas, elas serão removidas do Trusted Advisor.

Para obter mais informações, consulte os tópicos a seguir:

- Disabling and enabling individual controls (Desabilitar e habilitar controles individuais)
- Disabling or enabling a security standard (Desabilitar ou habilitar um padrão de segurança)

Quero encontrar recursos excluídos do Security Hub

No console do Trusted Advisor, você pode escolher o nome de controle do Security Hub e, em seguida, escolher a opção Excluded Items (Itens excluídos). Essa opção exibe todos os recursos que são suprimidos no Security Hub.

Se o status do fluxo de trabalho para um recurso estiver definido como `SUPPRESSED`, esse recurso é um item excluído no Trusted Advisor. Não é possível suprimir os recursos do Security Hub usando o console do Trusted Advisor. Para fazer isso, use o console do Security Hub. Para obter mais informações, consulte Setting the workflow status for findings (Definir o status do fluxo de trabalho para os resultados).

Quero habilitar ou desabilitar esse recurso para uma conta-membro que pertence a uma organização da AWS

Por padrão, as contas-membro herdam o recurso da conta de gerenciamento para o AWS Organizations. Se a conta de gerenciamento tiver ativado o recurso, todas as contas da organização também terão o recurso. Se você tiver uma conta-membro e desejar fazer alterações específicas em sua conta, entre em contato com o AWS Support.

Eu vejo vários Regiões da AWS para o mesmo recurso afetado para uma verificação do Security Hub

Alguns Serviços da AWS são globais e não são específicos de uma região, como IAM e Amazon CloudFront. Por padrão, recursos globais, como buckets do Amazon S3, aparecem na região Leste dos EUA (Norte da Virgínia).

Para verificações do Security Hub que avaliam recursos para serviços globais, é possível que você veja mais de um item para os recursos afetados. Por exemplo, se a verificação `Hardware MFA should be enabled for the root user` identificar que sua conta não ativou esse recurso, você verá várias regiões na tabela para o mesmo recurso.

Você pode configurar o Security Hub e o AWS Config para que várias regiões não apareçam para o mesmo recurso. Para obter mais informações, consulte AWS Foundational Best Practices controls que talvez você queira desabilitar.

Desativei o Security Hub ou o AWS Config em uma região

Se você interromper a gravação de recursos com o AWS Config ou desabilitar o Security Hub em uma Região da AWS, o Trusted Advisor não receberá mais dados para nenhum controle nessa região. O Trusted Advisor remove suas descobertas do Security Hub num prazo de sete a nove dias. Esse período é o melhor esforço e não é uma garantia. Para obter mais informações, consulte Disabling Security Hub (Desabilitar o Security Hub).

Para desabilitar esse recurso para sua conta, consulte Desabilitar o Security Hub do Trusted Advisor.

Meu controle está arquivado no Security Hub, mas ainda vejo as descobertas no Trusted Advisor

Quando o status `RecordState` é alterado para `ARCHIVED` em uma descoberta, o Trusted Advisor exclui a descoberta desse controle do Security Hub de sua conta. Você ainda pode ver a descoberta

no Trusted Advisor por até sete a nove dias antes de ser excluída. Esse período é o melhor esforço e não é uma garantia.

Continuo não conseguindo visualizar os resultados do Security Hub

Se você continuar a ter problemas com esse recurso, poderá criar um caso de suporte técnico na Central de AWS Support.

Optar por verificações do Trusted Advisor para o AWS Compute Optimizer

O Compute Optimizer é um serviço que analisa as configuração e as métricas de utilização dos seus recursos da AWS. Esse serviço relata se seus recursos estão configurados corretamente para eficiência e confiabilidade. Ele também sugere melhorias que você pode implementar para melhorar o desempenho da workload. Com o Compute Optimizer, você visualiza as mesmas recomendações em suas verificações do Trusted Advisor.

Você pode optar pelo uso apenas para sua Conta da AWS ou para todas as contas-membro que fazem parte de uma organização do AWS Organizations. Para obter mais informações, consulte Conceitos básicos no Guia do usuário do AWS Compute Optimizer.

Depois que você optar pelo uso do Compute Optimizer, as verificações a seguir receberão dados de suas funções do Lambda e volumes do Amazon EBS. A geração de descobertas e recomendações de otimização pode levar até 12 horas. A visualização de seus resultados no Trusted Advisor para as seguintes verificações pode levar até 48 horas:

Otimização de custo

- Volumes superprovisionados do Amazon EBS
- Funções superprovisionadas do AWS Lambda para tamanho de memória

Desempenho

- Volumes subprovisionados do Amazon EBS
- Funções subprovisionadas do AWS Lambda para tamanho de memória

Observações

- Os resultados dessas verificações são atualizados automaticamente várias vezes ao dia. Não é permitido fazer solicitações de atualização. Poderá levar algumas horas para que as alterações sejam exibidas. No momento, não é possível excluir recursos dessas verificações.
- O Trusted Advisor já tem as verificações de volumes subutilizados do Amazon EBS e volumes magnéticos superutilizados do Amazon EBS.

  Depois de optar pelo uso do Compute Optimizer, recomendamos que você use as novas verificações de volumes superprovisionados do Amazon EBS e volumes subprovisionados do Amazon EBS.

Informações relacionadas

Para obter mais informações, consulte os tópicos a seguir:

- Visualizar recomendações de volume do Amazon EBS no Guia do usuário do AWS Compute Optimizer
- Visualizar recomendações de funções do Lambda no Guia do usuário do AWS Compute Optimizer
- Configurar memória de função do Lambda no Guia do desenvolvedor do AWS Lambda
- Solicitar modificações em seus volumes do Amazon EBS no Guia do usuário do Amazon EC2 para instâncias do Linux

Conceitos básicos do AWS Trusted Advisor Priority

O Trusted Advisor Priority ajuda a proteger e otimizar sua Conta da AWS, para seguir as melhores práticas da AWS. Com o Trusted Advisor Priority, sua equipe da Conta da AWS pode monitorar proativamente a sua conta e criar recomendações priorizadas ao identificar oportunidades para você.

Por exemplo, a sua equipe de contas pode identificar se o seu usuário raiz da conta da AWS não tem autenticação multifator (MFA). A sua equipe de contas pode criar uma recomendação para que você possa tomar medidas imediatas em relação a uma verificação, como `MFA on Root Account`. A recomendação aparece como uma recomendação priorizada ativa na página do Trusted Advisor

Priority do console do Trusted Advisor. Em seguida, você segue as recomendações para resolver a questão.

As recomendações do Trusted Advisor Priority vêm dessas duas fontes:

- Serviços da AWS – Serviços como o Trusted Advisor, o AWS Security Hub e o AWS Well-Architected criam recomendações automaticamente. A sua equipe de contas compartilha essas recomendações com você para que elas apareçam no Trusted Advisor Priority.
- Sua equipe de contas: a sua equipe de contas pode criar recomendações manuais.

O Trusted Advisor Priority ajuda você a se concentrar nas recomendações mais importantes. Você e sua equipe de contas podem acompanhar o ciclo de vida da recomendação, desde o momento em que sua equipe de contas compartilhou a recomendação até o momento em que você a aceita, resolve ou rejeita. É possível usar o Trusted Advisor Priority para encontrar recomendações para todas as contas-membro em sua organização.

Tópicos

- Pré-requisitos
- Habilitar o Trusted Advisor Priority
- Visualizar recomendações priorizadas
- Reconhecer uma recomendação
- Ignorar uma recomendação
- Resolver uma recomendação
- Reabrir uma recomendação
- Baixar os detalhes da recomendação
- Registrar administradores delegados
- Cancelar o registro dos administradores delegados
- Gerenciar as notificações do Trusted Advisor Priority
- Desabilitar o Trusted Advisor Priority

Pré-requisitos

Você deve atender aos seguintes requisitos para usar o Trusted Advisor Priority:

- Você deve ter um plano Enterprise Support.
- Sua conta deve fazer parte de uma organização que tenha habilitado todos os recursos no AWS Organizations. Para obter mais informações, consulte Habilitar todos os atributos na sua organização no Manual do usuário do AWS Organizations.
- Sua organização deve ter o acesso confiável ao Trusted Advisor habilitado. Para habilitar o acesso confiável, faça login como conta de gerenciamento. Abra a página Sua organização no console do Trusted Advisor.
- É necessário estar conectado à sua conta da AWS para visualizar as recomendações do Trusted Advisor Priority para sua conta.
- Você deve estar conectado à conta de gerenciamento da organização ou a uma conta de administrador delegada para visualizar as recomendações agregadas em toda a organização. Para obter instruções sobre como registrar contas de administrador delegadas, consulte Registrar administradores delegados.
- É necessário ter permissões do AWS Identity and Access Management (IAM) para acessar o Trusted Advisor Priority. Para obter informações sobre como controlar o acesso ao Trusted Advisor Priority, consulte Gerencie o acesso ao AWS Trusted Advisor e AWS políticas gerenciadas para AWS Trusted Advisor.

Habilitar o Trusted Advisor Priority

Peça à sua equipe de contas para habilitar esse recurso para você. Você precisa ter um plano Enterprise Support e ser proprietário da conta de gerenciamento da sua organização. Se a página do Trusted Advisor Priority no console indicar que você precisa de acesso confiável com o AWS Organizations, escolha Habilitar o acesso confiável com o AWS Organizations. Para obter mais informações, consulte a seção Pré-requisitos.

Visualizar recomendações priorizadas

Após sua equipe de contas ter habilitado o Trusted Advisor Priority para você, será possível ver as recomendações mais recentes para a sua conta da AWS.

Para visualizar recomendações priorizadas

1. Faça login no console do Trusted Advisor em https://console.aws.amazon.com/trustedadvisor/home.
2. Na página do Trusted Advisor Priority, você pode visualizar os seguintes itens:

Se você estiver usando uma conta de gerenciamento ou de administrador delegado do AWS Organizations, alterne para a guia Minha conta.

- Ações necessárias: o número de recomendações que estão pendentes de resposta ou em andamento.
- Visão geral – As seguintes informações:
  - Recomendações rejeitadas nos últimos 90 dias
  - Recomendações resolvidas nos últimos 90 dias
  - Recomendações sem uma atualização há mais de 30 dias
  - Tempo médio para resolver recomendações

3. Na aba Ativo, a opção Recomendações priorizadas ativas mostra as recomendações que sua equipe de contas priorizou para você. A guia Fechado mostra recomendações resolvidas ou rejeitadas.

   - Para filtrar seus resultados, use as opções a seguir:
     - Recommendation (Recomendação): insira palavras-chave para pesquisar por nome. Pode ser um nome de verificação ou um nome personalizado que foi criado por sua equipe de contas.
     - Status: se a recomendação está com resposta pendente, em andamento, foi rejeitada ou foi resolvida.
     - Origem – A origem de uma recomendação priorizada. A recomendação pode vir dos Serviços da AWS, da sua equipe da Conta da AWS ou de um evento de serviço planejado.
     - Categoria – A categoria da recomendação, como segurança ou otimização de custos.
     - Age (Época): quando a sua equipe de contas compartilhou a recomendação com você.

4. Escolha uma recomendação para saber mais sobre seus detalhes, os recursos afetados e as ações recomendadas. Você pode então reconhecer ou rejeitar a recomendação.

Para ver as recomendações priorizadas em todas as contas da sua organização da AWS

Tanto a conta de gerenciamento quanto os administradores delegados do Trusted Advisor Priority podem ver as recomendações agregadas em toda a sua organização.

> **Note**
>
> As contas de membros não têm acesso às recomendações agregadas.

1. Faça login no console do Trusted Advisor em https://console.aws.amazon.com/trustedadvisor/home.
2. Na página do Trusted Advisor Priority, verifique se você está na guia Minha organização.
3. Para ver as recomendações para uma conta, selecione uma conta na lista suspensa Selecionar uma conta da sua organização. Ou você pode ver recomendações em todas as suas contas.

   Na guia Minha organização, você pode visualizar os seguintes itens:

   - Ações necessárias: o número de recomendações em sua organização que estão pendentes de resposta ou em andamento.
   - Visão geral: mostra os seguintes itens:

     - Recomendações rejeitadas nos últimos 90 dias.

     - Recomendações resolvidas nos últimos 90 dias.

     - Recomendações sem uma atualização há mais de 30 dias.

     - O tempo médio necessário para resolver as recomendações.
4. Na aba Ativo, a seção Recomendações priorizadas ativas mostra as recomendações que sua equipe de contas priorizou para você. A guia Fechado mostra recomendações resolvidas ou rejeitadas.

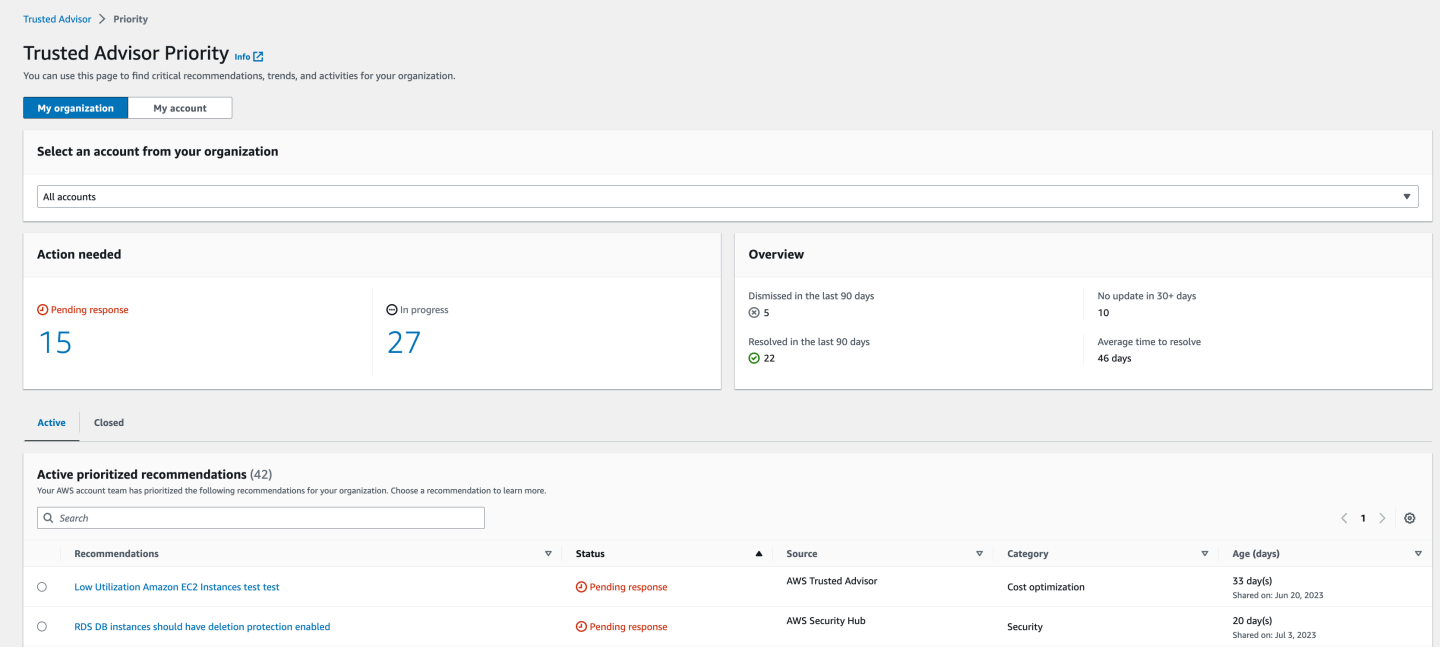
   Para filtrar seus resultados, use as opções a seguir:

   - Recommendation (Recomendação): insira palavras-chave para pesquisar por nome. Pode ser um nome de verificação ou um nome personalizado que foi criado por sua equipe de contas.
   - Status: se a recomendação está com resposta pendente, em andamento, foi rejeitada ou foi resolvida.
   - Origem – A origem de uma recomendação priorizada. A recomendação pode vir dos Serviços da AWS, da sua equipe da Conta da AWS ou de um evento de serviço planejado.
   - Categoria – A categoria da recomendação, como segurança ou otimização de custos.
   - Age (Época): quando a sua equipe de contas compartilhou a recomendação com você.

5. Escolha uma recomendação para ver mais detalhes, contas e recursos afetados e as ações recomendadas. Você pode então reconhecer ou rejeitar a recomendação.

Example : recomendações do Trusted Advisor Priority

O exemplo a seguir mostra 15 recomendações que estão pendentes de resposta e 27 recomendações que estão em andamento na seção Ação necessária. A imagem a seguir mostra duas das recomendações que estão pendentes de resposta na guia Recomendação priorizada ativa.



Reconhecer uma recomendação

Na aba Ativo, você pode aprender mais sobre a recomendação e depois decidir se deseja reconhecê-la.

Reconhecer uma recomendação

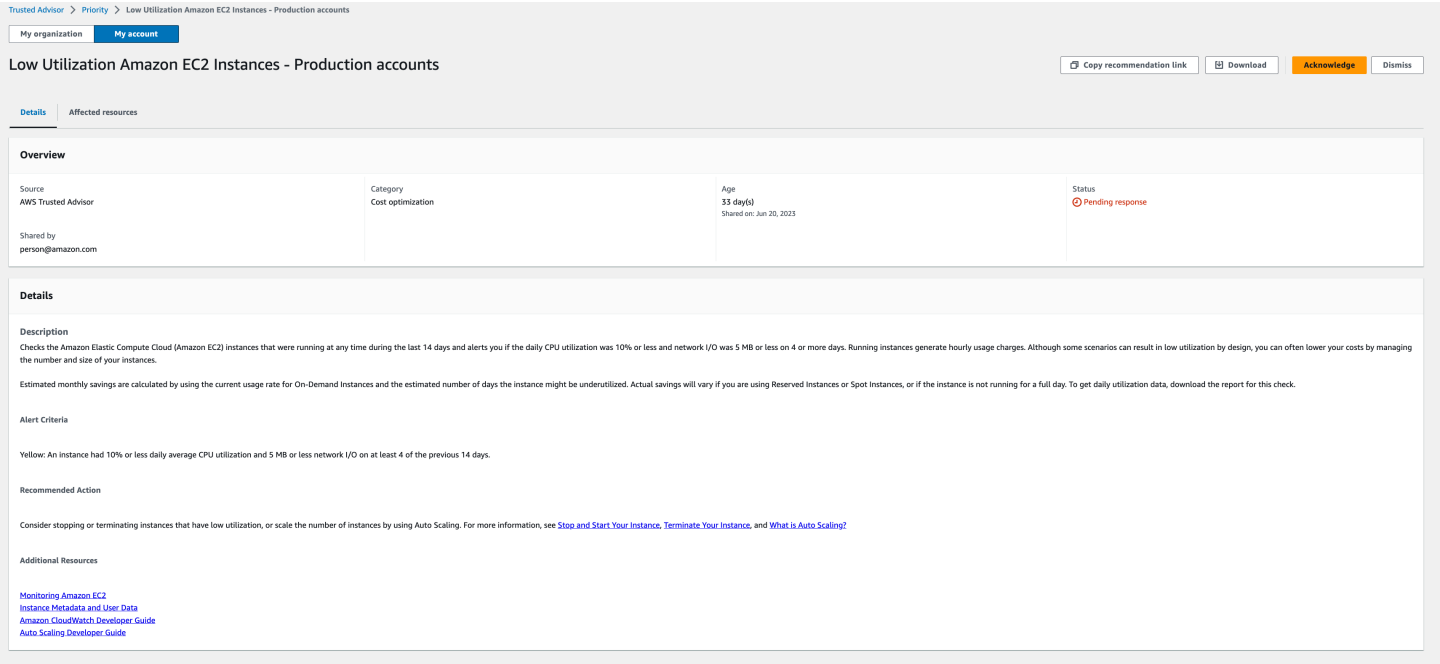
1. Faça login no console do Trusted Advisor em https://console.aws.amazon.com/trustedadvisor/home.
2. Se você estiver usando uma conta de gerenciamento ou de administrador delegado do AWS Organizations, alterne para a guia Minha conta.
3. Na página Trusted Advisor Priority, na aba Active (Ativo), escolha um nome de recomendação.
4. Na seção Detalhes, você pode revisar as ações recomendadas para resolver a recomendação.
5. Na seção Recursos afetados, você pode revisar os recursos afetados e filtrar por Status.

6. Escolha Eu aceito.
7. Na caixa de diálogo Reconhecer recomendação, escolha Confirmar.

   O status da recomendação muda para In progress (Em andamento). As recomendações em andamento ou pendentes de resposta aparecem na aba Active (Ativo) da página do Trusted Advisor Priority.
8. Siga as ações recomendadas para resolver a recomendação. Para obter mais informações, consulte Resolver uma recomendação.

Example : recomendação manual do Trusted Advisor Priority

A imagem a seguir mostra a recomendação de Instâncias EC2 de baixa utilização que está aguardando uma resposta.



Para reconhecer uma recomendação para todas as contas em sua organização da AWS

A conta de gerenciamento ou os administradores delegados do Trusted Advisor podem reconhecer uma recomendação para todas as contas afetadas.

> **Note**
>
> As contas de membros não têm acesso às recomendações agregadas.

1. Faça login no console do Trusted Advisor em https://console.aws.amazon.com/trustedadvisor/home.
2. Na página do Trusted Advisor Priority, verifique se você está na guia Minha organização.
3. Na guia Ativo, selecione o nome da recomendação.
4. Escolha Eu aceito.
5. Na caixa de diálogo Reconhecer recomendação, escolha Confirmar.

   O status da recomendação muda para In progress (Em andamento).
6. Siga as ações recomendadas para resolver a recomendação. Para obter mais informações, consulte Resolver uma recomendação.
7. Para ver os detalhes da recomendação, escolha o nome da recomendação.

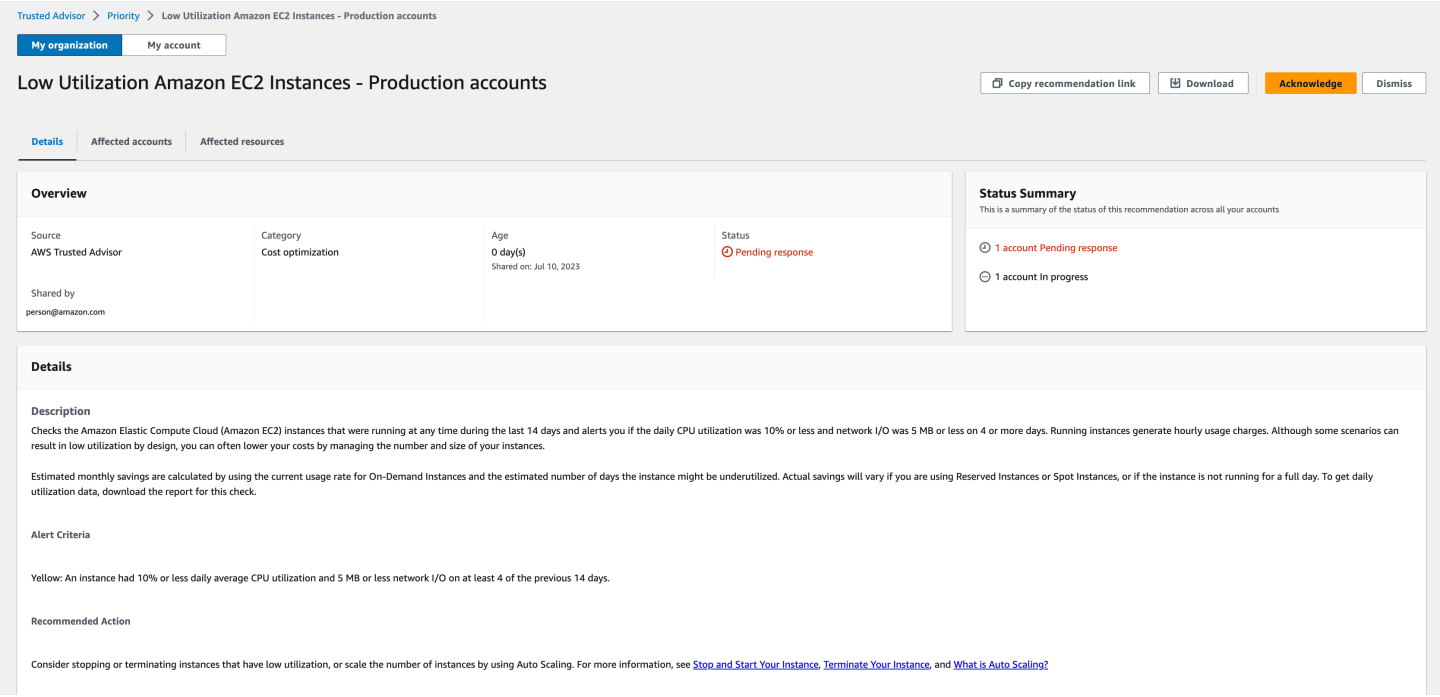
   Na seção Detalhes, você pode revisar as seguintes informações sobre a recomendação:

   - Uma Visão geral da recomendação e uma seção de Detalhes que abrange as ações de recomendação a serem concluídas.

     Um Resumo do status que mostra recomendações em todas as contas afetadas.
   - Na seção Contas afetadas, você pode analisar os recursos afetados em todas as suas contas. Você pode filtrar por Número da conta e Status.
   - Na seção Recursos afetados, você pode analisar os recursos afetados em todas as suas contas. Você pode filtrar por Número da conta e Status.

Example : recomendação manual do Trusted Advisor Priority

A imagem a seguir mostra a recomendação de Instâncias do Amazon EC2 com baixa utilização com uma resposta pendente. Uma conta afetada reconheceu a recomendação. Outra conta está pendente de resposta, tornando o status de recomendação Pendente de resposta.



Ignorar uma recomendação

Você também pode ignorar uma recomendação. Isso significa que você reconhece a recomendação, mas não a resolverá. Você pode ignorar uma recomendação se ela não for relevante para sua conta. Por exemplo, se você tem uma Conta da AWS de teste que planeja excluir, não precisa seguir as ações recomendadas.

Ignorar uma recomendação

1. Faça login no console do Trusted Advisor em https://console.aws.amazon.com/trustedadvisor/home.
2. Se você estiver usando uma conta de gerenciamento ou de administrador delegado do AWS Organizations, alterne para a guia Minha conta.
3. Na página Trusted Advisor Priority, na aba Active (Ativo), escolha um nome de recomendação.
4. Na página de detalhes da recomendação, reveja as informações sobre os recursos afetados.
5. Se essa recomendação não se aplica à sua conta, escolha Ignorar.
6. Na caixa de diálogo Ignorar recomendação, selecione um motivo pelo qual você não abordará a recomendação.
7. (Opcional) Insira uma nota detalhando por que você está rejeitando a recomendação. Se você escolher Outro, deverá inserir uma descrição na seção Nota.

8. Escolha Ignorar. O status da recomendação muda para Rejeitado e aparece na aba Fechado na página do Trusted Advisor Priority.

Para rejeitar uma recomendação para todas as contas em sua organização da AWS

A conta de gerenciamento ou o administrador delegado do Trusted Advisor Priority pode rejeitar uma recomendação para todas as suas contas.

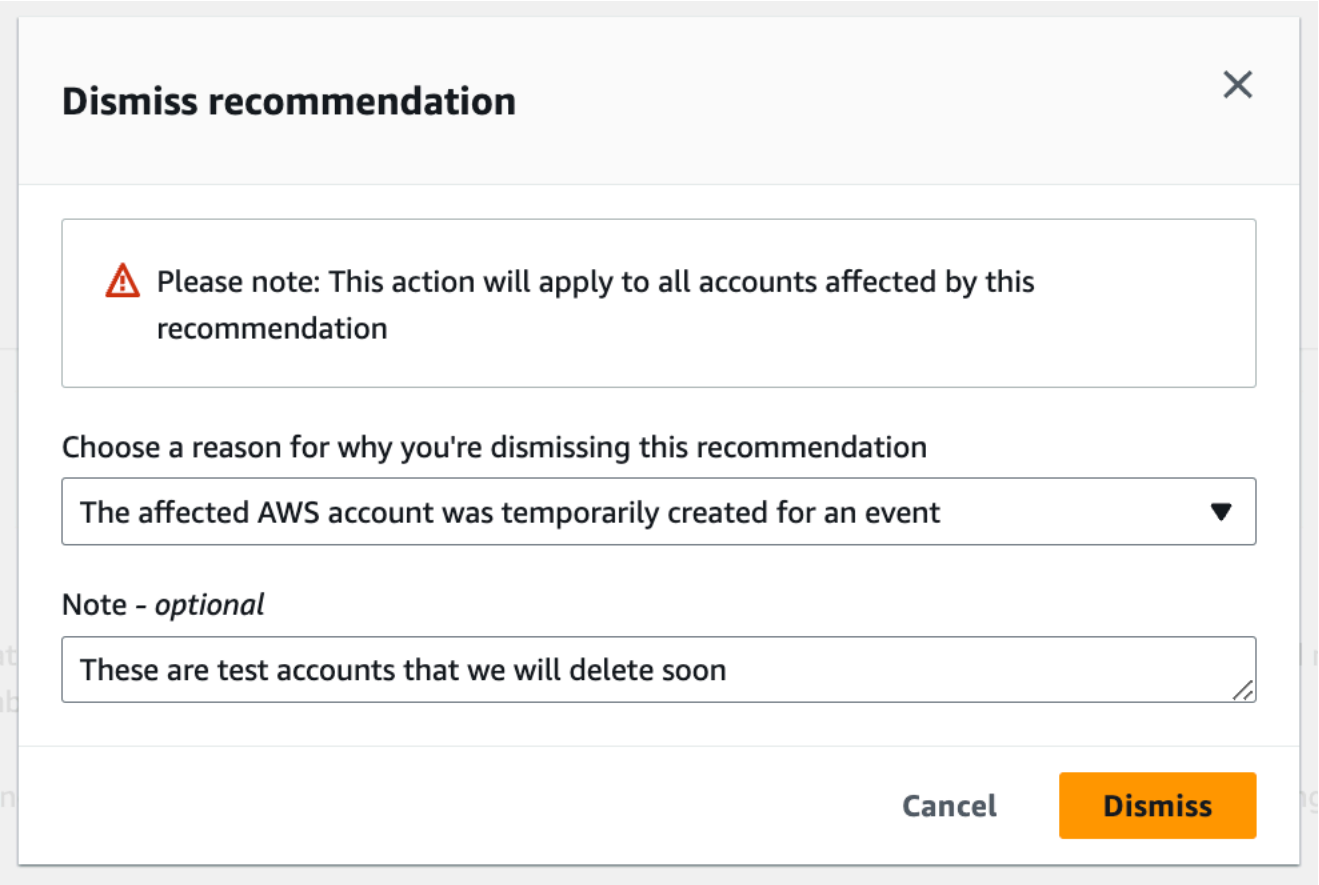
1. Faça login no console do Trusted Advisor em https://console.aws.amazon.com/trustedadvisor/home.
2. Na página do Trusted Advisor Priority, verifique se você está na guia Minha organização.
3. Na guia Ativo, selecione o nome da recomendação.
4. Se essa recomendação não se aplica à sua conta, escolha Ignorar.
5. Na caixa de diálogo Ignorar recomendação, selecione um motivo pelo qual você não abordará a recomendação.
6. (Opcional) Insira uma nota detalhando por que você está rejeitando a recomendação. Se você escolher Outro, deverá inserir uma descrição na seção Nota.
7. Escolha Ignorar. O status da recomendação muda para Rejeitado. A recomendação aparece na guia Fechado na página do Trusted Advisor Priority.

> **Note**
>
> Você pode escolher o nome da recomendação e escolher Exibir nota para descobrir o motivo de tê-la ignorado. Se a equipe da sua conta ignorou a recomendação para você, o endereço de e-mail deles aparecerá ao lado da nota.

O Trusted Advisor Priority também notifica a sua equipe de contas de que você ignorou a recomendação.

Example : Ignorar uma recomendação do Trusted Advisor Priority

O exemplo a seguir mostra como você pode ignorar uma recomendação.



Resolver uma recomendação

Depois de reconhecer a recomendação e concluir as ações recomendadas, você pode resolvê-la.

> **Tip**
>
> Depois de resolver uma recomendação, você não poderá reabri-la. Se você quiser rever a recomendação mais tarde, consulte Ignorar uma recomendação.

Para resolver uma recomendação

1. Faça login no console do Trusted Advisor em https://console.aws.amazon.com/trustedadvisor/home.
2. Na página do Trusted Advisor Priority, verifique se você está na guia Minha organização.
3. No Trusted Advisor Priority, selecione a recomendação e escolha Resolve (Resolver).

4. Na caixa de diálogo Resolver recomendação, escolha Resolver. As recomendações resolvidas aparecem na aba Closed (Fechado) na página Trusted Advisor Priority. Trusted Advisor O Priority notifica a sua equipe de contas de que você resolveu a recomendação.

Para resolver uma recomendação para todas as contas em sua organização da AWS

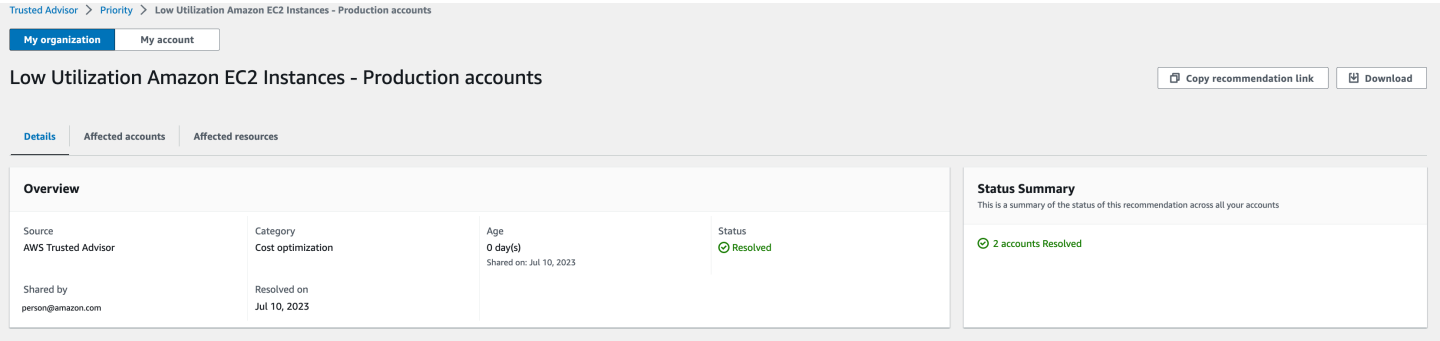
A conta de gerenciamento ou os administradores delegados do Trusted Advisor Priority podem resolver uma recomendação para todas as suas contas.

> **Note**
>
> As contas de membros não têm acesso às recomendações agregadas.

1. Faça login no console do Trusted Advisor em https://console.aws.amazon.com/trustedadvisor/home.
2. Se você estiver usando uma conta de gerenciamento ou de administrador delegado do AWS Organizations, vá para a guia Minha conta.
3. Na guia Ativo, selecione o nome da recomendação.
4. Se a recomendação não se aplica à sua conta, escolha Resolver.
5. Na caixa de diálogo Resolver recomendação, escolha Resolver. As recomendações resolvidas aparecem na aba Closed (Fechado) na página Trusted Advisor Priority. Trusted Advisor O Priority notifica a sua equipe de contas de que você resolveu a recomendação.

Example : recomendação manual do Trusted Advisor Priority

O exemplo a seguir mostra uma recomendação resolvida de Instâncias do Amazon EC2 de baixa utilização.



Reabrir uma recomendação

Depois de ignorar uma recomendação, você ou sua equipe de contas pode reabrir a recomendação.

Para reabrir uma recomendação

1. Faça login no console do Trusted Advisor em https://console.aws.amazon.com/trustedadvisor/home.
2. Se você estiver usando uma conta de gerenciamento ou de administrador delegado do AWS Organizations, alterne para a guia Minha conta.
3. Na página Trusted AdvisorPriority, escolha a aba Closed (Fechado).
4. Em Recomendações fechadas, selecione a recomendação Ignorada e escolha Reabrir.
5. Na caixa de diálogo Reabrir recomendação, descreva por que você está reabrindo a recomendação.
6. Selecione Reopen (Reabrir). O status da recomendação muda para In progress (Em andamento) e aparece na aba Active (Ativo).

> **Tip**
>
> Você pode escolher o nome da recomendação e escolher Exibir nota para descobrir o motivo de tê-la reaberto. Se a equipe da sua conta reabriu a recomendação para você, o nome deles aparecerá ao lado da nota.

7. Siga as etapas nos detalhes da recomendação.

Para reabrir uma recomendação para todas as contas em sua organização da AWS

A conta de gerenciamento ou os administradores delegados do Trusted Advisor Priority podem reabrir uma recomendação para todas as suas contas.

> **Note**
>
> As contas de membros não têm acesso às recomendações agregadas.

1. Faça login no console do Trusted Advisor em https://console.aws.amazon.com/trustedadvisor/home.

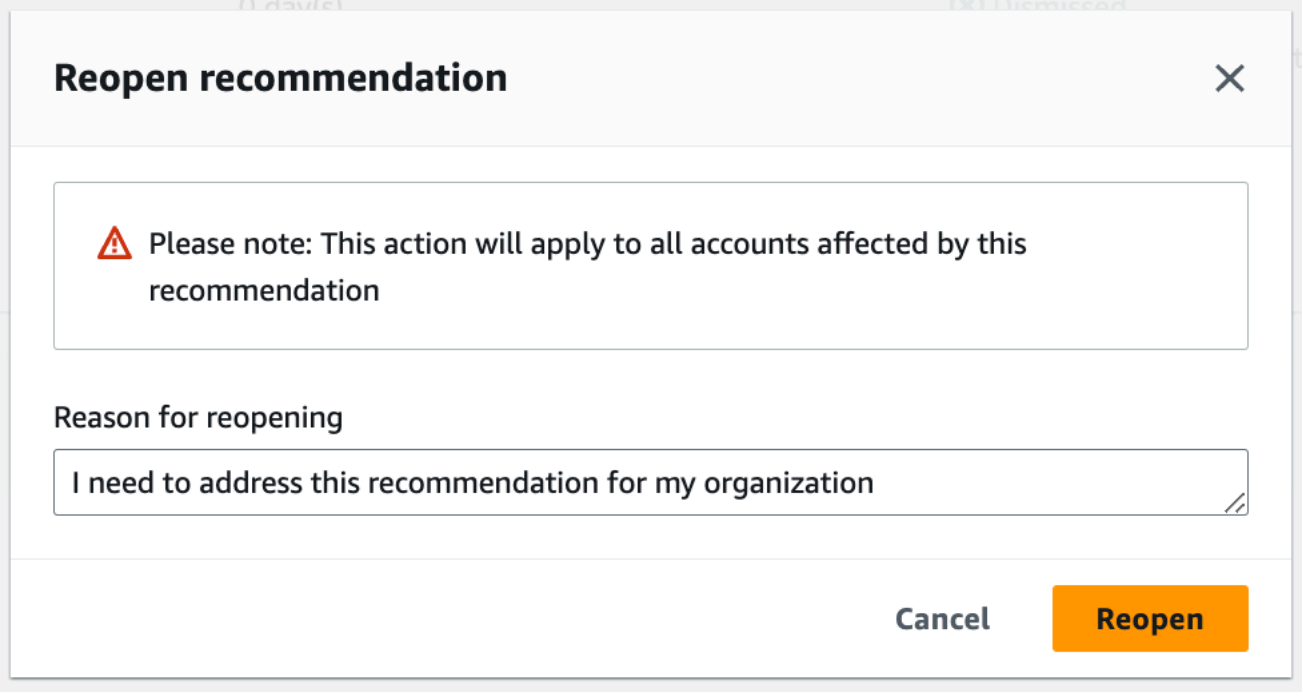
2. Na página do Trusted Advisor Priority, verifique se você está na guia Minha organização.
3. Em Recomendações fechadas, selecione a recomendação Ignorada e escolha Reabrir.
4. Na caixa de diálogo Reabrir recomendação, descreva por que você está reabrindo a recomendação.
5. Selecione Reopen (Reabrir). O status da recomendação muda para In progress (Em andamento) e aparece na aba Active (Ativo).

> **Tip**
>
> Você pode escolher o nome da recomendação e escolher Exibir nota para descobrir o motivo de tê-la reaberto. Se a equipe da sua conta reabriu a recomendação para você, o nome deles aparecerá ao lado da nota.

6. Siga as etapas nos detalhes da recomendação.

Example : reabrir uma recomendação no Trusted Advisor Priority

O exemplo a seguir mostra uma recomendação que você deseja reabrir.



Baixar os detalhes da recomendação

Também é possível baixar os resultados de uma recomendação priorizada do Trusted Advisor Priority.

> **Note**
>
> No momento, é possível fazer o download de apenas uma recomendação por vez.

Para baixar uma recomendação

1. Faça login no console do Trusted Advisor em https://console.aws.amazon.com/trustedadvisor/home.
2. Na página do Trusted Advisor Priority, selecione a recomendação e escolha Download (Baixar).
3. Abra o arquivo para ver os detalhes da recomendação.

Registrar administradores delegados

Você pode adicionar contas-membro que fazem parte de sua organização como administradores delegados. As contas de administrador delegadas podem revisar, reconhecer, resolver, ignorar e reabrir recomendações no Trusted Advisor Priority.

Depois de registrar uma conta, você deve conceder ao administrador delegado as permissões necessárias do AWS Identity and Access Management para acessar o Trusted Advisor Priority. Para obter mais informações, consulte AWS políticas gerenciadas para AWS Trusted Advisor e Gerencie o acesso ao AWS Trusted Advisor.

Você pode registrar até cinco contas-membro. Somente a conta de gerenciamento pode adicionar administradores delegados à organização. É necessário estar conectado à conta de gerenciamento da organização para registrar ou cancelar o registro de um administrador delegado.

Para registrar um administrador delegado

1. Faça login no console do Trusted Advisor em https://console.aws.amazon.com/trustedadvisor/home como a conta de gerenciamento.
2. No painel de navegação, em Preferences (Preferências), escolha Your organization (Sua organização).

3. Em Delegated administrator (Administrador delegado), escolha Register new account (Registrar nova conta).
4. Na caixa de diálogo, insira o ID da conta-membro e selecione Register (Inscrever-se).
5. (Opcional) Para cancelar o registro de uma conta, selecione uma conta e escolha Deregister (Cancelar registro). Na caixa de diálogo, selecione Deregister (Cancelar registro) novamente.

Cancelar o registro dos administradores delegados

Quando você cancelar o registro de uma conta-membro, essa conta não terá mais o mesmo acesso ao Trusted Advisor Priority que a conta de gerenciamento. Contas que não são mais de administradores delegados não receberão notificações por e-mail do Trusted Advisor Priority.

Para cancelar o registro de um administrador delegado

1. Faça login no console do Trusted Advisor em https://console.aws.amazon.com/trustedadvisor/home como a conta de gerenciamento.
2. No painel de navegação, em Preferences (Preferências), escolha Your organization (Sua organização).
3. Em Administradores delegados, selecione uma conta e escolha Cancelar registro.
4. Na caixa de diálogo, escolha Deregister (Cancelar registro).

Gerenciar as notificações do Trusted Advisor Priority

O Trusted Advisor Priority produz notificações por e-mail. Essa notificação por e-mail inclui um resumo das recomendações que sua equipe de contas priorizou para você. Você pode especificar a frequência com a qual recebe atualizações do Trusted Advisor Priority.

Se você registrou contas-membro como administradores delegados, eles também podem configurar suas contas para receber notificações por e-mail do Trusted Advisor Priority.

As notificações por e-mail do Trusted Advisor Priority não incluem resultados de verificação para contas individuais e são separadas da notificação semanal para recomendações do Trusted Advisor. Para obter mais informações, consulte Configurar as preferências de notificação.

> **Note**
>
> Somente a conta de gerenciamento ou o administrador delegado pode configurar notificações do Trusted Advisor Priority por e-mail.

Para gerenciar suas notificações do Trusted Advisor Priority.

1. Faça login no console do Trusted Advisor em https://console.aws.amazon.com/trustedadvisor/home como a conta de gerenciamento ou de administrador delegado.
2. No painel de navegação, em Preferences (Preferências), escolha Notifications (Notificações).
3. Em Priority, você poderá selecionar as opções a seguir.
   a. Daily (Diariamente): receber uma notificação por e-mail diariamente.
   b. Weekly (Semanalmente): receber uma notificação por e-mail uma vez por semana.
   c. Escolha as notificações a serem recebidas:
      - Resumo de recomendações priorizadas
      - Datas de resolução
4. Para Destinatários, selecione outros contatos dos quais deseja receber as notificações por e-mail. É possível adicionar e remover contatos da página Account Settings (Configurações da conta) no console do AWS Billing and Cost Management.
5. Em Language (Idioma), escolha o idioma da notificação por e-mail.
6. Escolha Save your preferences (Salvar suas preferências).

> **Note**
>
> O Trusted Advisor Priority envia notificações por e-mail pelo endereço noreply@notifications.trustedadvisor.us-west-2.amazonaws.com. Talvez seja necessário verificar se o seu cliente de e-mail não identifica esses e-mails como spam.

Desabilitar o Trusted Advisor Priority

Entre em contato com sua equipe de contas e peça que esse recurso seja desabilitado. Depois que esse recurso é desabilitado, as recomendações priorizadas não aparecem mais em seu console do Trusted Advisor.

Se você desabilitar o Trusted Advisor Priority e habilitá-lo mais tarde, ainda poderá visualizar as recomendações que a sua equipe de contas enviou antes de você desabilitar o Trusted Advisor Priority.

Comece a usar o AWS Trusted Advisor Engage (versão pré-visualização)

> **Note**
>
> O AWS Trusted Advisor Engage é uma versão de pré-visualização e está sujeita a alterações. Você pode acessar a versão de pré-visualização dos termos de serviço aqui https://aws.amazon.com/service-terms/.

Você pode usar o AWS Trusted Advisor Engage para aproveitar ao máximo seus planos do AWS Support, facilitando a visualização, a solicitação e o rastreamento de todas as suas interações proativas e a comunicação com sua equipe da Conta da AWS sobre as interações contínuas.

Por exemplo, você pode solicitar uma “Análise de negócios gerenciais” para sua equipe da Conta da AWS acessando a página Engage no console do AWS Trusted Advisor. Em seguida, um especialista da AWS será designado para atender à sua solicitação e acompanhará toda a interação.

Tópicos

- Pré-requisitos
- Visualize o painel de interações
- Visualize o catálogo de tipos de interação
- Solicitar uma interação
- Editar uma interação
- Enviar anexos e notas

- Alterar o status da interação
- Diferencie entre as interações recomendadas e solicitadas
- Pesquisar interações

Pré-requisitos

Você deve tomar as medidas necessárias para atender aos seguintes requisitos para usar o Trusted Advisor Engage:

- Você deve ter um plano Enterprise On-Ramp Support.
- Sua conta deve fazer parte de uma organização que tenha habilitado todos os recursos no AWS Organizations. Para obter mais informações, consulte Habilitar todos os atributos na sua organização no Manual do usuário do AWS Organizations.
- Sua organização deve ter o acesso confiável ao Trusted Advisor habilitado. Você pode habilitar o acesso confiável fazendo login como a conta de gerenciamento e acessando a página Sua organização no console do Trusted Advisor.
- Você precisa ter permissões do AWS Identity and Access Management (IAM) para acessar o Trusted Advisor Engage. Para obter informações sobre como controlar o acesso ao Trusted Advisor Engage, consulte Gerencie o acesso ao AWS Trusted Advisor.

> **Note**
>
> Qualquer conta em uma organização da AWS pode criar uma solicitação de interação. Se uma conta proprietária da interação for transferida para outra organização da AWS, a interação só ficará acessível por essa conta. Para limitar os controles, consulte Políticas de controle de serviço de exemplo para o AWS Trusted Advisor.

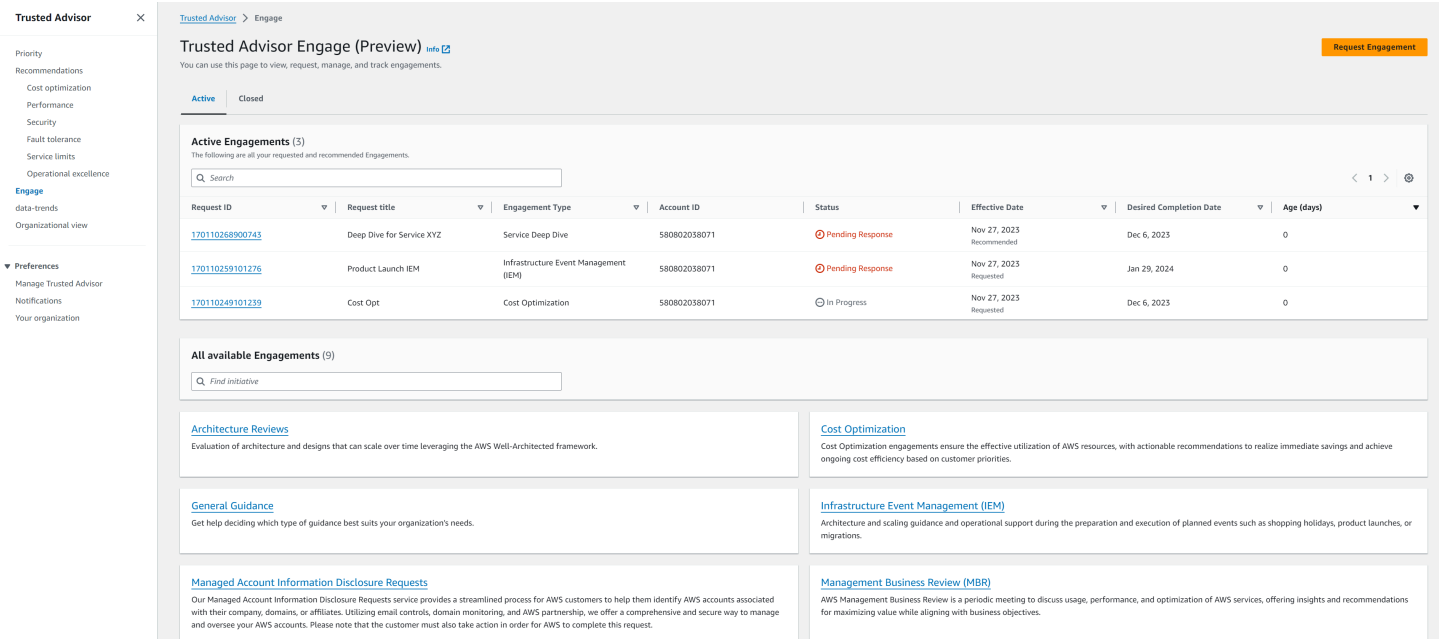
Visualize o painel de interações

Depois de obter os direitos de acesso, você pode acessar a página Trusted Advisor Engage no console do Trusted Advisor para visualizar um painel em que você pode gerenciar as interações com sua equipe da Conta da AWS.

Para gerenciar suas interações:

1. Faça login no console do Trusted Advisor em https://console.aws.amazon.com/trustedadvisor/home.
2. Na página Trusted Advisor Engage, você pode visualizar:
   - Botão Solicitação de interação
   - Tabela Interações ativas
   - Tabela Interações concluídas
   - Catálogo de todas as interações disponíveis

Example : painel de interações



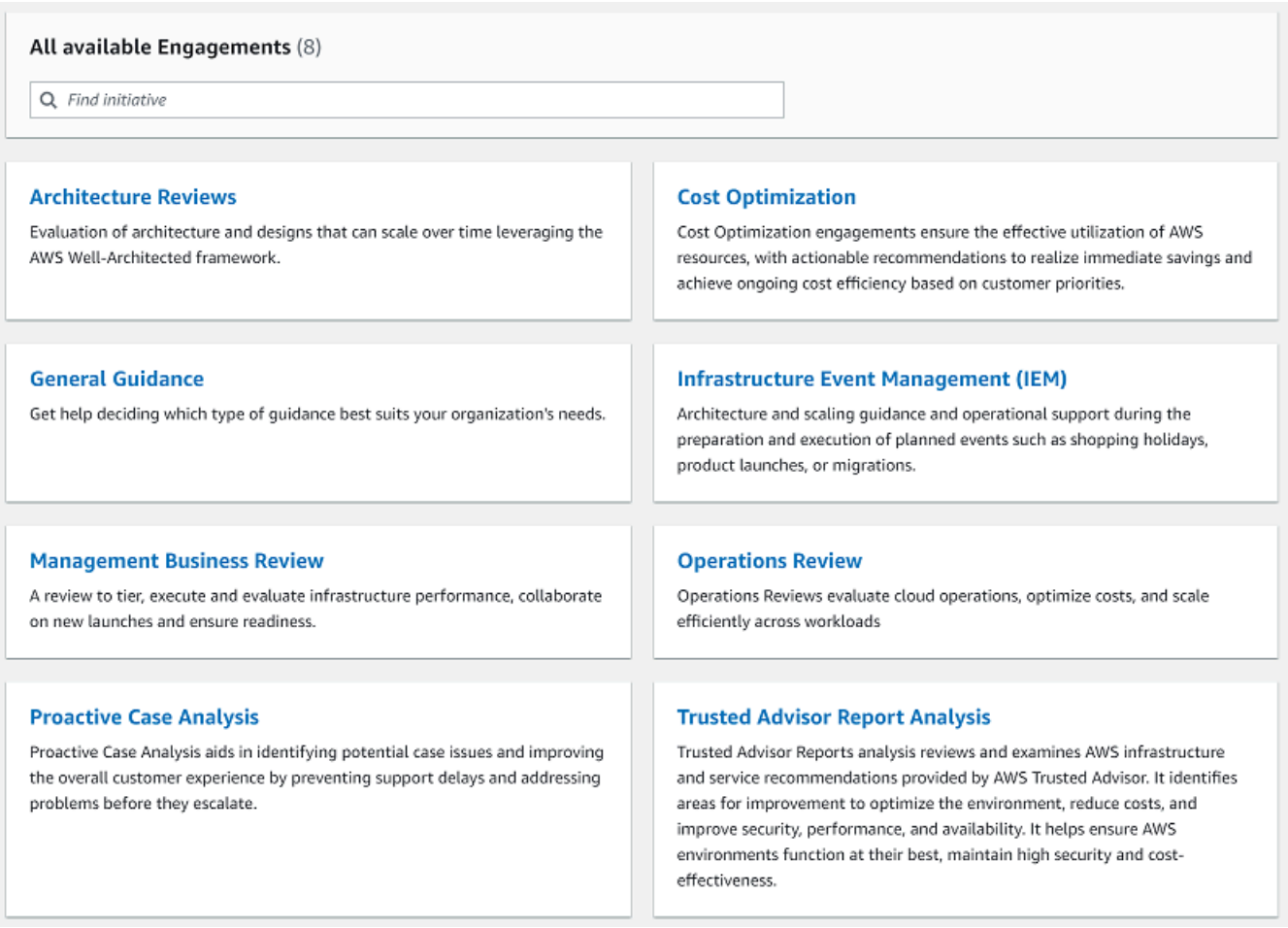
Visualize o catálogo de tipos de interação

Você pode ver o catálogo de tipos de interação para encontrar os tipos mais recentes de interação que podem ser solicitadas à sua equipe da Conta da AWS.

Visualizar o catálogo de tipos de interação:

1. Faça login no console do Trusted Advisor em https://console.aws.amazon.com/trustedadvisor/home.
2. Na página Trusted Advisor Engage, você pode encontrar o catálogo de tipos de interação.

Example : catálogo de tipos de interação



Solicitar uma interação

Você pode solicitar interações para sua equipe da Conta da AWS de acordo com os tipos de interação incluídos em seu plano de suporte da AWS.

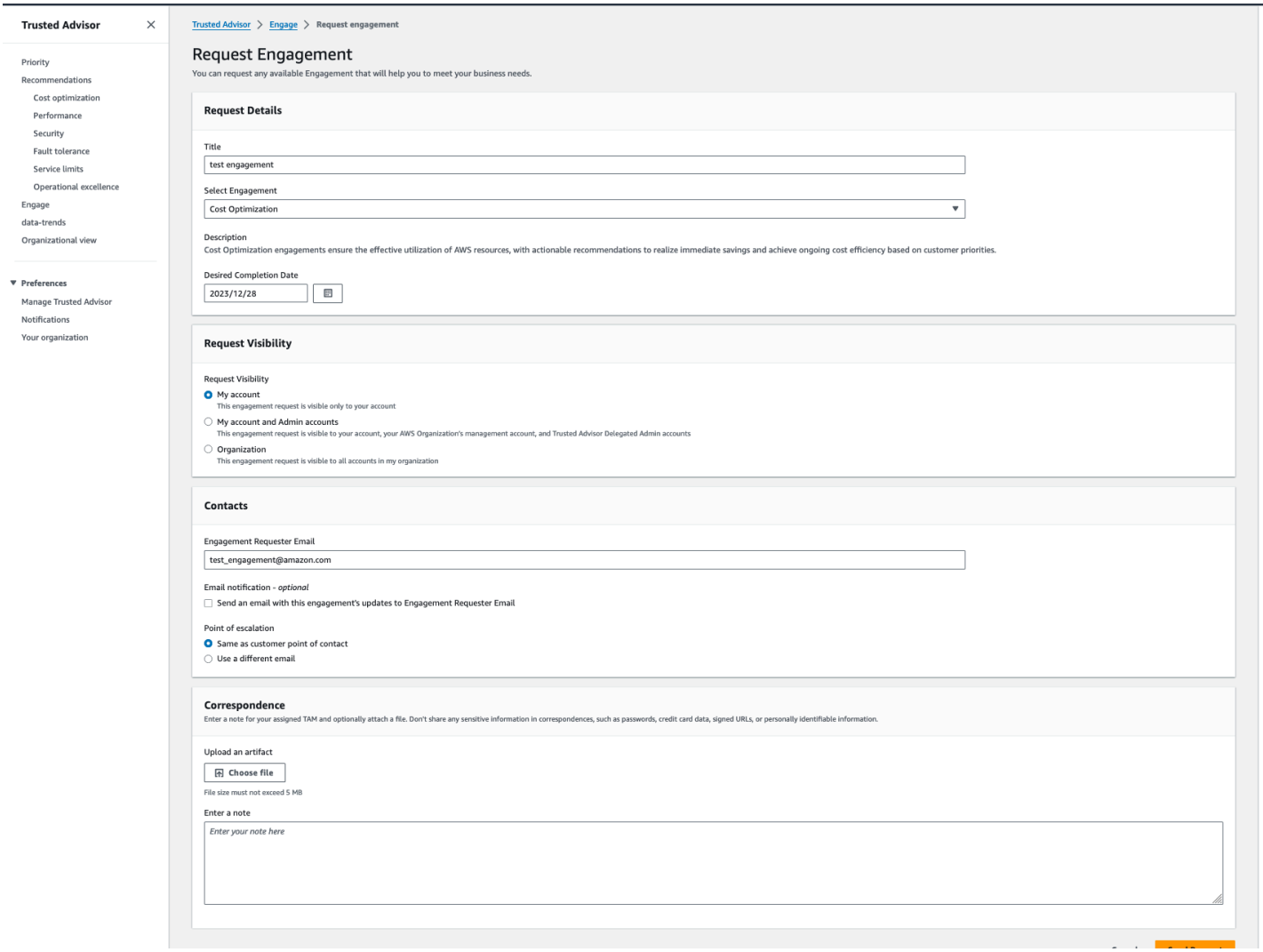
Para solicitar uma interação:

1. Faça login no console do Trusted Advisor em https://console.aws.amazon.com/trustedadvisor/home.
2. Na página Trusted Advisor Engage, escolha Solicitar interação.
3. Preencha:
   - Título
   - Selecione interação: o tipo de interação que você deseja solicitar.

- Data de conclusão desejada: a data de conclusão desejada da interação. Cada tipo de interação tem um prazo de entrega diferente, calculado na data mínima de conclusão desejada.
- Solicitar visibilidade:
  - Minha conta: essa solicitação de interação fica visível somente em sua conta.
  - Minha conta e contas de administrador: essa solicitação de interação fica visível em sua conta, na conta de gerenciamento e em todas as contas de administrador delegado da sua organização da AWS.
  - Organização: esta solicitação de interação fica visível para todas as contas da sua organização da AWS.
- E-mail do solicitante de engajamento: o endereço de e-mail que AWS será usado como o principal ponto de contato para esse compromisso.
- Configurações de notificação por e-mail: escolha se o e-mail do solicitante do engajamento receberá notificações por e-mail sobre o engajamento.
- Ponto de escalonamento: o endereço de e-mail que a AWS usará quando um escalonamento for necessário para essa interação.
- Correspondência: uma nota e um anexo de arquivo opcional para você fornecer detalhes sobre essa interação.

4. Escolha Enviar solicitação.

Example : solicitar interação



Editar uma interação

Você pode editar os detalhes da sua solicitação de interação.

Para editar uma interação:

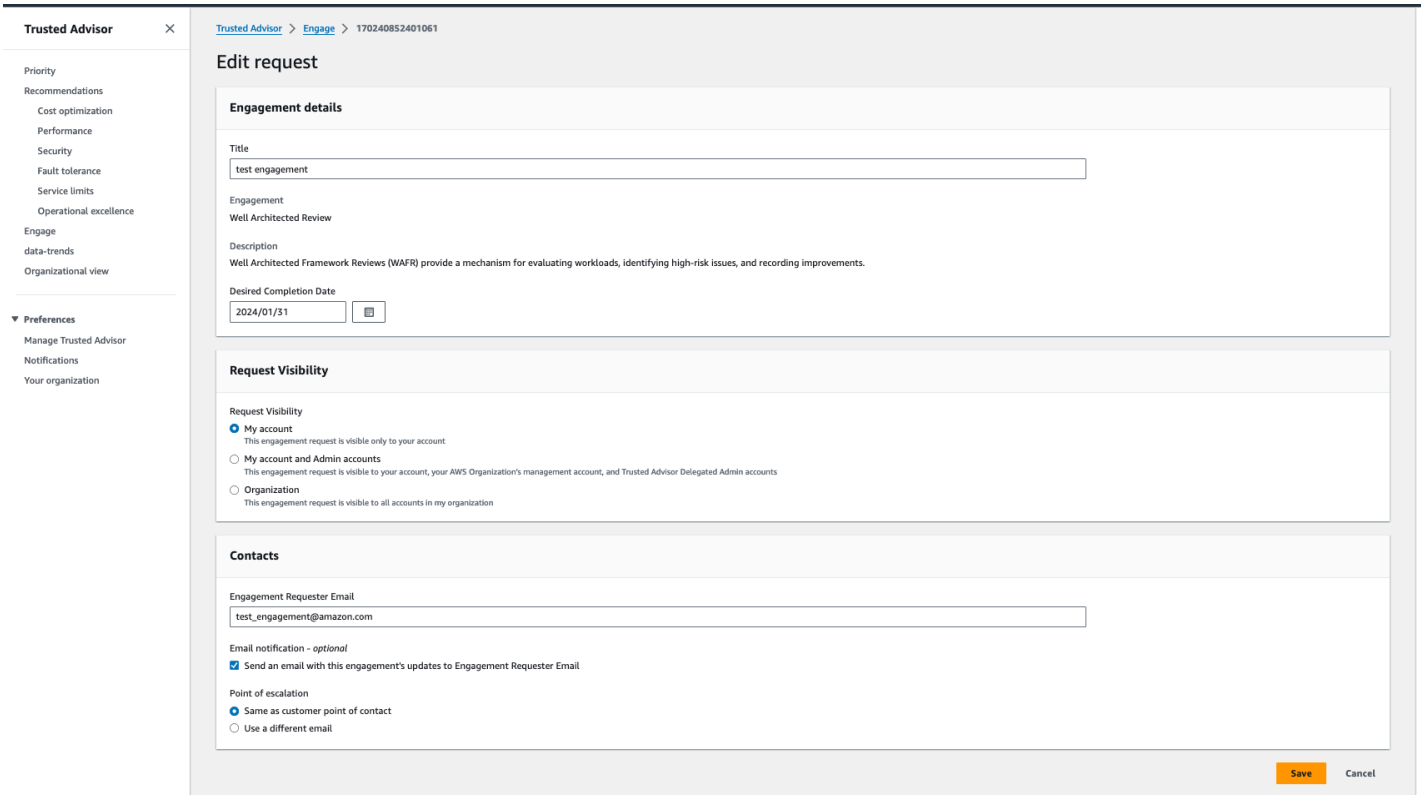
1. Faça login no console do Trusted Advisor em https://console.aws.amazon.com/trustedadvisor/home.
2. Na página Trusted Advisor Engage, selecione uma interação existente.
3. Selecione Edit (Editar).
4. Você pode editar:

    - Título

- Data de conclusão desejada: a data de conclusão desejada da interação. Cada tipo de interação tem um prazo de entrega diferente, calculado na data mínima de conclusão desejada.
- Solicitar visibilidade:
  - Minha conta: essa solicitação de interação fica visível somente em sua conta.
  - Minha conta e contas de administrador: essa solicitação de interação fica visível em sua conta, na conta de gerenciamento e em todas as contas de administrador delegado da sua organização da AWS.
  - Organização: esta solicitação de interação fica visível para todas as contas da sua organização da AWS.
- E-mail do solicitante de engajamento: o endereço de e-mail que AWS será usado como o principal ponto de contato para esse compromisso.
- Configurações de notificação por e-mail: escolha se o e-mail do solicitante do engajamento receberá notificações por e-mail sobre o engajamento.
- Ponto de escalonamento: o endereço de e-mail que a AWS usará quando um escalonamento for necessário para essa interação.

5. Escolha Salvar.

Example : editar interação



Enviar anexos e notas

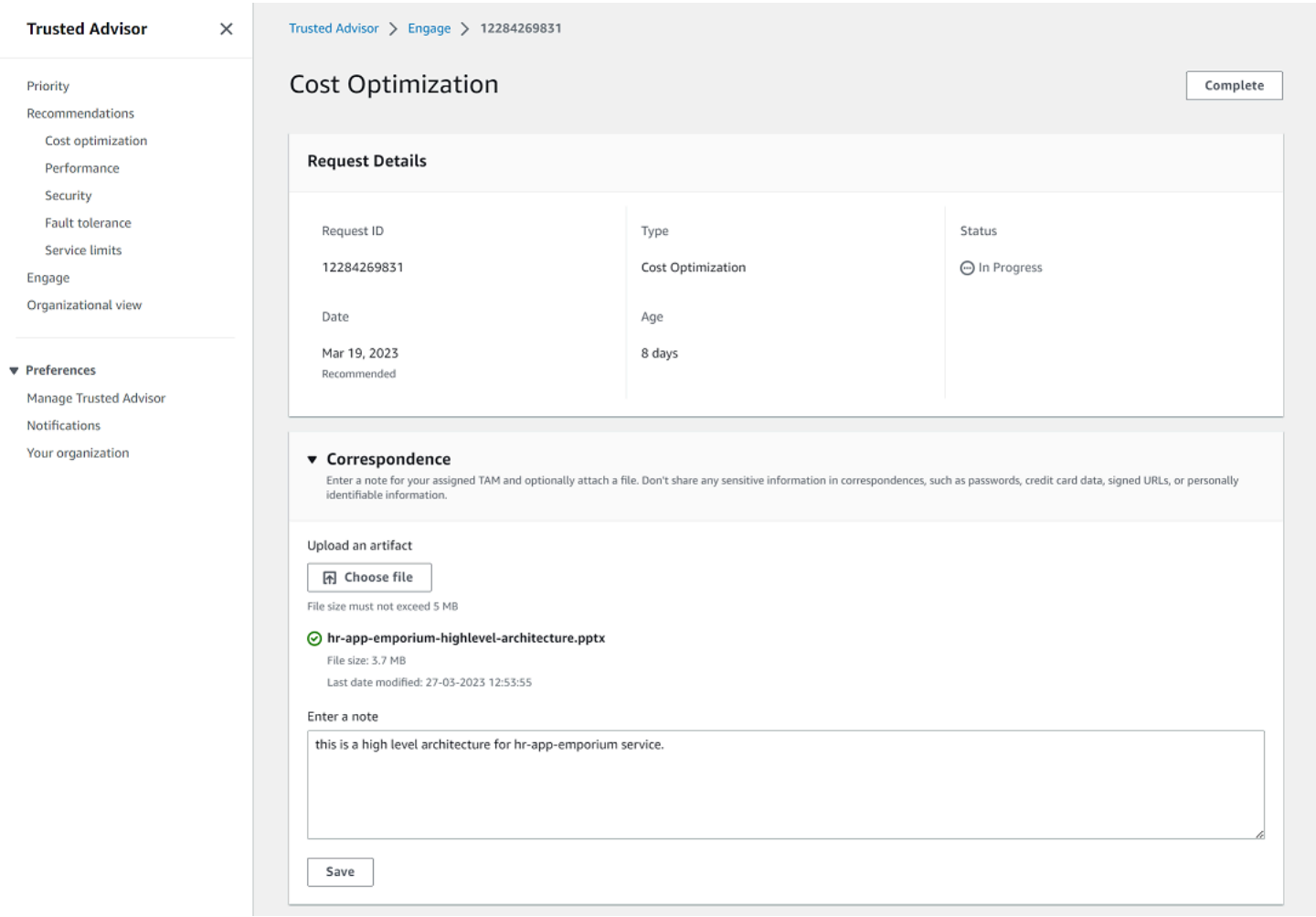
Você pode se comunicar com sua equipe da Conta da AWS em interações individuais enviando notas e anexos de arquivo para dar suporte à sua solicitação de interação. Você pode incluir um único anexo e uma nota por comunicação, só pode anexar arquivos a uma interação com a mesma Conta da AWS que solicitou a interação e não pode excluir anexos ou notas após o envio de uma comunicação.

Para anexar arquivos ou adicionar notas a uma solicitação de interação ativa:

1. Faça login no console do Trusted Advisor em https://console.aws.amazon.com/trustedadvisor/home.
2. Na página Trusted Advisor Engage, escolha o ID da interação ativa à qual você gostaria de anexar arquivos ou adicionar notas.
3. Escolha Correspondência para expandir o formulário.
4. Insira uma nota para o TAM atribuído e, opcionalmente, anexe um arquivo. Não compartilhe informações confidenciais em correspondências, como senhas, dados de cartão de crédito, URLs assinados ou informações de identificação pessoal.

5. Escolha Salvar.

Example : adicionar nota e anexar arquivo a uma interação



Alterar o status da interação

Você pode alterar o status das interações para cancelar as interações com resposta pendente, concluir as interações que estão em andamento e reabrir as interações marcadas como canceladas ou fechadas.

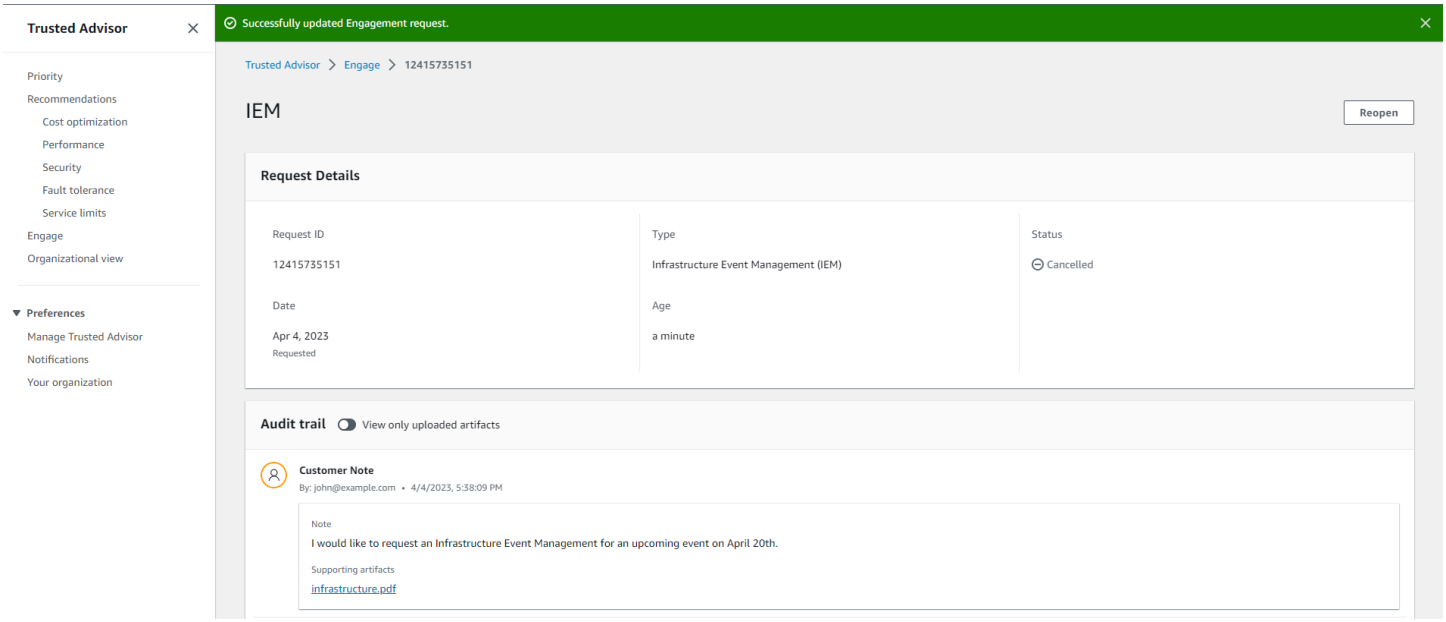
Para alterar o status de uma interação:

1. Faça login no console do Trusted Advisor em https://console.aws.amazon.com/trustedadvisor/home.
2. Na página Trusted Advisor Engage, escolha o ID da interação ativa cujo status você gostaria de alterar.

3. Na página de detalhes das interações, você pode alterar o status para Cancelada ou Concluída.

   - Você pode selecionar Cancelar quando o status da interação for Resposta pendente.
   - Você pode selecionar Concluída quando o status da interação estiver Em andamento.
   - Você pode selecionar Reabrir para interações concluídas. As interações canceladas são movidas para Resposta pendente, enquanto as interações concluídas são movidas para Em andamento.

Example : alterar o status da interação



Diferencie entre as interações recomendadas e solicitadas

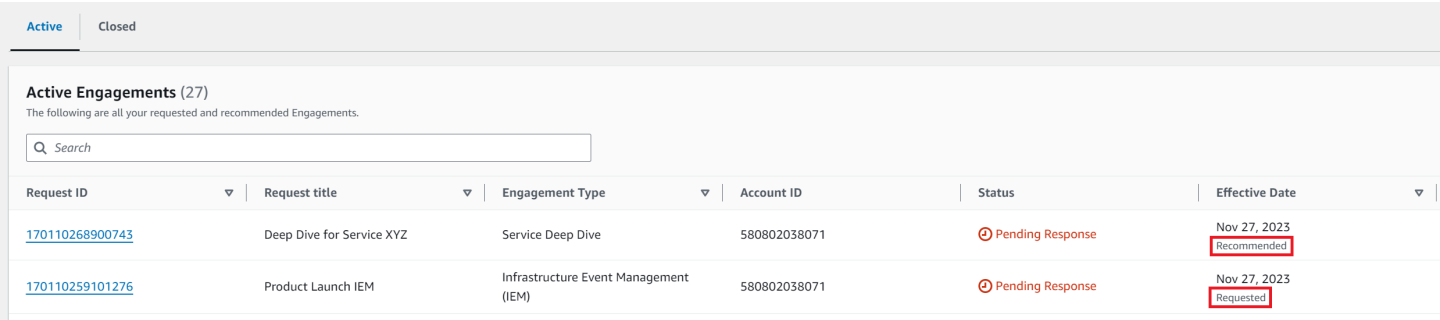
Você pode identificar a origem das interações para saber se uma interação foi solicitada por você ou recomendada pela sua equipe da Conta da AWS.

Para ver diferentes origens de interações ativas:

1. Faça login no console do Trusted Advisor em https://console.aws.amazon.com/trustedadvisor/home.
2. Na página Trusted AdvisorEngajamento, veja a coluna Data de vigência para distinguir entre compromissos recomendados e solicitados:

   - Recomendada: solicitação de interação criada por suas equipes da Conta da AWS.
   - Solicitada: solicitação de interação criada pelo usuário.

Example : diferencie entre as interações recomendadas e solicitadas



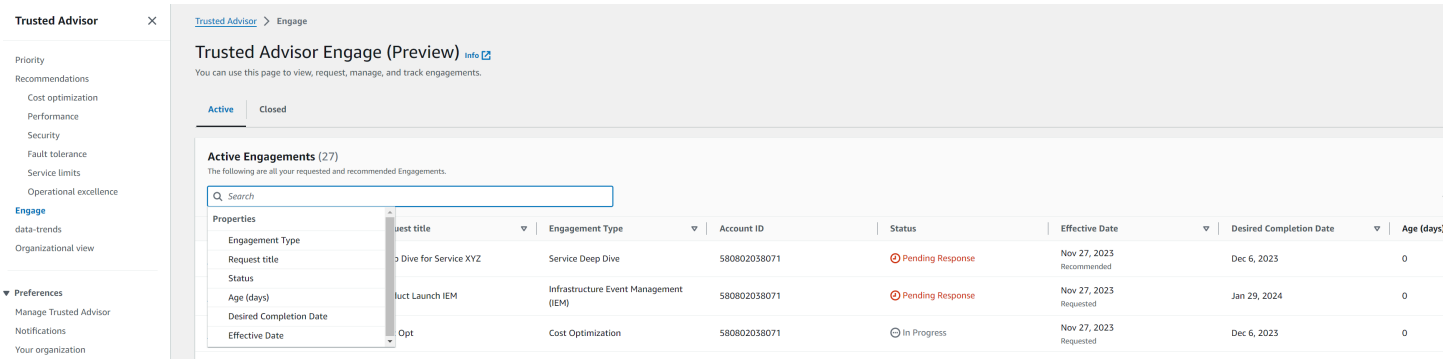
Pesquisar interações

Você pode pesquisar suas interações ativas e concluídas existentes usando filtros.

Para pesquisar interações:

1. Faça login no console do Trusted Advisor em https://console.aws.amazon.com/trustedadvisor/home.
2. Na página Trusted Advisor Engage, você pode selecionar os seguintes filtros:
   - Idade (dias)
   - Tipo de interação
   - Título da solicitação
   - Status
   - Data de conclusão desejada
   - Data de vigência

Example : pesquisar interações



Referência de verificação do AWS Trusted Advisor

É possível visualizar todas os nomes, descrições e IDs de verificações do Trusted Advisor na referência a seguir. Também é possível fazer login no console do Trusted Advisor para exibir mais informações sobre as verificações, ações recomendadas e seus status.

Se você tiver um plano de suporte Business, Enterprise On-Ramp ou Enterprise, poderá usar a API do AWS Trusted Advisor e a AWS Command Line Interface (AWS CLI) para acessar todas as verificações. Para obter informações, consulte os tópicos a seguir:

- Comece a usar a Trusted Advisor API
- Referência de API do AWS Trusted Advisor

> **Note**
>
> Se você tiver um plano de suporte Básico e de Desenvolvedor, poderá usar o console do Trusted Advisor para acessar todas as verificações na categoria de Limites do serviço e as seguintes verificações na categoria de segurança:
>
> - Snapshots públicos do Amazon EBS
> - Snapshots públicos do Amazon RDS
> - Permissões do bucket do Amazon S3
> - Uso do IAM
> - MFA na conta raiz
> - Grupos de segurança - Portas específicas irrestritas

Categorias de verificação

- Otimização de custo
- Performance
- Segurança
- Tolerância a falhas
- Limites do serviço
- Excelência operacional

Otimização de custo

É possível usar as verificações a seguir para a categoria de otimização de custos.

Nomes da verificação

- Conta da AWS que não faz parte do AWS Organizations
- Endpoints do Amazon Comprehend subutilizados
- Volumes superprovisionados do Amazon EBS
- Consolidação de instâncias do Amazon EC2 para Microsoft SQL Server
- Instâncias do Amazon EC2 superprovisionadas para Microsoft SQL Server
- Instâncias do Amazon EC2 interrompidas
- Vencimento da locação de instâncias reservadas do Amazon EC2
- Otimização de instâncias reservadas do Amazon EC2
- Repositório do Amazon ECR sem política de ciclo de vida configurada
- Otimização de nós ElastiCache reservados da Amazon
- Otimização de instâncias reservadas do Amazon OpenSearch Service
- Amazon RDS Idle DB Instances
- Otimização de nó reservado do Amazon Redshift
- Otimização de instância reservada do Amazon Relational Database Service (RDS)
- Conjuntos de registros de recursos de latência no Amazon Route 53.
- Política de ciclo de vida do bucket do Amazon S3 configurada
- Configuração de cancelamento de upload em várias partes incompleta do Amazon S3
- Buckets habilitados para a versão do Amazon S3 sem políticas de ciclo de vida configuradas
- O AWS Lambda funciona com tempo limite excessivo
- O AWS Lambda funciona com altas taxas de erro
- Funções superprovisionadas do AWS Lambda para tamanho de memória
- Problemas de alto risco do AWS Well-Architected para otimização de custos
- Balanceadores de carga obsoletos
- Instâncias do Amazon EC2 com pouca utilização
- Savings Plan

- Endereços de IP elástico não associados
- Volumes subutilizados do Amazon EBS
- Clusters subutilizados do Amazon Redshift

Conta da AWS que não faz parte do AWS Organizations

Descrição

Verifica se uma conta da AWS faz parte da conta de gerenciamento do AWS Organizations apropriada.

O AWS Organizations é um serviço de gerenciamento de contas para consolidar várias contas da AWS em uma organização gerenciada de forma centralizada. Isso permite que você estruture contas de forma centralizada para consolidação de faturamento e implemente políticas de propriedade e segurança à medida que suas workloads escalam na AWS.

Você pode especificar o ID da conta de gerenciamento usando o MasterAccountIdparâmetro das AWS Config regras.

Para obter mais informações, consulte O que é o AWS Organizations?

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c18d2gz127`

Origem

`AWS Config Managed Rule: account-part-of-organizations`

Critérios de alerta

Amarelo: esta conta da AWS não faz parte do AWS Organizations.

Recommended Action (Ação recomendada)

Adicione essa conta da AWS como parte do AWS Organizations.

Para obter mais informações, consulte o Tutorial: criar e configurar uma organização.

Colunas do relatório

- Status
- Região
- Recurso
- Regra do AWS Config
- Parâmetros de entrada
- Hora da última atualização

Endpoints do Amazon Comprehend subutilizados

Descrição

Verifica a configuração do throughput dos seus endpoints. Essa verificação alerta quando os endpoints não são usados ativamente para solicitações de inferência em tempo real. Um endpoint que não é usado por mais de 15 dias consecutivos é considerado subutilizado. Todos os endpoints acumulam cobranças com base tanto no conjunto de throughput, quanto no período em que o endpoint está ativo.

> **Note**
>
> Essa verificação é atualizada automaticamente uma vez por dia. Não é possível excluir recursos dessa verificação.

ID da verificação

`Cm24dfsM12`

Critérios de alerta

Amarelo: o endpoint está ativo, mas não foi usado para solicitações de inferência em tempo real nos últimos 15 dias.

Recommended Action (Ação recomendada)

Se o endpoint não tiver sido usado nos últimos 15 dias, recomendamos definir uma política de escalabilidade para o recurso usando Application Autoscaling (Autoescalabilidade de aplicações).

Se o endpoint tiver uma política de escalabilidade definida e não tiver sido usado nos últimos 30 dias, considere excluir o endpoint e usar inferência assíncrona. Para obter mais informações, consulte Deleting an endpoint with Amazon Comprehend (Excluir um endpoint com o Amazon Comprehend).

Colunas do relatório

- Status
- Região
- ARN do endpoint
- Unidade de inferência provisionada
- AutoScaling Status
- Motivo
- Hora da última atualização

Volumes superprovisionados do Amazon EBS

Descrição

Verifica os volumes do Amazon Elastic Block Store (Amazon EBS) que estavam em execução a qualquer momento durante o período retroativo. Essa verificação alerta se algum volume do EBS tiver sido provisionado em excesso para suas workloads. Quando há volumes superprovisionados, você está pagando por recursos não utilizados. Embora alguns cenários possam resultar em baixa otimização deliberadamente, geralmente você pode reduzir os custos alterando a configuração de seus volumes do EBS. As estimativas de economia mensal são calculadas usando a taxa de uso atual para volumes do EBS. A economia real variará se o volume não estiver presente por um mês inteiro.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`C0r6dfpM03`

Critérios de alerta

Amarelo: um volume do EBS que foi provisionado em excesso durante o período de retrospectiva. Para determinar se um volume está superprovisionado, consideramos todas as CloudWatch métricas padrão (incluindo IOPS e taxa de transferência). O algoritmo usado para identificar volumes do EBS provisionados em excesso segue as práticas recomendadas da AWS. O algoritmo é atualizado quando um novo padrão é identificado.

Recommended Action (Ação recomendada)

Considere reduzir o tamanho de volumes que têm baixa utilização.

Para obter mais informações, consulte Optar por verificações do Trusted Advisor para o AWS Compute Optimizer.

Colunas do relatório

- Status
- Região
- ID de volume
- Tipo de volume
- Tamanho do volume (GB)
- IOPS de referência do volume
- IOPS de intermitência do volume
- Throughput de intermitência do volume
- Tipo do volume recomendado
- Tamanho do volume recomendado (GB)
- IOPS de referência do volume recomendadas
- IOPS de intermitência do volume recomendadas
- Throughput de referência do volume recomendada
- Throughput de intermitência do volume recomendada
- Período de retrospectiva (dias)
- Oportunidade de economia (%)
- Economia mensal estimada

- Moeda da economia mensal estimada
- Hora da última atualização

Consolidação de instâncias do Amazon EC2 para Microsoft SQL Server

Descrição

Verifica suas instâncias do Amazon Elastic Compute Cloud (Amazon EC2) que estão executando o SQL Server nas últimas 24 horas. Essa verificação alerta se sua instância tiver menos do que o número mínimo de licenças do SQL Server. No Guia de licenciamento do Microsoft SQL Server, você está pagando 4 licenças de vCPU, mesmo que uma instância tenha apenas 1 ou 2 vCPUs. Você pode consolidar instâncias menores do SQL Server para ajudar a reduzir custos.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`Qsdfp3A4L2`

Critérios de alerta

Amarelo: uma instância com SQL Server tem menos de 4 vCPUs.

Recommended Action (Ação recomendada)

Considere consolidar workloads menores do SQL Server em instâncias com pelo menos 4 vCPUs.

Recursos adicionais

- Microsoft SQL Server na AWS
- Licenciamento da Microsoft na AWS
- Guia de licenciamento do Microsoft SQL Server

Colunas do relatório

- Status

- Região
- ID da instância
- Tipo de instância
- vCPU
- Mínimo de vCPU
- Edição do SQL Server
- Hora da última atualização

Instâncias do Amazon EC2 superprovisionadas para Microsoft SQL Server

Descrição

Verifica suas instâncias do Amazon Elastic Compute Cloud (Amazon EC2) que estão executando o SQL Server nas últimas 24 horas. Um banco de dados do SQL Server tem um limite de capacidade computacional para cada instância. Uma instância com o SQL Server Standard edition pode usar até 48 vCPUs. Uma instância com o SQL Server Web pode usar até 32 vCPUs. Essa verificação alerta se uma instância exceder esse limite de vCPUs.

Se sua instância estiver superprovisionada, você pagará o preço total sem perceber uma melhoria na performance. Você pode gerenciar o número e o tamanho de suas instâncias para ajudar a reduzir os custos.

As economias mensais estimadas são calculadas usando a mesma família de instâncias com o número máximo de vCPUs que uma instância do SQL Server pode usar e a definição de preço sob demanda. As economias reais variam se você estiver usando Instâncias Reservadas (RI), ou se a instância não estiver sendo executada por um dia inteiro.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`Qsdfp3A4L1`

Critérios de alerta

- Vermelho: uma instância com o SQL Server Standard Edition tem mais de 48 vCPUs.
- Vermelho: uma instância com o SQL Server Web Edition tem mais de 32 vCPUs.

Recommended Action (Ação recomendada)

Para a SQL Server Standard Edition, considere mudar para uma instância na mesma família de instâncias com 48 vCPUs. Para a SQL Server Web Edition, considere mudar para uma instância na mesma família de instâncias com 32 vCPUs. Se o uso de memória for intensivo, considere mudar para instâncias R5 otimizadas para memória. Para obter mais informações, consulte Best Practices for Deploying Microsoft SQL Server on Amazon EC2 (Práticas recomendadas para implantar o Microsoft SQL Server no Amazon EC2).

Recursos adicionais

- Microsoft SQL Server na AWS
- Você pode usar o Assistente de inicialização para simplificar a implantação do SQL Server no EC2.

Colunas do relatório

- Status
- Região
- ID da instância
- Tipo de instância
- vCPU
- Edição do SQL Server
- Máximo de vCPU
- Tipo de instância recomendado
- Economia mensal estimada
- Hora da última atualização

Instâncias do Amazon EC2 interrompidas

Descrição

Verifica se há instâncias do Amazon EC2 interrompidas por mais de 30 dias.

Você pode especificar o valor do número permitido de dias nos AWS Config parâmetros AllowedDaysof.

Para obter mais informações, consulte Por que o Amazon EC2 está sendo cobrado, se todas as minhas instâncias foram encerradas?

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c18d2gz150`

Origem

`AWS Config Managed Rule: ec2-stopped-instance`

Critérios de alerta

- Amarelo: há instâncias do Amazon EC2 interrompidas por mais tempo que o número permitido de dias.

Recommended Action (Ação recomendada)

Revise as instâncias do Amazon EC2 que estão interrompidas há 30 dias ou mais. Para evitar custos desnecessários, encerre todas as instâncias que não são mais necessárias.

Para obter mais informações, consulte Encerrar a instância.

Recursos adicionais

- Precificação sob demanda do Amazon EC2

Colunas do relatório

- Status
- Região
- Recurso
- Regra do AWS Config
- Parâmetros de entrada

- Hora da última atualização

Vencimento da locação de instâncias reservadas do Amazon EC2

Descrição

Verifica as instâncias reservadas do Amazon EC2 que estão programadas para expirar nos próximos 30 dias, ou que tenham expirado nos 30 dias anteriores.

As instâncias reservadas não são renovadas automaticamente. É possível continuar usando uma instância do Amazon EC2 coberta pela reserva sem interrupções, mas serão cobradas taxas sob demanda. Novas Instâncias Reservadas podem ter os mesmos parâmetros que as expiradas ou é possível comprar Instâncias Reservadas com parâmetros diferentes.

A economia mensal estimada é a diferença entre as taxas de Instância Sob demanda e Reservada para o mesmo tipo de instância.

ID da verificação

`1e93e4c0b5`

Critérios de alerta

- Amarelo: o leasing da instância reservada expira em menos de 30 dias.
- Amarelo: o leasing da instância reservada expirou nos últimos 30 dias.

Recommended Action (Ação recomendada)

Considere comprar uma nova instância reservada para substituir a que está se aproximando do final do prazo. Para obter mais informações, consulte How to Purchase Reserved Instances (Como comprar instâncias reservadas) e Buying Reserved Instances (Comprar instâncias reservadas).

Recursos adicionais

- Instâncias reservadas
- Instance Types (Tipos de instâncias)

Colunas do relatório

- Status
- Zona
- Tipo de instância

- Plataforma
- Contagem de instância
- Custo mensal atual
- Economia mensal estimada
- Data de validade
- ID da Instância reservada
- Motivo

Otimização de instâncias reservadas do Amazon EC2

Descrição

Uma parte importante na utilização da AWS envolve o equilíbrio do uso de instâncias reservadas (RI) e seu próprio uso de instâncias sob demanda. Esta verificação fornece recomendações sobre quais IRs ajudarão a reduzir os custos incorridos com o uso de Instâncias sob demanda.

Criamos essas recomendações analisando seu uso sob demanda nos últimos 30 dias. Em seguida, categorizamos o uso em categorias elegíveis para reservas. Simulamos cada combinação de reservas na categoria de uso gerada para identificar o número recomendado de cada tipo de IR a ser comprado. Esse processo de simulação e otimização nos permite maximizar sua economia de custos. Essa verificação abrange recomendações baseadas em Instâncias Reservadas Padrão com a opção de pagamento antecipado parcial.

Essa verificação não está disponível para contas vinculadas no faturamento consolidado. As recomendações para essa verificação só estão disponíveis para a conta de pagamento.

ID da verificação

`cX3c2R1chu`

Critérios de alerta

Amarelo: otimizar o uso de IRs adiantadas parciais pode ajudar a reduzir custos.

Recommended Action (Ação recomendada)

Consulte a página do Cost Explorer para obter recomendações mais detalhadas e personalizadas. Além disso, consulte o guia de compras para entender como comprar RIs e as opções disponíveis.

Recursos adicionais

- Informações sobre IRs e como elas podem economizar seu dinheiro podem ser encontradas aqui.
- Para obter mais informações sobre essa recomendação, consulte Reserved Instance Optimization Check Questions (Perguntas sobre verificação de otimização de instâncias reservadas) nas Perguntas frequentes sobre o Trusted Advisor.

Colunas do relatório

- Região
- Tipo de instância
- Plataforma
- Número recomendado de IRs para compra
- Utilização média esperada de IR
- Economia estimada com recomendações (mensal)
- Custo inicial das IRs
- Custos estimados das IRs (mensal)
- Custo estimado sob demanda após a compra recomendada de IR (mensal)
- Ponto de equilíbrio estimado (meses)
- Período de retrospectiva (dias)
- Prazo (anos)

Repositório do Amazon ECR sem política de ciclo de vida configurada

Descrição

Verifica se um repositório privado do Amazon ECR tem pelo menos uma política de ciclo de vida configurada. As políticas de ciclo de vida permitem que você defina um conjunto de regras para limpar automaticamente imagens de contêineres antigas ou não utilizadas. Isso lhe dá controle sobre o gerenciamento do ciclo de vida das imagens, permite que os repositórios do Amazon ECR sejam mais bem organizados e ajuda a reduzir os custos gerais de armazenamento.

Para obter mais informações, consulte Políticas de ciclo de vida.

ID da verificação

`c18d2gz128`

Origem

```
AWS Config Managed Rule: ecr-private-lifecycle-policy-configured
```

Critérios de alerta

Amarelo: um repositório privado do Amazon ECR não tem nenhuma política de ciclo de vida configurada.

Recommended Action (Ação recomendada)

Considere criar pelo menos uma política de ciclo de vida para seu repositório privado do Amazon ECR.

Para obter mais informações, consulte Criar uma política de ciclo de vida.

Recursos adicionais

- Políticas de ciclo de vida.
- Criar uma política de ciclo de vida.
- Exemplos de políticas de ciclo de vida.

Colunas do relatório

- Status
- Região
- Recurso
- Regra do AWS Config
- Parâmetros de entrada
- Hora da última atualização

Otimização de nós ElastiCache reservados da Amazon

Descrição

Verifica seu uso ElastiCache e fornece recomendações sobre a compra de nós reservados. Essas recomendações são oferecidas para reduzir os custos decorrentes do uso do ElastiCache On-Demand. Criamos essas recomendações analisando seu uso sob demanda nos últimos 30 dias.

Utilizamos essa análise para simular todas as combinações de reservas na categoria de utilização gerada. Isso nos permite recomendar o número de cada tipo de nó reservado a ser

comprado para maximizar a economia. Este verificação abrange recomendações baseadas na opção de pagamento antecipado parcial com compromisso de 1 ou 3 anos.

Essa verificação não está disponível para contas vinculadas no faturamento consolidado. As recomendações para essa verificação só estão disponíveis para a conta de pagamento.

ID da verificação

`h3L1otH3re`

Critérios de alerta

Amarelo: otimizar a compra de nós ElastiCache reservados pode ajudar a reduzir custos.

Recommended Action (Ação recomendada)

Consulte a página Cost Explorer para obter recomendações mais detalhadas, opções de personalização (por exemplo, período de retrospectiva, opção de pagamento etc.) e para comprar Nodes Reservados. ElastiCache

Recursos adicionais

- Informações sobre nós ElastiCache reservados e como eles podem economizar dinheiro podem ser encontradas aqui.
- Para obter mais informações sobre essa recomendação, consulte Reserved Instance Optimization Check Questions (Perguntas sobre verificação de otimização de instâncias reservadas) nas Perguntas frequentes sobre o Trusted Advisor.
- Para obter uma descrição mais detalhada dos campos, consulte a Documentação do Cost Explorer

Colunas do relatório

- Região
- Família
- Tipo de nó
- Descrição do produto
- Número recomendado de nós reservados para compra
- Utilização média esperada de nós reservados
- Economia estimada com recomendações (mensal)
- Custo inicial dos nós reservados
- Custo estimado dos nós reservados (mensal)

- Custo estimado sob demanda após a compra recomendada de nós reservados (mensal)
- Ponto de equilíbrio estimado (meses)
- Período de retrospectiva (dias)
- Prazo (anos)

Otimização de instâncias reservadas do Amazon OpenSearch Service

Descrição

Verifica seu uso do Amazon OpenSearch Service e fornece recomendações sobre a compra de instâncias reservadas. Essas recomendações são oferecidas para reduzir os custos decorrentes do uso do OpenSearch On-Demand. Criamos essas recomendações analisando seu uso sob demanda nos últimos 30 dias.

Utilizamos essa análise para simular todas as combinações de reservas na categoria de utilização gerada. Isso nos permite recomendar o número de cada tipo de instância reservada a ser comprada para maximizar a economia. Essa verificação abrange recomendações baseadas na opção de pagamento antecipado parcial com compromisso de 1 ou 3 anos.

Essa verificação não está disponível para contas vinculadas no faturamento consolidado. As recomendações para essa verificação só estão disponíveis para a conta de pagamento.

ID da verificação

`7ujm6yhn5t`

Critérios de alerta

Amarelo: otimizar a compra de instâncias reservadas do Amazon OpenSearch Service pode ajudar a reduzir custos.

Recommended Action (Ação recomendada)

Consulte a página Cost Explorer para obter recomendações mais detalhadas, opções de personalização (por exemplo, período de retrospectiva, opção de pagamento etc.) e para comprar instâncias reservadas do Amazon OpenSearch Service.

Recursos adicionais

- Informações sobre as Instâncias Reservadas do Amazon OpenSearch Service e como elas podem fazer você economizar dinheiro podem ser encontradas aqui.

- Para obter mais informações sobre essa recomendação, consulte Reserved Instance Optimization Check Questions (Perguntas sobre verificação de otimização de instâncias reservadas) nas Perguntas frequentes sobre o Trusted Advisor.
- Para obter uma descrição mais detalhada dos campos, consulte a Documentação do Cost Explorer

Colunas do relatório

- Região
- Classe de instância
- Tamanho de instância
- Número recomendado de instâncias reservadas para compra
- Utilização média esperada de instâncias reservadas
- Economia estimada com recomendações (mensal)
- Custo inicial das instâncias reservadas
- Custo estimado das instâncias reservadas (mensal)
- Custo estimado sob demanda após a compra recomendada de instâncias reservadas (mensal)
- Ponto de equilíbrio estimado (meses)
- Período de retrospectiva (dias)
- Prazo (anos)

Amazon RDS Idle DB Instances

Descrição

Verifica a configuração do Amazon Relational Database Service (Amazon RDS) para qualquer instância de banco de dados (DB) que pareça estar ociosa.

Se uma instância de banco de dados não tiver uma conexão por um longo período, será possível excluir a instância para reduzir custos. Uma instância de banco de dados será considerada ociosa se a instância não tiver tido uma conexão nos últimos 7 dias. Se o armazenamento persistente for necessário para dados na instância, é possível usar opções de custo mais baixo, como tirar e reter um snapshot do banco de dados. Os snapshots de banco de dados criados manualmente serão retidos até que você os exclua.

ID da verificação

`Ti39halfu8`

Critérios de alerta

Amarelo: uma instância de banco de dados ativa não teve uma conexão nos últimos 7 dias.

Recommended Action (Ação recomendada)

Considere fazer um snapshot da instância de banco de dados ociosa e, em seguida, interrompê-la ou excluí-la. Interromper a instância de banco de dados elimina alguns dos custos, mas não os custos de armazenamento. Uma instância interrompida mantém todos os backups automatizados com base no período de retenção configurado. Interromper uma instância de banco de dados geralmente incorre em custos adicionais quando comparado à exclusão da instância seguida pela retenção apenas do snapshot final. Consulte Stopping an Amazon RDS instance temporarily (Interromper uma instância do Amazon RDS temporariamente) e Deleting a DB Instance with a Final Snapshot (Excluir uma instância de banco de dados com um snapshot final).

Recursos adicionais

Backup e restauração

Colunas do relatório

- Região
- Nome da instância de banco de dados
- Multi-AZ
- Tipo de instância
- Armazenamento provisionado (GB)
- Dias desde a última conexão
- Economia mensal estimada (sob demanda)

Otimização de nó reservado do Amazon Redshift

Descrição

Verifica o uso do Amazon Redshift e fornece recomendações sobre a compra de nós reservados para ajudar a reduzir os custos incorridos com o uso do Amazon Redshift sob demanda.

Geramos essas recomendações analisando seu uso sob demanda nos últimos 30 dias. Utilizamos essa análise para simular todas as combinações de reservas na categoria de utilização gerada. Isso nos permite identificar o número ideal de cada tipo de nó reservado a ser

comprado para maximizar a economia. Essa verificação abrange recomendações baseadas na opção de pagamento antecipado parcial com compromisso de 1 ou 3 anos.

Essa verificação não está disponível para contas vinculadas no faturamento consolidado. As recomendações para essa verificação só estão disponíveis para a conta de pagamento.

ID da verificação

`1qw23er45t`

Critérios de alerta

Amarelo: otimizar a compra de nós reservados do Amazon Redshift pode ajudar a reduzir custos.

Recommended Action (Ação recomendada)

Consulte o Cost Explorer para obter recomendações mais detalhadas, opções de personalização (por exemplo, período de retrospectiva, opção de pagamento, etc.) e para comprar nós reservados do Amazon Redshift.

Recursos adicionais

- Informações sobre nós reservados do Amazon Redshift e como eles podem economizar seu dinheiro podem ser encontradas aqui.
- Para obter mais informações sobre essa recomendação, consulte Reserved Instance Optimization Check Questions (Perguntas sobre verificação de otimização de instâncias reservadas) nas Perguntas frequentes sobre o Trusted Advisor.
- Para obter uma descrição mais detalhada dos campos, consulte a Documentação do Cost Explorer

Colunas do relatório

- Região
- Família
- Tipo de nó
- Número recomendado de nós reservados para compra
- Utilização média esperada de nós reservados
- Economia estimada com recomendações (mensal)
- UpFront Custo dos nós reservados
- Custo estimado dos nós reservados (mensal)
- Custo estimado sob demanda após a compra recomendada de nós reservados (mensal)

- Ponto de equilíbrio estimado (meses)
- Período de retrospectiva (dias)
- Prazo (anos)

Otimização de instância reservada do Amazon Relational Database Service (RDS)

Descrição

Verifica o uso do RDS e fornece recomendações sobre a compra de instâncias reservadas para ajudar a reduzir os custos incorridos com o uso do RDS sob demanda.

Geramos essas recomendações analisando seu uso sob demanda nos últimos 30 dias. Utilizamos essa análise para simular todas as combinações de reservas na categoria de utilização gerada. Isso nos permite identificar o número ideal de cada tipo de instância reservada a ser comprada para maximizar a economia. Essa verificação abrange recomendações baseadas na opção de pagamento antecipado parcial com compromisso de 1 ou 3 anos.

Essa verificação não está disponível para contas vinculadas no faturamento consolidado. As recomendações para essa verificação só estão disponíveis para a conta de pagamento.

ID da verificação

`1qazXsw23e`

Critérios de alerta

Amarelo: otimizar a compra de instâncias reservadas do Amazon RDS pode ajudar a reduzir custos.

Recommended Action (Ação recomendada)

Consulte a página do Cost Explorer para obter recomendações mais detalhadas, opções de personalização (por exemplo, período de retrospectiva, opção de pagamento, etc.) e para comprar instâncias reservadas do Amazon RDS.

Recursos adicionais

- Informações sobre as instâncias reservadas do Amazon RDS e como elas podem economizar seu dinheiro podem ser encontradas aqui.
- Para obter mais informações sobre essa recomendação, consulte Reserved Instance Optimization Check Questions (Perguntas sobre verificação de otimização de instâncias reservadas) nas Perguntas frequentes sobre o Trusted Advisor.

- Para obter uma descrição mais detalhada dos campos, consulte a Documentação do Cost Explorer

Colunas do relatório

- Região
- Família
- Tipo de instância
- Modelo de licença
- Edição do banco de dados
- Mecanismo do banco de dados
- Opção de implantação
- Número recomendado de instâncias reservadas para compra
- Utilização média esperada de instâncias reservadas
- Economia estimada com recomendações (mensal)
- Custo inicial das instâncias reservadas
- Custo estimado das instâncias reservadas (mensal)
- Custo estimado sob demanda após a compra recomendada de instâncias reservadas (mensal)
- Ponto de equilíbrio estimado (meses)
- Período de retrospectiva (dias)
- Prazo (anos)

Conjuntos de registros de recursos de latência no Amazon Route 53.

Descrição

Verifica se há conjuntos de registros de latência do Amazon Route 53 configurados de forma ineficiente.

Para permitir ao Amazon Route 53 encaminhar consultas para o Região da AWScom a latência de rede mais baixa, você deverá criar conjuntos de registros de recurso de latência para um nome de domínio específico (como exemplo.com) em regiões diferentes. Se você criar apenas um conjunto de registros de recurso de latência para um nome de domínio, todas as consultas serão roteadas para uma região e você pagará um valor extra pelo roteamento baseado em latência sem obter os benefícios.

Zonas hospedadas criadas pela AWS não aparecerão nos resultados da verificação.

ID da verificação

`51fC20e7I2`

Critérios de alerta

Amarelo: apenas um conjunto de registros de recursos de latência está configurado para um nome de domínio específico.

Recommended Action (Ação recomendada)

Se você tiver recursos em várias regiões, defina um conjunto de registros de recursos de latência para cada região. Consulte Latency-Based Routing (Roteamento baseado em latência).

Se você tiver recursos em apenas uma Região da AWS, considere criar recursos em mais de uma Região da AWS e definir conjuntos de registros de recursos de latência para cada uma. Consulte Latency-Based Routing (Roteamento baseado em latência).

Se não desejar usar várias Regiões da AWS, será necessário utilizar um conjunto de registros de recursos simples. Consulte Working with Resource Record Sets (Trabalhar com conjuntos de registros de recursos).

Recursos adicionais

- Guia do desenvolvedor do Amazon Route 53
- Preços do Amazon Route 53

Colunas do relatório

- Nome da zona hospedada
- ID da zona hospedada
- Nome do conjunto de registros de recursos
- Tipo do conjunto de registros de recursos

Política de ciclo de vida do bucket do Amazon S3 configurada

Descrição

Verifica se um bucket do Amazon S3 tem uma política de ciclo de vida configurada. Uma política de ciclo de vida do Amazon S3 garante que os objetos do Amazon S3 dentro do bucket sejam armazenados de maneira econômica durante todo o ciclo de vida. Isso é importante para atender

aos requisitos regulamentares de retenção e armazenamento de dados. A configuração da política é um conjunto de regras que define as ações aplicadas pelo serviço do Amazon S3 a um grupo de objetos. Uma política de ciclo de vida permite automatizar a transição de objetos para classes de armazenamento de menor custo ou excluí-los à medida que envelhecem. Por exemplo, você pode fazer a transição de um objeto para o armazenamento Amazon S3 Standard-IA 30 dias após a criação, ou para o Amazon S3 Glacier após um ano.

Você também pode definir a expiração do objeto para que o Amazon S3 exclua o objeto em seu nome após um determinado período de tempo.

Você pode ajustar a configuração da verificação usando os parâmetros em suas regras do AWS Config.

Para obter mais informações, consulte Gerenciar seu ciclo de vida de armazenamento.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c18d2gz100`

Origem

`AWS Config Managed Rule: s3-lifecycle-policy-check`

Critérios de alerta

Amarelo: o bucket do Amazon S3 não tem uma política de ciclo de vida configurada.

Recommended Action (Ação recomendada)

Certifique-se de ter uma política de ciclo de vida configurada em seu bucket do Amazon S3.

Se sua organização não tiver uma política de retenção em vigor, considere usar o Amazon S3 Intelligent-Tiering para otimizar os custos.

Para obter informações sobre como definir sua política de ciclo de vida do Amazon S3, consulte Definir a configuração do ciclo de vida em um bucket.

Para obter informações sobre o Amazon S3 Intelligent-Tiering, consulte Classe de armazenamento Amazon S3 Intelligent-Tiering

Recursos adicionais

Definir a configuração do ciclo de vida em um bucket

Exemplos de configuração do S3 Lifecycle

Colunas do relatório

- Status
- Região
- Recurso
- Regra do AWS Config
- Parâmetros de entrada

Configuração de cancelamento de upload em várias partes incompleta do Amazon S3

Descrição

Verifica se cada bucket do Amazon S3 está configurado com uma regra de ciclo de vida para abortar carregamentos de várias partes que permanecem incompletos após 7 dias. É recomendável usar uma regra de ciclo de vida para abortar esses uploads incompletos e excluir o armazenamento associado.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente uma ou mais vezes por dia, e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c1cj39rr6v`

Critérios de alerta

Amarelo: o bucket de configuração do ciclo de vida não contém uma regra de ciclo de vida para abortar todos os uploads de várias partes que permanecem incompletos após 7 dias.

Recommended Action (Ação recomendada)

Analise a configuração do ciclo de vida dos buckets sem uma regra de ciclo de vida que limpe todos os carregamentos incompletos de várias partes. É improvável que os carregamentos que não sejam concluídos após 24 horas sejam concluídos. Clique aqui para seguir as instruções para criar uma regra de ciclo de vida. É recomendável que isso seja aplicado a todos os objetos em seu bucket. Se você precisar aplicar outras ações do ciclo de vida aos objetos selecionados em seu bucket, poderá ter várias regras com filtros diferentes. Verifique o painel da lente de armazenamento ou ligue para a ListMultipartUpload API para obter mais informações.

Recursos adicionais

Criação de uma configuração de ciclo de vida

Descobrindo e excluindo uploads incompletos de várias partes para reduzir os custos do Amazon S3

Carregando e copiando objetos usando o upload de várias partes

Elementos de configuração do ciclo de vida

Elementos para descrever as ações do ciclo de vida

Configuração do ciclo de vida para abortar carregamentos de várias partes

Colunas do relatório

- Status
- Região
- Nome do bucket
- ARN do bucket
- Regra de ciclo de vida para excluir MPU incompleta
- Dias após a iniciação
- Hora da última atualização

Buckets habilitados para a versão do Amazon S3 sem políticas de ciclo de vida configuradas

Descrição

Verifica se os buckets habilitados para a versão do Amazon S3 têm uma política de ciclo de vida configurada.

Para obter mais informações, consulte Gerenciar seu ciclo de vida de armazenamento.

Você pode especificar os nomes dos buckets que deseja verificar usando os parâmetros bucketNames nas suas regras do AWS Config.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c18d2gz171`

Origem

`AWS Config Managed Rule: s3-version-lifecycle-policy-check`

Critérios de alerta

Amarelo: um bucket habilitado para a versão do Amazon S3 que não tem uma política de ciclo de vida configurada.

Recommended Action (Ação recomendada)

Configure políticas de ciclo de vida para seus buckets do Amazon S3 para gerenciar seus objetos de modo que eles sejam armazenados de maneira econômica durante todo o ciclo de vida.

Para obter mais informações, consulte Definir configuração do ciclo de vida em um bucket.

Recursos adicionais

Gerenciando seu ciclo de vida de armazenamento

Definir a configuração do ciclo de vida em um bucket

Colunas do relatório

- Status
- Região
- Recurso
- Regra do AWS Config
- Parâmetros de entrada
- Hora da última atualização

O AWS Lambda funciona com tempo limite excessivo

Descrição

Verifica se há funções do Lambda com altas taxas de tempo limite que podem resultar em alto custo.

Encargos do Lambda com base em hora e número de execução de solicitações para sua função. Os tempos limite de função resultam em erros que podem causar novas tentativas. A repetição de funções incorrerá adicionalmente em cobranças de tempo de solicitação e execução.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`L4dfs2Q3C3`

Critérios de alerta

Amarelo: funções em que > 10% das chamadas terminam em erro devido a um tempo limite excedido em um determinado dia nos últimos 7 dias.

Recommended Action (Ação recomendada)

Inspecione o log de funções e os rastreamentos do X-Ray para determinar o que contribuiu para a alta duração da função. Implemente o log em seu código em partes relevantes, como

antes ou depois de chamadas de API ou conexões de banco de dados. Por padrão, os tempos limites dos clientes do AWS SDK podem ser maiores do que a duração da função configurada. Ajuste os clientes de conexão com a API e o SDK para tentar novamente ou desistir dentro do tempo limite da função. Se a duração esperada for maior que o tempo limite configurado, a configuração de tempo limite para a função poderá ser aumentada. Para obter mais informações, consulte Monitoring and troubleshooting Lambda applications (Monitorar e solucionar problemas de aplicações do Lambda).

Recursos adicionais

- Monitoramento e solução de problemas de aplicações do Lambda
- Lambda Function Retry Timeout SDK
- Usar o AWS Lambda com o AWS X-Ray
- Acessando CloudWatch os registros da Amazon para AWS Lambda
- Aplicação de exemplo do processador de erros para o AWS Lambda

Colunas do relatório

- Status
- Região
- ARN da função
- Taxa de tempo limite máximo diário
- Data da taxa de tempo limite máximo diário
- Taxa de tempo limite médio diário
- Configurações de tempo limite da função (milissegundos)
- Custo computacional diário perdido
- Invocações médias diárias
- Invocações do dia atual
- Taxa de tempo limite do dia atual
- Hora da última atualização

O AWS Lambda funciona com altas taxas de erro

Descrição

Verifica se há funções do Lambda com altas taxas de erro que podem resultar em custos mais altos.

Os encargos do Lambda são baseados na hora agregada e no número de execução de solicitações para sua função. Erros de função podem causar novas tentativas que incorrem em encargos adicionais.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`L4dfs2Q3C2`

Critérios de alerta

Amarelo: funções em que > 10% das chamadas terminam em erro em um determinado dia nos últimos 7 dias.

Recommended Action (Ação recomendada)

Considere as diretrizes a seguir para reduzir os erros. Os erros de função incluem erros retornados pelo código e pelo runtime da função.

Para ajudá-lo a solucionar erros do Lambda, o Lambda se integra a serviços como Amazon e. CloudWatch AWS X-Ray Você pode usar um conjunto de logs, métricas, alarmes e rastreamento do X-Ray para detectar e identificar rapidamente os problemas no código da função, na API ou em outros recursos compatíveis com seu aplicativo. Para obter mais informações, consulte Monitoring and troubleshooting Lambda applications (Monitorar e solucionar problemas de aplicações do Lambda).

Para obter mais informações sobre como lidar com erros com tempos de execução específicos, consulte Lidar com erros e novas tentativas automáticas no AWS Lambda.

Para procedimentos adicionais de soluções de problemas, consulte Troubleshooting issues in Lambda (Solução de problemas no Lambda).

Também é possível pode escolher entre um ecossistema de ferramentas de monitoramento e observabilidade fornecidas por parceiros do AWS Lambda. Para obter mais informações, consulte Parceiros do AWS Lambda.

Recursos adicionais

- Lidar com erros e novas tentativas automáticas no AWS Lambda
- Monitoring and troubleshooting Lambda applications (Monitorar e solucionar problemas de aplicações do Lambda)
- Lambda Function Retry Timeout SDK
- Troubleshooting issues in Lambda (Solução de problemas no Lambda)
- API Invoke Errors (Erros de invocação da API)
- Aplicação de exemplo do processador de erros para o AWS Lambda

Colunas do relatório

- Status
- Região
- ARN da função
- Taxa de erros máxima diária
- Data da taxa de erros máxima diária
- Taxa de erros média diária
- Custo computacional diário perdido
- Invocações médias diárias
- Invocações do dia atual

  Taxa de erros do dia atual
- Hora da última atualização

Funções superprovisionadas do AWS Lambda para tamanho de memória

Descrição

Verifica as funções do AWS Lambda que foram invocadas pelo menos uma vez durante o período retroativo. Essa verificação alerta se alguma das suas funções do Lambda tiver sido provisionada em excesso para o tamanho da memória. Quando há funções do Lambda que estão superprovisionadas para tamanhos de memória, você estará pagando por recursos não utilizados. Embora alguns cenários possam resultar em baixa utilização deliberadamente, geralmente você pode reduzir os custos alterando a configuração de memória de suas funções do Lambda. As estimativas de economia mensal são calculadas usando a taxa de uso atual para funções do Lambda.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`C0r6dfpM05`

Critérios de alerta

Amarelo: uma função do Lambda que foi provisionada em excesso para o tamanho da memória durante o período de retrospectiva. Para determinar se uma função Lambda está superprovisionada, consideramos todas as métricas padrão CloudWatch dessa função. O algoritmo usado para identificar funções do Lambda provisionadas em excesso segue as práticas recomendadas da AWS. O algoritmo é atualizado quando um novo padrão é identificado.

Recommended Action (Ação recomendada)

Considere reduzir o tamanho da memória das funções do Lambda.

Para obter mais informações, consulte Optar por verificações do Trusted Advisor para o AWS Compute Optimizer.

Colunas do relatório

- Status
- Região
- Nome da função
- Versão da função
- Tamanho da memória (MB)
- Tamanho da memória recomendado (MB)
- Período de retrospectiva (dias)
- Oportunidade de economia (%)
- Economia mensal estimada
- Moeda da economia mensal estimada
- Hora da última atualização

Problemas de alto risco do AWS Well-Architected para otimização de custos

Descrição

Verifica problemas de alto risco (HRIs – high risk issues) de suas workloads no pilar Otimização de custos. Essa verificação é baseada nas suas análises AWS-Well Architected. Os resultados da verificação dependem de você ter concluído ou não a avaliação da workload com o AWS Well-Architected.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`Wxdfp4B1L1`

Critérios de alerta

- Vermelho: pelo menos um problema ativo de alto risco foi identificado no pilar de otimização de custos para o AWS Well-Architected.
- Verde: nenhum problema ativo de alto risco foi detectado no pilar de otimização de custos para o AWS Well-Architected.

Recommended Action (Ação recomendada)

O AWS Well-Architected detectou problemas de alto risco durante a avaliação da workload. Esses problemas apresentam oportunidades para reduzir riscos e economizar dinheiro. Faça login na ferramenta AWS Well-Architected para revisar suas respostas e adotar medidas para resolver seus problemas ativos.

Colunas do relatório

- Status
- Região
- ARN da workload
- Nome da workload
- Nome do revisor

- Tipo de workload
- Data de início da workload
- Data da última modificação da workload
- Número de problemas de alto risco identificados para otimização de custos
- Número de problemas de alto risco resolvidos para otimização de custos
- Número de perguntas respondidas para otimização de custos
- Número total de perguntas no pilar de otimização de custos
- Hora da última atualização

Balanceadores de carga obsoletos

Descrição

Verifica a configuração do Elastic Load Balancing em busca de balanceadores de carga que estão ociosos.

Qualquer balanceador de carga configurado acumula cobranças. Se um balanceador de carga não tiver instâncias de backend associadas, ou se o tráfego de rede for gravemente limitado, o balanceador de carga não está sendo usado de forma eficaz. No momento, essa verificação verifica apenas o tipo de Classic Load Balancer dentro do serviço ELB. Ele não inclui outros tipos de ELB (Application Load Balancer, Network Load Balancer).

ID da verificação

`hjLMh88uM8`

Critérios de alerta

- Amarelo: um balanceador de carga não tem instâncias de back-end ativas.
- Amarelo: um balanceador de carga não tem instâncias de back-end íntegras.
- Amarelo: um balanceador de carga teve menos de 100 solicitações por dia nos últimos 7 dias.

Recommended Action (Ação recomendada)

Se o balanceador de carga não tiver instâncias de back-end ativas, considere registrar instâncias ou excluir o balanceador de carga. Consulte Registering Your Amazon EC2 Instances with Your Load Balancer (Registrar instâncias do Amazon EC2 com o balanceador de carga) ou Delete Your Load Balancer (Excluir o balanceador de carga).

Se o balanceador de carga não tiver instâncias de back-end íntegras, consulte Troubleshooting Elastic Load Balancing: Health Check Configuration (Solucionar problemas do Elastic Load Balancing: Configuração da verificação de integridade).

Se o balanceador de carga tiver uma contagem baixa de solicitações, considere excluir o balanceador de carga. Consulte Delete Your Load Balancer (Excluir o load balancer).

Recursos adicionais

- Managing Load Balancers (Gerenciar balanceadores de carga)
- Troubleshoot Elastic Load Balancing (Solucionar problemas do Elastic Load Balancing

Colunas do relatório

- Região
- Nome do balanceador de carga
- Motivo
- Economia mensal estimada

Instâncias do Amazon EC2 com pouca utilização

Descrição

Verifica as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) que estavam em execução a qualquer momento durante os últimos 14 dias. Essa verificação alerta se a utilização diária da CPU foi de 10% ou menos e a E/S da rede foi de 5 MB ou menos por pelo menos 4 dias.

As instâncias em execução geram cobrança por uso por hora Embora alguns cenários possam resultar em baixa utilização por projeto, você geralmente pode reduzir os custos gerenciando o número e o tamanho de suas instâncias.

As economias mensais estimadas são calculadas usando a taxa de uso atual para Instâncias sob demanda e o número estimado de dias em que a instância pode estar subutilizada. As economias reais variam se você estiver usando Instâncias Reservadas ou Instâncias Spot, ou se a instância não estiver sendo executada por um dia inteiro. Para obter dados de utilização diária, baixe o relatório desta verificação.

ID da verificação

`Qch7DwouX1`

Critérios de alerta

Amarelo: uma instância teve 10% ou menos de utilização média diária da CPU e 5 MB ou menos de E/S de rede em pelo menos 4 dos 14 dias anteriores.

Recommended Action (Ação recomendada)

Considere interromper ou encerrar instâncias com baixa utilização ou dimensionar o número de instâncias usando o Auto Scaling. Para obter mais informações, consulte Stop and Start Your Instance (Interromper e iniciar sua instância), Terminate Your Instance (Encerrar sua instância) e What is Auto Scaling? (O que é Auto Scaling?)

Recursos adicionais

- Monitoring Amazon EC2 (Monitorar o Amazon EC2)
- Instance Metadata and User Data (Metadados de instâncias e dados do usuário)
- Guia CloudWatch do usuário da Amazon
- Guia do desenvolvedor do Auto Scaling

Colunas do relatório

- Região/Zona de disponibilidade
- ID da instância
- Nome da instância
- Tipo de instância
- Economia mensal estimada
- Utilização da CPU média de 14 dias
- E/S de rede média de 14 dias
- Número de dias de baixa utilização

Savings Plan

Descrição

Verifica o uso do Amazon EC2, Fargate e Lambda nos últimos 30 dias e fornece recomendações de compra do Savings Plan. Essas recomendações permitem que você se comprometa com uma quantidade de uso consistente medida em dólares por hora por um período de um ou três anos em troca de tarifas com desconto.

Elas se originam no AWS Cost Explorer, capaz obter informações de recomendação mais detalhadas. Também é possível comprar um saving plan por meio do Cost Explorer. Essas recomendações devem ser consideradas uma alternativa às recomendações do RI. Sugerimos que você aja apenas em um conjunto de recomendações. Agir em ambos os conjuntos pode levar a um excesso de comprometimento.

Essa verificação não está disponível para contas vinculadas no faturamento consolidado. As recomendações para essa verificação só estão disponíveis para a conta de pagamento.

ID da verificação

`vZ2c2W1srf`

Critérios de alerta

Amarelo: otimizar a compra de Savings Plans pode ajudar a reduzir custos.

Recommended Action (Ação recomendada)

Consulte a página do Cost Explorer para obter recomendações mais detalhadas e personalizadas e para comprar Savings Plans.

Recursos adicionais

- Guia do usuário do Savings Plans
- Perguntas frequentes sobre o Savings Plans

Colunas do relatório

- Tipo de Savings Plans
- Opção de pagamento
- Custo adiantado
- Compromisso de compra por hora
- Utilização média estimada
- Economia mensal estimada
- Percentual estimado de economia
- Prazo (anos)
- Período de retrospectiva (dias)

Endereços de IP elástico não associados

Descrição

Verifica se há endereços IP elásticos (EIPs) que não estão associados a uma instância do Amazon Elastic Compute Cloud (Amazon EC2) em execução.

Os EIPs são endereços IP estáticos projetados para computação em nuvem dinâmica. Ao contrário dos endereços IP estáticos tradicionais, os EIPs mascaram a falha de uma instância ou Zona de disponibilidade remapeando um endereço IP público para outra instância da conta. Uma cobrança nominal é imposta para um EIP que não esteja associado a uma instância em execução.

ID da verificação

`Z4AUBRNSmz`

Critérios de alerta

Amarelo: um endereço IP elástico (EIP) alocado não está associado a uma instância do Amazon EC2 em execução.

Recommended Action (Ação recomendada)

Associe o EIP a uma instância ativa em execução ou libere o EIP não associado. Para obter mais informações, consulte Associating an Elastic IP Address with a Different Running Instance (Associar um endereço IP elástico a uma instância em execução diferente) e Releasing an Elastic IP Address (Liberar um endereço IP elástico).

Recursos adicionais

Endereços Elastic IP

Colunas do relatório

- Região
- Endereço IP

Volumes subutilizados do Amazon EBS

Descrição

Verifica configurações de volume do Amazon Elastic Block Store (Amazon EBS) e avisa quando os volumes parecem estar subutilizados.

As cobranças começam quando um volume é criado. Se um volume permanecer sem conexão ou tiver uma atividade de gravação muito baixa (excluindo volumes de inicialização) por um período, o volume está subutilizado. Recomendamos que você remova volumes subutilizados para reduzir custos.

ID da verificação

`DAvU99Dc4C`

Critérios de alerta

Amarelo: um volume não está vinculado ou teve menos de 1 IOPS por dia nos últimos 7 dias.

Recommended Action (Ação recomendada)

Considere criar um snapshot e excluir o volume para reduzir custos. Para obter mais informações, consulte Creating an Amazon EBS Snapshot (Criar um snapshot do Amazon EBS) e Deleting an Amazon EBS Volume (Excluir um volume do Amazon EBS).

Recursos adicionais

- Amazon Elastic Block Store (Amazon EBS)
- Como monitorar o status de seus volumes

Colunas do relatório

- Região
- ID de volume
- Nome do volume
- Tipo de volume
- Tamanho do volume
- Custo de armazenamento mensal
- ID do snapshot
- Nome do snapshot
- Idade do snapshot

> **Note**
>
> Se tiver optado pelo AWS Compute Optimizer em sua conta, recomendamos que use a verificação de superprovisionamento de volumes do Amazon EBS. Para obter mais

informações, consulte Optar por verificações do Trusted Advisor para o AWS Compute Optimizer.

Clusters subutilizados do Amazon Redshift

Descrição

Verifica a configuração do Amazon Redshift em busca de clusters que parecem estar subutilizados.

Se um cluster do Amazon Redshift não tiver uma conexão por um período prolongado ou estiver usando uma quantidade baixa de CPU, será possível usar opções de custo mais baixo, como reduzir o tamanho do cluster ou encerrar o cluster e fazer um snapshot final. Os snapshots finais são retidos mesmo depois que você exclui o cluster.

ID da verificação

`G31sQ1E9U`

Critérios de alerta

- Amarelo: um cluster em execução não teve uma conexão nos últimos 7 dias.
- Amarelo: um cluster em execução teve menos de 5% de utilização média da CPU em todo o cluster em 99% dos últimos 7 dias.

Recommended Action (Ação recomendada)

Considere desligar o cluster e fazer um snapshot final ou reduzir o tamanho do cluster. Consulte Shutting Down and Deleting Clusters (Desligar e excluir clusters) e Resizing a Cluster (Redimensionar um cluster).

Recursos adicionais

Guia CloudWatch do usuário da Amazon

Colunas do relatório

- Status
- Região
- Cluster
- Tipo de instância
- Motivo

- Economia mensal estimada

Performance

Melhore a performance do serviço verificando suas cotas de serviço (anteriormente conhecidas como limites), para que você possa aproveitar o throughput provisionado, monitorar instâncias utilizadas em excesso e detectar quaisquer recursos não utilizados.

É possível usar as verificações a seguir para a categoria de performance.

Nomes da verificação

- Cluster de banco de dados Amazon Aurora subprovisionado para carga de trabalho de leitura
- O ajuste de escala automático do Amazon DynamoDB não está habilitado
- Otimização do Amazon EBS não habilitada
- Configuração do anexo de volume de IOPS provisionadas (SSD) do Amazon EBS
- Volumes subprovisionados do Amazon EBS
- O grupo do Amazon EC2 Auto Scaling não está associado a um modelo de inicialização
- Otimização de throughput do Amazon EC2 para EBS
- O tipo de virtualização do EC2 é paravirtual
- Limite rígido de memória do Amazon ECS
- Otimização do modo throughput do Amazon EFS
- O parâmetro de autovacuum do Amazon RDS está desativado
- Os clusters de banco de dados do Amazon RDS suportam somente volumes de até 64 TiB
- Instâncias de banco de dados Amazon RDS nos clusters com classes de instância heterogêneas
- Instâncias de banco de dados Amazon RDS nos clusters com tamanhos de instância heterogêneos
- Os parâmetros de memória de banco de dados do Amazon RDS estão divergindo do padrão
- O parâmetro enable_index_onlyscan do Amazon RDS está desativado
- O parâmetro enable_indexscan do Amazon RDS está desativado
- O parâmetro general_logging do Amazon RDS está ativado
- Parâmetro Amazon RDS InnoDB_change_buffering usando menos do que o valor ideal
- O parâmetro innodb_open_files do Amazon RDS está baixo

- O parâmetro innodb_stats_persistent do Amazon RDS está desativado
- Instância do Amazon RDS subprovisionada para capacidade do sistema
- O volume magnético do Amazon RDS está em uso
- Grupos de parâmetros do Amazon RDS que não usam páginas grandes
- O parâmetro de cache de consulta do Amazon RDS está ativado
- A atualização da classe de instância de recursos do Amazon RDS é necessária
- A atualização das principais versões dos recursos do Amazon RDS é necessária
- Recursos do Amazon RDS usando a edição final do mecanismo de suporte sob licença incluída
- Conjuntos de registros de recursos do alias no Amazon Route 53.
- Funções subprovisionadas do AWS Lambda para tamanho de memória
- Funções do AWS Lambda sem limite de simultaneidade configurado
- Problemas de alto risco do AWS Well-Architected em relação à performance
- CloudFront Nomes de domínio alternativos
- CloudFront Otimização da entrega de conteúdo
- CloudFront Encaminhamento de cabeçalho e taxa de acertos de cache
- Instâncias do Amazon EC2 com alta utilização
- Grande número de regras de grupo de segurança do EC2 aplicadas a uma instância
- Grande número de regras em um grupo de segurança do EC2
- Volumes magnéticos do Amazon EBS utilizados em excesso

Cluster de banco de dados Amazon Aurora subprovisionado para carga de trabalho de leitura

Descrição

Verifica se o cluster de banco de dados Amazon Aurora tem os recursos para suportar uma carga de trabalho de leitura.

ID da verificação

`c1qf5bt038`

Critérios de alerta

Amarelo:

Aumento das leituras do banco de dados: a carga do banco de dados estava alta e o banco de dados estava lendo mais linhas do que escrevendo ou atualizando as linhas.

Recommended Action (Ação recomendada)

Recomendamos que você ajuste suas consultas para diminuir a carga do banco de dados ou adicionar uma instância de banco de dados de leitura ao seu cluster de banco de dados com a mesma classe e tamanho da instância de banco de dados gravadora no cluster. A configuração atual tem pelo menos uma instância de banco de dados com uma carga de banco de dados continuamente alta causada principalmente por operações de leitura. Distribua essas operações adicionando outra instância de banco de dados ao cluster e direcionando a carga de trabalho de leitura para o endpoint somente para leitura do cluster de banco de dados.

Recursos adicionais

Um cluster de banco de dados Aurora tem um endpoint de leitura para conexões somente de leitura. Esse endpoint usa balanceamento de carga para gerenciar as consultas que mais contribuem para a carga do banco de dados em seu cluster de banco de dados. O endpoint do leitor direciona essas instruções para as réplicas de leitura do Aurora e reduz a carga na instância primária. O endpoint do leitor também dimensiona a capacidade de lidar com consultas SELECT simultâneas com o número de réplicas de leitura do Aurora no cluster.

Para obter mais informações, consulte Adicionar réplicas do Aurora a um cluster de banco de dados e gerenciar o desempenho e a escalabilidade dos clusters de banco de dados Aurora.

Colunas do relatório

- Status
- Região
- Recurso
- Maior leitura (contagem) do banco de dados
- Último período de detecção
- Hora da última atualização

O ajuste de escala automático do Amazon DynamoDB não está habilitado

Descrição

Verifica se suas tabelas e índices secundários globais do Amazon DynamoDB têm o ajuste de escala automático ou sob demanda habilitado.

O ajuste de escala automático do Amazon DynamoDB usa o serviço de ajuste automático da aplicação para ajustar dinamicamente a capacidade de throughput provisionado em seu nome em resposta aos padrões de tráfego reais. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização. Quando a workload diminuir, o Application Auto Scaling diminuirá o throughput para que você não precise pagar por uma capacidade provisionada não utilizada.

Você pode ajustar a configuração da verificação usando os parâmetros em suas regras do AWS Config.

Para obter mais informações, consulte Gerenciar a capacidade de throughput automaticamente com o ajuste de escala automático do DynamoDB.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c18d2gz136`

Origem

AWS ConfigRegra gerenciada: dynamodb-autoscaling-enabled

Critérios de alerta

Amarelo: o ajuste de escala automático não está habilitado para suas tabelas do DynamoDB ou índices secundários globais.

Recommended Action (Ação recomendada)

A menos que você já tenha um mecanismo para escalar automaticamente o throughput provisionado da sua tabela do DynamoDB ou dos índices secundários globais com base nos requisitos da workload, considere ativar o ajuste de escala automático para suas tabelas do Amazon DynamoDB.

Para obter mais informações, consulte Utilizar o Console de Gerenciamento da AWS com o ajuste de escala automático do DynamoDB.

Recursos adicionais

Gerenciar a capacidade de throughput automaticamente com o ajuste de escala automático do DynamoDB

Colunas do relatório

- Status
- Região
- Recurso
- Regra do AWS Config
- Parâmetros de entrada
- Hora da última atualização

Otimização do Amazon EBS não habilitada

Descrição

Verifica se a otimização do Amazon EBS está habilitada para instâncias do Amazon EC2.

Uma instância otimizada para o Amazon EBS usa uma pilha de configuração otimizada e fornece capacidade adicional dedicada para E/S do Amazon EBS. Essa otimização proporciona a melhor performance para seus volumes do Amazon EBS ao minimizar a contenção entre a E/S do Amazon EBS e outro tráfego de sua instância.

Para obter mais informações, consulte Instâncias otimizadas para o Amazon EBS.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c18d2gz142`

Origem

AWS ConfigRegra gerenciada: ebs-optimized-instance

Critérios de alerta

Amarelo: a otimização do Amazon EBS não está habilitada em instâncias compatíveis do Amazon EC2.

Recommended Action (Ação recomendada)

Ative a otimização do Amazon EBS em instâncias compatíveis.

Para obter mais informações, consulte Habilitação da otimização do EBS na execução.

Recursos adicionais

Instâncias otimizadas para o Amazon EBS

Colunas do relatório

- Status
- Região
- Recurso
- Regra do AWS Config
- Parâmetros de entrada
- Hora da última atualização

Configuração do anexo de volume de IOPS provisionadas (SSD) do Amazon EBS

Descrição

Verificações de Volumes de IOPS provisionadas (SSD) que são anexados a uma instância do Amazon Elastic Compute Cloud (Amazon EC2) otimizável do Amazon EBS que não é otimizada para EBS.

Os volumes de IOPS provisionadas (SSD) no Amazon Elastic Block Store (Amazon EBS) foram projetados para fornecer a performance esperada somente quando estiverem conectados a uma instância otimizada para EBS.

ID da verificação

`PPkZrjsH2q`

Critérios de alerta

Amarelo: uma instância do Amazon EC2 que pode ser otimizada para EBS tem um volume de IOPS provisionadas (SSD) anexado, mas a instância não é otimizada para EBS.

Recommended Action (Ação recomendada)

Crie uma nova instância otimizada para EBS, desconecte o volume e reconecte o volume à sua nova instância. Para obter mais informações, consulte Amazon EBS-Optimized Instances (Instâncias otimizadas para Amazon EBS) e Attaching an Amazon EBS Volume to an Instance (Anexar um volume do Amazon EBS a uma instância).

Recursos adicionais

- Amazon EBS Volume Types (Tipos de volume do Amazon EBS)
- Amazon EBS Volume Performance (Performance de volumes do Amazon EBS)

Colunas do relatório

- Status
- Região/Zona de disponibilidade
- ID de volume
- Nome do volume
- Anexo de volume
- ID da instância
- Tipo de instância
- Otimizado para EBS

Volumes subprovisionados do Amazon EBS

Descrição

Verifica os volumes do Amazon Elastic Block Store (Amazon EBS) que estavam em execução a qualquer momento durante o período retroativo. Essa verificação alerta se algum volume do EBS tiver sido provisionado em escassez para suas workloads. Uma utilização alta e consistente pode indicar desempenho otimizado e estável, mas também pode indicar que um aplicativo não tem recursos suficientes.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`C0r6dfpM04`

Critérios de alerta

Amarelo: um volume do EBS que foi subprovisionado durante o período de retrospectiva. Para determinar se um volume está subprovisionado, consideramos todas as CloudWatch métricas padrão (incluindo IOPS e taxa de transferência). O algoritmo usado para identificar volumes do EBS subprovisionados segue as práticas recomendadas da AWS. O algoritmo é atualizado quando um novo padrão é identificado.

Recommended Action (Ação recomendada)

Considere aumentar o tamanho de volumes que têm alta utilização.

Para obter mais informações, consulte Optar por verificações do Trusted Advisor para o AWS Compute Optimizer.

Colunas do relatório

- Status
- Região
- ID de volume
- Tipo de volume
- Tamanho do volume (GB)
- IOPS de referência do volume
- IOPS de intermitência do volume
- Throughput de intermitência do volume
- Tipo do volume recomendado
- Tamanho do volume recomendado (GB)
- IOPS de referência do volume recomendadas
- IOPS de intermitência do volume recomendadas
- Throughput de referência do volume recomendada
- Throughput de intermitência do volume recomendada
- Período de retrospectiva (dias)
- Risco de performance

- Hora da última atualização

O grupo do Amazon EC2 Auto Scaling não está associado a um modelo de inicialização

Descrição

Verifica se um grupo do Amazon EC2 Auto Scaling foi criado de um modelo de inicialização do Amazon EC2.

Use um modelo de inicialização para criar seus grupos do Amazon EC2 Auto Scaling para garantir o acesso aos recursos e melhorias mais recentes do grupo do Auto Scaling. Por exemplo, versionamento e vários tipos de instância.

Para obter mais informações, consulte Launch templates.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c18d2gz102`

Origem

AWS ConfigRegra gerenciada: autoscaling-launch-template

Critérios de alerta

Amarelo: o grupo do Amazon EC2 Auto Scaling não está associado a um modelo de inicialização válido.

Recommended Action (Ação recomendada)

Use um modelo de inicialização do Amazon EC2 para criar seus grupos do Amazon EC2 Auto Scaling.

Para obter mais informações, consulte Create a launch template for an Auto Scaling group.

Recursos adicionais

- Modelos de inicialização
- Criar um modelo de inicialização

Colunas do relatório

- Status
- Região
- Recurso
- Regra do AWS Config
- Parâmetros de entrada
- Hora da última atualização

Otimização de throughput do Amazon EC2 para EBS

Descrição

Verifica se há volumes do Amazon EBS cuja performance pode ser afetada pela capacidade máxima de throughput da instância do Amazon EC2 à qual estão anexados.

Para otimizar a performance, você deve garantir que o throughput máximo de uma instância do Amazon EC2 seja maior do que o throughput máximo agregado dos volumes do EBS anexados. Essa verificação calcula o throughput total do volume do EBS para cada período de cinco minutos no dia anterior (com base no Tempo Universal Coordenado)) para cada instância otimizada para EBS e alerta se o uso em mais da metade desses períodos foi maior que 95% do throughput máximo da instância do EC2.

ID da verificação

`Bh2xRR2FGH`

Critérios de alerta

Amarelo: no dia anterior (UTC), a throughput agregada (megabytes/segundo) dos volumes do EBS anexados à instância do EC2 excedeu 95% da throughput publicada entre a instância e os volumes do EBS em mais de 50% do tempo.

Recommended Action (Ação recomendada)

Compare a throughput máxima de seus volumes do Amazon EBS (consulte Amazon EBS Volume Types (Tipos de volume do Amazon EBS) com a throughput máxima da instância do Amazon

EC2 à qual eles estão vinculados. Consulte Instance Types That Support EBS Optimization (Tipos de instâncias compatíveis com a otimização do EBS).

Considere anexar seus volumes a uma instância compatível com uma throughput mais alta para o Amazon EBS para obter a performance ideal.

Recursos adicionais

- Amazon EBS Volume Types (Tipos de volume do Amazon EBS)
- Amazon EBS-Optimized Instances (Instâncias otimizadas para Amazon EBS)
- Como monitorar o status de seus volumes
- Attaching an Amazon EBS Volume to an Instance (Vincular um volume de Amazon EBS a uma instância)
- Detaching an Amazon EBS Volume from an Instance (Desvincular um volume do Amazon EBS de uma instância)
- Deleting an Amazon EBS Volume (Excluir um volume do Amazon EBS)

Colunas do relatório

- Status
- Região
- ID da instância
- Tipo de instância
- Tempo próximo ao máximo

O tipo de virtualização do EC2 é paravirtual

Descrição

Verifica se o tipo de virtualização de uma instância do Amazon EC2 é paravirtual.

É uma prática recomendada usar instâncias de máquina virtual do hardware (HVM) em vez de instâncias paravirtuais, quando possível. Isso se deve a aprimoramentos na virtualização da HVM e à disponibilidade de drivers PV para AMIs da HVM, que eliminaram a lacuna de performance que existia historicamente entre os convidados PV e HVM. É importante observar que os tipos de instância da geração atual não são compatíveis com AMIs PV. Portanto, a escolha de um tipo de instância da HVM oferece a melhor performance e compatibilidade com o hardware moderno.

Para obter mais informações, consulte Tipos de virtualização da AMI em Linux.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c18d2gz148`

Origem

AWS ConfigRegra gerenciada: ec2- paravirtual-instance-check

Critérios de alerta

Amarelo: o tipo de virtualização das instâncias do Amazon EC2 é paravirtual.

Recommended Action (Ação recomendada)

Use a virtualização da HVM para suas instâncias do Amazon EC2 e use um tipo de instância compatível.

Para obter informações sobre como escolher o tipo de virtualização apropriado, consulte Compatibilidade para alterar o tipo de instância.

Recursos adicionais

Compatibilidade para alterar o tipo de instância

Colunas do relatório

- Status
- Região
- Recurso
- Regra do AWS Config
- Parâmetros de entrada
- Hora da última atualização

Limite rígido de memória do Amazon ECS

Descrição

Verifica se as definições de tarefas do Amazon ECS têm um limite de memória definido para suas definições de contêiner. A quantidade total de memória reservada para todos os contêineres dentro da tarefa deve ser menor que o valor da memória da tarefa.

Para obter mais informações, consulte Container definitions.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c18d2gz176`

Origem

AWS ConfigRegra gerenciada: ecs-task-definition-memory -hard-limit

Critérios de alerta

Amarelo: o limite rígido de memória do Amazon ECS não está definido.

Recommended Action (Ação recomendada)

Aloque memória para suas tarefas do Amazon ECS para evitar a falta de memória. Caso o container tente exceder a memória especificada, o contêiner então será encerrado.

Para obter mais informações, consulte Como posso alocar memórias para tarefas no Amazon ECS?.

Recursos adicionais

Cluster reservation

Colunas do relatório

- Status
- Região

- Recurso
- Regra do AWS Config
- Parâmetros de entrada
- Hora da última atualização

Otimização do modo throughput do Amazon EFS

Descrição

Verifica se o sistema de arquivos Amazon EFS do cliente está atualmente configurado para usar o modo Bursting Throughput.

Os sistemas de arquivos no modo Bursting Throughput do EFS [1] oferecem um nível básico consistente de throughput (50 KiB/s por GiB de dados no armazenamento EFS Standard) e usam um modelo de crédito para oferecer níveis mais altos de desempenho de “throughput contínuo” quando há “créditos contínuos” disponíveis. Quando você esgota seus créditos de burst, o desempenho do sistema de arquivos é limitado a esse nível inferior de nível básico, o que pode resultar em lentidão, tempos limite ou outras formas de impacto no desempenho dos usuários finais ou das aplicações.

ID da verificação

`c1dfprch02`

Critérios de alerta

- Amarelo: o sistema de arquivos está usando o modo Bursting Throughput.

Recommended Action (Ação recomendada)

Para permitir que seus usuários e aplicações alcancem a taxa de transferência desejada, recomendamos que você atualize a configuração do sistema de arquivos para o modo Elastic Throughput [2]. Quando estiver no modo Elastic Throughput, seu sistema de arquivos pode atingir até 10 GiB/s de taxa de transferência de leitura ou 3 GiB/s de taxa de transferência de gravação, dependendo da região da AWS [3], e você paga somente pela taxa de transferência que usar. Observe que você pode atualizar a configuração do sistema de arquivos para alternar entre os modos de throughput Elastic e Bursting sob demanda, e que os sistemas de arquivos no modo Elastic Throughput acumulam cobranças adicionais pela transferência de dados [4].

Recursos adicionais

- [1] Modos de throughput de desempenho do Amazon EFS

- [2] Modo de throughput Elastic de desempenho do Amazon EFS
- [3] Cotas e limites do Amazon EFS
- [4] Preços do Amazon EFS

Colunas do relatório

- Status
- Região
- ID do sistema de arquivos do EFS
- Modos de throughput
- Hora da última atualização

O parâmetro de autovacuum do Amazon RDS está desativado

Descrição

O parâmetro autovacuum está desativado para suas instâncias de banco de dados. Desligar o autovacuum aumenta o inchaço da tabela e do índice e afeta o desempenho.

Recomendamos que você ative o autovacuum em seus grupos de parâmetros de banco de dados.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

> **Note**
>
> Quando uma instância de banco de dados ou cluster de banco de dados é interrompido, você pode visualizar as recomendações do Amazon RDS Trusted Advisor por 3 a 5 dias. Depois de cinco dias, as recomendações não estão disponíveis emTrusted Advisor. Para visualizar as recomendações, abra o console do Amazon RDS e escolha Recomendações.

Se você excluir uma instância de banco de dados ou um cluster de banco de dados, as recomendações associadas a essas instâncias ou clusters não estarão disponíveis no Trusted Advisor console de gerenciamento do Amazon RDS.

ID da verificação

`c1qf5bt025`

Critérios de alerta

Amarelo: os grupos de parâmetros do banco de dados têm o autovacuum desativado.

Recommended Action (Ação recomendada)

Ative o parâmetro autovacuum em seus grupos de parâmetros do banco de dados.

Recursos adicionais

O banco de dados PostgreSQL requer manutenção periódica, conhecida como aspiração. O Autovacuum no PostgreSQL automatiza a execução dos comandos VACCUUM e ANALYZE. Esse processo reúne as estatísticas da tabela e exclui as linhas inativas. Quando o autovacuum é desativado, o aumento da tabela, o inchaço do índice e as estatísticas obsoletas afetarão o desempenho do banco de dados.

Para obter mais informações, consulte Entendendo o autovacuum no Amazon RDS para ambientes do Amazon RDS for PostgreSQL.

Colunas do relatório

- Status
- Região
- Recurso
- Nome do parâmetro
- Valor recomendado
- Hora da última atualização

Os clusters de banco de dados do Amazon RDS suportam somente volumes de até 64 TiB

Descrição

Seus clusters de banco de dados suportam volumes de até 64 TiB. As versões mais recentes do motor suportam volumes de até 128 TiB. Recomendamos que você atualize a versão do mecanismo do seu cluster de banco de dados para as versões mais recentes para suportar volumes de até 128 TiB.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

> **Note**
>
> Quando uma instância de banco de dados ou cluster de banco de dados é interrompido, você pode visualizar as recomendações do Amazon RDS Trusted Advisor por 3 a 5 dias. Depois de cinco dias, as recomendações não estão disponíveis emTrusted Advisor. Para visualizar as recomendações, abra o console do Amazon RDS e escolha Recomendações.
>
> Se você excluir uma instância de banco de dados ou um cluster de banco de dados, as recomendações associadas a essas instâncias ou clusters não estarão disponíveis no Trusted Advisor console de gerenciamento do Amazon RDS.

ID da verificação

`c1qf5bt017`

Critérios de alerta

Amarelo: os clusters de banco de dados têm suporte para volumes somente de até 64 TiB.

Recommended Action (Ação recomendada)

Atualize a versão do mecanismo de seus clusters de banco de dados para suportar volumes de até 128 TiB.

Recursos adicionais

Ao escalar seu aplicativo em um único cluster de banco de dados Amazon Aurora, você pode não atingir o limite se o limite de armazenamento for 128 TiB. O aumento do limite de armazenamento ajuda a evitar a exclusão dos dados ou a divisão do banco de dados em várias instâncias.

Para obter mais informações, consulte Limites de tamanho do Amazon Aurora.

Colunas do relatório

- Status
- Região
- Recurso
- Nome do motor
- Versão atual do motor
- Valor recomendado
- Hora da última atualização

Instâncias de banco de dados Amazon RDS nos clusters com classes de instância heterogêneas

Descrição

Recomendamos que você use a mesma classe e tamanho de instância de banco de dados para todas as instâncias de banco de dados em seu cluster de banco de dados.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

> **Note**
>
> Quando uma instância de banco de dados ou cluster de banco de dados é interrompido, você pode visualizar as recomendações do Amazon RDS Trusted Advisor por 3 a 5 dias. Depois de cinco dias, as recomendações não estão disponíveis emTrusted

Advisor. Para visualizar as recomendações, abra o console do Amazon RDS e escolha Recomendações.
Se você excluir uma instância de banco de dados ou um cluster de banco de dados, as recomendações associadas a essas instâncias ou clusters não estarão disponíveis no Trusted Advisor console de gerenciamento do Amazon RDS.

ID da verificação

`c1qf5bt009`

Critérios de alerta

Vermelho: clusters de banco de dados têm instâncias de banco de dados com classes de instância heterogêneas.

Recommended Action (Ação recomendada)

Use a mesma classe e tamanho de instância para todas as instâncias de banco de dados em seu cluster de banco de dados.

Recursos adicionais

Quando as instâncias de banco de dados em seu cluster de banco de dados usam diferentes classes ou tamanhos de instância de banco de dados, pode haver um desequilíbrio na carga de trabalho das instâncias de banco de dados. Durante um failover, uma das instâncias de banco de dados do leitor muda para uma instância de banco de dados gravadora. Se as instâncias de banco de dados usarem a mesma classe e tamanho de instância de banco de dados, a carga de trabalho poderá ser balanceada para as instâncias de banco de dados em seu cluster de banco de dados.

Para obter mais informações, consulte Réplicas do Aurora.

Colunas do relatório

- Status
- Região
- Recurso
- Valor recomendado
- Nome do motor
- Hora da última atualização

Instâncias de banco de dados Amazon RDS nos clusters com tamanhos de instância heterogêneos

Descrição

Recomendamos que você use a mesma classe e tamanho de instância de banco de dados para todas as instâncias de banco de dados em seu cluster de banco de dados.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

> **Note**
>
> Quando uma instância de banco de dados ou cluster de banco de dados é interrompido, você pode visualizar as recomendações do Amazon RDS Trusted Advisor por 3 a 5 dias. Depois de cinco dias, as recomendações não estão disponíveis emTrusted Advisor. Para visualizar as recomendações, abra o console do Amazon RDS e escolha Recomendações.
> Se você excluir uma instância de banco de dados ou um cluster de banco de dados, as recomendações associadas a essas instâncias ou clusters não estarão disponíveis no Trusted Advisor console de gerenciamento do Amazon RDS.

ID da verificação

`c1qf5bt008`

Critérios de alerta

Vermelho: clusters de banco de dados têm instâncias de banco de dados com tamanhos de instância heterogêneos.

Recommended Action (Ação recomendada)

Use a mesma classe e tamanho de instância para todas as instâncias de banco de dados em seu cluster de banco de dados.

Recursos adicionais

Quando as instâncias de banco de dados em seu cluster de banco de dados usam diferentes classes ou tamanhos de instância de banco de dados, pode haver um desequilíbrio na carga de trabalho das instâncias de banco de dados. Durante um failover, uma das instâncias de banco de dados do leitor muda para uma instância de banco de dados gravadora. Se as instâncias de banco de dados usarem a mesma classe e tamanho de instância de banco de dados, a carga de trabalho poderá ser balanceada para as instâncias de banco de dados em seu cluster de banco de dados.

Para obter mais informações, consulte Réplicas do Aurora.

Colunas do relatório

- Status
- Região
- Recurso
- Valor recomendado
- Nome do motor
- Hora da última atualização

Os parâmetros de memória de banco de dados do Amazon RDS estão divergindo do padrão

Descrição

Os parâmetros de memória das instâncias de banco de dados são significativamente diferentes dos valores padrão. Essas configurações podem afetar o desempenho e causar erros.

Recomendamos que você redefina os parâmetros de memória personalizados da instância de banco de dados para seus valores padrão no grupo de parâmetros do banco de dados.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

> **Note**
>
> Quando uma instância de banco de dados ou cluster de banco de dados é interrompido, você pode visualizar as recomendações do Amazon RDS Trusted Advisor por 3 a 5 dias. Depois de cinco dias, as recomendações não estão disponíveis emTrusted Advisor. Para visualizar as recomendações, abra o console do Amazon RDS e escolha Recomendações.
> Se você excluir uma instância de banco de dados ou um cluster de banco de dados, as recomendações associadas a essas instâncias ou clusters não estarão disponíveis no Trusted Advisor console de gerenciamento do Amazon RDS.

ID da verificação

`c1qf5bt020`

Critérios de alerta

Amarelo: os grupos de parâmetros do banco de dados têm parâmetros de memória que divergem consideravelmente dos valores padrão.

Recommended Action (Ação recomendada)

Redefina os parâmetros de memória para seus valores padrão.

Recursos adicionais

Para obter mais informações, consulte Melhores práticas para configurar parâmetros do Amazon RDS for MySQL, parte 1: Parâmetros relacionados ao desempenho.

Colunas do relatório

- Status
- Região
- Recurso
- Nome do parâmetro
- Valor recomendado
- Hora da última atualização

O parâmetro enable_index_onlyscan do Amazon RDS está desativado

Descrição

O planejador ou otimizador de consultas não pode usar o tipo de plano de varredura somente de índice quando está desativado.

Recomendamos que você defina o valor do parâmetro enable_indexonlyscan como 1.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

> **Note**
>
> Quando uma instância de banco de dados ou cluster de banco de dados é interrompido, você pode visualizar as recomendações do Amazon RDS Trusted Advisor por 3 a 5 dias. Depois de cinco dias, as recomendações não estão disponíveis emTrusted Advisor. Para visualizar as recomendações, abra o console do Amazon RDS e escolha Recomendações.
> Se você excluir uma instância de banco de dados ou um cluster de banco de dados, as recomendações associadas a essas instâncias ou clusters não estarão disponíveis no Trusted Advisor console de gerenciamento do Amazon RDS.

ID da verificação

`c1qf5bt028`

Critérios de alerta

Amarelo: grupos de parâmetros do banco de dados têm o parâmetro enable_indexonlyscan desativado.

Recommended Action (Ação recomendada)

Defina o parâmetro enable_indexonlyscan como 1.

Recursos adicionais

Quando você desativa o parâmetro enable_indexonlyscan, ele impede que o planejador de consultas selecione um plano de execução ideal. O planejador de consultas usa um tipo de plano diferente, como a varredura de índice, que pode aumentar o custo da consulta e o tempo de execução. O tipo de plano de varredura exclusivo do índice recupera os dados sem acessar os dados da tabela.

Para obter mais informações, consulte enable_indexonlyscan (boolean) no site de documentação do PostgreSQL.

Colunas do relatório

- Status
- Região
- Recurso
- Nome do parâmetro
- Valor recomendado
- Hora da última atualização

O parâmetro enable_indexscan do Amazon RDS está desativado

Descrição

O planejador ou otimizador de consultas não pode usar o tipo de plano de varredura de índice quando está desativado.

Recomendamos que você defina o valor do parâmetro enable_indexscan como 1.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

> **Note**
>
> Quando uma instância de banco de dados ou cluster de banco de dados é interrompido, você pode visualizar as recomendações do Amazon RDS Trusted Advisor por 3 a 5 dias. Depois de cinco dias, as recomendações não estão disponíveis emTrusted Advisor. Para visualizar as recomendações, abra o console do Amazon RDS e escolha Recomendações.
> Se você excluir uma instância de banco de dados ou um cluster de banco de dados, as recomendações associadas a essas instâncias ou clusters não estarão disponíveis no Trusted Advisor console de gerenciamento do Amazon RDS.

ID da verificação

`c1qf5bt029`

Critérios de alerta

Amarelo: os grupos de parâmetros do banco de dados têm o parâmetro enable_indexscan desativado.

Recommended Action (Ação recomendada)

Defina o parâmetro enable_indexscan como 1.

Recursos adicionais

Quando você desativa o parâmetro enable_indexscan, ele impede que o planejador de consultas selecione um plano de execução ideal. O planejador de consultas usa um tipo de plano diferente, como a varredura de índice, que pode aumentar o custo da consulta e o tempo de execução.

Para obter mais informações, consulte enable_indexscan (boolean) no site de documentação do PostgreSQL.

Colunas do relatório

- Status
- Região
- Recurso
- Nome do parâmetro
- Valor recomendado

- Hora da última atualização

O parâmetro general_logging do Amazon RDS está ativado

Descrição

O registro geral está ativado para sua instância de banco de dados. Essa configuração é útil para solucionar os problemas do banco de dados. No entanto, ativar o registro geral aumenta a quantidade de operações de I/O e o espaço de armazenamento alocado, o que pode resultar em contenção e degradação do desempenho.

Verifique seus requisitos de uso geral de registros. Recomendamos que você defina o valor do parâmetro general_logging como 0.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

> **Note**
>
> Quando uma instância de banco de dados ou cluster de banco de dados é interrompido, você pode visualizar as recomendações do Amazon RDS Trusted Advisor por 3 a 5 dias. Depois de cinco dias, as recomendações não estão disponíveis emTrusted Advisor. Para visualizar as recomendações, abra o console do Amazon RDS e escolha Recomendações.
> Se você excluir uma instância de banco de dados ou um cluster de banco de dados, as recomendações associadas a essas instâncias ou clusters não estarão disponíveis no Trusted Advisor console de gerenciamento do Amazon RDS.

ID da verificação

`c1qf5bt037`

Critérios de alerta

Amarelo: grupos de parâmetros do banco de dados têm general_logging ativado.

Recommended Action (Ação recomendada)

Verifique seus requisitos de uso geral de registros. Se não for obrigatório, recomendamos que você defina o valor do parâmetro general_logging como 0.

Recursos adicionais

O registro de consultas gerais é ativado quando o valor do parâmetro general_logging é 1. O registro geral de consultas contém registros das operações do servidor de banco de dados. O servidor grava informações nesse log quando os clientes se conectam ou se desconectam e os registros contêm cada instrução SQL recebida dos clientes. O registro geral de consultas é útil quando você suspeita de um erro em um cliente e deseja encontrar as informações que o cliente deve enviar ao servidor do banco de dados.

Para obter mais informações, consulte Visão geral dos registros do banco de dados RDS for MySQL.

Colunas do relatório

- Status
- Região
- Recurso
- Nome do parâmetro
- Valor recomendado
- Hora da última atualização

Parâmetro Amazon RDS InnoDB_change_buffering usando menos do que o valor ideal

Descrição

O buffer de alterações permite que uma instância de banco de dados MySQL adie algumas gravações, que são necessárias para manter índices secundários. Esse recurso foi útil em ambientes com discos lentos. A alteração na configuração do buffer melhorou um pouco o desempenho do banco de dados, mas causou um atraso na recuperação de falhas e longos tempos de desligamento durante a atualização.

Recomendamos que você defina o valor do parâmetro innodb_change_buffering como NONE.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

> **Note**
>
> Quando uma instância de banco de dados ou cluster de banco de dados é interrompido, você pode visualizar as recomendações do Amazon RDS Trusted Advisor por 3 a 5 dias. Depois de cinco dias, as recomendações não estão disponíveis emTrusted Advisor. Para visualizar as recomendações, abra o console do Amazon RDS e escolha Recomendações.
> Se você excluir uma instância de banco de dados ou um cluster de banco de dados, as recomendações associadas a essas instâncias ou clusters não estarão disponíveis no Trusted Advisor console de gerenciamento do Amazon RDS.

ID da verificação

`c1qf5bt021`

Critérios de alerta

Amarelo: os grupos de parâmetros do banco de dados têm o parâmetro innodb_change_buffering definido com um valor ótimo baixo.

Recommended Action (Ação recomendada)

Defina o valor do parâmetro innodb_change_buffering como NONE em seus grupos de parâmetros de banco de dados.

Recursos adicionais

Para obter mais informações, consulte Melhores práticas para configurar parâmetros do Amazon RDS for MySQL, parte 1: Parâmetros relacionados ao desempenho.

Colunas do relatório

- Status
- Região

- Recurso
- Nome do parâmetro
- Valor recomendado
- Hora da última atualização

O parâmetro innodb_open_files do Amazon RDS está baixo

Descrição

O parâmetro innodb_open_files controla o número de arquivos que o InnoDB pode abrir ao mesmo tempo. O InnoDB abre todos os arquivos de log e tablespace do sistema quando o mysqld está em execução.

Sua instância de banco de dados tem um valor baixo para o número máximo de arquivos que o InnoDB pode abrir ao mesmo tempo. Recomendamos que você defina o parâmetro innodb_open_files com um valor mínimo de 65.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

> **Note**
>
> Quando uma instância de banco de dados ou cluster de banco de dados é interrompido, você pode visualizar as recomendações do Amazon RDS Trusted Advisor por 3 a 5 dias. Depois de cinco dias, as recomendações não estão disponíveis emTrusted Advisor. Para visualizar as recomendações, abra o console do Amazon RDS e escolha Recomendações.
>
> Se você excluir uma instância de banco de dados ou um cluster de banco de dados, as recomendações associadas a essas instâncias ou clusters não estarão disponíveis no Trusted Advisor console de gerenciamento do Amazon RDS.

ID da verificação

`c1qf5bt033`

Critérios de alerta

Amarelo: os grupos de parâmetros do banco de dados têm a configuração de arquivos abertos do InnoDB configurada incorretamente.

Recommended Action (Ação recomendada)

Defina o parâmetro innodb_open_files para um valor mínimo de 65.

Recursos adicionais

O parâmetro innodb_open_files controla o número de arquivos que o InnoDB pode abrir ao mesmo tempo. O InnoDB mantém todos os arquivos de log e os arquivos de espaço de tabela do sistema abertos quando o mysqld está em execução. O InnoDB também precisa abrir alguns arquivos.ibd, se o modelo de file-per-table armazenamento for usado. Quando a configuração innodb_open_files está baixa, ela afeta o desempenho do banco de dados e o servidor pode falhar ao iniciar.

Para obter mais informações, consulte Opções de inicialização e variáveis do sistema do InnoDB - innodb_open_files no site da documentação. MySql

Colunas do relatório

- Status
- Região
- Recurso
- Nome do parâmetro
- Valor recomendado
- Hora da última atualização

O parâmetro innodb_stats_persistent do Amazon RDS está desativado

Descrição

Sua instância de banco de dados não está configurada para manter as estatísticas do InnoDB no disco. Quando as estatísticas não são armazenadas, elas são recalculadas sempre que a

instância é reiniciada e a tabela é acessada. Isso leva a variações no plano de execução da consulta. Você pode modificar o valor desse parâmetro global no nível da tabela.

Recomendamos que você defina o valor do parâmetro innodb_stats_persistent como ON.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

> **Note**
>
> Quando uma instância de banco de dados ou cluster de banco de dados é interrompido, você pode visualizar as recomendações do Amazon RDS Trusted Advisor por 3 a 5 dias. Depois de cinco dias, as recomendações não estão disponíveis emTrusted Advisor. Para visualizar as recomendações, abra o console do Amazon RDS e escolha Recomendações.
> Se você excluir uma instância de banco de dados ou um cluster de banco de dados, as recomendações associadas a essas instâncias ou clusters não estarão disponíveis no Trusted Advisor console de gerenciamento do Amazon RDS.

ID da verificação

`c1qf5bt032`

Critérios de alerta

Amarelo: os grupos de parâmetros do banco de dados têm estatísticas de otimizador que não persistem no disco.

Recommended Action (Ação recomendada)

Defina o valor do parâmetro innodb_stats_persistent como ON.

Recursos adicionais

Se o parâmetro innodb_stats_persistent estiver definido como ON, as estatísticas do otimizador persistirão quando a instância for reiniciada. Isso melhora a estabilidade do plano de execução

e o desempenho consistente das consultas. Você pode modificar a persistência das estatísticas globais no nível da tabela usando a cláusula STATS_PERSISTENT ao criar ou alterar uma tabela.

Para obter mais informações, consulte Melhores práticas para configurar parâmetros do Amazon RDS for MySQL, parte 1: Parâmetros relacionados ao desempenho.

Colunas do relatório

- Status
- Região
- Recurso
- Nome do parâmetro
- Valor recomendado
- Hora da última atualização

Instância do Amazon RDS subprovisionada para capacidade do sistema

Descrição

Verifica se a instância do Amazon RDS ou a instância de banco de dados Amazon Aurora tem a capacidade de sistema necessária para operar.

ID da verificação

`c1qf5bt039`

Critérios de alerta

Amarelo:

O ut-of-memory mata: Quando um processo no host do banco de dados é interrompido devido à redução de memória no nível do sistema operacional, o contador de eliminações de Out Of Memory (OOM) aumenta.

Troca excessiva: os valores das métricas os.memory.swap.in e os.memory.swap.out eram altos.

Recommended Action (Ação recomendada)

Recomendamos que você ajuste suas consultas para usar menos memória ou usar um tipo de instância de banco de dados com maior memória alocada. Quando a instância está com pouca memória, isso afeta o desempenho do banco de dados.

Recursos adicionais

O ut-of-memory kill foi detectado: o kernel Linux invoca o Out of Memory (OOM) Killer quando os processos em execução no host exigem mais do que a memória fisicamente disponível do sistema operacional. Nesse caso, o OOM Killer revisa todos os processos em execução e interrompe um ou mais processos, a fim de liberar memória do sistema e manter o sistema funcionando.

A troca é detectada: quando a memória não é suficiente no host do banco de dados, o sistema operacional envia algumas páginas mínimas usadas para o disco no espaço de troca. Esse processo de descarga afeta o desempenho do banco de dados.

Para obter mais informações, consulte Tipos de instância do Amazon RDS e Como escalar sua instância do Amazon RDS.

Colunas do relatório

- Status
- Região
- Recurso
- Ou ut-of-memory mata (contagem)
- Trocas excessivas (contagem)
- Último período de detecção
- Hora da última atualização

O volume magnético do Amazon RDS está em uso

Descrição

Suas instâncias de banco de dados estão usando armazenamento magnético. O armazenamento magnético não é recomendado para a maioria das instâncias de banco de dados. Escolha um tipo de armazenamento diferente: de uso geral (SSD) ou IOPS provisionado.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

> **Note**
>
> Quando uma instância de banco de dados ou cluster de banco de dados é interrompido, você pode visualizar as recomendações do Amazon RDS Trusted Advisor por 3 a 5 dias. Depois de cinco dias, as recomendações não estão disponíveis emTrusted Advisor. Para visualizar as recomendações, abra o console do Amazon RDS e escolha Recomendações.
> Se você excluir uma instância de banco de dados ou um cluster de banco de dados, as recomendações associadas a essas instâncias ou clusters não estarão disponíveis no Trusted Advisor console de gerenciamento do Amazon RDS.

ID da verificação

`c1qf5bt000`

Critérios de alerta

Amarelo: os recursos do Amazon RDS estão usando armazenamento magnético.

Recommended Action (Ação recomendada)

Escolha um tipo de armazenamento diferente: de uso geral (SSD) ou IOPS provisionado.

Recursos adicionais

O armazenamento magnético é um tipo de armazenamento de geração anterior. O uso geral (SSD) ou IOPS provisionado é o tipo de armazenamento recomendado para novos requisitos de armazenamento. Esses tipos de armazenamento oferecem desempenho superior e consistente, além de opções aprimoradas de tamanho de armazenamento.

Para obter mais informações, consulte Volumes da geração anterior.

Colunas do relatório

- Status
- Região
- Recurso
- Valor recomendado
- Nome do motor
- Hora da última atualização

Grupos de parâmetros do Amazon RDS que não usam páginas grandes

Descrição

Páginas grandes podem aumentar a escalabilidade do banco de dados, mas sua instância de banco de dados não está usando páginas grandes. Recomendamos que você defina o valor do parâmetro use_large_pages como SOMENTE no grupo de parâmetros de banco de dados para sua instância de banco de dados.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

> **Note**
>
> Quando uma instância de banco de dados ou cluster de banco de dados é interrompido, você pode visualizar as recomendações do Amazon RDS Trusted Advisor por 3 a 5 dias. Depois de cinco dias, as recomendações não estão disponíveis emTrusted Advisor. Para visualizar as recomendações, abra o console do Amazon RDS e escolha Recomendações.
> Se você excluir uma instância de banco de dados ou um cluster de banco de dados, as recomendações associadas a essas instâncias ou clusters não estarão disponíveis no Trusted Advisor console de gerenciamento do Amazon RDS.

ID da verificação

`c1qf5bt024`

Critérios de alerta

Amarelo: grupos de parâmetros do banco de dados não usam páginas grandes.

Recommended Action (Ação recomendada)

Defina o valor do parâmetro use_large_pages como SOMENTE em seus grupos de parâmetros de banco de dados.

Recursos adicionais

Para obter mais informações, consulte Como ativar HugePages uma instância do RDS para Oracle.

Colunas do relatório

- Status
- Região
- Recurso
- Nome do parâmetro
- Valor recomendado
- Hora da última atualização

O parâmetro de cache de consulta do Amazon RDS está ativado

Descrição

Quando as alterações exigirem que seu cache de consultas seja limpo, sua instância de banco de dados parecerá paralisada. A maioria das workloads não se beneficia de um cache de consultas. O cache de consultas foi removido do MySQL versão 8.0. Recomendamos que você defina o parâmetro query_cache_type como 0.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

> **Note**
>
> Quando uma instância de banco de dados ou cluster de banco de dados é interrompido, você pode visualizar as recomendações do Amazon RDS Trusted Advisor por 3 a 5 dias. Depois de cinco dias, as recomendações não estão disponíveis emTrusted Advisor. Para visualizar as recomendações, abra o console do Amazon RDS e escolha Recomendações.

Se você excluir uma instância de banco de dados ou um cluster de banco de dados, as recomendações associadas a essas instâncias ou clusters não estarão disponíveis no Trusted Advisor console de gerenciamento do Amazon RDS.

ID da verificação

`c1qf5bt022`

Critérios de alerta

Amarelo: grupos de parâmetros do banco de dados têm o cache de consultas ativado.

Recommended Action (Ação recomendada)

Defina o valor do parâmetro query_cache_type como 0 em seus grupos de parâmetros de banco de dados.

Recursos adicionais

Para obter mais informações, consulte Melhores práticas para configurar parâmetros do Amazon RDS for MySQL, parte 1: Parâmetros relacionados ao desempenho.

Colunas do relatório

- Status
- Região
- Recurso
- Nome do parâmetro
- Valor recomendado
- Hora da última atualização

A atualização da classe de instância de recursos do Amazon RDS é necessária

Descrição

Seu banco de dados está executando uma classe de instância de banco de dados da geração anterior. Substituímos as classes de instância de banco de dados de uma geração anterior por classes de instância de banco de dados com melhor custo, desempenho ou ambos. Recomendamos que você execute sua instância de banco de dados com uma classe de instância de banco de dados de uma geração mais recente.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

> **Note**
>
> Quando uma instância de banco de dados ou cluster de banco de dados é interrompido, você pode visualizar as recomendações do Amazon RDS Trusted Advisor por 3 a 5 dias. Depois de cinco dias, as recomendações não estão disponíveis emTrusted Advisor. Para visualizar as recomendações, abra o console do Amazon RDS e escolha Recomendações.
> Se você excluir uma instância de banco de dados ou um cluster de banco de dados, as recomendações associadas a essas instâncias ou clusters não estarão disponíveis no Trusted Advisor console de gerenciamento do Amazon RDS.

ID da verificação

`c1qf5bt015`

Critérios de alerta

Vermelho: as instâncias de banco de dados estão usando a classe de instância de banco de dados de fim de suporte.

Recommended Action (Ação recomendada)

Atualize para a classe de instância de banco de dados mais recente.

Recursos adicionais

Para ter mais informações, consulte Mecanismos de banco de dados com suporte a todas as classes de instâncias de banco de dados disponíveis.

Colunas do relatório

- Status
- Região

- Recurso
- Classe da instância de banco de dados
- Valor recomendado
- Nome do motor
- Hora da última atualização

A atualização das principais versões dos recursos do Amazon RDS é necessária

Descrição

Bancos de dados com a versão principal atual do mecanismo de banco de dados não serão suportados. Recomendamos que você atualize para a versão principal mais recente, que inclui novas funcionalidades e aprimoramentos.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

> **Note**
>
> Quando uma instância de banco de dados ou cluster de banco de dados é interrompido, você pode visualizar as recomendações do Amazon RDS Trusted Advisor por 3 a 5 dias. Depois de cinco dias, as recomendações não estão disponíveis emTrusted Advisor. Para visualizar as recomendações, abra o console do Amazon RDS e escolha Recomendações.
> Se você excluir uma instância de banco de dados ou um cluster de banco de dados, as recomendações associadas a essas instâncias ou clusters não estarão disponíveis no Trusted Advisor console de gerenciamento do Amazon RDS.

ID da verificação

`c1qf5bt014`

Critérios de alerta

Vermelho: os recursos do RDS estão usando as versões principais de fim de suporte.

Recommended Action (Ação recomendada)

Atualize para a versão principal mais recente do mecanismo de banco de dados.

Recursos adicionais

O Amazon RDS lança novas versões dos mecanismos de banco de dados compatíveis para manter seus bancos de dados com a versão mais recente. As novas versões lançadas podem incluir correções de bugs, aprimoramentos de segurança e outras melhorias no mecanismo de banco de dados. Você pode minimizar o tempo de inatividade necessário para a atualização da instância de banco de dados usando uma implantação azul/verde.

Para obter mais informações, consulte os seguintes recursos do :

- Atualizando uma versão do mecanismo de instância de banco de dados
- Atualizações do Amazon Aurora
- Usando implantações azul/verde do Amazon RDS para atualizações de banco de dados

Colunas do relatório

- Status
- Região
- Recurso
- Nome do motor
- Versão atual do motor
- Valor recomendado
- Hora da última atualização

Recursos do Amazon RDS usando a edição final do mecanismo de suporte sob licença incluída

Descrição

Recomendamos que você atualize a versão principal para a versão mais recente do mecanismo suportada pelo Amazon RDS para continuar com o suporte de licença atual. A versão do mecanismo do seu banco de dados não será compatível com a licença atual.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

> **Note**
>
> Quando uma instância de banco de dados ou cluster de banco de dados é interrompido, você pode visualizar as recomendações do Amazon RDS Trusted Advisor por 3 a 5 dias. Depois de cinco dias, as recomendações não estão disponíveis emTrusted Advisor. Para visualizar as recomendações, abra o console do Amazon RDS e escolha Recomendações.
> Se você excluir uma instância de banco de dados ou um cluster de banco de dados, as recomendações associadas a essas instâncias ou clusters não estarão disponíveis no Trusted Advisor console de gerenciamento do Amazon RDS.

ID da verificação

`c1qf5bt016`

Critérios de alerta

Vermelho: os recursos do Amazon RDS estão usando a edição final do mecanismo de suporte sob o modelo de licença incluída.

Recommended Action (Ação recomendada)

Recomendamos que você atualize seu banco de dados para a versão mais recente compatível com o Amazon RDS para continuar usando o modelo licenciado.

Recursos adicionais

Para obter mais informações, consulte Atualizações de versões principais da Oracle.

Colunas do relatório

- Status
- Região

- Recurso
- Nome do motor
- Versão atual do motor
- Valor recomendado
- Nome do motor
- Hora da última atualização

Conjuntos de registros de recursos do alias no Amazon Route 53.

Descrição

Verifica se há conjuntos de registros de recursos que podem ser alterados para conjuntos de registros de recurso do alias para melhorar a performance e economizar dinheiro.

Um conjunto de registros de recursos de alias roteia consultas DNS para um recurso da AWS (por exemplo, um balanceador de carga do Elastic Load Balancing ou um bucket do Amazon S3) ou para outro conjunto de registros de recurso do Route 53. Quando você usa conjuntos de registros de recurso do alias, o Route 53 roteia suas consultas DNS para recursos da AWS gratuitos.

Zonas hospedadas criadas pela AWS não aparecerão nos resultados da verificação.

ID da verificação

`B913Ef6fb4`

Critérios de alerta

- Amarelo: um conjunto de registros de recursos é um CNAME para um site do Amazon S3.
- Amarelo: um conjunto de registros de recursos é um CNAME para uma CloudFront distribuição da Amazon.
- Amarelo: um conjunto de registros de recursos é um CNAME para um balanceador de carga do Elastic Load Balancing.

Recommended Action (Ação recomendada)

Substitua os conjuntos de registros de recurso CNAME listados por conjuntos de registros de recursos de alias. Consulte Choosing Between Alias and Non-Alias Resource Record Sets (Escolher entre conjuntos de registros de recursos de alias e não alias).

Também é necessário alterar o tipo de registro CNAME para A ou AAAA, dependendo do recurso da AWS. Consulte Values that You Specify When You Create or Edit Amazon Route 53 Resource Record Sets (Valores especificados por você ao criar ou editar conjuntos de registros de recursos no Amazon Route 53).

Recursos adicionais

Encaminhar consultas para recursos da AWS

Colunas do relatório

- Status
- Nome da zona hospedada
- ID da zona hospedada
- Nome do conjunto de registros de recursos
- Tipo do conjunto de registros de recursos
- Identificador do conjunto de registros de recursos
- Alvo do alias

Funções subprovisionadas do AWS Lambda para tamanho de memória

Descrição

Verifica as funções do AWS Lambda que foram invocadas pelo menos uma vez durante o período retroativo. Essa verificação alerta se alguma das suas funções do Lambda tiver sido provisionada em escassez para o tamanho da memória. Quando você tem funções do Lambda que estão subprovisionadas para o tamanho da memória, essas funções demoram mais tempo para serem concluídas.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`COr6dfpM06`

Critérios de alerta

Amarelo: uma função do Lambda que foi subprovisionada para o tamanho da memória durante o período de retrospectiva. Para determinar se uma função Lambda está subprovisionada, consideramos todas as métricas padrão dessa função. CloudWatch O algoritmo usado para identificar funções do Lambda subprovisionadas segue as práticas recomendadas da AWS. O algoritmo é atualizado quando um novo padrão é identificado.

Recommended Action (Ação recomendada)

Considere aumentar o tamanho da memória das funções do Lambda.

Para obter mais informações, consulte Optar por verificações do Trusted Advisor para o AWS Compute Optimizer.

Colunas do relatório

- Status
- Região
- Nome da função
- Versão da função
- Tamanho da memória (MB)
- Tamanho da memória recomendado (MB)
- Período de retrospectiva (dias)
- Risco de performance
- Hora da última atualização

Funções do AWS Lambda sem limite de simultaneidade configurado

Descrição

Verifica se as funções do AWS Lambda estão configuradas com o limite de execuções simultâneas em nível de função.

A simultaneidade é o número de solicitações em andamento que sua função do AWS Lambda está tratando ao mesmo tempo. Para cada solicitação simultânea, o Lambda provisiona uma instância separada do seu ambiente de execução.

Você pode especificar o limite mínimo e máximo de simultaneidade usando os ConcurrencyLimitHighparâmetros concurrencyLimitLowe em suas AWS Config regras.

Para obter mais informações, consulte Escalabilidade de funções do Lambda.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c18d2gz181`

Origem

AWS ConfigRegra gerenciada: lambda-concurrency-check

Critérios de alerta

Amarelo: a função do Lambda não tem limite de simultaneidade configurado.

Recommended Action (Ação recomendada)

Certifique-se de que suas funções do Lambda tenham a simultaneidade configurada. Um limite de simultaneidade para suas funções do Lambda ajuda a garantir que sua função processe solicitações de forma confiável e previsível. Um limite de simultaneidade reduz o risco de sua função ficar sobrecarregada devido a um aumento repentino no tráfego.

Para obter mais informações, consulte Configuração da concorrência reservada.

Recursos adicionais

- Escalabilidade da função do Lambda
- Configurar a simultaneidade reservada

Colunas do relatório

- Status
- Região
- Recurso
- Regra do AWS Config
- Parâmetros de entrada
- Hora da última atualização

Problemas de alto risco do AWS Well-Architected em relação à performance

Descrição

Verifica problemas de alto risco (HRIs – high risk issues) de suas workloads no pilar Performance. Essa verificação é baseada nas suas análises AWS-Well Architected. Os resultados da verificação dependem de você ter concluído ou não a avaliação da workload com o AWS Well-Architected.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`Wxdfp4B1L2`

Critérios de alerta

- Vermelho: pelo menos um problema ativo de alto risco foi identificado no pilar de performance para o AWS Well-Architected.
- Verde: nenhum problema ativo de alto risco foi detectado no pilar de performance para o AWS Well-Architected.

Recommended Action (Ação recomendada)

O AWS Well-Architected detectou problemas de alto risco durante a avaliação da workload. Esses problemas apresentam oportunidades para reduzir riscos e economizar dinheiro. Faça login na ferramenta AWS Well-Architected para revisar suas respostas e adotar medidas para resolver seus problemas ativos.

Colunas do relatório

- Status
- Região
- ARN da workload
- Nome da workload
- Nome do revisor

- Tipo de workload
- Data de início da workload
- Data da última modificação da workload
- Número de problemas de alto risco identificados para performance
- Número de problemas de alto risco resolvidos para performance
- Número de perguntas respondidas para performance
- Número total de perguntas no pilar de performance
- Hora da última atualização

CloudFront Nomes de domínio alternativos

Descrição

Verifica CloudFront as distribuições da Amazon em busca de nomes de domínio alternativos (CNAMES) que tenham configurações de DNS definidas incorretamente.

Se uma CloudFront distribuição incluir nomes de domínio alternativos, a configuração de DNS dos domínios deverá encaminhar as consultas de DNS para essa distribuição.

> **Note**
>
> Essa verificação pressupõe que o DNS do Amazon Route 53 e a CloudFront distribuição da Amazon estejam configurados da mesma forma. Conta da AWS Como tal, a lista de alertas pode incluir recursos funcionando como esperado devido à configuração de DNS fora desta Conta da AWS.

ID da verificação

`N420c450f2`

Critérios de alerta

- Amarelo: uma CloudFront distribuição inclui nomes de domínio alternativos, mas a configuração de DNS não está configurada corretamente com um registro CNAME ou um registro de recurso de alias do Amazon Route 53.
- Amarelo: uma CloudFront distribuição inclui nomes de domínio alternativos, mas não Trusted Advisor pôde avaliar a configuração do DNS porque havia muitos redirecionamentos.

- Amarelo: uma CloudFront distribuição inclui nomes de domínio alternativos, mas não Trusted Advisor pôde avaliar a configuração do DNS por algum outro motivo, provavelmente devido a um tempo limite.

Recommended Action (Ação recomendada)

Atualize a configuração do DNS para encaminhar consultas ao DNS para a distribuição do CloudFront; consulte Using Alternate Domain Names (CNAMEs) (Usar nomes de domínio alternativos [CNAMEs]).

Se você estiver usando o Amazon Route 53 como seu serviço de DNS, consulte Roteamento de tráfego para uma distribuição CloudFront da Amazon Web usando seu nome de domínio. Se o tempo limite da verificação tiver expirado, experimente atualizar a verificação.

Recursos adicionais

Guia do CloudFront desenvolvedor da Amazon

Colunas do relatório

- Status
- ID de distribuição
- Nome do domínio da distribuição
- Usar um nome de domínio alternativo
- Motivo

CloudFront Otimização da entrega de conteúdo

Descrição

Verifica os casos em que a transferência de dados dos buckets do Amazon Simple Storage Service (Amazon S3) poderia ser acelerada usando a CloudFront Amazon, AWS o serviço global de entrega de conteúdo.

Quando você configura CloudFront para entregar seu conteúdo, as solicitações de seu conteúdo são automaticamente encaminhadas para o ponto de presença mais próximo onde o conteúdo está armazenado em cache. Esse roteamento permite que o conteúdo seja distribuído aos usuários com a melhor performance possível. Uma alta proporção de dados transferidos em comparação com os dados armazenados no bucket indica que você poderia se beneficiar do uso da Amazon CloudFront para entregar os dados.

ID da verificação

796d6f3D83

Critérios de alerta

- Amarelo: a quantidade de dados transferidos para fora do bucket para seus usuários por solicitações GET nos 30 dias anteriores à verificação é pelo menos 25 vezes maior do que a quantidade média de dados armazenados no bucket.
- Vermelho: a quantidade de dados transferidos para fora do bucket para seus usuários por solicitações GET nos 30 dias anteriores à verificação é pelo menos 10 TB e pelo menos 25 vezes maior do que a quantidade média de dados armazenados no bucket.

Recommended Action (Ação recomendada)

Considere usar CloudFront para obter um melhor desempenho. Veja os detalhes CloudFront do produto Amazon.

Se os dados transferidos forem de 10 TB por mês ou mais, consulte os CloudFront preços da Amazon para explorar possíveis reduções de custos.

Recursos adicionais

- Guia do CloudFront desenvolvedor da Amazon
- Estudo de caso da AWS: PBS

Colunas do relatório

- Status
- Região
- Nome do bucket
- Armazenamento do S3 (GB)
- Transferência de dados de saída (GB)
- Razão entre transferência e armazenamento

CloudFront Encaminhamento de cabeçalho e taxa de acertos de cache

Descrição

Verifica os cabeçalhos da solicitação HTTP que CloudFront atualmente recebe do cliente e encaminha para seu servidor de origem.

Alguns cabeçalhos, como data ou agente de usuário, reduzem significativamente a taxa de acertos do cache (a proporção de solicitações atendidas a partir de um cache de CloudFront borda). Isso aumenta a carga em sua origem e reduz o desempenho, pois CloudFront deve encaminhar mais solicitações para sua origem.

ID da verificação

`N415c450f2`

Critérios de alerta

Amarelo: um ou mais cabeçalhos de solicitação CloudFront encaminhados para sua origem podem reduzir significativamente a taxa de acertos do cache.

Recommended Action (Ação recomendada)

Considere se os cabeçalhos de solicitação oferecem benefícios suficientes para justificar o efeito negativo na taxa de acertos do cache. Se sua origem retornar o mesmo objeto, independentemente do valor de um determinado cabeçalho, recomendamos que você não configure CloudFront para encaminhar esse cabeçalho para a origem. Para obter mais informações, consulte Configuração CloudFront para armazenar objetos em cache com base em cabeçalhos de solicitação.

Recursos adicionais

- Aumentando a proporção de solicitações atendidas a partir de CloudFront caches de borda
- CloudFront Relatórios de estatísticas de cache
- Cabeçalhos e CloudFront comportamento da solicitação HTTP

Colunas do relatório

- ID de distribuição
- Nome do domínio da distribuição
- Padrão do caminho de comportamento do cache
- Cabeçalhos

Instâncias do Amazon EC2 com alta utilização

Descrição

Verifica as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) que estavam em execução a qualquer momento durante os últimos 14 dias. Um alerta será enviado se a utilização diária da CPU for superior a 90% em quatro ou mais dias.

A alta utilização consistente pode indicar performance otimizada e estável. No entanto, ela também pode indicar que uma aplicação não tem recursos suficientes. Para obter dados diários de utilização da CPU, baixe o relatório desta verificação.

ID da verificação

`ZRxQlPsb6c`

Critérios de alerta

Amarelo: uma instância teve mais de 90% de utilização média diária da CPU em pelo menos 4 dos 14 dias anteriores.

Recommended Action (Ação recomendada)

Considere adicionar mais instâncias. Para obter informações sobre como dimensionar o número de instâncias com base na demanda, consulte What is Auto Scaling? (O que é Auto Scaling?)

Recursos adicionais

- Monitoring Amazon EC2 (Monitorar o Amazon EC2)
- Instance Metadata and User Data (Metadados de instâncias e dados do usuário)
- Guia CloudWatch do usuário da Amazon
- Guia do usuário do Amazon EC2 Auto Scaling

Colunas do relatório

- Região/Zona de disponibilidade
- ID da instância
- Tipo de instância
- Nome da instância
- Utilização média da CPU por 14 dias
- Número de dias acima de 90% de utilização da CPU

Grande número de regras de grupo de segurança do EC2 aplicadas a uma instância

Descrição

Verifica instâncias do Amazon Elastic Compute Cloud (Amazon EC2) que têm um grande número de regras de grupo de segurança. A performance pode ser degradada se uma instância tiver um grande número de regras.

ID da verificação

`j3DFqYTe29`

Critérios de alerta

- Amarelo: uma instância do Amazon EC2-VPC tem mais de 50 regras de grupo de segurança.
- Amarelo: uma instância do Amazon EC2-Classic tem mais de 100 regras de grupo de segurança.

Recommended Action (Ação recomendada)

Reduza o número de regras associadas a uma instância excluindo regras desnecessárias ou sobrepostas. Para obter mais informações, consulte Deleting Rules from a Security Group (Excluir regras de um grupo de segurança).

Recursos adicionais

Amazon EC2 Security Groups (Grupos de segurança do Amazon EC2)

Colunas do relatório

- Região
- ID da instância
- Nome da instância
- ID da VPC
- Total de regras de entrada
- Total de regras de saída

Grande número de regras em um grupo de segurança do EC2

Descrição

Verifica cada grupo de segurança do Amazon Elastic Compute Cloud (Amazon EC2) em busca de um número excessivo de regras.

Se um grupo de segurança tiver um grande número de regras, a performance poderá ser degradada.

ID da verificação

`tfg86AVHAZ`

Critérios de alerta

- Amarelo: um grupo de segurança do Amazon EC2-VPC tem mais de 50 regras.
- Amarelo: um grupo de segurança do Amazon EC2-Classic tem mais de 100 regras.

Recommended Action (Ação recomendada)

Reduza o número de regras em um grupo de segurança excluindo regras desnecessárias ou sobrepostas. Para obter mais informações, consulte Deleting Rules from a Security Group (Excluir regras de um grupo de segurança).

Recursos adicionais

Amazon EC2 Security Groups (Grupos de segurança do Amazon EC2)

Colunas do relatório

- Região
- Nome do grupo de segurança
- ID do grupo
- Descrição
- Contagem de instância
- ID da VPC
- Total de regras de entrada
- Total de regras de saída

Volumes magnéticos do Amazon EBS utilizados em excesso

Descrição

Verifica se há volumes magnéticos do Amazon Elastic Block Store (Amazon EBS) que estejam potencialmente sendo utilizados em excesso e possam se beneficiar de uma configuração mais eficiente.

Um volume magnético é projetado para aplicações com requisitos de entrada/saída (E/S) moderado ou intermitentes e a taxa de IOPS não é garantida. Ele fornece aproximadamente 100 IOPS em média, com uma capacidade de esforço adequado para atingir centenas de IOPS. Para IOPS consistentemente mais altas, é possível usar um volume de IOPS provisionadas (SSD). Para IOPS intermitentes, é possível usar um volume de uso geral (SSD). Para obter mais informações, consulte Tipos de volumes do Amazon EBS.

Para obter uma lista dos tipos de instância compatíveis com o comportamento otimizado para EBS, consulte Amazon EBS-Optimized Instances (Instâncias otimizadas para Amazon EBS).

Para obter métricas de utilização diária, baixe o relatório desta verificação. O relatório detalhado mostra uma coluna para cada um dos últimos 14 dias. Se não houver volume do EBS ativo, a célula estará vazia. Se não houver dados suficientes para fazer uma medição confiável, a célula conterá `N/A`. Se houver dados suficientes, a célula conterá a mediana diária e o percentual da variância em relação à mediana (por exemplo, `256 / 20%`).

ID da verificação

`k3J2hns32g`

Critérios de alerta

Amarelo: um volume magnético do Amazon EBS é anexado a uma instância que pode ser otimizada para EBS ou faz parte de uma rede de computação de cluster com uma mediana diária de mais de 95 IOPS e varia em menos de 10% do valor mediano por pelo menos 7 dos últimos 14 dias.

Recommended Action (Ação recomendada)

Para IOPS consistentemente mais altas, é possível usar um volume de IOPS provisionadas (SSD). Para IOPS intermitentes, é possível usar um volume de uso geral (SSD). Para obter mais informações, consulte Tipos de volumes do Amazon EBS.

Recursos adicionais

Amazon Elastic Block Store (Amazon EBS)

Colunas do relatório

- Status
- Região
- ID de volume
- Nome do volume
- Número de dias acima
- Mediana diária máxima

> **Note**
>
> Se tiver optado pelo AWS Compute Optimizer em sua conta, recomendamos que use a verificação de subprovisionamento de volumes do Amazon EBS. Para obter mais informações, consulte Optar por verificações do Trusted Advisor para o AWS Compute Optimizer.

Segurança

É possível usar as verificações da categoria de segurança a seguir.

> **Note**
>
> Se você habilitou o Security Hub para o seu Conta da AWS, você pode ver suas descobertas no Trusted Advisor console. Para mais informações, consulte Visualizar os controles do AWS Security Hub no AWS Trusted Advisor.
> Você pode visualizar todos os controles no padrão de segurança AWS Foundational Security Best Practices, exceto os controles que têm a categoria: Recuperação > Resiliência. Para obter uma lista dos controles, consulte AWS Foundational Security Best Practices controls no Guia do usuário do AWS Security Hub .

Nomes da verificação

- Período de retenção do Amazon CloudWatch Log Group
- Fim do suporte para instâncias do Amazon EC2 com o Microsoft SQL Server
- Fim do suporte para instâncias do Amazon EC2 com o Microsoft Windows Server
- Fim do suporte padrão para instâncias do Amazon EC2 com Ubuntu LTS
- Clientes Amazon EFS que não usam data-in-transit criptografia
- Snapshots públicos do Amazon EBS
- A criptografia de armazenamento Aurora do Amazon RDS está desativada
- É necessário atualizar a versão secundária do mecanismo Amazon RDS
- Snapshots públicos do Amazon RDS
- Amazon RDS Security Group Access Risk

- A criptografia de armazenamento do Amazon RDS está desativada
- Registros CNAME incompatíveis do Amazon Route 53 apontando diretamente para buckets S3
- Framework de política de remetente e conjuntos de registros de recursos do Amazon Route 53 MX
- Permissões do bucket do Amazon S3
- Conexões de emparelhamento da Amazon VPC com resolução de DNS desabilitada
- AWS Backup Cofre sem política baseada em recursos para evitar a exclusão de pontos de recuperação
- AWS CloudTrail Registro
- AWS Lambda Funções usando tempos de execução obsoletos
- Problemas de alto risco do AWS Well-Architected em relação à segurança
- CloudFrontCertificados SSL personalizados no IAM Certificate Store
- CloudFront Certificado SSL no servidor de origem
- Segurança do ELB Listener
- Grupos de segurança do ELB
- Exposed Access Keys
- Alternância da chave de acesso do IAM
- Política de senhas do IAM
- Uso do IAM
- MFA na conta raiz
- Grupos de segurança - Portas específicas irrestritas
- Grupos de Segurança - Acesso Irrestrito

Período de retenção do Amazon CloudWatch Log Group

Descrição

Verifica se o período de retenção do grupo de CloudWatch registros da Amazon está definido para 365 dias ou outro número especificado.

Por padrão, os logs são mantidos indefinidamente e nunca expiram. No entanto, você pode ajustar a política de retenção de cada grupo de logs para estar em conformidade com os regulamentos do setor ou com os requisitos legais de um período específico.

Você pode especificar o tempo mínimo de retenção e os nomes dos grupos de registros usando os MinRetentionTimeparâmetros LogGroupNamese em suas AWS Config regras.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c18d2gz186`

Origem

`AWS Config Managed Rule: cw-loggroup-retention-period-check`

Critérios de alerta

Amarelo: o período de retenção de um grupo de CloudWatch registros da Amazon é menor que o número mínimo desejado de dias.

Recommended Action (Ação recomendada)

Configure um período de retenção de mais de 365 dias para seus dados de log armazenados no Amazon CloudWatch Logs para atender aos requisitos de conformidade.

Para obter mais informações, consulte Alterar a retenção de dados do registro em CloudWatch Registros.

Recursos adicionais

Alterando a retenção de CloudWatch registros

Colunas do relatório

- Status
- Região
- Recurso
- AWS Config Regra
- Parâmetros de entrada

- Hora da última atualização

Fim do suporte para instâncias do Amazon EC2 com o Microsoft SQL Server

Descrição

Verifica as versões do SQL Server das instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em execução nas últimas 24 horas. Essa verificação alerta se as versões estão próximas ou chegaram ao final do suporte. Cada versão do SQL Server oferece 10 anos de suporte, incluindo 5 anos de suporte convencional e 5 anos de suporte estendido. Após o término do suporte, a versão do SQL Server não receberá atualizações de segurança regulares. A execução de aplicações com versões do SQL Server sem suporte pode trazer riscos de segurança ou conformidade.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`Qsdfp3A4L3`

Critérios de alerta

- Vermelho: uma instância do EC2 tem uma versão do SQL Server que chegou ao fim do ciclo de suporte.
- Amarelo: uma instância do EC2 tem uma versão do SQL Server que chegará ao fim do ciclo de suporte em 12 meses.

Recommended Action (Ação recomendada)

Para modernizar suas workloads do SQL Server, considere refatorar para bancos de dados nativos da Nuvem AWS , como o Amazon Aurora. Para obter mais informações, consulte Modernizar cargas de trabalho do Windows com. AWS

Para migrar para um banco de dados totalmente gerenciado, considere redefinir a plataforma para o Amazon Relational Database Service (Amazon RDS). Para obter mais informações, consulte Amazon RDS for SQL Server (Amazon RDS para SQL Server).

Para atualizar seu SQL Server no Amazon EC2, considere usar o runbook de automação para simplificar sua atualização. Para obter mais informações, consulte a documentação do AWS Systems Manager.

Se você não conseguir atualizar seu SQL Server no Amazon EC2, considere o Programa de migração de fim do ciclo de suporte (EMP) para Windows Server. Para obter mais informações, acesse o EMP Website (Site do EMP).

Recursos adicionais

- Prepare-se para o fim do suporte ao SQL Server com AWS
- Microsoft SQL Server na AWS

Colunas do relatório

- Status
- Região
- ID da instância
- Versão do SQL Server
- Ciclo de suporte
- Fim do suporte
- Hora da última atualização

Fim do suporte para instâncias do Amazon EC2 com o Microsoft Windows Server

Descrição

Essa verificação alerta se as versões estão próximas ou chegaram ao final do suporte. Cada versão do Windows Server oferece 10 anos de suporte. Estão incluídos 5 anos de suporte convencional e 5 anos de suporte estendido. Após o fim do suporte, a versão do Windows Server não receberá atualizações de segurança regulares. Caso execute aplicativos com versões sem suporte do Windows Server, você arrisca a segurança ou a conformidade desses aplicativos.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`Qsdfp3A4L4`

Critérios de alerta

- Vermelho: uma instância do EC2 tem uma versão do Windows Server que chegou ao fim do suporte (Windows Server 2003, 2003 R2, 2008 e 2008 R2).
- Amarelo: uma instância do EC2 tem uma versão do Windows Server que chegará ao fim do suporte em menos de 18 meses (Windows Server 2012 e 2012 R2).

Recommended Action (Ação recomendada)

Para modernizar suas cargas de trabalho do Windows Server, considere as várias opções disponíveis em Modernizar cargas de trabalho do Windows com. AWS

Para atualizar seus workloads do Windows Server para que sejam executados em versões mais recentes desse servidor, você pode usar um runbook de automação. Para obter mais informações, consulte a documentação do AWS Systems Manager.

Siga o conjunto de etapas abaixo:

- a. Atualize a versão do Windows Server
- b. Parada forçada e início após a atualização
- c. Se estiver usando o EC2Config, migre para o EC2Launch

Colunas do relatório

- Status
- Região
- ID da instância
- Versão do Windows Server
- Ciclo de suporte
- Fim do suporte
- Hora da última atualização

Fim do suporte padrão para instâncias do Amazon EC2 com Ubuntu LTS

Descrição

Essa verificação alerta se as versões estão próximas ou chegaram ao fim do suporte padrão. É importante agir — migrando para o próximo LTS ou atualizando para o Ubuntu Pro. Após o fim

do suporte, suas máquinas 18.04 LTS não receberão nenhuma atualização de segurança. Com uma assinatura do Ubuntu Pro, sua implantação do Ubuntu 18.04 LTS pode receber Manutenção de Segurança Expandida (ESM) até 2028. Vulnerabilidades de segurança que permanecem sem correção abrem seus sistemas para hackers e para o potencial de uma grande violação.

ID da verificação

`c1dfprch15`

Critérios de alerta

Vermelho: uma instância do Amazon EC2 tem uma versão do Ubuntu que chegou ao fim do suporte padrão (Ubuntu 18.04 LTS, 18.04.1 LTS, 18.04.2 LTS, 18.04.3 LTS, 18.04.4 LTS, 18.04.5 LTS e 18.04.6 LTS).

Amarelo: uma instância do Amazon EC2 tem uma versão do Ubuntu que chegará ao fim do suporte padrão em menos de 6 meses (Ubuntu 20.04 LTS, 20.04.1 LTS, 20.04.2 LTS, 20.04.3 LTS, 20.04.4 LTS, 20.04.5 LTS e 20.04.6 LTS).

Verde: todas as instâncias do Amazon EC2 são compatíveis.

Recommended Action (Ação recomendada)

Para atualizar as instâncias LTS do Ubuntu 18.04 para uma versão LTS compatível, siga as etapas mencionadas neste artigo. Para atualizar as instâncias do Ubuntu 18.04 LTS para o Ubuntu Pro, visite o AWS License Manager console e siga as etapas mencionadas no guia do AWS License Manager usuário. Você também pode consultar o blog do Ubuntu que mostra uma demonstração passo a passo da atualização de instâncias do Ubuntu para o Ubuntu Pro.

Recursos adicionais

Para obter informações sobre preços, entre em contato com AWS Support.

Colunas do relatório

- Status
- Região
- Versão Ubuntu Lts
- Data esperada de fim do suporte
- ID da instância
- Ciclo de suporte
- Hora da última atualização

Clientes Amazon EFS que não usam data-in-transit criptografia

Descrição

Verifica se o sistema de arquivos Amazon EFS está montado usando data-in-transit criptografia. AWS recomenda que os clientes usem data-in-transit criptografia em todos os fluxos de dados para proteger os dados contra exposição acidental ou acesso não autorizado. O Amazon EFS recomenda que os clientes usem a configuração de montagem '-o tls' usando o auxiliar de montagem do Amazon EFS para criptografar dados em trânsito usando o TLS v1.2.

ID da verificação

`c1dfpnchv1`

Critérios de alerta

Amarelo: um ou mais clientes NFS para seu sistema de arquivos Amazon EFS não estão usando as configurações de montagem recomendadas que fornecem data-in-transit criptografia.

Verde: todos os clientes NFS do seu sistema de arquivos Amazon EFS estão usando as configurações de montagem recomendadas que fornecem data-in-transit criptografia.

Recommended Action (Ação recomendada)

Para aproveitar o recurso de data-in-transit criptografia no Amazon EFS, recomendamos que você remonte seu sistema de arquivos usando o auxiliar de montagem do Amazon EFS e as configurações de montagem recomendadas.

> **Note**
>
> Algumas distribuições do Linux não incluem uma versão do stunnel que suporte recursos TLS por padrão. Se você estiver usando uma distribuição Linux não suportada (consulte as distribuições suportadas aqui), recomendamos que você a atualize antes da remontagem com a configuração de montagem recomendada.

Recursos adicionais

- Criptografando dados em trânsito

Colunas do relatório

- Status
- Região

- ID do sistema de arquivos do EFS
- AZs com conexões não criptografadas
- Hora da última atualização

Snapshots públicos do Amazon EBS

Descrição

Verifica as configurações de permissão para seus snapshots de volume do Amazon Elastic Block Store (Amazon EBS) e alerta você se algum snapshot estiver acessível publicamente.

Ao tornar um instantâneo público, você concede a todos Contas da AWS os usuários acesso a todos os dados do instantâneo. Se quiser compartilhar um snapshot somente com usuários ou contas específicos, marque o snapshot como privado. Em seguida, especifique o usuário ou as contas com as quais você deseja compartilhar os dados do snapshot. Observe que, se você tiver o Bloqueio de Acesso Público ativado no modo “bloquear todo o compartilhamento”, seus instantâneos públicos não estarão acessíveis ao público e não aparecerão nos resultados dessa verificação.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas.

ID da verificação

`ePs02jT06w`

Critérios de alerta

Vermelho: O instantâneo do volume do EBS pode ser acessado publicamente.

Recommended Action (Ação recomendada)

A menos que você tenha certeza de que deseja compartilhar todos os dados do instantâneo com todos os Contas da AWS usuários, modifique as permissões: marque o instantâneo como privado e especifique as contas às quais você deseja conceder permissões. Para obter mais informações, consulte Sharing an Amazon EBS Snapshot (Compartilhar um snapshot do Amazon EBS). Use

Bloquear acesso público para instantâneos do EBS para controlar as configurações que permitem acesso público aos seus dados. Essa verificação não pode ser excluída da exibição no Trusted Advisor console.

Para modificar diretamente as permissões dos seus instantâneos, você pode usar um runbook no AWS Systems Manager console. Para obter mais informações, consulte `AWSSupport-ModifyEBSSnapshotPermission`.

Recursos adicionais

Amazon EBS Snapshots (Snapshots do Amazon EBS)

Colunas do relatório

- Status
- Região
- ID de volume
- ID do snapshot
- Descrição

A criptografia de armazenamento Aurora do Amazon RDS está desativada

Descrição

O Amazon RDS oferece suporte à criptografia em repouso para todos os mecanismos de banco de dados usando as chaves que você gerencia. AWS Key Management Service Em uma instância de banco de dados ativa com criptografia do Amazon RDS, os dados armazenados em repouso no armazenamento são criptografados, de forma semelhante aos backups automatizados, réplicas de leitura e snapshots.

Se a criptografia não estiver ativada durante a criação de um cluster de banco de dados Aurora, você deverá restaurar um snapshot descriptografado em um cluster de banco de dados criptografado.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

> **Note**
>
> Quando uma instância de banco de dados ou cluster de banco de dados é interrompido, você pode visualizar as recomendações do Amazon RDS Trusted Advisor por 3 a 5 dias. Depois de cinco dias, as recomendações não estão disponíveis em Trusted Advisor. Para visualizar as recomendações, abra o console do Amazon RDS e escolha Recomendações.
> Se você excluir uma instância de banco de dados ou um cluster de banco de dados, as recomendações associadas a essas instâncias ou clusters não estarão disponíveis no Trusted Advisor console de gerenciamento do Amazon RDS.

ID da verificação

`c1qf5bt005`

Critérios de alerta

Vermelho: os recursos do Amazon RDS Aurora não têm criptografia ativada.

Recommended Action (Ação recomendada)

Ative a criptografia de dados em repouso para o cluster de banco de dados.

Recursos adicionais

Você pode ativar a criptografia ao criar uma instância de banco de dados ou usar uma solução alternativa para ativar a criptografia em uma instância de banco de dados ativa. Você não pode modificar um cluster de banco de dados descriptografado em um cluster de banco de dados criptografado. No entanto, você pode restaurar um snapshot descriptografado em um cluster de banco de dados criptografado. Ao restaurar a partir do instantâneo descriptografado, você deve especificar uma chave. AWS KMS

Para obter mais informações, consulte Encrypting Amazon Aurora resources.

Colunas do relatório

- Status
- Região
- Recurso
- Nome do motor
- Hora da última atualização

É necessário atualizar a versão secundária do mecanismo Amazon RDS

Descrição

Os recursos de banco de dados não estão executando a versão secundária mais recente do mecanismo de banco de dados. A versão secundária mais recente contém as correções de segurança mais recentes e outras melhorias.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

> **Note**
>
> Quando uma instância de banco de dados ou cluster de banco de dados é interrompido, você pode visualizar as recomendações do Amazon RDS Trusted Advisor por 3 a 5 dias. Depois de cinco dias, as recomendações não estão disponíveis em Trusted Advisor. Para visualizar as recomendações, abra o console do Amazon RDS e escolha Recomendações.
> Se você excluir uma instância de banco de dados ou um cluster de banco de dados, as recomendações associadas a essas instâncias ou clusters não estarão disponíveis no Trusted Advisor console de gerenciamento do Amazon RDS.

ID da verificação

`c1qf5bt003`

Critérios de alerta

Vermelho: os recursos do Amazon RDS não estão executando a última versão secundária do mecanismo de banco de dados.

Recommended Action (Ação recomendada)

Atualize para a versão mais recente do motor.

Recursos adicionais

Recomendamos que você mantenha seu banco de dados com a versão secundária mais recente do mecanismo de banco de dados, pois essa versão inclui as correções de segurança e funcionalidade mais recentes. As atualizações da versão secundária do mecanismo de banco de dados contêm apenas as alterações que são compatíveis com versões secundárias anteriores da mesma versão principal do mecanismo de banco de dados.

Para obter mais informações, consulte Atualizar a versão de mecanismo de uma instância de banco de dados.

Colunas do relatório

- Status
- Região
- Recurso
- Nome do motor
- Versão atual do motor
- Valor recomendado
- Hora da última atualização

Snapshots públicos do Amazon RDS

Descrição

Verifica as configurações de permissão para os snapshots de banco de dados do Amazon Relational Database Service (Amazon RDS) e o alerta se algum snapshot estiver marcado como público.

Ao tornar um instantâneo público, você concede a todos Contas da AWS os usuários acesso a todos os dados do instantâneo. Se quiser compartilhar um snapshot somente com usuários ou contas específicos, marque o snapshot como privado. Em seguida, especifique o usuário ou as contas com as quais você deseja compartilhar os dados do snapshot.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas.

ID da verificação

`rSs93HQwa1`

Critérios de alerta

Vermelho: o snapshot Amazon RDS está marcado como público.

Recommended Action (Ação recomendada)

A menos que você tenha certeza de que deseja compartilhar todos os dados do instantâneo com todos os Contas da AWS usuários, modifique as permissões: marque o instantâneo como privado e especifique as contas às quais você deseja conceder permissões. Para obter mais informações, consulte Sharing a DB Snapshot or DB Cluster Snapshot (Compartilhar um snapshot de banco de dados ou do cluster de banco de dados). Essa verificação não pode ser excluída da exibição no Trusted Advisor console.

Para modificar diretamente as permissões dos seus instantâneos, você pode usar um runbook no AWS Systems Manager console. Para obter mais informações, consulte `AWSSupport-ModifyRDSSnapshotPermission`.

Recursos adicionais

Backing Up and Restoring Amazon RDS DB Instances (Backup e restauração de uma instância de banco de dados do Amazon RDS)

Colunas do relatório

- Status
- Região
- ID do cluster ou instância de banco de dados
- ID do snapshot

Amazon RDS Security Group Access Risk

Descrição

Verifica as configurações do grupo de segurança do Amazon Relational Database Service (Amazon RDS) e avisa quando uma regra de grupo de segurança concede acesso excessivamente permissivo ao banco de dados. A configuração recomendada para uma regra de grupo de segurança é permitir o acesso somente de grupos de segurança específicos do Amazon Elastic Compute Cloud (Amazon EC2) ou de um endereço IP específico.

ID da verificação

`nNauJisYIT`

Critérios de alerta

- Amarelo: uma regra de grupo de segurança de banco de dados faz referência a um grupo de segurança do Amazon EC2 que concede acesso global em uma destas portas: 20, 21, 22, 1433, 1434, 3306, 3389, 4333, 5432, 5500.
- Amarelo: uma regra de grupo de segurança de banco de dados concede acesso a mais de um endereço IP (o sufixo da regra CIDR não é /0 ou /32).
- Vermelho: uma regra de grupo de segurança de banco de dados concede acesso global (o sufixo da regra CIDR é /0).

Recommended Action (Ação recomendada)

Analise suas regras de grupo de segurança e restrinja o acesso a endereços IP ou intervalos de IP autorizados. Para editar um grupo de segurança, use a SecurityGroupIngress API AuthorizeDB ou o. AWS Management Console Para obter mais informações, consulte Trabalhar com grupos de segurança de banco de dados.

Recursos adicionais

- Amazon RDS Security Groups (Grupos de segurança do Amazon RDS)
- Classless Inter-Domain Routing (Roteamento sem classe entre domínios)
- List of TCP and UDP port numbers (Lista de números de portas TCP e UDP)

Colunas do relatório

- Status
- Região
- Nome do grupo de segurança do RDS
- Regra de entrada

- Motivo

A criptografia de armazenamento do Amazon RDS está desativada

Descrição

O Amazon RDS oferece suporte à criptografia em repouso para todos os mecanismos de banco de dados usando as chaves que você gerencia. AWS Key Management Service Em uma instância de banco de dados ativa com criptografia do Amazon RDS, os dados armazenados em repouso no armazenamento são criptografados, de forma semelhante aos backups automatizados, réplicas de leitura e snapshots.

Se a criptografia não estiver ativada durante a criação de uma instância de banco de dados, você deverá restaurar uma cópia criptografada do snapshot descriptografado antes de ativar a criptografia.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

> **Note**
>
> Quando uma instância de banco de dados ou cluster de banco de dados é interrompido, você pode visualizar as recomendações do Amazon RDS Trusted Advisor por 3 a 5 dias. Depois de cinco dias, as recomendações não estão disponíveis em Trusted Advisor. Para visualizar as recomendações, abra o console do Amazon RDS e escolha Recomendações.
> Se você excluir uma instância de banco de dados ou um cluster de banco de dados, as recomendações associadas a essas instâncias ou clusters não estarão disponíveis no Trusted Advisor console de gerenciamento do Amazon RDS.

ID da verificação

`c1qf5bt006`

Critérios de alerta

Vermelho: os recursos do Amazon RDS não têm criptografia ativada.

Recommended Action (Ação recomendada)

Ative a criptografia de dados em repouso para a instância de banco de dados.

Recursos adicionais

Você pode criptografar uma instância de banco de dados somente ao criar a instância de banco de dados. Para criptografar uma instância de banco de dados ativa existente:

Crie uma cópia criptografada da instância de banco de dados original

1. Crie um snapshot de sua instância de banco de dados.
2. Crie uma cópia criptografada do snapshot criado na etapa 1.
3. Restaure uma instância de banco de dados a partir do snapshot criptografado.

Para obter mais informações, consulte os seguintes recursos do :

- Criptografando recursos do Amazon RDS
- Copiar um DB snapshot

Colunas do relatório

- Status
- Região
- Recurso
- Nome do motor
- Hora da última atualização

Registros CNAME incompatíveis do Amazon Route 53 apontando diretamente para buckets S3

Descrição

Verifica as zonas hospedadas do Amazon Route 53 com registros CNAME apontando diretamente para os nomes de host do bucket do Amazon S3 e alerta se seu CNAME não coincidir com o nome do bucket do S3.

ID da verificação

`c1ng44jvbm`

Critérios de alerta

Vermelho: a zona hospedada do Amazon Route 53 tem registros CNAME apontando para nomes de host de bucket S3 incompatíveis.

Verde: nenhum registro CNAME incompatível encontrado na sua zona hospedada do Amazon Route 53.

Recommended Action (Ação recomendada)

Ao apontar registros CNAME para nomes de host de bucket do S3, você deve garantir que exista um bucket correspondente para qualquer registro CNAME ou alias que você configurar. Ao fazer isso, você evita o risco de seus registros CNAME serem falsificados. Você também impede que qualquer AWS usuário não autorizado hospede conteúdo da web defeituoso ou malicioso com seu domínio.

Para evitar apontar registros CNAME diretamente para nomes de host de bucket do S3, considere usar o controle de acesso de origem (OAC) para acessar seus ativos da web do bucket do S3 por meio da Amazon. CloudFront

Para obter mais informações sobre como associar o CNAME a um nome de host de bucket do Amazon S3, consulte Personalização de URLs do Amazon S3 com registros CNAME.

Recursos adicionais

- Como associar um nome de host a um bucket do Amazon S3
- Restringindo o acesso a uma origem do Amazon S3 com CloudFront

Colunas do relatório

- Status
- ID da zona hospedada
- ARN da zona hospedada
- Registros CNAME correspondentes
- Registros CNAME incompatíveis
- Hora da última atualização

Framework de política de remetente e conjuntos de registros de recursos do Amazon Route 53 MX

Descrição

Para cada conjunto de registros do recurso MX, verifica se o conjunto de registros do recurso TXT ou SPF contém um registro SPF válido. O registro deve começar com "`v=spf1`". O registro SPF especifica os servidores autorizados a enviar e-mail para seu domínio, o que ajuda a detectar e interromper a falsificação de endereços de e-mail e reduzir o spam. O Route 53 recomenda que você use um registro TXT em vez de um registro SPF. Trusted Advisor relata essa verificação como verde, desde que cada conjunto de registros de recursos MX tenha pelo menos um registro SPF ou TXT.

ID da verificação

`c9D319e7sG`

Critérios de alerta

Amarelo: um conjunto de registros de recursos MX não tem um registro de recurso TXT ou SPF contendo um valor de SPF válido.

Recommended Action (Ação recomendada)

Para cada conjunto de registros de recursos MX, crie um conjunto de registros de recursos TXT contendo um valor de SPF válido. Para obter mais informações, consulte Sender Policy Framework: SPF Record Syntax (Estrutura da política do remetente: Sintaxe de registros da SPF) e Creating Resource Record Sets By Using the Amazon Route 53 Console (Criar conjuntos de registros de recursos usando o console do Amazon Route 53).

Recursos adicionais

- Sender Policy Framework (Estrutura da política do remetente)
- MX record (Registro MX)

Colunas do relatório

- Nome da zona hospedada
- ID da zona hospedada
- Nome do conjunto de registros de recursos
- Status

Permissões do bucket do Amazon S3

Descrição

Verifica buckets no Amazon Simple Storage Service (Amazon S3) que têm permissões de acesso aberto ou que permitem acesso a qualquer usuário autenticado. AWS

Esta verificação examina permissões de bucket explícitas, bem como políticas de bucket que podem substituir essas permissões. Não é recomendável conceder permissões de acesso à lista a todos os usuários de um bucket do Amazon S3. Essas permissões podem levar a usuários não intencionais que listem objetos no bucket em alta frequência, o que pode resultar em cobranças maiores do que o esperado. As permissões que concedem acesso de carregamento e exclusão a todos podem levar a vulnerabilidades de segurança em seu bucket.

ID da verificação

`Pfx0RwqBli`

Critérios de alerta

- Amarelo: a ACL do bucket permite o acesso à lista para Todos ou Qualquer usuário da AWS autenticado.
- Amarelo: uma política do bucket permite qualquer tipo de acesso aberto.
- Amarelo: a política do bucket tem declarações que concedem acesso público. A configuração Block public and cross-account access to buckets that have public policies (Bloquear o acesso entre contas e público a buckets que têm políticas públicas) está ativada e restringiu o acesso apenas a usuários autorizados dessa conta até que as declarações públicas sejam removidas.
- Trusted Advisor Amarelo: não tem permissão para verificar a política ou a política não pôde ser avaliada por outros motivos.
- Vermelho: a ACL do bucket permite acesso de carregamento e exclusão à lista para Todos ou Qualquer usuário da AWS autenticado.

Recommended Action (Ação recomendada)

Se um bucket permitir acesso aberto, determine se o acesso aberto é realmente necessário. Caso contrário, atualize as permissões do bucket para restringir o acesso ao proprietário ou a usuários específicos. Use o bloqueio de acesso público do Amazon S3 para controlar as configurações que permitem acesso público a seus dados. Consulte Setting Bucket and Object Access Permissions (Configurar permissões de acesso ao bucket e a objetos).

Recursos adicionais

Managing Access Permissions to Your Amazon S3 Resources (Gerenciar permissões de acesso aos recursos do Amazon S3)

Colunas do relatório

- Status
- Nome da região
- Parâmetro de API da região
- Nome do bucket
- Lista de permissões da ACL
- Uploads/Exclusões permitidos pela ACL
- Acesso permitido pela política

Conexões de emparelhamento da Amazon VPC com resolução de DNS desabilitada

Descrição

Verifica se suas conexões de emparelhamento da VPC têm a resolução DNS habilitada para as VPCs aceitantes e solicitantes.

A resolução DNS para uma conexão de emparelhamento da VPC permite a resolução de nomes de hosts DNS público para endereços de IPv4 privados quando consultados em sua VPC. Isso permite o uso de nomes DNS para comunicação entre recursos em VPCs emparelhadas. A resolução de DNS em suas conexões de emparelhamento da VPC torna o desenvolvimento e o gerenciamento de aplicações mais simples e menos propensos a erros, além de garantir que os recursos sempre se comuniquem de forma privada pela conexão de emparelhamento da VPC.

Você pode especificar os IDs de VPC usando os parâmetros de VPCids em suas regras. AWS Config

Para obter mais informações, consulte Habilitar a resolução de DNS para a conexão de emparelhamento da VPC.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c18d2gz124`

Origem

`AWS Config Managed Rule: vpc-peering-dns-resolution-check`

Critérios de alerta

Amarelo: a resolução de DNS não está habilitada para as VPCs aceitantes e solicitantes em uma conexão de emparelhamento da VPC.

Recommended Action (Ação recomendada)

Habilite a resolução de DNS para suas conexões de emparelhamento da VPC.

Recursos adicionais

- Modificar opções de conexão de emparelhamento da VPC
- Atributos de DNS em sua VPC

Colunas do relatório

- Status
- Região
- Recurso
- AWS Config Regra
- Parâmetros de entrada
- Hora da última atualização

AWS Backup Cofre sem política baseada em recursos para evitar a exclusão de pontos de recuperação

Descrição

Verifica se AWS Backup os cofres têm uma política baseada em recursos anexada que impede a exclusão do ponto de recuperação.

A política baseada em recursos evita a exclusão inesperada de pontos de recuperação, o que permite aplicar o controle de acesso com o mínimo de privilégios aos dados de backup.

Você pode especificar os AWS Identity and Access Management ARNs que não deseja que a regra verifique no principalArnListparâmetro de suas AWS Config regras.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c18d2gz152`

Origem

`AWS Config Managed Rule: backup-recovery-point-manual-deletion-disabled`

Critérios de alerta

Amarelo: há AWS Backup cofres que não têm uma política baseada em recursos para evitar a exclusão de pontos de recuperação.

Recommended Action (Ação recomendada)

Crie políticas baseadas em recursos para seus AWS Backup cofres para evitar a exclusão inesperada de pontos de recuperação.

A política deve incluir uma declaração “Negar” com as PutBackupVaultAccessPolicy permissões backup:UpdateRecoveryPointLifecycle, backup: e backup:. DeleteRecoveryPoint

Para obter mais informações, consulte Definir políticas de acesso em cofres de backup.

Colunas do relatório

- Status
- Região
- Recurso
- AWS Config Regra
- Parâmetros de entrada
- Hora da última atualização

AWS CloudTrail Registro

Descrição

Verifica seu uso de AWS CloudTrail. CloudTrail fornece maior visibilidade da atividade em você, Conta da AWS registrando informações sobre chamadas de AWS API feitas na conta. É possível usar esses logs para determinar, por exemplo, quais ações um determinado usuário executou durante um período especificado ou quais usuários executaram ações em um recurso específico durante um período especificado.

Como CloudTrail entrega arquivos de log para um bucket do Amazon Simple Storage Service (Amazon S3) CloudTrail , é necessário ter permissões de gravação para o bucket. Se uma trilha se aplicar a todas as regiões (o padrão ao criar uma nova trilha), ela aparecerá várias vezes no relatório do Trusted Advisor .

ID da verificação

`vjafUGJ9H0`

Critérios de alerta

- Amarelo: CloudTrail relata erros de entrega de registros de uma trilha.
- Vermelho: uma trilha não foi criada para uma região ou o log está desativado para uma trilha.

Recommended Action (Ação recomendada)

Para criar uma trilha e iniciar o log via console, acesse o console do AWS CloudTrail.

Para iniciar o log, consulte Stopping and Starting Logging for a Trail (Parar e iniciar o log para uma trilha).

Se você receber erros de entrega de log, verifique se o bucket existe e se a política necessária está vinculada ao bucket. Consulte Amazon S3 Bucket Policy (Política de buckets do Amazon S3).

Recursos adicionais

- AWS CloudTrail Guia do usuário
- Supported Regions (Regiões compatíveis)
- Supported Services (Serviços compatíveis)

Colunas do relatório

- Status
- Região
- Nome da trilha
- Status do log
- Nome do bucket
- Data da última entrega

AWS Lambda Funções usando tempos de execução obsoletos

Descrição

Verifica as funções do Lambda cuja versão $LATEST está configurada para usar um tempo de execução que está se aproximando da descontinuação ou está obsoleto. Os tempos de execução obsoletos não são elegíveis para atualizações de segurança ou suporte técnico

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

As versões publicadas da função do Lambda são imutáveis, o que significa que elas podem ser invocadas, mas não atualizadas. Somente a versão `$LATEST` de uma função do Lambda pode ser atualizada. Para obter mais informações, consulte Lambda function versions (Versões da função do Lambda).

ID da verificação

`L4dfs2Q4C5`

Critérios de alerta

- Vermelho: A versão $LATEST da função está configurada para usar um tempo de execução que já está obsoleto.
- Amarelo: a versão $LATEST da função está sendo executada em um tempo de execução que será descontinuado em 180 dias.

Recommended Action (Ação recomendada)

Caso tenha funções que estão sendo executadas em um runtime que está prestes a ser descontinuado, prepare-se para realizar a migração para um tempo de execução compatível. Para obter mais informações, consulte Runtime support policy (Política de suporte ao tempo de execução).

Recomendamos excluir as versões anteriores da função que não estão mais sendo usadas.

Recursos adicionais

Lambda runtimes (Tempos de execução do Lambda)

Colunas do relatório

- Status
- Região
- ARN da função
- Runtime
- Dias até a descontinuação
- Data da defasagem
- Invocações médias diárias
- Hora da última atualização

Problemas de alto risco do AWS Well-Architected em relação à segurança

Descrição

Verifica problemas de alto risco (HRIs – high risk issues) de suas workloads no pilar Segurança. Essa verificação é baseada nas suas análises AWS-Well Architected. Os resultados da

verificação dependem de você ter concluído ou não a avaliação da workload com o AWS Well-Architected.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`Wxdfp4B1L3`

Critérios de alerta

- Vermelho: Pelo menos um problema ativo de alto risco foi identificado no pilar de segurança da AWS Well-Architected.
- Verde: Nenhum problema ativo de alto risco foi detectado no pilar de segurança do AWS Well-Architected.

Recommended Action (Ação recomendada)

AWS O Well-Architected detectou problemas de alto risco durante a avaliação da carga de trabalho. Esses problemas apresentam oportunidades para reduzir riscos e economizar dinheiro. Faça login na ferramenta AWS Well-Architected para revisar suas respostas e adotar medidas para resolver seus problemas ativos.

Colunas do relatório

- Status
- Região
- ARN da workload
- Nome da workload
- Nome do revisor
- Tipo de workload
- Data de início da workload
- Data da última modificação da workload
- Número de problemas de alto risco identificados para segurança
- Número de problemas de alto risco resolvidos para segurança

- Número de perguntas para segurança
- Número total de perguntas no pilar de segurança
- Hora da última atualização

CloudFrontCertificados SSL personalizados no IAM Certificate Store

Descrição

Verifica os certificados SSL em busca de nomes de domínio CloudFront alternativos no armazenamento de certificados do IAM. Essa verificação alerta se um certificado expirou, expirará em breve, usa criptografia desatualizada ou não está configurado corretamente para a distribuição.

Quando um certificado personalizado para um nome de domínio alternativo expira, os navegadores que exibem seu CloudFront conteúdo podem mostrar uma mensagem de aviso sobre a segurança do seu site. Certificados criptografados usando o algoritmo de hash SHA-1 estão sendo preteridos por navegadores da Web, como Chrome e Firefox.

Os certificados devem conter um nome de domínio que corresponda ao Nome de Domínio de Origem ou ao nome de domínio no cabeçalho de host de uma solicitação de visualizador. Se não corresponder, CloudFront retornará um código de status HTTP 502 (gateway inválido) para o usuário. Para obter mais informações, consulte Usar nomes de domínio alternativos e HTTPS.

ID da verificação

`N425c450f2`

Critérios de alerta

- Vermelho: um certificado SSL personalizado expirou.
- Amarelo: um certificado SSL personalizado irá expirar nos próximos sete dias.
- Amarelo: um certificado SSL personalizado foi criptografado usando o algoritmo de hash SHA-1.
- Amarelo: um ou mais nomes de domínio alternativos na distribuição não aparecem no campo Common Name (Nome comum) ou Subject Alternative Names (Nomes alternativos da entidade) do certificado SSL personalizado.

Recommended Action (Ação recomendada)

Renove um certificado expirado ou um certificado que está prestes a expirar.

Substitua um certificado que foi criptografado com o algoritmo de hash SHA-1 por um certificado criptografado com o algoritmo de hash SHA-256.

Substitua o certificado por um certificado que contenha os valores aplicáveis nos campos Common name (Nome comum) ou Subject Alternative Domain Names (Nomes de domínio alternativos da entidade).

Recursos adicionais

Using an HTTPS Connection to Access Your Objects (Usar uma conexão HTTPS para acessar seus objetos)

Colunas do relatório

- Status
- ID de distribuição
- Nome do domínio da distribuição
- Nome do certificado
- Motivo

CloudFront Certificado SSL no servidor de origem

Descrição

Verifica o servidor de origem em busca de certificados SSL expirados, prestes a expirar, ausentes ou que usem criptografia desatualizada. Se um certificado tiver um desses problemas, CloudFront responderá às solicitações de seu conteúdo com o código de status HTTP 502, Bad Gateway.

Certificados criptografados com o algoritmo de hash SHA-1 estão sendo recusados por navegadores da Web como Chrome e Firefox. Dependendo do número de certificados SSL que você associou às suas CloudFront distribuições, essa verificação pode adicionar alguns centavos por mês à sua fatura com seu provedor de hospedagem na web, por exemplo, AWS se você estiver usando o Amazon EC2 ou o Elastic Load Balancing como origem para sua distribuição. CloudFront Essa verificação não valida sua cadeia de certificados de origem ou autoridades de certificação. Você pode verificá-los em sua CloudFront configuração.

ID da verificação

`N430c450f2`

Critérios de alerta

- Vermelho: um certificado SSL na sua origem expirou ou está faltando.

- Amarelo: um certificado SSL na sua origem irá expirar nos próximos trinta dias.
- Amarelo: um certificado SSL na sua origem foi criptografado com o algoritmo de hash SHA-1.
- Amarelo: não é possível localizar um certificado SSL na sua origem. A conexão pode ter falhado devido a um tempo limite expirado ou a outros problemas de conexão HTTPS.

Recommended Action (Ação recomendada)

Renove o certificado na origem se ele tiver expirado ou estiver prestes a expirar.

Adicione um certificado se não houver um.

Substitua um certificado que foi criptografado com o algoritmo de hash SHA-1 por um certificado criptografado com o algoritmo de hash SHA-256.

Recursos adicionais

Using Alternate Domain Names and HTTPS (Usar nomes de domínio alternativos e HTTPS)

Colunas do relatório

- Status
- ID de distribuição
- Nome do domínio da distribuição
- Origem
- Motivo

Segurança do ELB Listener

Descrição

Verifica se há balanceadores de carga com ouvintes que não usam as configurações de segurança recomendadas para comunicação criptografada. AWS recomenda o uso de um protocolo seguro (HTTPS ou SSL), políticas de up-to-date segurança, bem como cifras e protocolos seguros.

Quando você usa um protocolo seguro para uma conexão de front-end (cliente para balanceador de carga), as solicitações são criptografadas entre seus clientes e o balanceador de carga, o que cria um ambiente mais seguro. O Elastic Load Balancing fornece políticas de segurança predefinidas com cifras e protocolos que seguem as melhores práticas de segurança. AWS

Novas versões de políticas predefinidas são lançadas à medida que novas configurações se tornam disponíveis.

ID da verificação

`a2sEc6ILx`

Critérios de alerta

- Amarelo: um balanceador de carga não tem um ouvinte que usa um protocolo seguro (HTTPS ou SSL).
- Amarelo: um ouvinte do balanceador de carga usa uma política de segurança SSL predefinida desatualizada.
- Amarelo: um ouvinte do balanceador de carga usa uma cifra ou um protocolo que não é recomendado.
- Vermelho: um ouvinte do balanceador de carga usa uma cifra ou um protocolo inseguro.

Recommended Action (Ação recomendada)

Se o tráfego para o balanceador de carga precisar ser seguro, use o protocolo HTTPS ou SSL para a conexão front-end.

Atualize seu balanceador de carga para a versão mais recente da política de segurança SSL predefinida.

Use somente as cifras e os protocolos recomendados.

Para obter mais informações, consulte Listener Configurations for Elastic Load Balancing. (Configurações do ouvinte para Elastic Load Balancing).

Recursos adicionais

- Listener Configurations Quick Reference (Referência rápida de configurações do ouvinte)
- Update SSL Negotiation Configuration of Your Load Balancer (Atualizar a configuração de negociação SSL do seu balanceador de carga)
- SSL Negotiation Configurations for Elastic Load Balancing (Configurações de negociação SSL para Elastic Load Balancing)
- SSL Security Policy Table (Tabela de políticas de segurança de SSL)

Colunas do relatório

- Status

- Região
- Nome do balanceador de carga
- Porta do balanceador de carga
- Motivo

Grupos de segurança do ELB

Descrição

Verifica se há balanceadores de carga configurados com um grupo de segurança ausente ou um grupo de segurança que permite o acesso a portas que não estão configuradas para o balanceador de carga.

Se um grupo de segurança associado a um balanceador de carga for excluído, o balanceador de carga não funcionará conforme esperado. Se um grupo de segurança permitir o acesso a portas que não estão configuradas para o balanceador de carga, aumentará o risco de perda de dados ou ataques mal-intencionados.

ID da verificação

`xSqX82fQu`

Critérios de alerta

- Amarelo: as regras de entrada de um grupo de segurança da Amazon VPC associado a um balanceador de carga permitem acesso a portas que não estão definidas na configuração de ouvinte do balanceador de carga.
- Vermelho: não existe um grupo de segurança associado a um balanceador de carga.

Recommended Action (Ação recomendada)

Configure as regras do grupo de segurança para restringir o acesso somente às portas e aos protocolos definidos na configuração do ouvinte do balanceador de carga, além do protocolo ICMP para oferecer suporte à descoberta de MTU de caminho. Consulte Listeners for Your Classic Load Balancer (Ouvintes para seu Classic Load Balancer) e Security Groups for Load Balancers in a VPC (Grupos de segurança para balanceadores de carga em uma VPC).

Se um grupo de segurança estiver faltando, aplique um novo grupo de segurança ao balanceador de carga. Crie regras de grupo de segurança que restrinjam o acesso somente às portas e aos protocolos definidos na configuração do ouvinte do balanceador de carga. Consulte Security

Groups for Load Balancers in a VPC (Grupos de segurança para balanceadores de carga em uma VPC).

Recursos adicionais

- Guia do usuário do Elastic Load Balancing
- Configure Your Classic Load Balancer (Configurar o Classic Load Balancer)

Colunas do relatório

- Status
- Região
- Nome do balanceador de carga
- IDs de grupos de segurança
- Motivo

Exposed Access Keys

Descrição

Verifica os repositórios de código populares em busca de chaves de acesso expostas ao público e o uso irregular do Amazon Elastic Compute Cloud (Amazon EC2) que pode ser o resultado de uma chave de acesso comprometida.

Uma chave de acesso consiste em um ID da chave de acesso e uma chave de acesso secreta. As chaves de acesso expostas representam um risco de segurança para sua conta e para outros usuários, podem levar a cobranças excessivas de atividades ou abuso não autorizados e violar os Contrato do cliente da AWS.

Se a chave de acesso estiver exposta, tome medidas imediatas para proteger a sua conta. Para proteger sua conta de cobranças excessivas, limita AWS temporariamente sua capacidade de criar alguns AWS recursos. Isso não torna sua conta segura. Ela limita apenas parcialmente o uso não autorizado pelo qual é possível ser cobrado.

> **Note**
>
> Essa verificação não garante a identificação de chaves de acesso expostas nem de instâncias do EC2 comprometidas. Em última análise, você é responsável pela segurança e proteção de suas chaves de acesso e AWS recursos.

Os resultados dessa verificação são atualizados automaticamente, e não são permitidas solicitações de atualização. Não é possível excluir recursos dessa verificação.

Se for exibido um prazo para uma chave de acesso, AWS poderá suspendê-la Conta da AWS se o uso não autorizado não for interrompido até essa data. Se você acredita que esse alerta é um erro, entre em contato com o AWS Support.

As informações exibidas em Trusted Advisor podem não refletir o estado mais recente da sua conta. Nenhuma chave de acesso exposta será marcada como resolvida até que todas as chaves de acesso expostas na conta tenham sido resolvidas. Esta sincronização de dados poderá demorar até uma semana.

ID da verificação

`12Fnkpl8Y5`

Critérios de alerta

- Vermelho: Potencialmente comprometido — AWS identificou um ID de chave de acesso e uma chave de acesso secreta correspondente que foram expostos na Internet e podem ter sido comprometidos (usados).
- Vermelho: Exposto — AWS identificou um ID de chave de acesso e uma chave de acesso secreta correspondente que foram expostos na Internet.
- Vermelho: suspeito: o uso irregular do Amazon EC2 indica que uma chave de acesso pode ter sido comprometida, mas não foi identificada como exposta na Internet.

Recommended Action (Ação recomendada)

Exclua a chave de acesso afetada o mais rápido possível. Se a chave estiver associada a um usuário do IAM, consulte Managing Access Keys for IAM Users(Gerenciar chaves de acesso para usuários do IAM).

Verifique se há uso não autorizado em sua conta. Faça login no AWS Management Console e verifique se há recursos suspeitos em cada console de serviço. Preste atenção especial à execução de instâncias do Amazon EC2, solicitações de instância spot, chaves de acesso e usuários do IAM. Você também pode verificar o uso geral no Billing and Cost Management console (Console do Billing and Cost Management).

Recursos adicionais

- Melhores práticas para gerenciar chaves de AWS acesso

- AWS Diretrizes de auditoria de segurança

Colunas do relatório

- Access Key ID
- Nome do usuário (IAM ou Root)
- Tipo de fraude
- ID do caso
- Hora da atualização
- Local
- Prazo
- Uso (USD por dia)

Alternância da chave de acesso do IAM

Descrição

Verifica se há chaves de acesso ativas do IAM que não foram alternadas nos últimos 90 dias.

Ao alternar as chaves de acesso regularmente, você reduz a chance de que uma chave comprometida possa ser usada sem seu conhecimento para acessar recursos. Para efeitos desta verificação, a data e hora da última alternância é quando a chave de acesso foi criada ou habilitada mais recentemente. O número da chave de acesso e a data vêm das informações do `access_key_1_last_rotated` e `access_key_2_last_rotated` no relatório de credenciais do IAM mais recente.

Como a frequência de regeneração de um relatório de credenciais é restrita, atualizar essa verificação pode não refletir alterações recentes. Para obter mais informações, consulte Obter relatórios de credenciais da sua conta da Conta da AWS.

Para criar e girar chaves de acesso, um usuário deve ter as permissões apropriadas. Para obter mais informações, consulte Allow Users to Manage Their Own Passwords, Access Keys, and SSH Keys (Permitir que os usuários gerenciem suas próprias senhas, chaves de acesso e chaves SSH).

ID da verificação

`DqdJqYeRm5`

Critérios de alerta

- Verde: a chave de acesso está ativa e foi girada nos últimos 90 dias.
- Amarelo: a chave de acesso está ativa e foi girada nos últimos 2 anos, mas há mais de 90 dias.
- Vermelho: a chave de acesso está ativa, mas não foi girada nos últimos 2 anos.

Recommended Action (Ação recomendada)

Gire as chaves de acesso regularmente. Consulte Rotating Access Keys (Girar chaves de acesso) e Managing Access Keys for IAM Users (Girar chaves de acesso para usuários do IAM).

Recursos adicionais

- Práticas recomendadas do IAM
- How to rotate access keys for IAM users (Como girar chaves de acesso para usuários do IAM)

Colunas do relatório

- Status
- IAM user (Usuário do IAM)
- Chave de acesso
- Chave girada por último
- Motivo

Política de senhas do IAM

Descrição

Verifica a política de senhas da sua conta e avisa quando uma política de senhas não está habilitada ou se os requisitos de conteúdo de senha não foram habilitados.

Os requisitos de conteúdo de senha aumentam a segurança geral da AWS impondo a criação de senhas de usuário fortes. Quando você cria ou altera uma política de senhas, a alteração é aplicada imediatamente para novos usuários, mas não exige que os usuários existentes alterem as suas senhas.

ID da verificação

`Yw2K9puPzl`

Critérios de alerta

- Amarelo: uma política de senha está habilitada, mas pelo menos um requisito de conteúdo não está habilitado.

- Vermelho: nenhuma política de senha está habilitada.

Recommended Action (Ação recomendada)

Se alguns requisitos de conteúdo não estiverem habilitados, considere habilitá-los. Se nenhuma política de senha estiver habilitada, crie e configure uma. Consulte Setting an Account Password Policy for IAM Users (Definir uma política de senhas de contas para usuários do IAM).

Recursos adicionais

Gerenciamento de senhas

Colunas do relatório

- Política de senha
- Letras maiúsculas
- Letras minúsculas
- Número
- Não alfanuméricos

Uso do IAM

Descrição

Verifica para você o uso do IAM. Você pode usar o IAM para criar usuários, grupos e funções no AWS. Você também pode usar permissões para controlar o acesso aos recursos da AWS . Essa verificação destina-se a desencorajar o uso do acesso raiz verificando a existência de pelo menos um usuário do IAM. Você pode ignorar o alerta se estiver seguindo a prática recomendada de centralizar identidades e configurar usuários em um provedor de identidade externo ou no AWS IAM Identity Center.

ID da verificação

`zXCkfM1nI3`

Critérios de alerta

Amarelo: nenhum usuário do IAM foi criado para esta conta.

Recommended Action (Ação recomendada)

Crie um usuário do IAM ou use AWS IAM Identity Center para criar usuários adicionais cujas permissões são limitadas para realizar tarefas específicas em seu AWS ambiente.

Recursos adicionais

- O que é AWS IAM Identity Center?
- What Is IAM? (O que é o IAM?)

MFA na conta raiz

Descrição

Verifica a conta raiz e avisa se a autenticação multifator (MFA) não estiver habilitada.

Para aumentar a segurança, recomendamos que você proteja sua conta usando o MFA, que exige que o usuário insira um código de autenticação exclusivo de seu hardware de MFA ou dispositivo virtual ao interagir com os sites associados. AWS Management Console

ID da verificação

`7DAFEmoDos`

Critérios de alerta

Vermelho: a MFA não está habilitada na conta root.

Recommended Action (Ação recomendada)

Faça login na sua conta root e ative um dispositivo MFA. Consulte Checking MFA Status (Verificar status de MFA) e Setting Up an MFA Device (Configurar um dispositivo MFA).

Recursos adicionais

Usando dispositivos Multi-Factor Authentication (MFA) com AWS

Grupos de segurança - Portas específicas irrestritas

Descrição

Verifica grupos de segurança para regras que permitam acesso irrestrito (0.0.0.0/0) a portas específicas.

O acesso irrestrito aumenta as oportunidades de atividades maliciosas (invasões, denial-of-service ataques, perda de dados). As portas com maior risco são sinalizadas em vermelho, e aquelas com menos risco são sinalizadas em amarelo. As portas sinalizadas em verde são normalmente usadas por aplicações que exigem acesso irrestrito, como HTTP e SMTP.

Se você configurou intencionalmente seus grupos de segurança dessa maneira, recomendamos o uso de medidas de segurança adicionais para proteger a infraestrutura (como tabelas IP).

> **Note**
>
> Essa verificação avalia apenas os grupos de segurança criados por você e as respetivas regras de entrada para endereços IPv4. Os grupos de segurança criados pelo AWS Directory Service são sinalizados em vermelho ou amarelo, mas eles não representam um risco de segurança e podem ser ignorados com segurança ou excluídos. Para obter mais informações, consulte as Perguntas frequentes sobre o Trusted Advisor.

> **Note**
>
> Essa verificação não inclui o caso de uso quando uma lista de prefixos gerenciada pelo cliente concede acesso a 0.0.0.0/0 e é usada como fonte com um grupo de segurança.

ID da verificação

`HCP4007jGY`

Critérios de alerta

- Verde: o acesso às portas 80, 25, 443 ou 465 é irrestrito.
- Vermelho: o acesso às portas 20, 21, 1433, 1434, 3306, 3389, 4333, 5432 ou 5500 é irrestrito.
- Amarelo: o acesso a qualquer outra porta é irrestrito.

Recommended Action (Ação recomendada)

Restrinja o acesso somente aos endereços IP necessários. Para restringir o acesso a um endereço IP específico, defina o sufixo como /32 (por exemplo, 192.0.2.10/32). Certifique-se de excluir regras excessivamente permissivas após criar regras mais restritivas.

Recursos adicionais

- Amazon EC2 Security Groups (Grupos de segurança do Amazon EC2)

  List of TCP and UDP port numbers (Lista de números de portas TCP e UDP)
- Classless Inter-Domain Routing (Roteamento sem classe entre domínios)

Colunas do relatório

- Status
- Região
- Nome do grupo de segurança
- ID do grupo de segurança
- Protocolo
- Porta de origem
- Porta de destino

Grupos de Segurança - Acesso Irrestrito

Descrição

Verifica os grupos de segurança em busca de regras que permitem acesso irrestrito a um recurso.

O acesso irrestrito aumenta as oportunidades de atividades maliciosas (invasões, denial-of-service ataques, perda de dados).

> **Note**
>
> Essa verificação avalia apenas os grupos de segurança criados por você e as respetivas regras de entrada para endereços IPv4. Os grupos de segurança criados pelo AWS Directory Service são sinalizados em vermelho ou amarelo, mas eles não representam um risco de segurança e podem ser ignorados com segurança ou excluídos. Para obter mais informações, consulte as Perguntas frequentes sobre o Trusted Advisor.

> **Note**
>
> Essa verificação não inclui o caso de uso quando uma lista de prefixos gerenciada pelo cliente concede acesso a 0.0.0.0/0 e é usada como fonte com um grupo de segurança.

ID da verificação

`1iG5NDGVre`

Critérios de alerta

Vermelho: uma regra de grupo de segurança tem um endereço IP de origem com um sufixo /0 para portas diferentes de 25, 80 ou 443.

Recommended Action (Ação recomendada)

Restrinja o acesso somente aos endereços IP necessários. Para restringir o acesso a um endereço IP específico, defina o sufixo como /32 (por exemplo, 192.0.2.10/32). Certifique-se de excluir regras excessivamente permissivas após criar regras mais restritivas.

Recursos adicionais

- Amazon EC2 Security Groups (Grupos de segurança do Amazon EC2)
- Classless Inter-Domain Routing (Roteamento sem classe entre domínios)

Colunas do relatório

- Status
- Região
- Nome do grupo de segurança
- ID do grupo de segurança
- Protocolo
- Porta de origem
- Porta de destino
- Intervalo de IP

Tolerância a falhas

É possível usar as verificações a seguir para a categoria de tolerância a falhas.

Nomes da verificação

- ALB Multi-AZ
- O retrocesso do cluster MySQL do Amazon Aurora não está habilitado
- Acessibilidade da instância de banco de dados do Amazon Aurora
- Failover CloudFront do Amazon Origin
- Risco de acesso ao endpoint do Amazon Comprehend

- Clusters AZ únicos do Amazon DocumentDB
- Recuperação do Amazon oint-in-time DynamoDB P
- Tabela do Amazon DynamoDB não incluída no plano de backup
- Amazon EBS não incluído no plano AWS Backup
- Snapshots do Amazon EBS
- O Amazon EC2 Auto Scaling não tem a verificação de integridade do ELB habilitada.
- O grupo do Amazon EC2 Auto Scaling tem o rebalanceamento de capacidade habilitado
- O Amazon EC2 Auto Scaling não está implantado em várias AZs ou não atende ao número mínimo de AZs
- Saldo da zona de disponibilidade do Amazon EC2
- Monitoramento detalhado do Amazon EC2 não habilitado
- Driver do Amazon ECS AWS Logs em modo de bloqueio
- Serviço do Amazon ECS usando uma única AZ
- Estratégia de posicionamento multi-AZ do Amazon ECS
- Redundância de destino sem montagem do Amazon EFS
- Amazon EFS não está no AWS Backup plano
- Clusters Amazon ElastiCache Multi-AZ
- Backup automático de clusters do Amazon ElastiCache Redis
- Clusters multi-AZ do Amazon MemoryDB
- Agentes do Amazon MSK que hospedam muitas partições
- Domínios do Amazon OpenSearch Service com menos de três nós de dados
- Amazon RDS Backups
- Os clusters de banco de dados do Amazon RDS têm uma instância de banco de dados.
- Clusters de banco de dados Amazon RDS com todas as instâncias na mesma zona de disponibilidade
- Clusters de banco de dados Amazon RDS com todas as instâncias de leitura na mesma zona de disponibilidade
- Monitoramento aprimorado de instâncias de banco de dados do Amazon RDS não habilitado
- As instâncias de banco de dados do Amazon RDS têm o escalonamento automático de armazenamento desativado

- Instâncias de banco de dados do Amazon RDS que não usam a implantação Multi-AZ
- Amazon RDS DiskQueueDepth
- Amazon RDS FreeStorageSpace
- O parâmetro log_output do Amazon RDS está definido como tabela
- A configuração do parâmetro innodb_default_row_format do Amazon RDS não é segura
- O parâmetro innodb_flush_log_at_trx_commit do Amazon RDS não é 1
- O parâmetro max_user_connections do Amazon RDS está baixo
- Amazon RDS Multi-AZ
- Amazon RDS não está no plano AWS Backup
- As réplicas de leitura do Amazon RDS estão abertas no modo gravável
- Os backups automatizados de recursos do Amazon RDS estão desativados
- O parâmetro sync_binlog do Amazon RDS está desativado
- O cluster de banco de dados do RDS não tem a replicação multi-AZ habilitada
- Instância multi-AZ em espera do RDS não habilitada
- Amazon RDS ReplicaLag
- O parâmetro synchronous_commit do Amazon RDS está desativado
- Snapshots automatizados do cluster do Amazon Redshift
- Verificações de integridade excluídas pelo Amazon Route 53
- Conjuntos de registros de recursos de failover no Amazon Route 53.
- Conjuntos de registros de recursos de TTL alta no Amazon Route 53.
- Delegações do servidor de nomes do Amazon Route 53
- Amazon Route 53 Resolver Redundância da zona de disponibilidade do endpoint
- Registro em bucket do Amazon S3
- Replicação de bucket do Amazon S3 não habilitada
- Versionamento em bucket do Amazon S3
- Balanceadores de carga de aplicações, redes e gateways não abrangem várias zonas de disponibilidade
- IPs disponíveis para ajuste de escala automático em sub-redes
- Verificação de integridade do grupo de Auto Scaling

- Recursos do grupo do Auto Scaling
- Clusters do AWS CloudHSM que executam instâncias do HSM em uma única AZ
- AWS Direct Connect Redundância de conexão
- AWS Direct Connect Redundância de localização
- AWS Direct Connect Resiliência de localização
- AWS Direct Connect Redundância de interface virtual
- AWS Lambda funções sem uma fila de mensagens mortas configurada
- AWS Lambda Sobre destinos de eventos de falha
- O AWS Lambda habilitado para VPC funciona sem redundância Multi-AZ
- AWS Resilience Hub Verificação de componentes do aplicativo
- AWS Resilience Hub política violada
- AWS Resilience Hub pontuações de resiliência
- AWS Resilience Hub idade de avaliação
- AWS Site-to-Site VPN tem pelo menos um túnel no status DOWN
- Problemas de alto risco do AWS Well-Architected em relação à confiabilidade
- O Classic Load Balancer não tem várias AZs configuradas
- Descarga de conexão do ELB
- Balanceamento de carga entre zonas do ELB
- Otimização do Load Balancer
- Independência da AZ do NAT Gateway
- Balanceamento de carga cruzada dos Network Load Balancers
- NLB - Recurso voltado para a Internet em sub-rede privada
- NLB Multi-AZ
- Número de Regiões da AWS em um conjunto de replicação do Incident Manager
- Verificação de aplicação de AZ única
- Interface VPC, endpoint, interfaces de rede em várias AZs
- Redundância de túnel da VPN
- Redundância de zona de disponibilidade do ActiveMQ

- Redundância de zona de disponibilidade do RabbitMQ

ALB Multi-AZ

Descrição

Verifica se seus Application Load Balancers estão configurados para usar mais de uma zona de disponibilidade (AZ). Uma AZ é um local distinto, isolado de falhas em outras zonas. Configure seu balanceador de carga em várias AZs na mesma região para ajudar a melhorar a disponibilidade da carga de trabalho.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c1dfprch08`

Critérios de alerta

Amarelo: ALB está em um único AZ.

Verde: o ALB tem duas ou mais AZs.

Recommended Action (Ação recomendada)

Certifique-se de que seu balanceador de carga esteja configurado com pelo menos duas zonas de disponibilidade.

Para obter mais informações, consulte Zonas de disponibilidade do seu Application Load Balancer.

Recursos adicionais

Para obter mais informações, consulte a seguinte documentação do :

- Como o Elastic Load Balancing funciona
- Regiões, zonas de disponibilidade e zonas locais

Colunas do relatório

- Status
- Região
- Nome do ALB
- Regra ALB
- ARN DO LABORATÓRIO
- Número de AZs
- Hora da última atualização

O retrocesso do cluster MySQL do Amazon Aurora não está habilitado

Descrição

Verifica se um cluster MySQL do Amazon Aurora tem o retrocesso habilitado.

O retrocesso do cluster MySQL do Amazon Aurora é um recurso que permite restaurar um cluster do banco de dados Aurora para um momento anterior sem criar um novo cluster. Ele permite reverter o banco de dados para um ponto específico no tempo dentro de um período de retenção, sem a necessidade de restaurar de um snapshot.

Você pode ajustar a janela de tempo de retrocesso (horas) no BacktrackWindowInHoursparâmetro das AWS Config regras.

Para ter mais informações, consulte Retrocesso de um cluster de bancos de dados Aurora.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

```
c18d2gz131
```

Origem

```
AWS Config Managed Rule: aurora-mysql-backtracking-enabled
```

Critérios de alerta

Amarelo: o retrocesso de clusters MySQL do Amazon Aurora não está habilitado.

Recommended Action (Ação recomendada)

Ative o retrocesso em seu cluster MySQL do Amazon Aurora.

Para ter mais informações, consulte Retrocesso de um cluster de bancos de dados Aurora.

Recursos adicionais

Retrocesso de um cluster do banco de dados Aurora

Colunas do relatório

- Status
- Região
- Recurso
- AWS Config Regra
- Parâmetros de entrada
- Hora da última atualização

Acessibilidade da instância de banco de dados do Amazon Aurora

Descrição

Verifica os casos em que um cluster de banco de dados do Amazon Aurora tem instâncias públicas e privadas.

Quando a instância de banco de dados primária falhar, uma réplica pode ser promovida para ser a instância primária. Se essa réplica for privada, os usuários com acesso apenas público não poderão mais se conectar ao banco de dados após o failover. Recomendamos que todas as instâncias de banco de dados em um cluster tenham a mesma acessibilidade.

ID da verificação

`xuy7H1avtl`

Critérios de alerta

Amarelo: as instâncias em um cluster de banco de dados do Aurora têm acessibilidade diferente (uma mistura de pública e privada).

Recommended Action (Ação recomendada)

Modifique a configuração `Publicly Accessible` das instâncias no cluster de banco de dados para que todas sejam públicas ou privadas. Para obter mais detalhes, consulte as instruções para instâncias do MySQL em Modifying a DB Instance Running the MySQL Database Engine (Modificar uma instância de banco de dados com o mecanismo de banco de dados MySQL).

Recursos adicionais

Tolerância a falhas para um cluster de banco de dados do Aurora

Colunas do relatório

- Status
- Região
- Cluster
- Instâncias de banco de dados públicas
- Instâncias de banco de dados privadas
- Motivo

Failover CloudFront do Amazon Origin

Descrição

Verifica se um grupo de origem está configurado para distribuições que incluem duas origens na Amazon CloudFront.

Para obter mais informações, consulte Otimizando a alta disponibilidade com failover de CloudFront origem.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c18d2gz112`

Origem

```
AWS Config Managed Rule: cloudfront-origin-failover-enabled
```

Critérios de alerta

Amarelo: o failover de CloudFront origem da Amazon não está ativado.

Recommended Action (Ação recomendada)

Certifique-se de ativar o recurso de failover de origem para suas CloudFront distribuições para ajudar a garantir a alta disponibilidade da entrega de seu conteúdo aos usuários finais. Quando você ativa esse recurso, o tráfego será roteado automaticamente para o servidor de origem de backup se o servidor de origem primário não estiver disponível. Isso minimiza o possível tempo de inatividade e garante a disponibilidade contínua do seu conteúdo.

Colunas do relatório

- Status
- Região
- Recurso
- AWS Config Regra
- Parâmetros de entrada
- Hora da última atualização

Risco de acesso ao endpoint do Amazon Comprehend

Descrição

Verifica as permissões da chave AWS Key Management Service (AWS KMS) para um endpoint em que o modelo subjacente foi criptografado usando chaves gerenciadas pelo cliente. Se a chave gerenciada pelo cliente estiver desabilitada, ou se a política de chaves foi alterada para alterar as permissões permitidas para o Amazon Comprehend, a disponibilidade do endpoint pode ser afetada.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`Cm24dfsM13`

Critérios de alerta

Vermelho: a chave gerenciada pelo cliente está desabilitada ou a política de chaves foi modificada para alterar as permissões para acesso do Amazon Comprehend.

Recommended Action (Ação recomendada)

Se a chave gerenciada pelo cliente estiver desabilitada, recomendamos habilitá-la. Para obter mais informações, consulte Enabling keys (Habilitar chaves). Se a política de chaves foi alterada e você quiser continuar usando o endpoint, recomendamos que você atualize a política de AWS KMS chaves. Para obter mais informações, consulte Alterar uma política de chaves.

Recursos adicionais

AWS KMS Permissões

Colunas do relatório

- Status
- Região
- ARN do endpoint
- ARN do modelo
- KMS KeyId
- Hora da última atualização

Clusters AZ únicos do Amazon DocumentDB

Descrição

Verifica se há clusters do Amazon DocumentDB configurados como Single-AZ.

Executar cargas de trabalho do Amazon DocumentDB em uma arquitetura Single-AZ não é suficiente para cargas de trabalho altamente críticas e a recuperação de uma falha de componente pode levar até 10 minutos. Os clientes devem implantar instâncias de réplica em zonas de disponibilidade adicionais para garantir a disponibilidade durante a manutenção, falhas de instâncias, falhas de componentes ou falhas na zona de disponibilidade.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente uma ou mais vezes por dia, e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c15vnddn2x`

Critérios de alerta

Amarelo: o cluster Amazon DocumentDB tem instâncias em menos de três zonas de disponibilidade.

Verde: o cluster Amazon DocumentDB tem instâncias em três zonas de disponibilidade.

Recommended Action (Ação recomendada)

Se seu aplicativo exigir alta disponibilidade, modifique sua instância de banco de dados para habilitar o Multi-AZ usando instâncias de réplica. Veja a alta disponibilidade e replicação do Amazon DocumentDB

Recursos adicionais

Entendendo a tolerância a falhas do cluster Amazon DocumentDB

Regiões e zonas de disponibilidade

Colunas do relatório

- Status
- Região
- Availability Zone (zona de disponibilidade)
- DB Cluster Identifier
- ARN do cluster de banco de dados
- Hora da última atualização

Recuperação do Amazon oint-in-time DynamoDB P

Descrição

Verifica se a recuperação para um ponto no tempo está habilitada para as tabelas do Amazon DynamoDB.

A recuperação para um ponto no tempo ajuda a proteger as tabelas do DynamoDB contra operações acidentais de gravação ou exclusão. Com a recuperação para um ponto no tempo, você não precisa se preocupar com a criação, a manutenção ou a programação de backups sob demanda. A recuperação para um ponto no tempo restaura as tabelas para qualquer ponto no tempo durante os últimos 35 dias. O DynamoDB mantém backups incrementais da tabela.

Para obter mais informações, consulte P oint-in-time recovery for DynamoDB.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c18d2gz138`

Origem

`AWS Config Managed Rule: dynamodb-pitr-enabled`

Critérios de alerta

Amarelo: a oint-in-time recuperação P não está habilitada para suas tabelas do DynamoDB.

Recommended Action (Ação recomendada)

Ative a point-in-time recuperação no Amazon DynamoDB para fazer backup contínuo dos dados da tabela.

Para obter mais informações, consulte oint-in-time Recuperação P: Como funciona.

Recursos adicionais

oint-in-time Recuperação P para DynamoDB

Colunas do relatório

- Status
- Região
- Recurso
- AWS Config Regra
- Parâmetros de entrada
- Hora da última atualização

Tabela do Amazon DynamoDB não incluída no plano de backup

Descrição

Verifica se as tabelas do Amazon DynamoDB fazem parte de um plano. AWS Backup

AWS Backup fornece backups incrementais para tabelas do DynamoDB que capturam as alterações feitas desde o último backup. Incluir tabelas do DynamoDB em AWS Backup um plano ajuda a proteger seus dados contra cenários de perda acidental de dados e automatiza o processo de backup. Isso fornece uma solução de backup confiável e escalável para suas tabelas do DynamoDB, ajudando a garantir que seus dados valiosos estejam protegidos e disponíveis para recuperação, conforme necessário.

Para obter mais informações, consulte Criação de backups de tabelas do DynamoDB com AWS Backup

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

```
c18d2gz107
```

Origem

```
AWS Config Managed Rule: dynamodb-in-backup-plan
```

Critérios de alerta

Amarelo: a tabela do Amazon DynamoDB não está incluída no plano. AWS Backup

Recommended Action (Ação recomendada)

Certifique-se de que suas tabelas do Amazon DynamoDB façam parte de um plano. AWS Backup

Recursos adicionais

Backups agendados

O que é AWS Backup?

Criar planos de backup usando o console do AWS Backup

Colunas do relatório

- Status
- Região
- Recurso
- AWS Config Regra
- Parâmetros de entrada
- Hora da última atualização

Amazon EBS não incluído no plano AWS Backup

Descrição

Verifica se os volumes do Amazon EBS estão presentes nos planos de backup do. AWS Backup

Inclua volumes do Amazon EBS em um AWS Backup plano para automatizar backups regulares dos dados armazenados nesses volumes. Isso protege você contra perda de dados, facilita o gerenciamento de dados e permite a restauração de dados quando necessário. Um plano de backup ajuda a garantir que seus dados estejam seguros e que você seja capaz de atingir os objetivos de tempo e ponto de recuperação (RTO/RPO) para suas aplicações e serviços.

Para obter mais informações, consulte Creating a backup plan

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c18d2gz106`

Origem

`AWS Config Managed Rule: ebs-in-backup-plan`

Critérios de alerta

Amarelo: o volume do Amazon EBS não está incluído no AWS Backup plano.

Recommended Action (Ação recomendada)

Certifique-se de que seus volumes do Amazon EBS façam parte de um AWS Backup plano.

Recursos adicionais

Criação de planos de backup usando o AWS Backup console

O que é AWS Backup?

Conceitos básicos 3: criar um backup agendado

Colunas do relatório

- Status
- Região
- Recurso
- AWS Config Regra
- Parâmetros de entrada
- Hora da última atualização

Snapshots do Amazon EBS

Descrição

Verifica a idade dos snapshots para seus volumes do Amazon Elastic Block Store (Amazon EBS) (disponível ou em uso).

Mesmo que os volumes do Amazon EBS sejam replicados, poderão ocorrer falhas. Os snapshots são mantidos no Amazon Simple Storage Service (Amazon S3) para armazenamento e recuperação duráveis. point-in-time

ID da verificação

`H7IgTzjTYb`

Critérios de alerta

- Amarelo: o snapshot de volume mais recente tem entre 7 e 30 dias.
- Vermelho: o snapshot de volume mais recente tem mais de 30 dias.
- Vermelho: o volume não tem um snapshot.

Recommended Action (Ação recomendada)

Crie snapshots semanais ou mensais de seus volumes. Para obter mais informações, consulte Creating an Amazon EBS Snapshot (Criar um snapshot do Amazon EBS).

Recursos adicionais

Amazon Elastic Block Store (Amazon EBS)

Colunas do relatório

- Status
- Região
- ID de volume
- Nome do volume
- ID do snapshot
- Nome do snapshot
- Idade do snapshot
- Anexo de volume
- Motivo

O Amazon EC2 Auto Scaling não tem a verificação de integridade do ELB habilitada.

Descrição

Verifica se os grupos do Amazon EC2 Auto Scaling que estão associados a um Classic Load Balancer estão usando as verificações de integridade do Elastic Load Balancing. As verificações de integridade padrão para um grupo do Auto Scaling são somente verificações de status do Amazon EC2. Se uma instância falhar nessas verificações de status, ela será marcada como não íntegra e será encerrada. O Amazon EC2 Auto Scaling inicia uma nova instância de substituição. A verificação de integridade do Elastic Load Balancing monitora periodicamente as instâncias do Amazon EC2 para detectar e encerrar instâncias não íntegras e, em seguida, iniciar novas instâncias.

Para obter mais informações, consulte Adicionar verificações de saúde do Elastic Load Balancing.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c18d2gz104`

Origem

`AWS Config Managed Rule: autoscaling-group-elb-healthcheck-required`

Critérios de alerta

Amarelo: o grupo do Amazon EC2 Auto Scaling anexado ao Classic Load Balancer não habilitou as verificações de integridade do Elastic Load Balancing.

Recommended Action (Ação recomendada)

Certifique-se de que seus grupos de Auto Scaling associados a um Classic Load Balancer usem as verificações de integridade do Elastic Load Balancing.

As verificações de integridade do Elastic Load Balancing informam se o balanceador de carga está íntegro e disponível para lidar com solicitações. Isso garante alta disponibilidade para sua aplicação.

Para obter mais informações, consulte Add Elastic Load Balancing health checks to an Auto Scaling group

Colunas do relatório

- Status
- Região
- Recurso
- AWS Config Regra
- Parâmetros de entrada
- Hora da última atualização

O grupo do Amazon EC2 Auto Scaling tem o rebalanceamento de capacidade habilitado

Descrição

Verifica se o Rebalanceamento de capacidade está habilitado para grupos do Amazon EC2 Auto Scaling que usam vários tipos de instância.

Configurar grupos do Amazon EC2 Auto Scaling com rebalanceamento de capacidade ajuda a garantir que as instâncias do Amazon EC2 sejam distribuídas uniformemente entre as zonas de disponibilidade, independentemente dos tipos de instância e das opções de compra. Ele usa uma política de rastreamento de destino associada ao grupo, como a utilização da CPU ou o tráfego de rede.

Para obter mais informações, consulte Auto Scaling groups with multiple instance types and purchase options.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

```
AWS Config c18d2gz103
```

Origem

AWS Config Regra gerenciada: autoscaling-capacity-rebalancing

Critérios de alerta

Amarelo: o rebalanceamento da capacidade do grupo do Amazon EC2 Auto Scaling não está habilitado.

Recommended Action (Ação recomendada)

Certifique-se de que o rebalanceamento de capacidade esteja habilitado para os grupos do Amazon EC2 Auto Scaling que usam vários tipos de instância.

Para obter mais informações, consulte Enable Capacity Rebalancing (console)

Colunas do relatório

- Status
- Região
- Recurso
- AWS Config Regra
- Parâmetros de entrada
- Hora da última atualização

O Amazon EC2 Auto Scaling não está implantado em várias AZs ou não atende ao número mínimo de AZs

Descrição

Verifica se o grupo do Amazon EC2 Auto Scaling está implantado em várias zonas de disponibilidade ou no número mínimo de zonas de disponibilidade especificado. Implante instâncias do Amazon EC2 em várias zonas de disponibilidade para garantir a alta disponibilidade.

Você pode ajustar o número mínimo de zonas de disponibilidade usando o minAvailibilityZonesparâmetro em suas AWS Config regras.

Para obter mais informações, consulte Auto Scaling groups with multiple instance types and purchase options.

ID da verificação

`c18d2gz101`

Origem

`AWS Config Managed Rule: autoscaling-multiple-az`

Critérios de alerta

Vermelho: o grupo do Amazon EC2 Auto Scaling não tem várias AZs configuradas ou não atende ao número mínimo de AZs especificado.

Recommended Action (Ação recomendada)

Certifique-se de que seu grupo do Amazon EC2 Auto Scaling esteja configurado com várias AZs. Implante instâncias do Amazon EC2 em várias zonas de disponibilidade para garantir a alta disponibilidade.

Recursos adicionais

Criar um grupo do Auto Scaling usando um modelo de execução

Criar um grupo do Auto Scaling usando uma configuração de execução

Colunas do relatório

- Status
- Região
- Recurso
- AWS Config Regra
- Parâmetros de entrada
- Hora da última atualização

Saldo da zona de disponibilidade do Amazon EC2

Descrição

Verifica a distribuição das instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em zonas de disponibilidade de uma região.

As zonas de disponibilidade são locais distintos dentro de uma região e são isoladas das falhas que ocorrem em outras zonas de disponibilidade. Elas fornecem conectividade de rede de baixa latência e custo reduzido entre as zonas de disponibilidade na mesma região. Ao iniciar as

instâncias em várias zonas de disponibilidade, é possível proteger suas aplicações de falhas de um único ponto de falha.

ID da verificação

`wuy7G1zxql`

Critérios de alerta

- Amarelo: a região tem instâncias em várias zonas, mas a distribuição é desigual (a diferença entre a maior e a menor contagem de instâncias nas zonas de disponibilidade utilizadas é maior que 20%).
- Vermelho: a região tem instâncias somente em uma única zona de disponibilidade.

Recommended Action (Ação recomendada)

Equilibre suas instâncias do Amazon EC2 uniformemente entre várias zonas de disponibilidade. Você pode fazer isso executando instâncias manualmente ou usando o Auto Scaling para fazer isso automaticamente. Para obter mais informações, consulte Launch Your Instance (Iniciar sua instância) e Load Balance Your Auto Scaling Group (Balancear a carga do seu grupo do Auto Scaling.

Recursos adicionais

Guia do usuário do Amazon EC2 Auto Scaling

Colunas do relatório

- Status
- Região
- Instâncias da zona a
- Instâncias da zona b
- Instâncias da zona c
- Instâncias da zona e
- Instâncias da zona f
- Motivo

Monitoramento detalhado do Amazon EC2 não habilitado

Descrição

Verifica se o monitoramento detalhado está habilitado para suas instâncias do Amazon EC2.

O monitoramento detalhado do Amazon EC2 fornece métricas mais frequentes, publicadas em intervalos de um minuto, em vez dos intervalos de cinco minutos usados no monitoramento básico do Amazon EC2. Habilitar o monitoramento detalhado para o Amazon EC2 ajuda a gerenciar melhor seus recursos do Amazon EC2, permitindo que você encontre tendências e atue com mais rapidez.

Para obter mais informações, consulte Monitoramento básico e monitoramento detalhado.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`AWS Config c18d2gz144`

Origem

AWS Config Regra gerenciada: ec2- instance-detailed-monitoring-enabled

Critérios de alerta

Amarelo: o monitoramento detalhado não está habilitado para instâncias do Amazon EC2.

Recommended Action (Ação recomendada)

Ative o monitoramento detalhado de suas instâncias do Amazon EC2 para aumentar a frequência com que os dados métricos do Amazon EC2 são publicados na CloudWatch Amazon (de intervalos de 5 a 1 minuto).

Colunas do relatório

- Status
- Região
- Recurso
- AWS Config Regra
- Parâmetros de entrada
- Hora da última atualização

Driver do Amazon ECS AWS Logs em modo de bloqueio

Descrição

Verifica as definições de tarefas do Amazon ECS configuradas com o driver de registro de AWS registros no modo de bloqueio. Um driver configurado no modo de bloqueio arrisca a disponibilidade do sistema.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente uma ou mais vezes por dia, e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c1dvkm4z6b`

Critérios de alerta

Amarelo: O modo do parâmetro de configuração de registro do driver awslogs está definido como bloqueado ou ausente. Um parâmetro de modo ausente indica uma configuração de bloqueio padrão.

Verde: a definição de tarefa do Amazon ECS não está usando o driver awslogs ou o driver awslogs está configurado no modo sem bloqueio.

Recommended Action (Ação recomendada)

Para reduzir o risco de disponibilidade, considere alterar a definição da tarefa Configuração do driver de AWS registros de bloqueio para não bloqueio. Com o modo sem bloqueio, você precisará definir um valor para o max-buffer-size parâmetro. Para obter mais informações e orientações sobre parâmetros de configuração, consulte. Consulte Prevenção da perda de registros com o modo sem bloqueio no driver de registro do contêiner AWS Logs

Recursos adicionais

Usando o driver AWS de registro de registros

Escolhendo opções de registro de contêineres para evitar contrapressão

Prevenindo a perda de registros com o modo sem bloqueio no driver de registro do contêiner AWS Logs

Colunas do relatório

- Status
- Região
- ARN de definição de tarefa
- Nomes de definição de contêiner
- Hora da última atualização

Serviço do Amazon ECS usando uma única AZ

Descrição

Verifica se a configuração do serviço usa uma única zona de disponibilidade (AZ).

Uma AZ é um local distinto, isolado de falhas em outras zonas. Isso oferece suporte para conectividade de rede de baixa latência e custo reduzido entre AZs na mesma Região da AWS. Ao iniciar as instâncias em várias zonas de disponibilidade, é possível proteger suas aplicações de um único ponto de falha.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c1z7dfpz01`

Critérios de alerta

- Amarelo: um serviço do Amazon ECS está executando todas as tarefas em uma única AZ.
- Verde: um serviço do Amazon ECS está executando tarefas em pelo menos duas AZs diferentes.

Recommended Action (Ação recomendada)

Crie pelo menos mais uma tarefa para o serviço em outra AZ.

Recursos adicionais

Capacidade e disponibilidade do Amazon ECS

Colunas do relatório

- Status
- Região
- Nome do cluster do ECS/Nome do serviço do ECS
- Número de Zonas de disponibilidade
- Hora da última atualização

Estratégia de posicionamento multi-AZ do Amazon ECS

Descrição

Verifica se o serviço do Amazon ECS usa a estratégia de posicionamento de propagação com base na Zona de Disponibilidade (AZ). Essa estratégia distribui tarefas em todas as zonas de disponibilidade da mesma forma Região da AWS e pode ajudar a proteger seus aplicativos de um único ponto de falha.

Para tarefas que são executadas como parte de um serviço do Amazon ECS, a propagação é a estratégia padrão de posicionamento de tarefas.

Essa verificação também analisa se a propagação é a primeira ou a única estratégia em sua lista de estratégias de posicionamento habilitadas.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c1z7dfpz02`

Critérios de alerta

- Amarelo: a distribuição por zona de disponibilidade está desabilitada ou não é a primeira estratégia na sua lista de estratégias de posicionamento habilitadas para seu serviço do Amazon ECS.
- Verde: a distribuição por zona de disponibilidade é a primeira estratégia em sua lista de estratégias de posicionamento habilitadas ou a única estratégia de posicionamento habilitada para o seu serviço do Amazon ECS.

Recommended Action (Ação recomendada)

Habilite a estratégia de distribuição de tarefas para distribuir tarefas em várias AZs. Verifique se a distribuição por zona de disponibilidade é a primeira estratégia para todas as estratégias de posicionamento de tarefas habilitadas ou a única estratégia usada. Caso opte por gerenciar o posicionamento da AZ, você poderá usar um serviço espelhado em outra AZ para mitigar esses riscos.

Recursos adicionais

Estratégias de posicionamento de tarefas do Amazon ECS

Colunas do relatório

- Status
- Região
- Nome do cluster do ECS/Nome do serviço do ECS
- Estratégia de distribuição de tarefas habilitada e aplicada corretamente
- Hora da última atualização

Redundância de destino sem montagem do Amazon EFS

Descrição

Verifica se existem destinos de montagem em várias zonas de disponibilidade para um sistema de arquivos do Amazon EFS.

Uma zona de disponibilidade é um local distinto, isolado de falhas em outras zonas. Ao criar destinos de montagem em várias zonas de disponibilidade separadas geograficamente dentro de uma região da AWS, você pode alcançar os mais altos níveis de disponibilidade e durabilidade para seus sistemas de arquivos do Amazon EFS.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c1dfprch01`

Critérios de alerta

- Amarelo: o sistema de arquivos tem um destino de montagem criado em uma única zona de disponibilidade.

  Verde: o sistema de arquivos tem dois ou mais destinos de montagem criados em várias zonas de disponibilidade.

Recommended Action (Ação recomendada)

Para sistemas de arquivos do EFS que usam classes de armazenamento One Zone, recomendamos que você crie novos sistemas de arquivos que usem classes de armazenamento Standard, restaurando um backup para um novo sistema de arquivos. Em seguida, crie destinos de montagem em várias zonas de disponibilidade.

Para sistemas de arquivos do EFS que usam classes de armazenamento Standard, recomendamos criar destinos de montagem em várias zonas de disponibilidade.

Recursos adicionais

- Gerenciamento de destinos de montagem usando o console do Amazon EFS
- Cotas e limites do Amazon EFS

Colunas do relatório

- Status
- Região
- ID do sistema de arquivos do EFS
- Número de destinos de montagem
- Número de AZs
- Hora da última atualização

Amazon EFS não está no AWS Backup plano

Descrição

Verifica se os sistemas de arquivos do Amazon EFS estão incluídos nos planos de backup com AWS Backup.

AWS Backup é um serviço de backup unificado projetado para simplificar a criação, migração, restauração e exclusão de backups, ao mesmo tempo em que fornece relatórios e auditoria aprimorados.

Para ter mais informações, consulte Backing up your Amazon EFS file systems (Fazer backup de seus sistemas de arquivos Amazon EFS).

ID da verificação

`c18d2gz117`

Origem

`AWS Config Managed Rule: EFS_IN_BACKUP_PLAN`

Critérios de alerta

Vermelho: o Amazon EFS não está incluído no AWS Backup plano.

Recommended Action (Ação recomendada)

Certifique-se de que seus sistemas de arquivos Amazon EFS estejam incluídos em seu AWS Backup plano para se proteger contra perda acidental de dados ou corrupção de dados.

Recursos adicionais

Fazer backup dos sistemas de arquivos do Amazon EFS

Backup e restauração do Amazon EFS usando AWS Backup.

Colunas do relatório

- Status
- Região
- Recurso
- AWS Config Regra
- Parâmetros de entrada

- Hora da última atualização

Clusters Amazon ElastiCache Multi-AZ

Descrição

Verifica os ElastiCache clusters implantados em uma única zona de disponibilidade (AZ). Essa verificação alerta você se multi-AZ estiver inativo em um cluster.

As implantações em várias AZs aumentam a disponibilidade do ElastiCache cluster ao replicar de forma assíncrona em réplicas somente para leitura em uma AZ diferente. Quando ocorre uma manutenção planejada do cluster ou quando um nó primário não está disponível, a réplica é ElastiCache automaticamente promovida para primária. Esse failover permite que as operações de gravação em clusters sejam retomadas e não exige a intervenção de um administrador.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`ECHdfsQ402`

Critérios de alerta

- Verde: multi-AZ está ativo no cluster.
- Amarelo: multi-AZ está inativo no cluster.

Recommended Action (Ação recomendada)

Crie pelo menos uma réplica por fragmento em uma AZ diferente da primária.

Recursos adicionais

Para obter mais informações, consulte Minimizando o tempo de inatividade no Redis com ElastiCache o Multi-AZ.

Colunas do relatório

- Status

- Região
- Nome do cluster
- Hora da última atualização

Backup automático de clusters do Amazon ElastiCache Redis

Descrição

Verifica se os clusters Amazon ElastiCache for Redis têm o backup automático ativado e se o período de retenção do snapshot está acima do limite padrão especificado ou de 15 dias. Quando os backups automáticos estão habilitados, ElastiCache cria um backup do cluster diariamente.

Você pode especificar o limite de retenção de instantâneos desejado usando os snapshotRetentionPeriodparâmetros de suas AWS Config regras.

Para obter mais informações, consulte Backup e restauração ElastiCache para Redis.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c18d2gz178`

Origem

`AWS Config Managed Rule: elasticache-redis-cluster-automatic-backup-check`

Critérios de alerta

Vermelho: os clusters Amazon ElastiCache for Redis não têm o backup automático ativado ou o período de retenção de snapshots está abaixo do limite.

Recommended Action (Ação recomendada)

Certifique-se de que os clusters Amazon ElastiCache for Redis tenham o backup automático ativado e que o período de retenção de snapshots esteja acima do limite padrão especificado ou

de 15 dias. Os backups automáticos podem ajudar a proteger contra a perda de dados. Em caso de falha, você pode criar um cluster e restaurar seus dados usando o backup mais recente.

Para obter mais informações, consulte Backup e restauração ElastiCache para Redis.

Recursos adicionais

Para obter mais informações, consulte Programação de backups automáticos.

Colunas do relatório

- Status
- Região
- Nome do cluster
- Hora da última atualização

Clusters multi-AZ do Amazon MemoryDB

Descrição

Verifica clusters do MemoryDB que são implantados em uma única zona de disponibilidade (AZ). Essa verificação alerta você se multi-AZ estiver inativo em um cluster.

As implantações em várias AZs aprimoram a disponibilidade do cluster do MemoryDB ao replicar, de forma assíncrona, para réplicas somente leitura em uma AZ diferente. Quando ocorre uma manutenção planejada do cluster, ou quando um nó primário não está disponível, o MemoryDB promove automaticamente uma réplica a primária. Esse failover permite que as operações de gravação em clusters sejam retomadas e não exige a intervenção de um administrador.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`MDBdfsQ401`

Critérios de alerta

- Verde: multi-AZ está ativo no cluster.
- Amarelo: multi-AZ está inativo no cluster.

Recommended Action (Ação recomendada)

Crie pelo menos uma réplica por fragmento em uma AZ diferente da primária.

Recursos adicionais

Para obter mais informações, consulte Minimizing downtime in MemoryDB with Multi-AZ (Minimizar o tempo de inatividade no MemoryDB com multi-AZ).

Colunas do relatório

- Status
- Região
- Nome do cluster
- Hora da última atualização

Agentes do Amazon MSK que hospedam muitas partições

Descrição

Verifica se os agentes de um cluster do Managed Streaming for Kafka (MSK) não têm mais do que o número recomendado de partições atribuídas.

ID da verificação

`Cmsvnj8vf1`

Critérios de alerta

- Vermelho: seu agente do MSK atingiu ou excedeu 100% do limite máximo de partição recomendado
- Amarelo: seu MSK atingiu 80% do limite máximo de partição recomendado

Recommended Action (Ação recomendada)

Siga as práticas recomendadas do MSK para escalar seu cluster do MSK ou excluir qualquer partição não utilizada.

Recursos adicionais

- Dimensionamento correto de seu cluster

Colunas do relatório

- Status
- Região
- ARN do cluster
- ID do agente
- Contagem de partições

Domínios do Amazon OpenSearch Service com menos de três nós de dados

Descrição

Verifica se os domínios do Amazon OpenSearch Service estão configurados com pelo menos três nós de dados e ZoneAwarenessEnabled se são verdadeiros. Quando ZoneAwarenessEnabled ativado, o Amazon OpenSearch Service garante que cada fragmento principal e sua réplica correspondente sejam alocados em diferentes zonas de disponibilidade.

Para obter mais informações, consulte Configuração de um domínio Multi-AZ no Amazon OpenSearch Service.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c18d2gz183`

Origem

`AWS Config Managed Rule: opensearch-data-node-fault-tolerance`

Critérios de alerta

Amarelo: os domínios do Amazon OpenSearch Service são configurados com menos de três nós de dados.

Recommended Action (Ação recomendada)

Certifique-se de que os domínios do Amazon OpenSearch Service estejam configurados com no mínimo três nós de dados. Configure um domínio Multi-AZ para aumentar a disponibilidade do cluster do Amazon OpenSearch Service alocando nós e replicando dados em três zonas de disponibilidade na mesma região. Isso evita a perda de dados e minimiza o tempo de inatividade em caso de falha do nó ou do datacenter (AZ).

Para obter mais informações, consulte Aumentar a disponibilidade do Amazon OpenSearch Service implantando em três zonas de disponibilidade.

Recursos adicionais

- Aumente a disponibilidade do Amazon OpenSearch Service implantando em três zonas de disponibilidade

Colunas do relatório

- Status
- Região
- Recurso
- AWS Config Regra
- Parâmetros de entrada
- Hora da última atualização

Amazon RDS Backups

Descrição

Verifica backups automatizados de instâncias de banco de dados do Amazon RDS.

Por padrão, os backups são habilitados com um período de retenção de um dia. Os backups reduzem o risco de perda inesperada de dados e permitem a point-in-time recuperação.

ID da verificação

`opQPADkZvH`

Critérios de alerta

Vermelho: uma instância de banco de dados tem o período de retenção de backup definido como 0 dias.

Recommended Action (Ação recomendada)

Defina o período de retenção para o backup automatizado da instância de banco de dados para 1 a 35 dias, conforme apropriado para os requisitos da sua aplicação. Consulte Working With Automated Backups (Trabalhar com backups automáticos).

Recursos adicionais

Conceitos básicos do Amazon RDS

Colunas do relatório

- Status
- Região/Zona de disponibilidade
- Instância de banco de dados
- ID da VPC
- Período de retenção de backup

Os clusters de banco de dados do Amazon RDS têm uma instância de banco de dados.

Descrição

Adicione pelo menos outra instância de banco de dados ao cluster de banco de dados para melhorar a disponibilidade e o desempenho.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

> **Note**
>
> Quando uma instância de banco de dados ou cluster de banco de dados é interrompido, você pode visualizar as recomendações do Amazon RDS Trusted Advisor por 3 a 5 dias. Depois de cinco dias, as recomendações não estão disponíveis em Trusted Advisor. Para visualizar as recomendações, abra o console do Amazon RDS e escolha Recomendações.

Se você excluir uma instância de banco de dados ou um cluster de banco de dados, as recomendações associadas a essas instâncias ou clusters não estarão disponíveis no Trusted Advisor console de gerenciamento do Amazon RDS.

ID da verificação

`c1qf5bt011`

Critérios de alerta

Amarelo: os clusters de banco de dados têm apenas uma instância de banco de dados.

Recommended Action (Ação recomendada)

Adicione uma instância de banco de dados de leitura ao cluster de banco de dados.

Recursos adicionais

Na configuração atual, uma instância de banco de dados é usada para operações de leitura e gravação. Você pode adicionar outra instância de banco de dados para permitir a redistribuição de leitura e uma opção de failover.

Para obter mais informações, consulte Alta disponibilidade do Amazon Aurora.

Colunas do relatório

- Status
- Região
- Recurso
- Nome do motor
- Classe da instância de banco de dados
- Hora da última atualização

Clusters de banco de dados Amazon RDS com todas as instâncias na mesma zona de disponibilidade

Descrição

No momento, os clusters de banco de dados estão em uma única zona de disponibilidade. Use várias zonas de disponibilidade para melhorar a disponibilidade.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

> **Note**
>
> Quando uma instância de banco de dados ou cluster de banco de dados é interrompido, você pode visualizar as recomendações do Amazon RDS Trusted Advisor por 3 a 5 dias. Depois de cinco dias, as recomendações não estão disponíveis em Trusted Advisor. Para visualizar as recomendações, abra o console do Amazon RDS e escolha Recomendações.
> Se você excluir uma instância de banco de dados ou um cluster de banco de dados, as recomendações associadas a essas instâncias ou clusters não estarão disponíveis no Trusted Advisor console de gerenciamento do Amazon RDS.

ID da verificação

`c1qf5bt007`

Critérios de alerta

Amarelo: os clusters de banco de dados têm todas as instâncias na mesma zona de disponibilidade.

Recommended Action (Ação recomendada)

Adicione as instâncias de banco de dados a várias zonas de disponibilidade no cluster de banco de dados.

Recursos adicionais

Recomendamos que você adicione as instâncias de banco de dados a várias zonas de disponibilidade em um cluster de banco de dados. Adicionar instâncias de banco de dados a várias zonas de disponibilidade melhora a disponibilidade do seu cluster de banco de dados.

Para obter mais informações, consulte Alta disponibilidade do Amazon Aurora.

Colunas do relatório

- Status
- Região
- Recurso
- Nome do motor
- Hora da última atualização

Clusters de banco de dados Amazon RDS com todas as instâncias de leitura na mesma zona de disponibilidade

Descrição

Todas as instâncias do leitor do seu cluster de banco de dados estão na mesma zona de disponibilidade. Recomendamos que você distribua as instâncias do Reader em várias zonas de disponibilidade em seu cluster de banco de dados.

A distribuição aumenta a disponibilidade do banco de dados e melhora o tempo de resposta ao reduzir a latência da rede entre os clientes e o banco de dados.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

> **Note**
>
> Quando uma instância de banco de dados ou cluster de banco de dados é interrompido, você pode visualizar as recomendações do Amazon RDS Trusted Advisor por 3 a 5 dias. Depois de cinco dias, as recomendações não estão disponíveis em Trusted Advisor. Para visualizar as recomendações, abra o console do Amazon RDS e escolha Recomendações.
> Se você excluir uma instância de banco de dados ou um cluster de banco de dados, as recomendações associadas a essas instâncias ou clusters não estarão disponíveis no Trusted Advisor console de gerenciamento do Amazon RDS.

ID da verificação

`c1qf5bt018`

Critérios de alerta

Vermelho: os clusters de banco de dados têm as instâncias do leitor na mesma zona de disponibilidade.

Recommended Action (Ação recomendada)

Distribua as instâncias do leitor em várias zonas de disponibilidade.

Recursos adicionais

As zonas de disponibilidade (AZs) são locais distintos entre si para fornecer isolamento em caso de interrupções em cada AWS região. Recomendamos distribuir a instância primária e as instâncias de leitor no cluster de banco de dados em várias AZs para melhorar a disponibilidade do cluster de banco de dados. Você pode criar um cluster Multi-AZ usando a API AWS Management Console AWS CLI,, ou Amazon RDS ao criar o cluster. É possível modificar o cluster existente do Aurora em um cluster multi-AZ adicionando uma nova instância de leitor e especificando uma AZ diferente.

Para obter mais informações, consulte Alta disponibilidade do Amazon Aurora.

Colunas do relatório

- Status
- Região
- Recurso
- Nome do motor
- Hora da última atualização

Monitoramento aprimorado de instâncias de banco de dados do Amazon RDS não habilitado

Descrição

Verifica se as instâncias de banco de dados do Amazon RDS têm o monitoramento avançado habilitado.

O monitoramento aprimorado do Amazon RDS fornece métricas em tempo real para o sistema operacional (SO) no qual a instância do banco de dados é executada. Todas as métricas do sistema e as informações de processo das instâncias de banco de dados do Amazon RDS podem ser visualizadas no console do Amazon RDS. E você pode personalizar o painel. Com o monitoramento aprimorado, você tem visibilidade do status de operação da sua instância do Amazon RDS quase em tempo real, permitindo que você responda aos problemas operacionais com mais rapidez.

Você pode especificar o intervalo de monitoramento desejado usando o parâmetro MonitoringInterval de suas regras. AWS Config

Para obter mais informações, consulte Visão geral do monitoramento avançado e Métricas do sistema operacional em monitoramento avançado.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c18d2gz158`

Origem

`AWS Config Managed Rule: rds-enhanced-monitoring-enabled`

Critérios de alerta

Amarelo: suas instâncias de banco de dados do Amazon RDS não têm o monitoramento avançado habilitado ou não estão configuradas com o intervalo desejado.

Recommended Action (Ação recomendada)

Ative o monitoramento avançado para suas instâncias de banco de dados do Amazon RDS para melhorar a visibilidade do status da operação da sua instância do Amazon RDS.

Para obter mais informações, consulte Monitorar métricas do SO com o monitoramento avançado.

Recursos adicionais

Métricas do sistema operacional em monitoramento avançado

Colunas do relatório

- Status
- Região
- Recurso
- AWS Config Regra
- Parâmetros de entrada
- Hora da última atualização

As instâncias de banco de dados do Amazon RDS têm o escalonamento automático de armazenamento desativado

Descrição

O escalonamento automático de armazenamento do Amazon RDS não está ativado para sua instância de banco de dados. Quando há um aumento na carga de trabalho do banco de dados, o escalonamento automático do RDS Storage escala automaticamente a capacidade de armazenamento sem tempo de inatividade.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

> **Note**
>
> Quando uma instância de banco de dados ou cluster de banco de dados é interrompido, você pode visualizar as recomendações do Amazon RDS Trusted Advisor por 3 a 5 dias. Depois de cinco dias, as recomendações não estão disponíveis em Trusted Advisor. Para visualizar as recomendações, abra o console do Amazon RDS e escolha Recomendações.

Se você excluir uma instância de banco de dados ou um cluster de banco de dados, as recomendações associadas a essas instâncias ou clusters não estarão disponíveis no Trusted Advisor console de gerenciamento do Amazon RDS.

ID da verificação

`c1qf5bt013`

Critérios de alerta

Vermelho: as instâncias de banco de dados não têm o escalonamento automático de armazenamento ativado.

Recommended Action (Ação recomendada)

Ative o escalonamento automático de armazenamento do Amazon RDS com um limite máximo de armazenamento especificado.

Recursos adicionais

O escalonamento automático de armazenamento do Amazon RDS escala automaticamente a capacidade de armazenamento sem tempo de inatividade quando a carga de trabalho do banco de dados aumenta. O escalonamento automático do armazenamento monitora o uso do armazenamento e aumenta automaticamente a capacidade quando o uso está próximo da capacidade de armazenamento provisionada. Você pode especificar um limite máximo no armazenamento que o Amazon RDS pode alocar para a instância de banco de dados. Não há custo adicional para o escalonamento automático do armazenamento. Você paga somente pelos recursos do Amazon RDS que são alocados à sua instância de banco de dados. Recomendamos que você ative o escalonamento automático de armazenamento do Amazon RDS.

Para ter mais informações, consulte Gerenciar a capacidade automaticamente com o dimensionamento automático de armazenamento do Amazon RDS.

Colunas do relatório

- Status
- Região
- Recurso
- Valor recomendado
- Nome do motor
- Hora da última atualização

Instâncias de banco de dados do Amazon RDS que não usam a implantação Multi-AZ

Descrição

Recomendamos que você use a implantação multi-AZ. As implantações multi-AZ aumentam a disponibilidade e a durabilidade da instância de banco de dados.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

> **Note**
>
> Quando uma instância de banco de dados ou cluster de banco de dados é interrompido, você pode visualizar as recomendações do Amazon RDS Trusted Advisor por 3 a 5 dias. Depois de cinco dias, as recomendações não estão disponíveis em Trusted Advisor. Para visualizar as recomendações, abra o console do Amazon RDS e escolha Recomendações.
> Se você excluir uma instância de banco de dados ou um cluster de banco de dados, as recomendações associadas a essas instâncias ou clusters não estarão disponíveis no Trusted Advisor console de gerenciamento do Amazon RDS.

ID da verificação

`c1qf5bt019`

Critérios de alerta

Amarelo: as instâncias de banco de dados não estão usando a implantação Multi-AZ.

Recommended Action (Ação recomendada)

Configure o Multi-AZ para as instâncias de banco de dados afetadas.

Recursos adicionais

Em uma implantação Multi-AZ do Amazon RDS, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica os dados em uma instância em uma zona de

disponibilidade diferente. Quando detecta uma falha, o Amazon RDS automaticamente passa para uma instância em espera sem intervenção manual.

Para obter mais informações, consulte Preços do .

Colunas do relatório

- Status
- Região
- Recurso
- Nome do motor
- Hora da última atualização

Amazon RDS DiskQueueDepth

Descrição

Verifica se a CloudWatch métrica DiskQueueDepth mostra que o número de gravações em fila no armazenamento do banco de dados da Instância RDS cresceu até um nível em que uma investigação operacional deve ser sugerida.

ID da verificação

`Cmsvnj8db3`

Critérios de alerta

- Vermelho: a DiskQueueDepth CloudWatch métrica excedeu 10
- Amarelo: a DiskQueueDepth CloudWatch métrica é maior que 5, mas menor ou igual a 10
- Verde: a DiskQueueDepth CloudWatch métrica é menor ou igual a 5

Recommended Action (Ação recomendada)

Considere migrar para instâncias e volumes de armazenamento que suportem as características de leitura e gravação.

Colunas do relatório

- Status
- Região
- ARN da instância de banco de dados

- DiskQueueDepth Métrica

Amazon RDS FreeStorageSpace

Descrição

Verifica se a FreeStorageSpace CloudWatch métrica de uma instância de banco de dados do RDS aumentou acima de um limite operacionalmente razoável.

ID da verificação

`Cmsvnj8db2`

Critérios de alerta

- Vermelho: FreeStorageSpace atingiu ou excedeu 90% da capacidade total
- FreeStorageSpace Amarelo: está entre 80% e 90% da capacidade total
- Verde: FreeStorageSpace é menos de 80% da capacidade total

Recommended Action (Ação recomendada)

Aumente o espaço de armazenamento para a instância de banco de dados do RDS que está com pouco espaço de armazenamento gratuito usando o Amazon RDS Management Console, a API do Amazon RDS ou a interface da linha de comando da AWS.

Colunas do relatório

- Status
- Região
- ARN da instância de banco de dados
- FreeStorageSpace Métrica (MB)
- Armazenamento alocado para instâncias de banco de dados (MB)
- Porcentagem de armazenamento usado da instância de banco de dados

O parâmetro log_output do Amazon RDS está definido como tabela

Descrição

Quando log_output é definido como TABLE, mais armazenamento é usado do que quando log_output é definido como FILE. Recomendamos que você defina o parâmetro como FILE, para evitar atingir o limite de tamanho de armazenamento.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

> **Note**
>
> Quando uma instância de banco de dados ou cluster de banco de dados é interrompido, você pode visualizar as recomendações do Amazon RDS Trusted Advisor por 3 a 5 dias. Depois de cinco dias, as recomendações não estão disponíveis em Trusted Advisor. Para visualizar as recomendações, abra o console do Amazon RDS e escolha Recomendações.
> Se você excluir uma instância de banco de dados ou um cluster de banco de dados, as recomendações associadas a essas instâncias ou clusters não estarão disponíveis no Trusted Advisor console de gerenciamento do Amazon RDS.

ID da verificação

`c1qf5bt023`

Critérios de alerta

Amarelo: os grupos de parâmetros do banco de dados têm o parâmetro log_output definido como TABLE.

Recommended Action (Ação recomendada)

Defina o valor do parâmetro log_output como FILE em seus grupos de parâmetros de banco de dados.

Recursos adicionais

Para obter mais informações, consulte Arquivos de log do banco de dados MySQL.

Colunas do relatório

- Status
- Região
- Recurso

- Nome do parâmetro
- Valor recomendado
- Hora da última atualização

A configuração do parâmetro innodb_default_row_format do Amazon RDS não é segura

Descrição

Sua instância de banco de dados encontra um problema conhecido: uma tabela criada em uma versão do MySQL anterior à 8.0.26 com o row_format definido como COMPACT ou REDUNDANT fica inacessível e irrecuperável quando o índice excede 767 bytes.

Recomendamos que você defina o valor do parâmetro innodb_default_row_format como DYNAMIC.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

> **Note**
>
> Quando uma instância de banco de dados ou cluster de banco de dados é interrompido, você pode visualizar as recomendações do Amazon RDS Trusted Advisor por 3 a 5 dias. Depois de cinco dias, as recomendações não estão disponíveis em Trusted Advisor. Para visualizar as recomendações, abra o console do Amazon RDS e escolha Recomendações.
> Se você excluir uma instância de banco de dados ou um cluster de banco de dados, as recomendações associadas a essas instâncias ou clusters não estarão disponíveis no Trusted Advisor console de gerenciamento do Amazon RDS.

ID da verificação

`c1qf5bt036`

Critérios de alerta

Vermelho: grupos de parâmetros do banco de dados têm uma configuração insegura para o parâmetro innodb_default_row_format.

Recommended Action (Ação recomendada)

Defina o parâmetro innodb_default_row_format como DYNAMIC.

Recursos adicionais

Quando uma tabela é criada com a versão do MySQL inferior à 8.0.26 com row_format definido como COMPACT ou REDUNDANT, a criação de índices com um prefixo de chave menor que 767 bytes não é obrigatória. Depois que o banco de dados for reiniciado, essas tabelas não poderão ser acessadas nem recuperadas.

Para obter mais informações, consulte Alterações no MySQL 8.0.26 (2021-07-20, Disponibilidade geral) no site de documentação do MySQL.

Colunas do relatório

- Status
- Região
- Recurso
- Nome do parâmetro
- Valor recomendado
- Hora da última atualização

O parâmetro innodb_flush_log_at_trx_commit do Amazon RDS não é 1

Descrição

O valor do parâmetro innodb_flush_log_at_trx_commit da sua instância de banco de dados não é um valor seguro. Esse parâmetro controla a persistência das operações de confirmação no disco.

Recomendamos que você defina o parâmetro innodb_flush_log_at_trx_commit como 1.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

> **Note**
>
> Quando uma instância de banco de dados ou cluster de banco de dados é interrompido, você pode visualizar as recomendações do Amazon RDS Trusted Advisor por 3 a 5 dias. Depois de cinco dias, as recomendações não estão disponíveis em Trusted Advisor. Para visualizar as recomendações, abra o console do Amazon RDS e escolha Recomendações.
> Se você excluir uma instância de banco de dados ou um cluster de banco de dados, as recomendações associadas a essas instâncias ou clusters não estarão disponíveis no Trusted Advisor console de gerenciamento do Amazon RDS.

ID da verificação

`c1qf5bt030`

Critérios de alerta

Amarelo: grupos de parâmetros do banco de dados têm innodb_flush_log_at_trx_commit definido como diferente de 1.

Recommended Action (Ação recomendada)

Defina o valor do parâmetro innodb_flush_log_at_trx_commit como 1

Recursos adicionais

A transação do banco de dados é durável quando o buffer de log é salvo no armazenamento durável. No entanto, salvar no disco afeta o desempenho. Dependendo do valor definido para o parâmetro innodb_flush_log_at_trx_commit, o comportamento de como os registros são gravados e salvos no disco pode variar.

- Quando o valor do parâmetro é 1, os registros são gravados e salvos no disco após cada transação confirmada.

- Quando o valor do parâmetro é 0, os registros são gravados e salvos no disco uma vez por segundo.
- Quando o valor do parâmetro é 2, os registros são gravados após a confirmação de cada transação e salvos no disco uma vez por segundo. Os dados são movidos do buffer de memória do InnoDB para o cache do sistema operacional, que também está na memória.

> **Note**
>
> Quando o valor do parâmetro não é 1, o InnoDB não garante as propriedades ACID. As transações recentes do último segundo podem ser perdidas quando o banco de dados falha.

Para ter mais informações, consulte Best practices for configuring parameters for Amazon RDS for MySQL, part 1: Parameters related to performance.

Colunas do relatório

- Status
- Região
- Recurso
- Nome do parâmetro
- Valor recomendado
- Hora da última atualização

O parâmetro max_user_connections do Amazon RDS está baixo

Descrição

Sua instância de banco de dados tem um valor baixo para o número máximo de conexões simultâneas para cada conta de banco de dados.

Recomendamos definir o parâmetro max_user_connections para um número maior que 5.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

> **Note**
>
> Quando uma instância de banco de dados ou cluster de banco de dados é interrompido, você pode visualizar as recomendações do Amazon RDS Trusted Advisor por 3 a 5 dias. Depois de cinco dias, as recomendações não estão disponíveis em Trusted Advisor. Para visualizar as recomendações, abra o console do Amazon RDS e escolha Recomendações.
> Se você excluir uma instância de banco de dados ou um cluster de banco de dados, as recomendações associadas a essas instâncias ou clusters não estarão disponíveis no Trusted Advisor console de gerenciamento do Amazon RDS.

ID da verificação

`c1qf5bt034`

Critérios de alerta

Amarelo: os grupos de parâmetros do banco de dados têm max_user_connections configurados incorretamente.

Recommended Action (Ação recomendada)

Aumente o valor do parâmetro max_user_connections para um número maior que 5.

Recursos adicionais

A configuração max_user_connections controla o número máximo de conexões simultâneas permitidas para uma conta de usuário do MySQL. Atingir esse limite de conexão causa falhas nas operações de administração de instâncias do Amazon RDS, como backup, aplicação de patches e alterações de parâmetros.

Para obter mais informações, consulte Definindo limites de recursos da conta no site de documentação do MySQL.

Colunas do relatório

- Status
- Região
- Recurso
- Nome do parâmetro
- Valor recomendado
- Hora da última atualização

Amazon RDS Multi-AZ

Descrição

Verifica instâncias de banco de dados implantadas em uma única zona de disponibilidade (AZ).

As implantações Multi-AZ melhoram a disponibilidade do banco de dados replicando de forma síncrona para uma instância em espera em outra zona de disponibilidade. Durante a manutenção planejada do banco de dados ou a falha de uma instância de banco de dados ou de uma zona de disponibilidade, o Amazon RDS faz failover automático para o standby. Esse failover permite que as operações de banco de dados sejam retomadas rapidamente sem intervenção administrativa. Como o Amazon RDS não oferece suporte à implantação Multi-AZ para o Microsoft SQL Server, essa verificação não examina instâncias do SQL Server.

ID da verificação

`f2iK5R6Dep`

Critérios de alerta

Amarelo: uma instância de banco de dados é implantada em uma única zona de disponibilidade.

Recommended Action (Ação recomendada)

Se a aplicação exigir alta disponibilidade, modifique sua instância de banco de dados para habilitar a implantação Multi-AZ. Consulte High Availability (Multi-AZ) (Alta disponibilidade [Multi-AZ]).

Recursos adicionais

Regiões e zonas de disponibilidade

Colunas do relatório

- Status

- Região/Zona de disponibilidade
- Instância de banco de dados
- ID da VPC
- Multi-AZ

Amazon RDS não está no plano AWS Backup

Descrição

Verifica se suas instâncias de banco de dados do Amazon RDS estão incluídas em um plano de backup no AWS Backup.

AWS Backup é um serviço de backup totalmente gerenciado que facilita a centralização e a automatização do backup de dados em todos os serviços. AWS

Incluir sua instância de banco de dados do Amazon RDS em um plano de backup é importante para obrigações de conformidade regulatória, recuperação de desastres, políticas comerciais para proteção de dados e metas de continuidade de negócios.

Para obter mais informações, consulte What is AWS Backup?.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c18d2gz159`

Origem

`AWS Config Managed Rule: rds-in-backup-plan`

Critérios de alerta

Amarelo: Uma instância de banco de dados Amazon RDS não está incluída em um plano de backup com AWS Backup.

Recommended Action (Ação recomendada)

Inclua suas instâncias de banco de dados do Amazon RDS em um plano de backup com AWS Backup.

Para obter mais informações, consulte Backup e restauração do Amazon RDS usando o AWS Backup.

Recursos adicionais

Atribuir recursos a um plano de backup

Colunas do relatório

- Status
- Região
- Recurso
- AWS Config Regra
- Parâmetros de entrada
- Hora da última atualização

As réplicas de leitura do Amazon RDS estão abertas no modo gravável

Descrição

A instância de banco de dados tem uma réplica de leitura no modo de gravação, que permite que os clientes realizem atualizações.

Recomendamos que você defina o parâmetro read_only para que as réplicas de leitura não estejam no TrueIfReplicamodo gravável.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

> **Note**
>
> Quando uma instância de banco de dados ou cluster de banco de dados é interrompido, você pode visualizar as recomendações do Amazon RDS Trusted Advisor por 3 a 5 dias. Depois de cinco dias, as recomendações não estão disponíveis em Trusted Advisor. Para visualizar as recomendações, abra o console do Amazon RDS e escolha Recomendações.
> Se você excluir uma instância de banco de dados ou um cluster de banco de dados, as recomendações associadas a essas instâncias ou clusters não estarão disponíveis no Trusted Advisor console de gerenciamento do Amazon RDS.

ID da verificação

`c1qf5bt035`

Critérios de alerta

Amarelo: os grupos de parâmetros do banco de dados ativam o modo gravável para as réplicas de leitura.

Recommended Action (Ação recomendada)

Defina o valor do parâmetro read_only como. TrueIfReplica

Recursos adicionais

O parâmetro read_only controla a permissão de gravação dos clientes em uma instância de banco de dados. O valor padrão para esse parâmetro é TrueIfReplica. Para uma instância de réplica, TrueIfReplicadefine o valor read_only como ON (1) e desativa qualquer atividade de gravação dos clientes. Para uma instância mestre/gravadora, TrueIfReplicadefine o valor como OFF (0) e ativa a atividade de gravação dos clientes para a instância. Quando a réplica de leitura é aberta no modo gravável, os dados armazenados nessa instância podem divergir da instância primária, o que causa erros de replicação.

Para obter mais informações, consulte Melhores práticas para configurar parâmetros do Amazon RDS for MySQL, parte 2: Parâmetros relacionados à replicação no site de documentação do MySQL.

Colunas do relatório

- Status
- Região

- Recurso
- Nome do parâmetro
- Valor recomendado
- Hora da última atualização

Os backups automatizados de recursos do Amazon RDS estão desativados

Descrição

Os backups automatizados estão desativados em seus recursos de banco de dados. Os backups automatizados permitem a point-in-time recuperação da sua instância de banco de dados.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

> **Note**
>
> Quando uma instância de banco de dados ou cluster de banco de dados é interrompido, você pode visualizar as recomendações do Amazon RDS Trusted Advisor por 3 a 5 dias. Depois de cinco dias, as recomendações não estão disponíveis em Trusted Advisor. Para visualizar as recomendações, abra o console do Amazon RDS e escolha Recomendações.
> Se você excluir uma instância de banco de dados ou um cluster de banco de dados, as recomendações associadas a essas instâncias ou clusters não estarão disponíveis no Trusted Advisor console de gerenciamento do Amazon RDS.

ID da verificação

`c1qf5bt001`

Critérios de alerta

Vermelho: os recursos do Amazon RDS não têm backups automatizados ativados

Recommended Action (Ação recomendada)

Ative os backups automatizados com um período de retenção de até 14 dias.

Recursos adicionais

Os backups automatizados permitem a point-in-time recuperação de suas instâncias de banco de dados. Recomendamos ativar os backups automatizados. Quando você ativa backups automatizados para uma instância de banco de dados, o Amazon RDS executa automaticamente um backup completo dos seus dados diariamente durante a janela de backup de sua preferência. O backup captura registros de transações quando há atualizações na sua instância de banco de dados. Você obtém armazenamento de backup até o tamanho de armazenamento da sua instância de banco de dados sem custo adicional.

Para obter mais informações, consulte os seguintes recursos do :

- Habilitando backups automatizados
- Desmistificando os custos de armazenamento de backup do Amazon RDS

Colunas do relatório

- Status
- Região
- Recurso
- Valor recomendado
- Nome do motor
- Hora da última atualização

O parâmetro sync_binlog do Amazon RDS está desativado

Descrição

A sincronização do log binário com o disco não é aplicada antes que as confirmações das transações sejam reconhecidas na instância de banco de dados.

Recomendamos que você defina o valor do parâmetro sync_binlog como 1.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

> **Note**
>
> Quando uma instância de banco de dados ou cluster de banco de dados é interrompido, você pode visualizar as recomendações do Amazon RDS Trusted Advisor por 3 a 5 dias. Depois de cinco dias, as recomendações não estão disponíveis em Trusted Advisor. Para visualizar as recomendações, abra o console do Amazon RDS e escolha Recomendações.
> Se você excluir uma instância de banco de dados ou um cluster de banco de dados, as recomendações associadas a essas instâncias ou clusters não estarão disponíveis no Trusted Advisor console de gerenciamento do Amazon RDS.

ID da verificação

`c1qf5bt031`

Critérios de alerta

Amarelo: os grupos de parâmetros do banco de dados têm o registro binário síncrono desativado.

Recommended Action (Ação recomendada)

Defina o parâmetro sync_binlog como 1.

Recursos adicionais

O parâmetro sync_binlog controla como o MySQL envia o log binário para o disco. Quando o valor desse parâmetro é definido como 1, ele ativa a sincronização do log binário com o disco antes que as transações sejam confirmadas. Quando o valor desse parâmetro é definido como 0, ele desativa a sincronização do log binário com o disco. Normalmente, o servidor MySQL depende do sistema operacional para enviar o log binário para o disco regularmente, semelhante a outros arquivos. O valor do parâmetro sync_binlog definido como 0 pode melhorar o desempenho. No entanto, durante uma falha de energia ou uma falha no sistema operacional,

o servidor perde todas as transações confirmadas que não foram sincronizadas com os registros binários.

Para obter mais informações, consulte Melhores práticas para configurar parâmetros do Amazon RDS for MySQL, parte 2: Parâmetros relacionados à replicação.

Colunas do relatório

- Status
- Região
- Recurso
- Nome do parâmetro
- Valor recomendado
- Hora da última atualização

O cluster de banco de dados do RDS não tem a replicação multi-AZ habilitada

Descrição

Verifica se seus clusters de banco de dados do Amazon RDS têm a replicação multi-AZ habilitada.

Um cluster de banco de dados multi-AZ tem uma instância de banco de dados de gravador e duas instâncias de banco de dados de leitor em três zonas de disponibilidade separadas. Clusters de banco de dados multi-AZ oferecem alta disponibilidade, maior capacidade para workloads de leitura e menor latência quando comparados a implantações multi-AZ.

Para obter mais informações, consulte Criar um cluster de banco de dados multi-AZ.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c18d2gz161`

Origem

AWS Config Managed Rule: rds-cluster-multi-az-enabled

Critérios de alerta

Amarelo: seu cluster de bancos de dados do Amazon RDS não tem a replicação multi-AZ configurada

Recommended Action (Ação recomendada)

Ative a implantação do cluster de banco de dados multi-AZ ao criar um cluster de banco de dados do Amazon RDS.

Para obter mais informações, consulte Criar um cluster de banco de dados multi-AZ.

Recursos adicionais

Implantações de clusters de banco de dados multi-AZ

Colunas do relatório

- Status
- Região
- Recurso
- AWS Config Regra
- Parâmetros de entrada
- Hora da última atualização

Instância multi-AZ em espera do RDS não habilitada

Descrição

Verifica se suas instâncias de banco de dados do Amazon RDS têm uma réplica multi-AZ em espera configurada.

O Multi-AZ do Amazon RDS fornece alta disponibilidade e durabilidade para instâncias de banco de dados ao replicar dados para uma réplica em espera em uma zona de disponibilidade diferente. Isso fornece failover automático, melhora o desempenho e aumenta a durabilidade dos dados. Em uma implantação de instância de banco de dados multi-AZ, o Amazon RDS provisiona e mantém automaticamente uma réplica em espera síncrona em outra zona de disponibilidade. A instância de banco de dados primária é replicada simultaneamente através de zonas de disponibilidade para uma réplica em espera, a fim de proporcionar a redundância de dados e

minimizar os picos de latência durante os backups do sistema. Executar uma instância de banco de dados com alta disponibilidade aumenta a disponibilidade durante a manutenção planejada do sistema. Também pode ajudar a proteger bancos de dados contra falhas na instância de banco de dados e interrupção da zona de disponibilidade.

Para obter mais informações, consulte Implantações de instâncias de banco de dados multi-AZ.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c18d2gz156`

Origem

`AWS Config Managed Rule: rds-multi-az-support`

Critérios de alerta

Amarelo: uma instância do banco de dados do Amazon RDS não tem a replicação multi-AZ configurada.

Recommended Action (Ação recomendada)

Ative a implantação multi-AZ ao criar uma instância de banco de dados do Amazon RDS.

Essa verificação não pode ser excluída da exibição no Trusted Advisor console.

Recursos adicionais

Implantações de instâncias de banco de dados multi-AZ

Colunas do relatório

- Status
- Região
- Recurso
- AWS Config Regra
- Parâmetros de entrada

- Hora da última atualização

Amazon RDS ReplicaLag

Descrição

Verifica se a ReplicaLag CloudWatch métrica de uma instância de banco de dados do RDS aumentou acima de um limite operacionalmente razoável na última semana.

ReplicaLag A métrica mede o número de segundos em que uma réplica de leitura está atrás da instância primária. O atraso na replicação ocorre quando as atualizações assíncronas feitas na réplica de leitura não conseguem acompanhar as atualizações que ocorrem na instância primária do banco de dados. No caso de uma falha na instância primária, os dados podem faltar na réplica de leitura se ela ReplicaLag estiver acima de um limite operacionalmente razoável.

ID da verificação

`Cmsvnj8db1`

Critérios de alerta

- Vermelho: a ReplicaLag métrica excedeu 60 segundos pelo menos uma vez durante a semana.
- Amarelo: a ReplicaLag métrica excedeu 10 segundos pelo menos uma vez durante a semana.
- Verde: ReplicaLag é inferior a 10 segundos.

Recommended Action (Ação recomendada)

Há várias causas possíveis ReplicaLag para aumentar além dos níveis operacionalmente seguros. Por exemplo, isso pode ser causado por instâncias de réplica recentemente substituídas ou lançadas de backups antigos, e essas réplicas exigem um tempo considerável para “alcançar” a instância primária do banco de dados e as transações em tempo real. Isso ReplicaLag pode diminuir com o tempo à medida que a recuperação ocorre. Outro exemplo poderia ser o fato de que a velocidade de transação que pode ser alcançada na instância primária do banco de dados é maior do que o processo de replicação ou a infraestrutura de réplica é capaz de corresponder. Isso ReplicaLag pode aumentar com o tempo, pois a replicação não consegue acompanhar o desempenho do banco de dados principal. Finalmente, a carga de trabalho pode ser interrompida em diferentes períodos do dia/mês/etc. que resultam em atrasos ocasionais. ReplicaLag Sua equipe deve investigar qual possível causa raiz contribuiu ReplicaLag para o alto nível do banco de dados e, possivelmente, alterar o tipo de instância do banco de dados ou outras características da carga de trabalho para garantir que a continuidade dos dados na réplica atenda aos seus requisitos.

Recursos adicionais

- Trabalhar com réplicas de leitura para o Amazon RDS para PostgreSQL
- Trabalhar com a replicação MySQL no Amazon RDS
- Trabalhar com réplicas de leitura MySQL

Colunas do relatório

- Status
- Região
- ARN da instância de banco de dados
- ReplicaLag Métrica

O parâmetro synchronous_commit do Amazon RDS está desativado

Descrição

Quando o parâmetro synchronous_commit é desativado, os dados podem ser perdidos em uma falha no banco de dados. A durabilidade do banco de dados está em risco.

Recomendamos que você ative o parâmetro synchronous_commit.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

> **Note**
>
> Quando uma instância de banco de dados ou cluster de banco de dados é interrompido, você pode visualizar as recomendações do Amazon RDS Trusted Advisor por 3 a 5 dias. Depois de cinco dias, as recomendações não estão disponíveis em Trusted Advisor. Para visualizar as recomendações, abra o console do Amazon RDS e escolha Recomendações.
> Se você excluir uma instância de banco de dados ou um cluster de banco de dados, as recomendações associadas a essas instâncias ou clusters não estarão disponíveis no Trusted Advisor console de gerenciamento do Amazon RDS.

ID da verificação

`c1qf5bt026`

Critérios de alerta

Vermelho: grupos de parâmetros de banco de dados têm o parâmetro synchronous_commit desativado.

Recommended Action (Ação recomendada)

Ative o parâmetro synchronous_commit em seus grupos de parâmetros de banco de dados.

Recursos adicionais

O parâmetro synchronous_commit define a conclusão do processo Write-Ahead Logging (WAL) antes que o servidor do banco de dados envie uma notificação bem-sucedida ao cliente. Essa confirmação é chamada de confirmação assíncrona porque o cliente reconhece a confirmação antes que o WAL salve a transação no disco. Se o parâmetro synchronous_commit estiver desativado, as transações poderão ser perdidas, a durabilidade da instância de banco de dados poderá ser comprometida e os dados poderão ser perdidos quando um banco de dados falhar.

Para obter mais informações, consulte Arquivos de log do banco de dados MySQL.

Colunas do relatório

- Status
- Região
- Recurso
- Nome do parâmetro
- Valor recomendado
- Hora da última atualização

Snapshots automatizados do cluster do Amazon Redshift

Descrição

Verifica se os snapshots automáticos estão habilitados para seus clusters do Amazon Redshift.

O Amazon Redshift tira automaticamente snapshots incrementais que rastreiam as alterações no cluster desde o snapshot automatizado anterior. Os snapshots automatizados retêm todos os dados necessários para restaurar um cluster a partir de um snapshot. Para desativar snapshots

automatizados, defina o período de retenção como zero. Não é possível desabilitar snapshots automatizados para tipos de nó RA3.

Você pode especificar o período de retenção mínimo e máximo desejado usando o MaxRetentionPeriodparâmetro MinRetentionPeriode de suas AWS Config regras.

Snapshots e backups do Amazon Redshift

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c18d2gz135`

Origem

`AWS Config Managed Rule: redshift-backup-enabled`

Critérios de alerta

Vermelho: o Amazon Redshift não tem snapshots automatizados configurados dentro do período de retenção desejado.

Recommended Action (Ação recomendada)

Certifique-se de que os snapshots automáticos estejam habilitados para seus clusters do Amazon Redshift.

Para obter mais informações, consulte “Gerenciamento de snapshots usando o console”.

Recursos adicionais

Snapshots e backups do Amazon Redshift

Para ter mais informações, consulte Trabalhar com backups.

Colunas do relatório

- Status
- Região

- Recurso
- AWS Config Regra
- Parâmetros de entrada
- Hora da última atualização

Verificações de integridade excluídas pelo Amazon Route 53

Descrição

Verifica conjuntos de registros de recursos associados a verificações de integridade que foram excluídas.

O Route 53 não impede a exclusão de uma verificação de integridade associada a um ou mais conjuntos de registros de recursos. Se você excluir uma verificação de integridade sem atualizar os conjuntos de registros de recursos associados, o roteamento de consultas DNS para a configuração de failover de DNS não funcionará conforme o planejado.

As zonas hospedadas criadas por AWS serviços não aparecerão nos resultados da sua verificação.

ID da verificação

`Cb877eB72b`

Critérios de alerta

Amarelo: um conjunto de registros de recursos está associado a uma verificação de integridade que foi excluída.

Recommended Action (Ação recomendada)

Crie uma nova verificação de integridade e associe-a ao conjunto de registros de recursos. Consulte Creating, Updating, and Deleting Health Checks (Criar, atualizar e excluir verificações de integridade) e Adding Health Checks to Resource Record Sets (Adicionar verificações de integridade a conjuntos de registros de recursos).

Recursos adicionais

- Amazon Route 53 Health Checks and DNS Failover (Verificações de integridade do Amazon Route 53 e failover de DNS)
- How Health Checks Work in Simple Amazon Route 53 Configurations (Como as verificações de integridade funcionam em configurações simples do Amazon Route 53)

Colunas do relatório

- Nome da zona hospedada
- ID da zona hospedada
- Nome do conjunto de registros de recursos
- Tipo do conjunto de registros de recursos
- Identificador do conjunto de registros de recursos

Conjuntos de registros de recursos de failover no Amazon Route 53.

Descrição

Verifica se há conjuntos de registros de recurso de failover do Amazon Route 53 que tenham uma configuração incorreta.

Quando as verificações de integridade do Amazon Route 53 determinarem que o recurso principal não está íntegro, o Amazon Route 53 responderá a consultas com um conjunto de registros de recurso de backup secundário. Crie conjuntos de registros de recursos primários e secundários configurados corretamente para que o failover funcione.

As zonas hospedadas criadas por AWS serviços não aparecerão nos resultados da sua verificação.

ID da verificação

`b73EEdD790`

Critérios de alerta

- Amarelo: um conjunto de registros de recursos de failover primário não tem um conjunto de registros de recursos secundário correspondente.
- Amarelo: um conjunto de registros de recursos de failover secundário não tem um conjunto de registros de recursos primário correspondente.
- Amarelo: conjuntos de registros de recursos primários e secundários com o mesmo nome estão associados à mesma verificação de integridade.

Recommended Action (Ação recomendada)

Se um conjunto de recursos de failover não estiver presente, crie o conjunto de registros de recursos correspondente. Consulte Creating Failover Resource Record Sets (Criar conjuntos de registros de recursos de failover).

Se os conjuntos de registros de recursos estiverem associados à mesma verificação de integridade, crie verificações de integridade separadas para cada uma. Consulte Creating, Updating, and Deleting Health Checks (Criar, atualizar e excluir verificações de integridade).

Recursos adicionais

Amazon Route 53 Health Checks and DNS Failover (Verificações de integridade do Amazon Route 53 e failover de DNS)

Colunas do relatório

- Nome da zona hospedada
- ID da zona hospedada
- Nome do conjunto de registros de recursos
- Tipo do conjunto de registros de recursos
- Motivo

Conjuntos de registros de recursos de TTL alta no Amazon Route 53.

Descrição

Verifica conjuntos de registros de recursos que podem se beneficiar de um valor menor time-to-live (TTL).

TTL é o número de segundos que um conjunto de registros de recursos é armazenado em cache pelos resolvedores de DNS. Quando você especifica uma TTL longa, os resolvedores de DNS demoram mais para solicitar registros DNS atualizados, o que pode causar atrasos desnecessários no redirecionamento do tráfego. Por exemplo, uma TTL longa cria um atraso entre quando o failover de DNS detecta uma falha de endpoint e quando ele responde redirecionando o tráfego.

As zonas hospedadas criadas por AWS serviços não aparecerão nos resultados da sua verificação.

ID da verificação

`C056F80cR3`

Critérios de alerta

- Amarelo: um conjunto de registros de recursos com política de roteamento Failover tem um TTL maior que 60 segundos.

- Amarelo: um conjunto de registros de recursos com uma verificação de integridade associada tem um TTL maior que 60 segundos.

Recommended Action (Ação recomendada)

Insira um valor de TTL de 60 segundos para os conjuntos de registros de recursos listados. Para obter mais informações consulte Working with Resource Record Sets (Trabalhar com conjuntos de registros de recursos).

Recursos adicionais

Amazon Route 53 Health Checks and DNS Failover (Verificações de integridade do Amazon Route 53 e failover de DNS)

Colunas do relatório

- Status
- Nome da zona hospedada
- ID da zona hospedada
- Nome do conjunto de registros de recursos
- Tipo do conjunto de registros de recursos
- ID do conjunto de registros de recursos
- TTL

Delegações do servidor de nomes do Amazon Route 53

Descrição

Verifica as zonas hospedadas do Amazon Route 53 para as quais seu registrador de domínio ou DNS não está usando os servidores de nome corretos do Route 53.

Quando você cria uma zona hospedada, o Route 53 atribui um conjunto de quatro servidores de nome à zona hospedada. Os nomes desses servidores são ns-###.awsdns-##.com, .net, .org e .co.uk, em que ### e ## normalmente representam números diferentes. Para que o Route 53 possa rotear consultas de DNS para o seu domínio, você deverá atualizar a configuração do servidor de nomes da empresa de registro de domínios para remover os servidores de nomes atribuídos pela empresa de registro de domínios. Em seguida, você deverá adicionar todos os quatro servidores de nome no conjunto de delegação do Route 53. Para obter disponibilidade máxima, adicione todos os quatro servidores de nome do Route 53.

As zonas hospedadas criadas por AWS serviços não aparecerão nos resultados da sua verificação.

ID da verificação

`cF171Db240`

Critérios de alerta

Amarelo: uma zona hospedada para a qual o registrador do seu domínio não usa todos os quatro servidores de nomes do Route 53 no conjunto de delegações.

Recommended Action (Ação recomendada)

Adicione ou atualize os registros do servidor de nomes com seu registrador ou com o serviço de DNS atual do seu domínio para incluir todos os quatro servidores de nomes em seu conjunto de delegações do Route 53. Para encontrar esses valores, consulte Getting the Name Servers for a Hosted Zone (Obter os servidores de nomes de uma zona hospedada). Para obter informações sobre como adicionar ou atualizar registros do servidor de nomes, consulte Creating and Migrating Domains and Subdomains to Amazon Route 53 (Criar e migrar domínios e subdomínios para o Amazon Route 53).

Recursos adicionais

Trabalhar com zonas hospedadas

Colunas do relatório

- Nome da zona hospedada
- ID da zona hospedada
- Número de delegações de servidor de nomes usadas

Amazon Route 53 Resolver Redundância da zona de disponibilidade do endpoint

Descrição

Verifica se a configuração do serviço tem endereços IP especificados em pelo menos duas zonas de disponibilidade (AZs) para redundância. Uma AZ é um local distinto, isolado de falhas em outras zonas. Ao especificar endereços IP em várias AZs na mesma região, você pode ajudar a proteger suas aplicações de um único ponto de falha.

ID da verificação

`Chrv231ch1`

Critérios de alerta

- Amarelo: os endereços IP são especificados somente em uma AZ
- Verde: os endereços IP são especificados em pelo menos duas AZs

Recommended Action (Ação recomendada)

Especifique endereços IP em pelo menos duas zonas de disponibilidade para redundância.

Recursos adicionais

- Se você precisar que mais de um endpoint da interface de rede elástica esteja disponível o tempo todo, recomendamos que você crie pelo menos uma interface de rede a mais do que a necessária, para garantir que você tenha capacidade adicional disponível para lidar com possíveis picos de tráfego. A interface de rede adicional também garante a disponibilidade durante as operações de serviço, como manutenção ou atualizações.
- Alta disponibilidade de endpoints do Resolver

Colunas do relatório

- Status
- Região
- Atributo ARN
- Número de AZs

Registro em bucket do Amazon S3

Descrição

Verifica a configuração de registro em log dos buckets do Amazon Simple Storage Service (Amazon S3).

Quando o log de acesso ao servidor está habilitado, os logs de acesso detalhados são entregues de hora em hora para um bucket que você escolher. Um registro de log contém detalhes sobre a solicitação, tais como o tipo da solicitação, os recursos especificados na solicitação e a data e hora em que a solicitação foi processada. Por padrão, o registro em log do bucket não está habilitado. Você deve habilitar o registro em log se quiser realizar auditorias de segurança ou saber mais sobre usuários e padrões de uso.

Quando o registro é inicialmente habilitado, a configuração é validada automaticamente. No entanto, modificações futuras podem resultar em falhas de registro. Essa verificação examina

permissões explícitas de bucket do Amazon S3, mas não examina políticas de bucket associadas que podem substituir as permissões de bucket.

ID da verificação

`BueAdJ7NrP`

Critérios de alerta

- Amarelo: o bucket não tem registro em log de acesso ao servidor habilitado.
- Amarelo: as permissões do bucket de destino não incluem a conta raiz, portanto, não é Trusted Advisor possível verificá-la.
- Vermelho: o bucket de destino não existe.
- Vermelho: o bucket de destino e o bucket de origem têm proprietários diferentes.
- Vermelho: o entregador de logs não tem permissões de gravação no bucket de destino.

Recommended Action (Ação recomendada)

Ative o registro em log do bucket para a maioria dos buckets. Consulte Enabling Logging Using the Console (Habilitar o registro em log usando o console) e Enabling Logging Programmatically (Habilitar o registro em log por programação).

Se as permissões do bucket de destino não incluírem a conta raiz e você Trusted Advisor quiser verificar o status de registro, adicione a conta raiz como beneficiária. Consulte Editing Bucket Permissions (Editar permissões do bucket).

Se o bucket de destino não existir, selecione um bucket existente como destino ou crie um novo bucket e selecione-o. Consulte Managing Bucket Logging (Gerenciar o log de buckets).

Se o destino e a origem tiverem proprietários diferentes, altere o bucket de destino para um que tenha o mesmo proprietário que o bucket de origem. Consulte Managing Bucket Logging (Gerenciar o log de buckets).

Se o entregador de logs não tiver permissões de gravação no destino (gravação não habilitada), conceda permissões de upload/exclusão ao grupo de entrega de logs. Consulte Editing Bucket Permissions (Editar permissões do bucket).

Recursos adicionais

- Working with Buckets (Trabalhar com buckets)
- Server Access Logging (Log de acesso ao servidor)
- Server Access Log Format (Formato do log de acesso ao servidor)

- Deleting Log Files (Excluir arquivos de log)

Colunas do relatório

- Status
- Região
- Nome do bucket
- Nome do destino
- O destino existe
- Mesmo proprietário
- Gravação habilitada
- Motivo

Replicação de bucket do Amazon S3 não habilitada

Descrição

Verifica se seus buckets do Amazon S3 têm regras de replicação habilitadas para replicação entre regiões, replicação na mesma região ou ambas.

A replicação é a cópia automática e assíncrona de objetos entre buckets na mesma região ou em regiões diferentes. AWS A replicação copia os objetos recém-criados e as atualizações de objeto de um bucket de origem para um bucket de destino. Use a replicação de buckets do Amazon S3 para ajudar a melhorar a resiliência e a conformidade de suas aplicações e armazenamento de dados.

Para obter mais informações, consulte Replicação de objetos.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c18d2gz119`

Origem

```
AWS Config Managed Rule: s3-bucket-replication-enabled
```

Critérios de alerta

Amarelo: as regras de replicação de bucket do Amazon S3 não estão habilitadas para replicação entre regiões, replicação na mesma região ou ambas.

Recommended Action (Ação recomendada)

Ative as regras de replicação de bucket do Amazon S3 para melhorar a resiliência e a conformidade de suas aplicações e armazenamento de dados.

Para obter mais informações, consulte View your backup jobs and recovery points e Configuração da replicação.

Recursos adicionais

Passo a passo: exemplos para configurar a replicação

Colunas do relatório

- Status
- Região
- Recurso
- AWS Config Regra
- Parâmetros de entrada
- Hora da última atualização

Versionamento em bucket do Amazon S3

Descrição

Verifica os buckets do Amazon Simple Storage Service que não têm versionamento habilitado ou que têm versionamento suspenso.

Quando o versionamento está habilitado, é possível se recuperar facilimente de ações não intencionais do usuário e de falhas de aplicação. O versionamento permite preservar, recuperar e restaurar todas as versões de cada objeto armazenado em um bucket. É possível usar regras

de ciclo de vida para gerenciar todas as versões de dos objetos, bem como os custos associados, arquivando objetos automaticamente na classe de armazenamento do Glacier. As regras também podem ser configuradas para remover versões de seus objetos após um período especificado. Também é possível exigir autenticação multifator (MFA) para qualquer exclusão de objeto ou alteração de configuração nos buckets.

O versionamento não poderá ser desabilitado depois que ele for habilitado. No entanto, ele poderá ser suspenso, o que impedirá que novas versões de objetos sejam criadas. O uso do versionamento pode aumentar os custos do Amazon S3, pois você pagará pelo armazenamento de várias versões de um objeto.

ID da verificação

`R365s2Qddf`

Critérios de alerta

- Verde: o versionamento está habilitado para o bucket.
- Amarelo: o versionamento não está habilitado para o bucket.
- Amarelo: o versionamento está suspenso para o bucket.

Recommended Action (Ação recomendada)

Habilite o versionamento do bucket na maioria dos buckets para evitar exclusão ou substituição acidental. Consulte Using Versioning (Usar versionamento) e Enabling Versioning Programmatically (Habilitar o versionamento por programação).

Se o versionamento do bucket estiver suspenso, considere reabilitá-lo. Para obter informações sobre como trabalhar com objetos em um bucket com versionamento suspenso, consulte Managing Objects in a Versioning-Suspended Bucket (Gerenciar objetos em um bucket com versionamento suspenso).

Quando o versionamento está habilitado ou suspenso, é possível definir regras de configuração de ciclo de vida para marcar determinadas versões de objeto como expiradas ou remover permanentemente versões de objetos desnecessárias. Para obter mais informações, consulte Gerenciamento do ciclo de vida de objetos.

A exclusão da MFA exige autenticação adicional quando o status de versionamento do bucket é alterado ou quando as versões de um objeto são excluídas. Ela exige que o usuário insira credenciais e um código de um dispositivo de autenticação aprovado. Para obter mais informações, consulte Exclusão MFA.

Recursos adicionais

Working with Buckets (Trabalhar com buckets)

Colunas do relatório

- Status
- Região
- Nome do bucket
- Versionamento
- Exclusão da MFA habilitada

Balanceadores de carga de aplicações, redes e gateways não abrangem várias zonas de disponibilidade

Descrição

Verifica se os balanceadores de carga (balanceador de carga de aplicação, rede e gateway) estão configurados com sub-redes em várias zonas de disponibilidade.

Você pode especificar as zonas de disponibilidade mínimas desejadas nos minAvailabilityZonesparâmetros de suas AWS Config regras.

Para obter mais informações, consulte Availability Zones for your Application Load Balancer, Availability Zones - Network Load Balancers e Create a Gateway Load Balancer.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

```
c18d2gz169
```

Origem

```
AWS Config Managed Rule: elbv2-multiple-az
```

Critérios de alerta

Amarelo: balanceadores de carga de aplicação, rede ou gateway configurados com sub-redes em menos de duas zonas de disponibilidade.

Recommended Action (Ação recomendada)

Configure seus balanceadores de carga de aplicação, rede e gateway com sub-redes em várias zonas de disponibilidade.

Recursos adicionais

Zonas de disponibilidade para seu Application Load Balancer

Zonas de disponibilidade (Elastic Load Balancing)

Criar um Gateway Load Balancer

Colunas do relatório

- Status
- Região
- Recurso
- AWS Config Regra
- Parâmetros de entrada
- Hora da última atualização

IPs disponíveis para ajuste de escala automático em sub-redes

Descrição

Verifica se há IPs disponíveis suficientes entre as sub-redes de destino. Ter IPs suficientes disponíveis para uso ajudaria quando o Auto Scaling Group atingisse seu tamanho máximo e precisasse iniciar instâncias adicionais.

ID da verificação

`Cjxm268ch1`

Critérios de alerta

- Vermelho: o número máximo de instâncias e endereços IP que podem ser criados por um ASG excede o número de endereços IP restantes nas sub-redes configuradas.

- Verde: há endereços IP suficientes disponíveis para a escala restante possível no ASG.

Recommended Action (Ação recomendada)

Aumentar o número de endereços IP disponíveis

Colunas do relatório

- Status
- Região
- Atributo ARN
- Número máximo de instâncias que podem ser criadas
- Número de instâncias disponíveis

Verificação de integridade do grupo de Auto Scaling

Descrição

Examina a configuração da verificação de integridade para grupos do Auto Scaling.

Se o Elastic Load Balancing estiver sendo usado em um grupo do Auto Scaling, a configuração recomendada será habilitar uma verificação de integridade do Elastic Load Balancing. Se uma verificação de integridade do Elastic Load Balancing não estiver sendo usada, o Auto Scaling poderá atuar somente na integridade da instância do Amazon Elastic Compute Cloud (Amazon EC2). O Auto Scaling não atuará na aplicação em execução na instância.

ID da verificação

`CLOG40CD08`

Critérios de alerta

- Amarelo: um grupo do Auto Scaling tem um balanceador de carga associado, mas a verificação de integridade do Elastic Load Balancing não está habilitada.
- Amarelo: um grupo do Auto Scaling não tem um balanceador de carga associado, mas a verificação de integridade do Elastic Load Balancing está habilitada.

Recommended Action (Ação recomendada)

Se o grupo do Auto Scaling tiver um balanceador de carga associado, mas a verificação de integridade do Elastic Load Balancing não estiver habilitada, consulte Add an Elastic Load Balancing Health Check to your Auto Scaling Group (Adicionar uma verificação de integridade do Elastic Load Balancing ao grupo do Auto Scaling).

Se a verificação de integridade do Elastic Load Balancing estiver habilitada, mas nenhum balanceador de carga estiver associado ao grupo do Auto Scaling, consulte Set Up an Auto-Scaled and Load-Balanced Application (Configurar uma aplicação com autoescalabilidade e balanceamento de carga).

Recursos adicionais

Guia do usuário do Amazon EC2 Auto Scaling

Colunas do relatório

- Status
- Região
- Nome do grupo do Auto Scaling
- Balanceador de carga associado
- Verificação de integridade

Recursos do grupo do Auto Scaling

Descrição

Verifica a disponibilidade de recursos associados às configurações de execução e aos grupos do Auto Scaling.

Os grupos do Auto Scaling que apontam para recursos indisponíveis não podem iniciar novas instâncias do Amazon Elastic Compute Cloud (Amazon EC2). Quando configurado corretamente, o Auto Scaling faz com que o número de instâncias do Amazon EC2 aumente perfeitamente durante picos de demanda e diminua automaticamente durante quedas de demanda. Os grupos do Auto Scaling e as configurações de execução que apontam para recursos indisponíveis não funcionam como pretendido.

ID da verificação

`8CNsSllI5v`

Critérios de alerta

- Vermelho: um grupo do Auto Scaling está associado a um balanceador de carga excluído.
- Vermelho: uma configuração de inicialização está associada a uma imagem de máquina da Amazon (AMI) excluída.

Recommended Action (Ação recomendada)

Se o balanceador de carga tiver sido excluído, crie um novo balanceador de carga ou grupo de destino e associe-o ao grupo do Auto Scaling ou crie um novo grupo do Auto Scaling sem o balanceador de carga. Para obter informações sobre como criar um novo grupo do Auto Scaling com um novo balanceador de carga, consulte Set Up an Auto-Scaled and Load-Balanced Application (Configurar uma aplicação com autoescalabilidade e balanceamento de carga). Para obter informações sobre como criar um novo grupo do Auto Scaling sem um balanceador de carga, consulte Create Auto Scaling Group (Criar grupo do Auto Scaling) em Getting Started With Auto Scaling Using the Console (Introdução ao Auto Scaling usando o console).

Se a AMI tiver sido excluída, crie um novo modelo de inicialização ou uma nova versão de modelo de inicialização usando uma AMI válida e associe-a a um grupo do Auto Scaling. Consulte Create Launch Configuration (Criar configuração de inicialização) em Getting Started With Auto Scaling Using the Console (Introdução ao Auto Scaling usando o console).

Recursos adicionais

- Troubleshooting Auto Scaling: Amazon EC2 AMIs (Solução de problemas do Auto Scaling: AMIs do Amazon EC2).
- Troubleshooting Auto Scaling: Load Balancer Configuration (Solução de problemas do Auto Scaling: Configuração do balanceador de carga)
- Guia do usuário do Amazon EC2 Auto Scaling

Colunas do relatório

- Status
- Região
- Nome do grupo do Auto Scaling
- Tipo de execução
- Tipo de recurso
- Nome do recurso

Clusters do AWS CloudHSM que executam instâncias do HSM em uma única AZ

Descrição

Verifica clusters que executam instâncias do HSM em uma única zona de disponibilidade (AZ). Essa verificação alerta você se seus clusters correm o risco de não ter o backup mais recente.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`hc0dfs7601`

Critérios de alerta

- Amarelo: um cluster do CloudHSM está executando todas as instâncias do HSM em uma única zona de disponibilidade há mais de uma hora.
- Verde: um cluster do CloudHSM está executando todas as instâncias do HSM em pelo menos duas zonas de disponibilidade diferentes.

Recommended Action (Ação recomendada)

Crie pelo menos mais uma instância para o cluster em outra zona de disponibilidade.

Recursos adicionais

Melhores práticas para AWS CloudHSM

Colunas do relatório

- Status
- Região
- ID do cluster
- Número de instâncias do HSM
- Hora da última atualização

AWS Direct Connect Redundância de conexão

Descrição

Verifica Regiões da AWS se tem apenas uma AWS Direct Connect conexão. A conectividade com seus AWS recursos deve ter duas conexões Direct Connect configuradas o tempo todo para fornecer redundância no caso de um dispositivo não estar disponível.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas.

ID da verificação

`0t121N1Ty3`

Critérios de alerta

Amarelo: Região da AWS Tem apenas uma AWS Direct Connect conexão.

Recommended Action (Ação recomendada)

Configure uma conexão Direct Connect adicional Região da AWS para proteger contra a indisponibilidade do dispositivo. Para obter mais informações, consulte Configure Redundant Connections with AWS Direct Connect. Para se proteger contra a indisponibilidade de sites e adicionar redundância de local, configure a conexão do Direct Connect adicional em um local diferente do Direct Connect.

Recursos adicionais

- Conceitos básicos do AWS Direct Connect
- Perguntas frequentes sobre o AWS Direct Connect

Colunas do relatório

- Status
- Região
- Marca de hora
- Local
- ID da conexão

AWS Direct Connect Redundância de localização

Descrição

Verifica Regiões da AWS com uma ou mais AWS Direct Connect conexões e apenas um AWS Direct Connect local. A conectividade com seus AWS recursos deve ter conexões Direct Connect

configuradas em diferentes locais do Direct Connect para fornecer redundância caso um local não esteja disponível.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas.

ID da verificação

`8M012Ph3U5`

Critérios de alerta

Amarelo: As conexões Direct Connect no não Região da AWS estão configuradas em locais diferentes.

Recommended Action (Ação recomendada)

Configure uma conexão do Direct Connect adicional em um local diferente do Direct Connect para se proteger contra indisponibilidade de locais. Para obter mais informações, consulte Introdução ao AWS Direct Connect.

Recursos adicionais

- Conceitos básicos do AWS Direct Connect
- Perguntas frequentes sobre o AWS Direct Connect

Colunas do relatório

- Status
- Região
- Marca de hora
- Local
- Detalhes da conexão

AWS Direct Connect Resiliência de localização

Descrição

Verifica a resiliência da AWS Direct Connect localização associada a cada um dos seus gateways privados virtuais ou gateways de trânsito.

Essa verificação alerta você se algum dos seus gateways privados virtuais ou gateways Direct Connect não estiver configurado para usar pelo menos dois locais do Direct Connect. A falta de resiliência do local pode resultar em tempo de inatividade inesperado e em uma experiência de conectividade ruim.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas.

ID da verificação

`c1dfpnchv2`

Critérios de alerta

Vermelho: O gateway privado virtual ou o gateway Direct Connect não tem interfaces virtuais configuradas para se conectar a dispositivos em vários locais do Direct Connect.

Amarelo: o gateway privado virtual ou o gateway Direct Connect é configurado com várias interfaces virtuais para se conectar a dispositivos diferentes no mesmo local do Direct Connect. Mas ele não está configurado para se conectar a dispositivos em vários locais do Direct Connect.

Verde: o gateway privado virtual ou o gateway Direct Connect está configurado para utilizar pelo menos dois locais do Direct Connect.

Recommended Action (Ação recomendada)

Para criar resiliência de localização do Direct Connect, você pode configurar o gateway privado virtual ou o gateway Direct Connect para se conectar a pelo menos dois locais distintos do Direct Connect. Para obter mais informações, consulte Recomendação de AWS Direct Connect resiliência.

Recursos adicionais

AWS Direct Connect Recomendações de resiliência

AWS Direct Connect Teste de failover

Colunas do relatório

- Status
- Região
- Hora da última atualização
- Status de resiliência
- Local
- ID da conexão
- ID do Gateway

AWS Direct Connect Redundância de interface virtual

Descrição

Verifica se há gateways privados virtuais com interfaces AWS Direct Connect virtuais (VIFs) que não estão configuradas em pelo menos duas AWS Direct Connect conexões. A conectividade com o gateway privado virtual deve ter várias VIFs configuradas em várias conexões e locais do Direct Connect. Isso fornece redundância no caso de um dispositivo ou local não estar disponível.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas.

ID da verificação

`4g3Nt5M1Th`

Critérios de alerta

Amarelo: um gateway privado virtual tem menos de duas interfaces virtuais ou as interfaces não estão configuradas para várias conexões do Direct Connect.

Recommended Action (Ação recomendada)

Configure pelo menos duas interfaces virtuais configuradas para duas conexões do Direct Connect para se proteger contra indisponibilidade de dispositivos ou locais. Consulte Create a Virtual Interface (Criar uma interface virtual).

Recursos adicionais

- Conceitos básicos do AWS Direct Connect
- Perguntas frequentes sobre o AWS Direct Connect
- Trabalhando com interfaces AWS Direct Connect virtuais

Colunas do relatório

- Status
- Região
- Marca de hora
- ID do Gateway
- Local para VIF
- ID da conexão para VIF

AWS Lambda funções sem uma fila de mensagens mortas configurada

Descrição

Verifica se uma AWS Lambda função está configurada com uma fila de mensagens mortas.

Uma fila de mensagens mortas é um recurso AWS Lambda que permite capturar e analisar eventos com falha, fornecendo uma maneira de lidar com esses eventos adequadamente. Seu código pode gerar uma exceção, expirar ou ficar sem memória, resultando em falhas nas execuções assíncronas da sua função do Lambda. Uma fila de mensagens não entregues armazena mensagens de invocações com falha, fornecendo uma maneira de lidar com as mensagens e solucionar as falhas.

Você pode especificar o recurso de fila de mensagens mortas que deseja verificar usando o parâmetro DLQArns em suas regras. AWS Config

Para obter mais informações, consulte Filas de mensagens não entregues.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c18d2gz182`

Origem

`AWS Config Managed Rule: lambda-dlq-check`

Critérios de alerta

Amarelo: AWS Lambda a função não tem fila de mensagens mortas configurada.

Recommended Action (Ação recomendada)

Certifique-se de que suas AWS Lambda funções tenham uma fila de mensagens mortas configurada para controlar o tratamento de mensagens para todas as invocações assíncronas com falha.

Para obter mais informações, consulte Filas de mensagens não entregues.

Recursos adicionais

- Robust Serverless Application Design with AWS Lambda Dead Letter Queues

Colunas do relatório

- Status
- Região
- Recurso
- AWS Config Regra
- Parâmetros de entrada
- Hora da última atualização

AWS Lambda Sobre destinos de eventos de falha

Descrição

Verifica se as funções do Lambda em sua conta têm o destino do evento com falha ou a fila de mensagens não entregues (DLQ) configurados para invocações assíncronas, para que os registros de invocações com falha possam ser encaminhados a um destino para posterior investigação ou processamento.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c1dfprch05`

Critérios de alerta

- Amarelo: a função não tem nenhum destino de evento com falha ou a DLQ configurados.

Recommended Action (Ação recomendada)

Configure o destino do evento com falha ou a DLQ para que suas funções do Lambda enviem invocações com falha junto com outros detalhes para um dos serviços de destino da AWS disponíveis para depuração ou processamento adicionais.

Recursos adicionais

- Invocação assíncrona
- AWS Lambda Sobre destinos de eventos de falha

Colunas do relatório

- Status
- Região
- A função com a versão que está sinalizada.
- Percentual de redução de solicitações assíncronas no dia atual
- Solicitações assíncronas do dia atual
- Percentual médio diário de redução de solicitações assíncronas

- Média diária de solicitações assíncronas
- Hora da última atualização

O AWS Lambda habilitado para VPC funciona sem redundância Multi-AZ

Descrição

Verifica a versão $LATEST das funções Lambda habilitadas para VPC que são vulneráveis à interrupção do serviço em uma única zona de disponibilidade. É uma prática recomendada que as funções habilitadas para VPC estejam conectadas a várias zonas de disponibilidade para alta disponibilidade.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`L4dfs2Q4C6`

Critérios de alerta

Amarelo: a versão $LATEST de uma função Lambda habilitada para VPC está conectada a sub-redes em uma única zona de disponibilidade.

Recommended Action (Ação recomendada)

Ao configurar funções para acessar sua VPC, escolha sub-redes em várias zonas de disponibilidade para garantir alta disponibilidade.

Recursos adicionais

- Configurar uma função do Lambda para acessar recursos em uma VPC
- Resiliência em AWS Lambda

Colunas do relatório

- Status
- Região
- ARN da função

- ID da VPC
- Invocações médias diárias
- Hora da última atualização

AWS Resilience Hub Verificação de componentes do aplicativo

Descrição

Verifica se um componente do aplicativo (AppComponent) em seu aplicativo é irrecuperável. Se um AppComponent não se recuperar no caso de um evento de interrupção, você poderá experimentar perda de dados desconhecida e tempo de inatividade do sistema.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas.

ID da verificação

`RH23stmM04`

Critérios de alerta

Vermelho: AppComponent é irrecuperável.

Recommended Action (Ação recomendada)

Para garantir que seu AppComponent seja recuperável, analise e implemente as recomendações de resiliência e, em seguida, execute uma nova avaliação. Para obter mais informações sobre a revisão das recomendações de resiliência, consulte Recursos adicionais.

Recursos adicionais

Analisando as recomendações de resiliência

Conceitos AWS Resilience Hub

AWS Resilience Hub Guia do usuário

Colunas do relatório

- Status

- Região
- Nome da aplicação
- AppComponent Nome
- Hora da última atualização

AWS Resilience Hub política violada

Descrição

Verifica se o Resilience Hub tem aplicações que não atendem ao objetivo de tempo de recuperação (RTO) e ao objetivo de ponto de recuperação (RPO) definidos pela política. A verificação alertará você se sua aplicação não atender aos objetivos de RTO e RPO que você definiu para uma aplicação no Resilience Hub.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente, e não são permitidas solicitações de atualização. Não é possível excluir recursos dessa verificação.

ID da verificação

`RH23stmM02`

Critérios de alerta

- Verde: a aplicação tem uma política e atende aos objetivos de RTO e RPO.
- Amarelo: a aplicação ainda não foi avaliada.
- Vermelho: a aplicação tem uma política, mas não atende aos objetivos de RTO e RPO.

Recommended Action (Ação recomendada)

Faça login no console do Resilience Hub e analise as recomendações para que sua aplicação atenda aos objetivos de RTO e RPO.

Recursos adicionais

Conceitos do Resilience Hub

Colunas do relatório

- Status

- Região
- Nome da aplicação
- Hora da última atualização

AWS Resilience Hub pontuações de resiliência

Descrição

Verifique se você realizou uma avaliação para suas aplicações no Resilience Hub. Essa verificação alerta você quando suas pontuações de resiliência estão abaixo de um valor específico.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente, e não são permitidas solicitações de atualização. Não é possível excluir recursos dessa verificação.

ID da verificação

`RH23stmM01`

Critérios de alerta

- Verde: sua aplicação tem uma pontuação de resiliência de 70 ou superior.
- Amarelo: sua aplicação tem uma pontuação de resiliência de 40 a 69.
- Amarelo: a aplicação ainda não foi avaliada.
- Vermelho: sua aplicação tem uma pontuação de resiliência inferior a 40.

Recommended Action (Ação recomendada)

Faça login no console do Resilience Hub e faça uma avaliação para sua aplicação. Leia as recomendações para melhorar a pontuação de resiliência.

Recursos adicionais

Conceitos do Resilience Hub

Colunas do relatório

- Status

- Região
- Nome da aplicação
- Pontuação de resiliência da aplicação
- Hora da última atualização

AWS Resilience Hub idade de avaliação

Descrição

Verifica há quanto tempo você realizou uma avaliação da aplicação pela última vez. Essa verificação alerta você caso não tenha executado uma avaliação da aplicação por um determinado número de dias.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`RH23stmM03`

Critérios de alerta

- Verde: sua avaliação da aplicação foi executada nos últimos 30 dias.
- Amarelo: sua avaliação da aplicação não foi executada nos últimos 30 dias.

Recommended Action (Ação recomendada)

Faça login no console do Resilience Hub e faça uma avaliação para sua aplicação.

Recursos adicionais

Conceitos do Resilience Hub

Colunas do relatório

- Status
- Região
- Nome da aplicação

- Dias desde a execução da última avaliação
- Tempo de execução da última avaliação
- Hora da última atualização

AWS Site-to-Site VPN tem pelo menos um túnel no status DOWN

Descrição

Verifica o número de túneis ativos para cada um dos seus s. AWS Site-to-Site VPN

Uma VPN sempre deve ter dois túneis configurados. Isso fornece redundância em caso de interrupção ou manutenção planejada dos dispositivos no endpoint da AWS. Para alguns hardware, apenas um túnel fica ativo de cada vez. Se uma VPN não tiver túneis ativos, as cobranças da VPN ainda poderão ser aplicadas.

Para obter mais informações, consulte O que é o AWS Site-to-Site VPN?

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

```
c18d2gz123
```

Origem

```
AWS Config Managed Rule: vpc-vpn-2-tunnels-up
```

Critérios de alerta

Amarelo: uma Site-to-Site VPN tem pelo menos um túnel DESATIVADO.

Recommended Action (Ação recomendada)

Certifique-se de que dois túneis estejam configurados para conexões VPN. E, se o seu hardware suportar, verifique se os dois túneis estão ativos. Caso não precise mais de uma conexão VPN, exclua-a para evitar cobranças.

Para obter mais informações, consulte O dispositivo de gateway do cliente e o conteúdo disponível no Centro de Conhecimentos da AWS.

Recursos adicionais

- AWS Site-to-Site VPN Guia do usuário
- Adicionar um gateway privado virtual à VPC

Colunas do relatório

- Status
- Região
- Recurso
- AWS Config Regra
- Parâmetros de entrada
- Hora da última atualização

Problemas de alto risco do AWS Well-Architected em relação à confiabilidade

Descrição

Verifica problemas de alto risco (HRIs – high risk issues) de suas workloads no pilar Confiabilidade. Essa verificação é baseada nas suas análises AWS-Well Architected. Os resultados da verificação dependem de você ter concluído ou não a avaliação da workload com o AWS Well-Architected.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`Wxdfp4B1L4`

Critérios de alerta

- Vermelho: Pelo menos um problema ativo de alto risco foi identificado no pilar de confiabilidade do AWS Well-Architected.

- Verde: Nenhum problema ativo de alto risco foi detectado no pilar de confiabilidade do AWS Well-Architected.

Recommended Action (Ação recomendada)

AWS O Well-Architected detectou problemas de alto risco durante a avaliação da carga de trabalho. Esses problemas apresentam oportunidades para reduzir riscos e economizar dinheiro. Faça login na ferramenta AWS Well-Architected para revisar suas respostas e adotar medidas para resolver seus problemas ativos.

Colunas do relatório

- Status
- Região
- ARN da workload
- Nome da workload
- Nome do revisor
- Tipo de workload
- Data de início da workload
- Data da última modificação da workload
- Número de problemas de alto risco identificados para confiabilidade
- Número de problemas de alto risco resolvidos para confiabilidade
- Número de perguntas respondidas para confiabilidade
- Número total de perguntas no pilar de confiabilidade
- Hora da última atualização

O Classic Load Balancer não tem várias AZs configuradas

Descrição

Verifica se o Classic Load Balancer abrange várias zonas de disponibilidade (AZs).

O balanceador de carga distribui o tráfego de entrada da aplicação entre várias instâncias do Amazon EC2 em diversas zonas de disponibilidade. Por padrão, o load balancer distribui tráfego uniformemente entre as Zonas de disponibilidade que você habilitar para o load balancer. Se uma zona de disponibilidade sofrer uma interrupção, os nós do balanceador de carga encaminharão automaticamente as solicitações para as instâncias íntegras registradas em uma ou mais zonas de disponibilidade.

Você pode ajustar o número mínimo de zonas de disponibilidade usando o minAvailabilityZonesparâmetro em suas AWS Config regras

Para obter mais informações, consulte O que é o Classic Load Balancer?

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c18d2gz154`

Origem

`AWS Config Managed Rule: clb-multiple-az`

Critérios de alerta

Amarelo: o Classic Load Balancer não tem multi-AZ configurado ou não atende ao número mínimo de AZs especificado.

Recommended Action (Ação recomendada)

Certifique-se de que seus Classic Load Balancers tenham várias zonas de disponibilidade configuradas. Distribua seu balanceador de carga entre várias AZs para garantir que você tenha alta disponibilidade da sua aplicação.

Para obter mais informações, consulte Tutorial: criar um Classic Load Balancer

Colunas do relatório

- Status
- Região
- Recurso
- AWS Config Regra
- Parâmetros de entrada
- Hora da última atualização

Descarga de conexão do ELB

Descrição

Verifica se há balanceadores de carga que não têm descarga de conexão habilitada.

Quando a descarga de conexão não está habilitada e você cancela o registro de uma instância do Amazon EC2 de um balanceador de carga, o balanceador de carga interrompe o roteamento do tráfego para essa instância e fecha a conexão. Quando a descarga de conexão está habilitada, o balanceador de carga para de enviar novas solicitações para a instância cancelada, mas mantém a conexão aberta para atender as solicitações ativas.

ID da verificação

`7qGXsKIUw`

Critérios de alerta

Amarelo: a drenagem da conexão não está habilitada para um balanceador de carga.

Recommended Action (Ação recomendada)

Habilite a drenagem de conexão para o balanceador de carga. Para obter mais informações, consulte Connection Draining (Drenagem da conexão) e Enable or Disable Connection Draining for Your Load Balancer (Habilitar ou desabilitar a drenagem de conexões para o balanceador de carga).

Recursos adicionais

Elastic Load Balancing Concepts (Conceitos do Elastic Load Balancing)

Colunas do relatório

- Status
- Região
- Nome do balanceador de carga
- Motivo

Balanceamento de carga entre zonas do ELB

Descrição

Com o balanceamento de carga entre zonas desabilitado, existe o risco de indisponibilidade do serviço devido à distribuição desigual do tráfego ou à sobrecarga de backend. Esse

problema pode ocorrer quando os clientes armazenam incorretamente informações de DNS. O problema também pode ocorrer quando há um número desigual de instâncias em cada zona de disponibilidade (por exemplo, se você tiver retirado algumas instâncias para manutenção).

ID da verificação

`xdeXZKIUy`

Critérios de alerta

Amarelo: o balanceamento de carga entre zonas não está habilitado para um balanceador de carga.

Recommended Action (Ação recomendada)

Confirme se as instâncias do Amazon EC2 registradas com o balanceador de carga são iniciadas em várias zonas de disponibilidade e, em seguida, habilite o balanceamento de carga entre zonas para o balanceador de carga. Para obter mais informações, consulte Availability Zones and Regions (Zonas de disponibilidade e regiões) e Enable or Disable Cross-Zone Load Balancing for Your Load Balancer (Habilitar ou desabilitar o balanceamento de carga entre zonas para o balanceador de carga).

Recursos adicionais

- Request Routing (Roteamento de solicitações)
- Elastic Load Balancing Concepts (Conceitos do Elastic Load Balancing)

Colunas do relatório

- Status
- Região
- Nome do balanceador de carga
- Motivo

Otimização do Load Balancer

Descrição

Verifica a configuração do balanceador de carga.

Para ajudar a aumentar o nível de tolerância a falhas no Amazon Elastic Compute Cloud (Amazon EC2) ao usar o Elastic Load Balancing, recomendamos a execução de um número igual de instâncias em várias zonas de disponibilidade de uma região. Um balanceador de

carga configurado acumula cobranças, portanto, essa é uma verificação de otimização de custo também.

ID da verificação

`iqdCTZKCUp`

Critérios de alerta

- Amarelo: um balanceador de carga está habilitado para uma única zona de disponibilidade.
- Amarelo: um balanceador de carga está habilitado para uma zona de disponibilidade que não tem instâncias ativas.
- Amarelo: as instâncias do Amazon EC2 registradas com um balanceador de carga estão distribuídas de forma desigual entre as zonas de disponibilidade. (A diferença entre a maior e a menor contagem de instâncias nas zonas de disponibilidade utilizadas é maior que 1 e superior a 20% da contagem mais alta.)

Recommended Action (Ação recomendada)

Certifique-se de que o balanceador de carga aponte para instâncias ativas e íntegras em pelo menos duas zonas de disponibilidade. Para obter mais informações sobre zonas de disponibilidade, consulte Add Availability Zone (Adicionar zona de disponibilidade).

Se o balanceador de carga estiver configurado para uma zona de disponibilidade sem instâncias íntegras ou se houver um desequilíbrio de instâncias entre as zonas de disponibilidade, determine se todas as zonas de disponibilidade serão necessárias. Omita quaisquer zonas de disponibilidade desnecessárias e garanta que haja uma distribuição equilibrada de instâncias entre as zonas de disponibilidade restantes. Para obter mais informações, consulte Remove Availability Zone (Remover zona de disponibilidade).

Recursos adicionais

- Availability Zones and Regions (Zonas de disponibilidade e regiões)
- Managing Load Balancers (Gerenciar balanceadores de carga)
- Best Practices in Evaluating Elastic Load Balancing (Práticas recomendadas de avaliação do Elastic Load Balancing)

Colunas do relatório

- Status
- Região
- Nome do balanceador de carga

- Nº de zonas
- Instâncias da zona a
- Instâncias da zona b
- Instâncias da zona c
- Instâncias da zona d
- Instâncias da zona e
- Instâncias da zona f
- Motivo

Independência da AZ do NAT Gateway

Descrição

Verifica se seus NAT Gateways estão configurados com independência da zona de disponibilidade (AZ).

Um NAT Gateway permite que os recursos em sua sub-rede privada se conectem com segurança a serviços fora da sub-rede usando os endereços IP do NAT Gateway e eliminem qualquer tráfego de entrada não solicitado. Cada NAT Gateway opera em uma zona de disponibilidade (AZ) designada e é criado com redundância somente nessa AZ. Portanto, seus recursos em uma determinada AZ devem usar um NAT Gateway na mesma AZ para que qualquer possível interrupção de um NAT Gateway ou de sua AZ não afete seus recursos em outra AZ.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c1dfptbg10`

Critérios de alerta

- Vermelho: o tráfego da sua sub-rede em uma AZ está sendo roteado por meio de um NATGW em outra AZ.

- Vermelho: o tráfego da sua sub-rede em uma AZ está sendo roteado por meio de um NATGW na mesma AZ.

Recommended Action (Ação recomendada)

Verifique a AZ da sua sub-rede e roteie o tráfego por meio de um NAT Gateway na mesma AZ.

Se não houver nenhum NATGW na AZ, crie um e direcione seu tráfego de sub-rede por ele.

Se você tiver a mesma tabela de rotas associada a sub-redes em diferentes AZs, mantenha essa tabela de rotas associada às sub-redes que residem na mesma AZ do NAT Gateway e, para sub-redes na outra AZ, associe uma tabela de rotas separada a uma rota para um NAT Gateway nessa outra AZ.

Recomendamos escolher uma janela de manutenção para mudanças de arquitetura em sua Amazon VPC.

Recursos adicionais

- Como criar um NAT Gateway
- Como configurar rotas para diferentes casos de uso do NAT Gateway

Colunas do relatório

- Status
- Região
- Zona de disponibilidade da NAT
- ID da NAT
- Zona de disponibilidade de sub-rede
- ID da sub-rede
- ID da tabela de rotas
- ARN da NAT
- Hora da última atualização

Balanceamento de carga cruzada dos Network Load Balancers

Descrição

Verifica se o balanceamento de carga entre zonas está habilitado nos Network Load Balancers.

O balanceamento de carga entre zonas ajuda a manter uma distribuição uniforme do tráfego de entrada entre instâncias em diferentes zonas de disponibilidade. Isso impede que o balanceador de carga roteie todo o tráfego para instâncias na mesma zona de disponibilidade, o que pode causar uma distribuição desigual do tráfego e uma possível sobrecarga. O recurso também ajuda na confiabilidade da aplicação ao rotear automaticamente o tráfego para instâncias íntegras em outras zonas de disponibilidade no caso de uma falha em uma única zona de disponibilidade.

Para obter mais informações, consulte Cross-zone load balancing.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c18d2gz105`

Origem

`AWS Config Managed Rule: nlb-cross-zone-load-balancing-enabled`

Critérios de alerta

- Amarelo: o Network Load Balancer não tem o balanceamento de carga entre zonas habilitado.

Recommended Action (Ação recomendada)

Certifique-se de que o balanceamento de carga entre zonas esteja habilitado nos Network Load Balancers.

Recursos adicionais

Balanceamento de carga entre zonas (Network Load Balancers)

Colunas do relatório

- Status
- Região
- Recurso
- AWS Config Regra

- Parâmetros de entrada
- Hora da última atualização

NLB - Recurso voltado para a Internet em sub-rede privada

Descrição

Verifica se um Network Load Balancer (NLB) voltado para a Internet está configurado com uma sub-rede privada. Um Network Load Balancer (NLB) voltado para a Internet deve ser configurado em sub-redes públicas para receber tráfego. Uma sub-rede pública é definida como uma sub-rede que tem uma rota direta para um gateway da Internet. Se a sub-rede estiver configurada como privada, sua Zona de Disponibilidade (AZ) não receberá tráfego, o que pode causar problemas de disponibilidade.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c1dfpnchv4`

Critérios de alerta

Vermelho: o NLB está configurado com uma ou mais sub-redes privadas

Verde: Nenhuma sub-rede privada está configurada para NLB voltado para a Internet

Recommended Action (Ação recomendada)

Confirme se as sub-redes configuradas em um balanceador de carga voltado para a Internet são públicas. Uma sub-rede pública é definida como uma sub-rede que tem uma rota direta para um gateway da Internet. Use uma das seguintes opções:

- Crie um novo balanceador de carga e selecione uma sub-rede diferente com uma rota direta para um gateway da Internet.
- Altere a sub-rede atualmente conectada ao balanceador de carga de privada para pública. Para fazer isso, altere sua tabela de rotas e associe um gateway de internet.

Recursos adicionais

- Configurar um balanceador de carga e um ouvinte
- Sub-redes para sua VPC
- Associar um gateway a uma tabela de rotas

Colunas do relatório

- Status
- Região
- Braço do NLB
- Nome do NLB
- ID da sub-rede
- Esquema NLB
- Tipo de sub-rede
- Hora da última atualização

NLB Multi-AZ

Descrição

Verifica se seus balanceadores de carga de rede estão configurados para usar mais de uma zona de disponibilidade (AZ). Uma AZ é um local distinto, isolado de falhas em outras zonas. Configure seu balanceador de carga em várias AZs na mesma região para ajudar a melhorar a disponibilidade da carga de trabalho.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c1dfprch09`

Critérios de alerta

Amarelo: o NLB está em um único AZ.

Verde: o NLB tem duas ou mais AZs.

Recommended Action (Ação recomendada)

Certifique-se de que seu balanceador de carga esteja configurado com pelo menos duas zonas de disponibilidade.

Recursos adicionais

Para obter mais informações, consulte a seguinte documentação do :

- Zonas de disponibilidade
- AWS Well-Architected - Implemente a carga de trabalho em vários locais
- Regiões e zonas de disponibilidade

Colunas do relatório

- Status
- Região
- Número de AZs
- ARN DO NLB
- Nome do NLB
- Hora da última atualização

Número de Regiões da AWS em um conjunto de replicação do Incident Manager

Descrição

Verifica se a configuração de um conjunto de replicação do Incident Manager usa mais de um Região da AWS para oferecer suporte ao failover e à resposta regionais. Para incidentes criados por CloudWatch alarmes ou EventBridge eventos, o Incident Manager cria um incidente da mesma forma que a Região da AWS regra de alarme ou evento. Se o Incident Manager estiver temporariamente indisponível nessa região, o sistema tentará criar um incidente em outra região no conjunto de replicação. Se o conjunto de replicação incluir somente uma região, o sistema não conseguirá criar um registro de incidente enquanto o Incident Manager estiver indisponível.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`cIdfp1js9r`

Critérios de alerta

- Verde: o conjunto de replicação contém mais de uma região.
- Amarelo: o conjunto de replicação contém uma região.

Recommended Action (Ação recomendada)

Adicione pelo menos mais uma região ao conjunto de replicação.

Recursos adicionais

Para obter mais informações, consulte Cross-region Incident management.

Colunas do relatório

- Status
- Multirregião
- Conjunto de replicação
- Hora da última atualização

Verificação de aplicação de AZ única

Descrição

Verifica, por meio de padrões de rede, se o tráfego de saída da rede está sendo roteado por uma única zona de disponibilidade (AZ).

Uma AZ é um local distinto, isolado de qualquer impacto em outras zonas. Ao distribuir seu serviço em várias AZs, você limita o raio de ação de uma falha na AZ.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c1dfptbg11`

Critérios de alerta

- Amarelo: sua aplicação pode ser implantada em apenas uma AZ com base nos padrões de rede de saída observados. Se isso for verdade e sua aplicação esperar alta disponibilidade, recomendamos que você provisione os recursos da aplicação e implemente seus fluxos de rede para utilizar várias zonas de disponibilidade.

Recommended Action (Ação recomendada)

Se sua aplicação exigir alta disponibilidade, considere implementar uma arquitetura multi-AZ para aumentar a disponibilidade.

Colunas do relatório

- Status
- Região
- ID da VPC
- Hora da última atualização

Interface VPC, endpoint, interfaces de rede em várias AZs

Descrição

Verifica se os endpoints da interface AWS PrivateLink VPC estão configurados para usar mais de uma zona de disponibilidade (AZ). Uma AZ é um local distinto, isolado de falhas em outras zonas. Isso oferece suporte à conectividade de rede barata e de baixa latência entre AZs na mesma região. AWS Selecione sub-redes em várias AZs ao criar endpoints de interface para ajudar a proteger seus aplicativos contra um único ponto de falha.

> **Note**
>
> Atualmente, essa verificação inclui somente endpoints de interface.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c1dfprch10`

Critérios de alerta

Amarelo: o VPC endpoint está em uma única AZ.

Verde: o VPC endpoint está em pelo menos duas AZs.

Recommended Action (Ação recomendada)

Certifique-se de que seu endpoint de interface VPC esteja configurado com pelo menos duas zonas de disponibilidade.

Recursos adicionais

Para obter mais informações, consulte a seguinte documentação do :

- Acesse um AWS serviço usando uma interface VPC endpoint
- Endereço IP privado da interface de rede do endpoint
- AWS PrivateLink conceitos
- Regiões e zonas de disponibilidade

Colunas do relatório

- Status
- Região
- ID do VPC Endpoint
- É Multi AZ

- Hora da última atualização

Redundância de túnel da VPN

Descrição

Verifica o número de túneis ativos para cada uma de suas VPNs.

Uma VPN sempre deve ter dois túneis configurados. Isso fornece redundância em caso de interrupção ou manutenção planejada dos dispositivos no endpoint AWS . Para alguns hardware, apenas um túnel fica ativo de cada vez. Se uma VPN não tiver túneis ativos, as cobranças da VPN ainda poderão ser aplicadas. Para obter mais informações, consulte o Guia do administrador do AWS Client VPN.

ID da verificação

`S45wrEXrLz`

Critérios de alerta

- Amarelo: uma VPN tem um túnel ativo (isso é normal para alguns dispositivos de hardware).
- Amarelo: uma VPN não tem túneis ativos.

Recommended Action (Ação recomendada)

Certifique-se de que dois túneis estejam configurados para sua conexão VPN e que ambos estejam ativos se o seu hardware for compatível. Caso não precise mais de uma conexão VPN, exclua-a para evitar cobranças desnecessárias. Para obter mais informações, consulte Your Customer Gateway (Seu gateway do cliente) ou Deleting a VPN connection (Excluir uma conexão VPN).

Recursos adicionais

- AWS Guia do usuário da VPN Site-to-Site
- Adicionar um hardware de gateway privado virtual à VPC

Colunas do relatório

- Status
- Região
- ID da VPN
- VPC
- Gateway privado virtual

- Gateway do cliente
- Túneis ativos
- Motivo

Redundância de zona de disponibilidade do ActiveMQ

Descrição

Verifica se os agentes do Amazon MQ for ActiveMQ estão configurados para alta disponibilidade com um agente ativo ou em espera em várias zonas de disponibilidade.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c1t3k8mqv1`

Critérios de alerta

- Amarelo: um agente do Amazon MQ for ActiveMQ está configurado em uma única zona de disponibilidade.

  Verde: um agente do Amazon MQ for ActiveMQ está configurado em pelo menos duas zonas de disponibilidade.

Recommended Action (Ação recomendada)

Crie um novo agente com o modo de implantação ativo ou em espera.

Recursos adicionais

- Criar um agente do ActiveMQ

Colunas do relatório

- Status
- Região
- ID do agente do ActiveMQ

- Tipo de mecanismo de agente
- Modo de implantação
- Hora da última atualização

Redundância de zona de disponibilidade do RabbitMQ

Descrição

Verifica se os agentes do Amazon MQ for RabbitMQ estão configurados para alta disponibilidade com instâncias de cluster em várias zonas de disponibilidade.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c1t3k8mqv2`

Critérios de alerta

- Amarelo: um agente do Amazon MQ for RabbitMQ está configurado em uma única zona de disponibilidade.

  Verde: um agente do Amazon MQ for RabbitMQ está configurado em várias zonas de disponibilidade.

Recommended Action (Ação recomendada)

Crie um novo agente com o modo de implantação de cluster.

Recursos adicionais

- Criar um agente do RabbitMQ

Colunas do relatório

- Status
- Região
- ID do agente do RabbitMQ

- Tipo de mecanismo de agente
- Modo de implantação
- Hora da última atualização

Limites do serviço

Consulte as verificações a seguir para a categoria de limites do serviço (também conhecida como cotas).

Todas as verificações nesta categoria têm as seguintes descrições:

Critérios de alerta

- Amarelo: 80% do limite atingido.
- Vermelho: 100% do limite atingido.
- Azul: o Trusted Advisor não conseguiu recuperar a utilização ou os limites em uma ou mais Regiões da AWS.

Recommended Action (Ação recomendada)

Se você espera exceder um limite de serviço, solicite um aumento diretamente no console do Service Quotas. Se o Service Quotas ainda não oferecer suporte ao seu serviço, você poderá criar um caso de suporte na Central de suporte.

Colunas do relatório

- Status
- Serviço
- Região
- Valor do limite
- Uso atual

> **Note**
>
> - Os valores são baseados em snapshots, portanto seu uso atual pode ser diferente. Os dados de cota e uso podem levar até 24 horas para refletir qualquer alteração. Nos casos em que as cotas foram recentemente aumentadas, é possível ver temporariamente a utilização que excede a cota.

Nomes da verificação

- Grupos de Auto Scaling
- Configurações de execução do Auto Scaling
- CloudFormation Pilhas
- Capacidade de leitura do DynamoDB
- Capacidade de gravação do DynamoDB
- Eventos de snapshot do EBS
- Armazenamento de volume EBS de disco rígido frio (sc1)
- Armazenamento de volume EBS (gp2) de uso geral SSD
- Armazenamento de volumes SSD de uso geral (gp3) do EBS
- Armazenamento de volume (padrão) magnético EBS
- IOPS agregadas do volume de IOPS provisionadas (SSD) do EBS
- Armazenamento de volumes SSD de IOPS provisionadas (io1) do EBS
- Armazenamento de volumes SSD de IOPS provisionadas (io2) do EBS
- Armazenamento de volume HDD otimizados para throughput (st1) EBS
- Instâncias sob demanda do EC2
- Leases de instâncias reservadas do EC2
- Endereços IP elásticos do EC2 clássico
- Endereços de IP elástico do EC2-VPC
- Balanceadores de carga da aplicação do ELB
- Balanceadores de carga clássico do ELB
- Balanceadores de carga da rede do ELB
- Grupo do IAM
- Perfis de instância do IAM
- Políticas do IAM
- Perfis do IAM
- Certificados do servidor do IAM
- Usuários do IAM
- Fragmentos do Kinesis por região
- Uso do armazenamento do código do Lambda

- Grupos de parâmetros de clusters do RDS
- Funções do cluster do RDS
- Clusters do RDS
- Instâncias de banco de dados do RDS
- Snapshots manuais do banco de dados do RDS
- Grupos de parâmetros de banco de dados do RDS
- Grupos de segurança de banco de dados do RDS
- Assinaturas de eventos do RDS
- Autor. máx. do RDS por grupo de segurança
- Grupos de opção do RDS
- Réplicas de leitura do RDS por mestre
- Instâncias reservadas do RDS
- Grupos de sub-rede do RDS
- Sub-redes do RDS por grupo de sub-rede
- Cota de armazenamento total do RDS
- Zonas hospedadas do Route 53
- Verificações de integridade máx. do Route 53
- Conjuntos de delegações reutilizáveis do Route 53
- Políticas de tráfego do Route 53
- Instâncias de política de tráfego do Route 53
- Cota de envio diário do SES
- VPC
- Gateways da Internet da VPC

Grupos de Auto Scaling

Descrição

Verifica o uso superior a 80% da cota dos grupos do Auto Scaling.

ID da verificação

`fW7HH0l7J9`

Recursos adicionais

Auto Scaling quotas (Cotas do Auto Scaling)

Configurações de execução do Auto Scaling

Descrição

Verifica o uso superior a 80% da cota de configurações de execução do Auto Scaling.

ID da verificação

`aW7HH0l7J9`

Recursos adicionais

Auto Scaling quotas (Cotas do Auto Scaling)

CloudFormation Pilhas

Descrição

Verifica o uso de mais de 80% da cota de CloudFormation pilhas.

ID da verificação

`gW7HH0l7J9`

Recursos adicionais

Cotas do AWS CloudFormation

Capacidade de leitura do DynamoDB

Descrição

Verifica o uso que corresponde a mais de 80% do limite da throughput provisionada do DynamoDB para leituras por Conta da AWS.

ID da verificação

`6gtQddfEw6`

Recursos adicionais

DynamoDB quotas (Cotas do DynamoDB)

Capacidade de gravação do DynamoDB

Descrição

Verifica o uso que corresponde a mais de 80% do limite da throughput provisionada do DynamoDB para gravações por Conta da AWS.

ID da verificação

`c5ftjdfkMr`

Recursos adicionais

DynamoDB quotas (Cotas do DynamoDB)

Eventos de snapshot do EBS

Descrição

Verifica o uso superior a 80% da cota de snapshots ativos do EBS.

ID da verificação

`eI7KK0l7J9`

Recursos adicionais

Amazon EBS limits (Limites do Amazon EBS)

Armazenamento de volume EBS de disco rígido frio (sc1)

Descrição

Verifica o uso superior a 80% da cota de armazenamento de volume do EBS Cold HDD (sc1).

ID da verificação

`gH5CC0e3J9`

Recursos adicionais

Amazon EBS limits (Limites do Amazon EBS)

Armazenamento de volume EBS (gp2) de uso geral SSD

Descrição

Verifica o uso superior a 80% da cota de armazenamento de volume do SSD de uso geral do EBS (gp2).

ID da verificação

`dH7RR0l6J9`

Recursos adicionais

Amazon EBS limits (Limites do Amazon EBS)

Armazenamento de volumes SSD de uso geral (gp3) do EBS

Descrição

Verifica o uso superior a 80% da cota de armazenamento de volume do SSD de uso geral do EBS (gp3).

ID da verificação

`dH7RR0l6J3`

Recursos adicionais

Amazon EBS limits (Limites do Amazon EBS)

Armazenamento de volume (padrão) magnético EBS

Descrição

Verifica o uso superior a 80% da cota de armazenamento de volume (padrão) magnético do EBS.

ID da verificação

`cG7HH0l7J9`

Recursos adicionais

Amazon EBS limits (Limites do Amazon EBS)

IOPS agregadas do volume de IOPS provisionadas (SSD) do EBS

Descrição

Verifica o uso superior a 80% da cota de IOPS agregadas de volume de IOPS provisionadas (SSD) do EBS.

ID da verificação

`tV7YY0l7J9`

Recursos adicionais

Amazon EBS limits (Limites do Amazon EBS)

Armazenamento de volumes SSD de IOPS provisionadas (io1) do EBS

Descrição

Verifica o uso superior a 80% da cota de armazenamento de volumes SSD (io1) de IOPS provisionadas do EBS.

ID da verificação

`gI7MM0l7J9`

Recursos adicionais

Amazon EBS limits (Limites do Amazon EBS)

Armazenamento de volumes SSD de IOPS provisionadas (io2) do EBS

Descrição

Verifica o uso superior a 80% da cota de armazenamento de volumes SSD (io2) de IOPS provisionadas do EBS.

ID da verificação

`gI7MM0l7J2`

Recursos adicionais

Amazon EBS limits (Limites do Amazon EBS)

Armazenamento de volume HDD otimizados para throughput (st1) EBS

Descrição

Verifica o uso superior a 80% da cota de armazenamento de volume HDD otimizado para a throughput do EBS (st1).

ID da verificação

`wH7DD0l3J9`

Recursos adicionais

Amazon EBS limits (Limites do Amazon EBS)

Instâncias sob demanda do EC2

Descrição

Verifica o uso superior a 80% da cota de instâncias sob demanda do EC2.

ID da verificação

`0Xc6LMYG8P`

Recursos adicionais

Amazon EC2 quotas (Cotas do Amazon EC2)

Leases de instâncias reservadas do EC2

Descrição

Verifica o uso superior a 80% da cota de leases de instância reservada do EC2.

ID da verificação

`iH7PP0l7J9`

Recursos adicionais

Amazon EC2 quotas (Cotas do Amazon EC2)

Endereços IP elásticos do EC2 clássico

Descrição

Verifica o uso superior a 80% da cota de endereços IP elásticos do EC2 clássico.

ID da verificação

`aW9HH0l8J6`

Recursos adicionais

Amazon EC2 quotas (Cotas do Amazon EC2)

Endereços de IP elástico do EC2-VPC

Descrição

Verifica o uso superior a 80% da cota de endereços IP elásticos do EC2-VPC.

ID da verificação

`lN7RR0l7J9`

Recursos adicionais

VPC Elastic IP quotas (Cotas de IP elástico da VPC)

Balanceadores de carga da aplicação do ELB

Descrição

Verifica o uso superior a 80% da cota dos balanceadores de carga da aplicação do ELB.

ID da verificação

`EM8b3yLRTr`

Recursos adicionais

Elastic Load Balancing

Balanceadores de carga clássico do ELB

Descrição

Verifica o uso superior a 80% da cota dos balanceadores de carga da clássicos do ELB.

ID da verificação

`iK7000l7J9`

Recursos adicionais

Elastic Load Balancing

Balanceadores de carga da rede do ELB

Descrição

Verifica o uso superior a 80% da cota dos balanceadores de carga da rede do ELB.

ID da verificação

`8wIqYSt25K`

Recursos adicionais

Elastic Load Balancing

Grupo do IAM

Descrição

Verifica o uso superior a 80% da cota do grupo do IAM.

ID da verificação

`sU7XX0l7J9`

Recursos adicionais

IAM quotas (Cotas do IAM)

Perfis de instância do IAM

Descrição

Verifica o uso superior a 80% da cota de perfis de instância do IAM.

ID da verificação

`n07SS0l7J9`

Recursos adicionais

IAM quotas (Cotas do IAM)

Políticas do IAM

Descrição

Verifica o uso superior a 80% da cota de políticas do IAM.

ID da verificação

`pR7UU0l7J9`

Recursos adicionais

IAM quotas (Cotas do IAM)

Perfis do IAM

Descrição

Verifica o uso superior a 80% da cota de funções do IAM.

ID da verificação

`oQ7TT0l7J9`

Recursos adicionais

IAM quotas (Cotas do IAM)

Certificados do servidor do IAM

Descrição

Verifica o uso superior a 80% da cota de certificados de servidor do IAM.

ID da verificação

`rT7WW0l7J9`

Recursos adicionais

IAM quotas (Cotas do IAM)

Usuários do IAM

Descrição

Verifica o uso superior a 80% da cota de usuários do IAM.

ID da verificação

`qS7VV0l7J9`

Recursos adicionais

IAM quotas (Cotas do IAM)

Fragmentos do Kinesis por região

Descrição

Verifica o uso superior a 80% da cota de fragmentos do Kinesis por região.

ID da verificação

`bW7HH0l7J9`

Recursos adicionais

Kinesis quotas (Cotas do Kinesis)

Uso do armazenamento do código do Lambda

Descrição

Verifica se o uso do armazenamento de código é superior a 80% do limite da conta.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c1dfprch07`

Critérios de alerta

- Amarelo: 80% do limite atingido.

Recommended Action (Ação recomendada)

Identifique as funções ou versões do Lambda não utilizadas e remova-as para liberar o armazenamento de código para sua conta na região. Se precisar de armazenamento adicional, crie um caso de suporte na Central de Suporte. Se você espera exceder um limite de serviço, solicite um aumento diretamente no console do Service Quotas. Se o Service Quotas ainda não oferecer suporte ao seu serviço, você poderá criar um caso de suporte na Central de suporte.

Recursos adicionais

- Uso do armazenamento de código Lambda

Colunas do relatório

- Status
- Região
- O ARN da função qualificada para esse recurso.
- O uso do armazenamento do código da função é MegaBytes com 2 decimais.
- A quantidade de versões na função
- Hora da última atualização

Grupos de parâmetros de clusters do RDS

Descrição

Verifica o uso superior a 80% da cota de grupos de parâmetro do cluster do RDS.

ID da verificação

`jtlIMO3qZM`

Recursos adicionais

Amazon RDS quotas (Cotas do Amazon RDS)

Funções do cluster do RDS

Descrição

Verifica o uso superior a 80% da cota de funções de cluster do RDS.

ID da verificação

`7fuccf1Mx7`

Recursos adicionais

Amazon RDS quotas (Cotas do Amazon RDS)

Clusters do RDS

Descrição

Verifica o uso superior a 80% da cota de clusters do RDS.

ID da verificação

`gjqMBn6pjz`

Recursos adicionais

Amazon RDS quotas (Cotas do Amazon RDS)

Instâncias de banco de dados do RDS

Descrição

Verifica o uso superior a 80% da cota de instâncias de banco de dados do RDS.

ID da verificação

`XG0aXHpIEt`

Recursos adicionais

Amazon RDS quotas (Cotas do Amazon RDS)

Snapshots manuais do banco de dados do RDS

Descrição

Verifica o uso superior a 80% da cota de snapshots manuais do banco de dados do RDS.

ID da verificação

`dV84wpqRUs`

Recursos adicionais

Amazon RDS quotas (Cotas do Amazon RDS)

Grupos de parâmetros de banco de dados do RDS

Descrição

Verifica o uso superior a 80% da cota de grupos de parâmetros do banco de dados do RDS.

ID da verificação

`jEECYg2YVU`

Recursos adicionais

Amazon RDS quotas (Cotas do Amazon RDS)

Grupos de segurança de banco de dados do RDS

Descrição

Verifica o uso superior a 80% da cota de grupos de segurança do banco de dados do RDS.

ID da verificação

`gfZAn3W7wl`

Recursos adicionais

Amazon RDS quotas (Cotas do Amazon RDS)

Assinaturas de eventos do RDS

Descrição

Verifica o uso superior a 80% da cota de assinaturas de eventos do RDS.

ID da verificação

`keAhfbH5yb`

Recursos adicionais

Amazon RDS quotas (Cotas do Amazon RDS)

Autor. máx. do RDS por grupo de segurança

Descrição

Verifica o uso superior a 80% de autorizações máximas do RDS por cotas de grupo de segurança.

ID da verificação

`dBkuNCvqn5`

Recursos adicionais

Amazon RDS quotas (Cotas do Amazon RDS)

Grupos de opção do RDS

Descrição

Verifica o uso superior a 80% da cota de grupos de opção do RDS.

ID da verificação

`3Njm0DJQO9`

Recursos adicionais

Amazon RDS quotas (Cotas do Amazon RDS)

Réplicas de leitura do RDS por mestre

Descrição

Verifica o uso superior a 80% das réplicas de leitura do RDS por cota mestre.

ID da verificação

`pYW8UkYz2w`

Recursos adicionais

Amazon RDS quotas (Cotas do Amazon RDS)

Instâncias reservadas do RDS

Descrição

Verifica o uso superior a 80% da cota de Instâncias Reservadas do RDS.

ID da verificação

`UUDv0a5r34`

Recursos adicionais

Amazon RDS quotas (Cotas do Amazon RDS)

Grupos de sub-rede do RDS

Descrição

Verifica o uso superior a 80% da cota de grupos de sub-rede do RDS.

ID da verificação

`dYWBaXaaMM`

Recursos adicionais

Amazon RDS quotas (Cotas do Amazon RDS)

Sub-redes do RDS por grupo de sub-rede

Descrição

Verifica o uso superior a 80% de sub-redes do RDS por cota de grupo de sub-rede.

ID da verificação

`jEhCtdJK0Y`

Recursos adicionais

Amazon RDS quotas (Cotas do Amazon RDS)

Cota de armazenamento total do RDS

Descrição

Verifica o uso superior a 80% da cota de armazenamento total do RDS.

ID da verificação

`P1jhKWEmLa`

Recursos adicionais

Amazon RDS quotas (Cotas do Amazon RDS)

Zonas hospedadas do Route 53

Descrição

Verifica o uso superior a 80% da cota de zonas hospedadas do Route 53 por conta.

ID da verificação

`dx3xfcdfMr`

Recursos adicionais

Route 53 quotas (Cotas do Route 53)

Verificações de integridade máx. do Route 53

Descrição

Verifica o uso superior a 80% da cota de verificações de integridade do Route 53 por conta.

ID da verificação

`ru4xfcdfMr`

Recursos adicionais

Route 53 quotas (Cotas do Route 53)

Conjuntos de delegações reutilizáveis do Route 53

Descrição

Verifica o uso superior a 80% da cota de conjuntos de delegações reutilizáveis do Route 53 por conta.

ID da verificação

`ty3xfcdfMr`

Recursos adicionais

Route 53 quotas (Cotas do Route 53)

Políticas de tráfego do Route 53

Descrição

Verifica o uso superior a 80% da cota de políticas de tráfego do Route 53 por conta.

ID da verificação

`dx3xfbjfMr`

Recursos adicionais

Route 53 quotas (Cotas do Route 53)

Instâncias de política de tráfego do Route 53

Descrição

Verifica o uso superior a 80% da cota de instâncias de política de tráfego do Route 53 por conta.

ID da verificação

`dx8afcdfMr`

Recursos adicionais

Route 53 quotas (Cotas do Route 53)

Cota de envio diário do SES

Descrição

Verifica o uso superior a 80% da cota de envio diário do Amazon SES.

ID da verificação

`hJ7NN0l7J9`

Recursos adicionais

Amazon SES quotas (Cotas do Amazon SQS)

VPC

Descrição

Verifica o uso superior a 80% da cota da VPC.

ID da verificação

`jL7PP0l7J9`

Recursos adicionais

VPC quotas (Cotas de VPC)

Gateways da Internet da VPC

Descrição

Verifica o uso superior a 80% da cota de gateways da Internet da VPC.

ID da verificação

`kM7QQ0l7J9`

Recursos adicionais

VPC quotas (Cotas de VPC)

Excelência operacional

Você pode usar as verificações a seguir para a categoria de excelência operacional.

Nomes da verificação

- O Amazon API Gateway não está registrando em log os logs de execução
- APIs REST do Amazon API Gateway sem rastreamento do X-Ray habilitado
- Registro de CloudFront acesso da Amazon configurado
- A ação CloudWatch de alarme da Amazon está desativada
- Instância do Amazon EC2 não gerenciada pelo AWS Systems Manager
- Repositório do Amazon ECR com a imutabilidade de tags desabilitada

- Clusters do Amazon ECS com o Container Insights desabilitado
- Registro em log de tarefas do Amazon ECS não habilitado
- Registro OpenSearch do Amazon Service CloudWatch não configurado
- Instâncias de banco de dados Amazon RDS nos clusters com grupos de parâmetros heterogêneos
- O monitoramento aprimorado do Amazon RDS está desativado
- O Amazon RDS Performance Insights está desativado
- O parâmetro track_counts do Amazon RDS está desativado
- Registro em log de auditoria de clusters do Amazon Redshift
- Amazon S3 não tem as notificações de eventos habilitadas
- Tópicos do Amazon SNS não estão registrando em log o status da entrega de mensagens
- Amazon VPC sem logs de fluxo
- Application Load Balancers e Classic Load Balancers sem logs de acesso habilitados
- Notificação de pilha do AWS CloudFormation
- Registo em log de eventos de dados do AWS CloudTrail para objetos em um bucket S3
- Registro em log do projeto do AWS CodeBuild
- Monitoramento e reversão automática do AWS CodeDeploy habilitados
- AWS CodeDeployO Lambda está usando all-at-once a configuração de implantação
- Os relatórios de integridade aprimorada do AWS Elastic Beanstalk não estão configurados
- AWS Elastic Beanstalk com as atualizações gerenciadas da plataforma desabilitadas
- A versão da plataforma do AWS Fargate não é a mais recente
- Associação do Gerenciador de Estados do AWS Systems Manager em status de não conformidade
- CloudTrail as trilhas não estão configuradas com o Amazon CloudWatch Logs
- A proteção contra exclusão do Elastic Load Balancing não está habilitada para balanceadores de carga
- Verificação da proteção contra exclusão do cluster de banco de dados do RDS
- Verificação de atualização automática de versão secundária da instância de banco de dados do RDS

O Amazon API Gateway não está registrando em log os logs de execução

Descrição

Verifica se o Amazon API Gateway tem CloudWatch registros ativados no nível de registro desejado.

Ative o CloudWatch registro de métodos de API REST ou rotas de WebSocket API no Amazon API Gateway para coletar registros de execução em CloudWatch registros para solicitações recebidas por suas APIs. As informações contidas nos logs de execução ajudam a identificar e solucionar problemas relacionados à sua API.

Você pode especificar o ID do nível de registro em log (ERROR, INFO) no parâmetro loggingLevel nas regras do AWS Config.

Consulte a API REST ou a documentação WebSocket da API para obter mais informações sobre o CloudWatch registro no Amazon API Gateway.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c18d2gz125`

Origem

`AWS Config Managed Rule: api-gw-execution-logging-enabled`

Critérios de alerta

Amarelo: a configuração de CloudWatch registro para coleta de registros de execução não está habilitada no nível de registro desejado para um Amazon API Gateway.

Recommended Action (Ação recomendada)

Ative o CloudWatch registro para registros de execução de suas APIs REST do Amazon API Gateway ou WebSocket APIs com o nível de registro apropriado (ERROR, INFO).

Para obter mais informações, consulte Criar um log de fluxo

Recursos adicionais

- Configurando o CloudWatch registro em log para uma API REST no API Gateway
- Configurando o registro em log para uma API WebSocket

Colunas do relatório

- Status
- Região
- Recurso
- Regra do AWS Config
- Parâmetros de entrada
- Hora da última atualização

APIs REST do Amazon API Gateway sem rastreamento do X-Ray habilitado

Descrição

Verifica se as APIs REST do Amazon API Gateway têm o rastreamento do AWS X-Ray habilitado.

Ative o rastreamento do X-Ray para suas APIs REST para permitir que o API Gateway exemplifique solicitações de invocação de API com informações de rastreamento. Isso permite que você aproveite o rastreamento e a análise de solicitações do AWS X-Ray à medida que passam pelas APIs REST do API Gateway em direção aos serviços de downstream.

Para obter mais informações, consulte Rastrear solicitações de usuário para APIs REST usando o X-Ray.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c18d2gz126`

Origem

```
AWS Config Managed Rule: api-gw-xray-enabled
```

Critérios de alerta

Amarelo: o rastreamento do X-Ray não está ativado para uma API REST do API Gateway.

Recommended Action (Ação recomendada)

Ative o rastreamento X-Ray para suas APIs REST do API Gateway.

Para obter mais informações, consulte Configurar o AWS X-Ray com APIs REST do API Gateway.

Recursos adicionais

- Rastrear solicitações de usuário para APIs REST usando o X-Ray
- O que é AWS X-Ray?

Colunas do relatório

- Status
- Região
- Recurso
- Regra do AWS Config
- Parâmetros de entrada
- Hora da última atualização

Registro de CloudFront acesso da Amazon configurado

Descrição

Verifica se CloudFront as distribuições da Amazon estão configuradas para capturar informações dos registros de acesso ao servidor Amazon S3. Os registros de acesso ao servidor Amazon S3 contêm informações detalhadas sobre cada solicitação de usuário recebida. CloudFront

Você pode ajustar o nome do bucket do Amazon S3 para armazenar registros de acesso ao servidor, usando o BucketName parâmetro S3 em suas regras. AWS Config

Para obter mais informações, consulte Configurar e usar logs padrão (logs de acesso).

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c18d2gz110`

Origem

`AWS Config Managed Rule: cloudfront-accesslogs-enabled`

Critérios de alerta

Amarelo: o registro de CloudFront acesso à Amazon não está ativado

Recommended Action (Ação recomendada)

Certifique-se de ativar o registro de CloudFront acesso para capturar informações detalhadas sobre cada solicitação de usuário CloudFront recebida.

É possível habilitar os logs padrão ao criar ou atualizar uma distribuição.

Para obter mais informações, consulte Valores especificados ao criar ou atualizar uma distribuição.

Recursos adicionais

- Valores especificados ao criar ou atualizar uma distribuição
- Configurar e usar logs padrão (logs de acesso)

Colunas do relatório

- Status
- Região
- Recurso
- Regra do AWS Config
- Parâmetros de entrada
- Hora da última atualização

A ação CloudWatch de alarme da Amazon está desativada

Descrição

Verifica se sua ação CloudWatch de alarme da Amazon está desativada.

Você pode usar a AWS CLI para habilitar ou desabilitar o recurso de ação em seu alarme. Ou você pode habilitar ou desabilitar programaticamente o recurso de ação usando o AWS SDK. Quando o recurso de ação de alarme está desativado, CloudWatch não executa nenhuma ação definida em nenhum estado (OK, INSUFFICIENT_DATA, ALARM).

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c18d2gz109`

Origem

`AWS Config Managed Rule: cloudwatch-alarm-action-enabled-check`

Critérios de alerta

Amarelo: a ação CloudWatch de alarme da Amazon não está ativada. Nenhuma ação é executada em nenhum estado de alarme.

Recommended Action (Ação recomendada)

Ative ações em seus CloudWatch alarmes, a menos que você tenha um motivo válido para desativá-las, como para fins de teste.

Se o CloudWatch alarme não for mais necessário, exclua-o para evitar custos desnecessários.

Para obter mais informações, consulte enable-alarm-actionsna Referência de AWS CLI comandos e func (*CloudWatch) EnableAlarmActions na Referência da AWS API SDK for Go.

Colunas do relatório

- Status
- Região

- Recurso
- Regra do AWS Config
- Parâmetros de entrada
- Hora da última atualização

Instância do Amazon EC2 não gerenciada pelo AWS Systems Manager

Descrição

Verifica se as instâncias do Amazon EC2 em sua conta são gerenciadas pelo AWS Systems Manager.

O Systems Manager ajuda você a entender e controlar o estado atual da sua instância do Amazon EC2 e das configurações do sistema operacional. Com o Systems Manager, você pode coletar informações de configuração e inventário de software sobre seu conjunto de instâncias, incluindo o software instalado nelas. Isso permite que você acompanhe a configuração detalhada do sistema, os níveis de patch do sistema operacional, as configurações da aplicação e outros detalhes sobre sua implantação.

Para obter mais informações, consulte Configuração do Systems Manager para instâncias do EC2.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c18d2gz145`

Origem

`AWS Config Managed Rule: ec2-instance-managed-by-systems-manager`

Critérios de alerta

Amarelo: as instâncias do Amazon EC2 não são gerenciadas pelo Systems Manager.

Recommended Action (Ação recomendada)

Configure sua instância do Amazon EC2 para ser gerenciada pelo Systems Manager.

Essa verificação não pode ser excluída da visualização no console do Trusted Advisor.

Para obter mais informações, consulte Why is my EC2 instance not displaying as a managed node or showing a "Connection lost" status in Systems Manager?.

Recursos adicionais

Configuração do Systems Manager para instâncias do EC2

Colunas do relatório

- Status
- Região
- Recurso
- Regra do AWS Config
- Parâmetros de entrada
- Hora da última atualização

Repositório do Amazon ECR com a imutabilidade de tags desabilitada

Descrição

Verifica se um repositório privado do Amazon ECR tem a imutabilidade de tags de imagem desativada.

Ative a imutabilidade de tags de imagem para um repositório privado do Amazon ECR para impedir que as tags de imagem sejam substituídas. Isso permite que você confie nas tags descritivas como um mecanismo confiável para rastrear e identificar imagens de forma exclusiva. Por exemplo, se a imutabilidade de tags de imagem estiver ativada, os usuários poderão usar uma tag de imagem de forma confiável para correlacionar uma versão de imagem implantada com a compilação que produziu essa imagem.

Para obter mais informações, consulte Mutabilidade de tag de imagem.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c18d2gz129`

Origem

`AWS Config Managed Rule: ecr-private-tag-immutability-enabled`

Critérios de alerta

Amarelo: um repositório privado do Amazon ECR não tem a imutabilidade de tags ativada.

Recommended Action (Ação recomendada)

Ative a imutabilidade de tags de imagem para seus repositórios privados do Amazon ECR.

Para obter mais informações, consulte Mutabilidade de tag de imagem.

Colunas do relatório

- Status
- Região
- Recurso
- Regra do AWS Config
- Parâmetros de entrada
- Hora da última atualização

Clusters do Amazon ECS com o Container Insights desabilitado

Descrição

Verifica se o Amazon CloudWatch Container Insights está ativado para seus clusters do Amazon ECS.

CloudWatch O Container Insights coleta, agrega e resume métricas e registros de seus aplicativos e microsserviços em contêineres. As métricas incluem a utilização de recursos, como CPU, memória, disco e rede.

Para obter mais informações, consulte Amazon ECS CloudWatch Container Insights.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c18d2gz173`

Origem

`AWS Config Managed Rule: ecs-container-insights-enabled`

Critérios de alerta

Amarelo: o cluster do Amazon ECS não tem insights de contêiner habilitados.

Recommended Action (Ação recomendada)

Ative o CloudWatch Container Insights em seus clusters do Amazon ECS.

Para obter mais informações, consulte Como usar o Container Insights.

Recursos adicionais

Informações sobre CloudWatch contêineres do Amazon ECS

Colunas do relatório

- Status
- Região
- Recurso
- Regra do AWS Config
- Parâmetros de entrada

- Hora da última atualização

Registro em log de tarefas do Amazon ECS não habilitado

Descrição

Verifica se a configuração do log está definida nas configurações de tarefas ativas do Amazon ECS.

Verificar a configuração de logs nas definições de tarefas do Amazon ECS garante que os logs gerados pelos contêineres sejam configurados e armazenados adequadamente. Isso ajuda a identificar e solucionar problemas com mais rapidez, otimizar a performance e atender aos requisitos de conformidade.

Por padrão, os logs capturados mostram a saída do comando que você normalmente veria em um terminal interativo, caso executasse o contêiner localmente. O driver awslogs passa esses registros do Docker para o Amazon Logs. CloudWatch

Para obter mais informações, consulte Using the awslogs log driver.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c18d2gz175`

Origem

`AWS Config Managed Rule: ecs-task-definition-log-configuration`

Critérios de alerta

Amarelo: a definição de tarefas do Amazon ECS não tem uma configuração de logs.

Recommended Action (Ação recomendada)

Considere especificar a configuração do driver de registro na definição do contêiner para enviar informações de registro ao CloudWatch Logs ou a um driver de registro diferente.

Para obter mais informações, consulte LogConfiguration.

Recursos adicionais

Considere especificar a configuração do driver de registro na definição do contêiner para enviar informações de registro ao CloudWatch Logs ou a um driver de registro diferente.

Para obter mais informações, consulte Example task definitions.

Colunas do relatório

- Status
- Região
- Recurso
- Regra do AWS Config
- Parâmetros de entrada
- Hora da última atualização

Registro OpenSearch do Amazon Service CloudWatch não configurado

Descrição

Verifica se os domínios do Amazon OpenSearch Service estão configurados para enviar registros para o Amazon CloudWatch Logs.

O monitoramento dos registros é crucial para manter a confiabilidade, a disponibilidade e o desempenho do OpenSearch Serviço.

Os logs lentos de pesquisa, os logs lentos de indexação e os logs de erros são úteis para solucionar problemas de performance e estabilidade da sua workload. Esses logs precisam ser habilitados para capturar dados.

Você pode especificar quais tipos de log deseja filtrar (erro, pesquisa, índice) usando o parâmetro logTypes em suas regras do AWS Config.

Para obter mais informações, consulte Monitoramento de domínios OpenSearch do Amazon Service.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c18d2gz184`

Origem

`AWS Config Managed Rule: opensearch-logs-to-cloudwatch`

Critérios de alerta

Amarelo: o Amazon OpenSearch Service não tem uma configuração de registro com o Amazon CloudWatch Logs

Recommended Action (Ação recomendada)

Configure os domínios de OpenSearch serviço para publicar registros no CloudWatch Logs.

Para obter mais informações, consulte Enabling log publishing (console).

Recursos adicionais

- Métricas OpenSearch de cluster do serviço de monitoramento com a Amazon CloudWatch

Colunas do relatório

- Status
- Região
- Recurso
- Regra do AWS Config
- Parâmetros de entrada
- Hora da última atualização

Instâncias de banco de dados Amazon RDS nos clusters com grupos de parâmetros heterogêneos

Descrição

Recomendamos que todas as instâncias de banco de dados no cluster de banco de dados usem o mesmo grupo de parâmetros de banco de dados.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

> **Note**
>
> Quando uma instância de banco de dados ou cluster de banco de dados é interrompido, você pode visualizar as recomendações do Amazon RDS Trusted Advisor por 3 a 5 dias. Depois de cinco dias, as recomendações não estão disponíveis emTrusted Advisor. Para visualizar as recomendações, abra o console do Amazon RDS e escolha Recomendações.
> Se você excluir uma instância de banco de dados ou um cluster de banco de dados, as recomendações associadas a essas instâncias ou clusters não estarão disponíveis no Trusted Advisor console de gerenciamento do Amazon RDS.

ID da verificação

`c1qf5bt010`

Critérios de alerta

Amarelo: clusters de banco de dados têm instâncias de banco de dados com grupos de parâmetros heterogêneos.

Recommended Action (Ação recomendada)

Associe a instância de banco de dados ao grupo de parâmetros de banco de dados associado à instância do gravador em seu cluster de banco de dados.

Recursos adicionais

Quando as instâncias de banco de dados em seu cluster de banco de dados usam grupos de parâmetros de banco de dados diferentes, pode haver um comportamento inconsistente durante um failover ou problemas de compatibilidade entre as instâncias de banco de dados em seu cluster de banco de dados.

Para obter mais informações, consulte Trabalhar com grupos de parâmetros.

Colunas do relatório

- Status
- Região
- Recurso
- Valor recomendado
- Nome do motor
- Hora da última atualização

O monitoramento aprimorado do Amazon RDS está desativado

Descrição

Seus recursos de banco de dados não têm o monitoramento aprimorado ativado. O monitoramento avançado fornece métricas do sistema operacional em tempo real para monitoramento e solução de problemas.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

> **Note**
>
> Quando uma instância de banco de dados ou cluster de banco de dados é interrompido, você pode visualizar as recomendações do Amazon RDS Trusted Advisor por 3 a 5 dias. Depois de cinco dias, as recomendações não estão disponíveis emTrusted

Advisor. Para visualizar as recomendações, abra o console do Amazon RDS e escolha Recomendações.
Se você excluir uma instância de banco de dados ou um cluster de banco de dados, as recomendações associadas a essas instâncias ou clusters não estarão disponíveis no Trusted Advisor console de gerenciamento do Amazon RDS.

ID da verificação

`c1qf5bt004`

Critérios de alerta

Amarelo: os recursos do Amazon RDS não têm o Enhanced Monitoring ativado.

Recommended Action (Ação recomendada)

Ative o monitoramento aprimorado.

Recursos adicionais

O monitoramento aprimorado do Amazon RDS fornece visibilidade adicional sobre a integridade de suas instâncias de banco de dados. Recomendamos que você ative o Monitoramento aprimorado. Quando a opção Enhanced Monitoring é ativada para sua instância de banco de dados, ela coleta métricas vitais do sistema operacional e informações do processo.

Para obter mais informações, consulte Monitorar métricas do SO com o monitoramento avançado.

Colunas do relatório

- Status
- Região
- Recurso
- Valor recomendado
- Nome do motor
- Hora da última atualização

O Amazon RDS Performance Insights está desativado

Descrição

O Amazon RDS Performance Insights monitora a carga da sua instância de banco de dados para ajudá-lo a analisar e resolver problemas de desempenho do banco de dados. Recomendamos que você ative o Performance Insights.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

> **Note**
>
> Quando uma instância de banco de dados ou cluster de banco de dados é interrompido, você pode visualizar as recomendações do Amazon RDS Trusted Advisor por 3 a 5 dias. Depois de cinco dias, as recomendações não estão disponíveis emTrusted Advisor. Para visualizar as recomendações, abra o console do Amazon RDS e escolha Recomendações.
> Se você excluir uma instância de banco de dados ou um cluster de banco de dados, as recomendações associadas a essas instâncias ou clusters não estarão disponíveis no Trusted Advisor console de gerenciamento do Amazon RDS.

ID da verificação

`c1qf5bt012`

Critérios de alerta

Amarelo: os recursos do Amazon RDS não têm o Performance Insights ativado.

Recommended Action (Ação recomendada)

Habilite o Performance Insights.

Recursos adicionais

O Performance Insights usa um método leve de coleta de dados que não afeta o desempenho de seus aplicativos. O Performance Insights ajuda você a avaliar rapidamente a carga do banco de dados.

Para obter mais informações, consulte Monitoramento da carga do banco de dados com Performance Insights no Amazon RDS.

Colunas do relatório

- Status
- Região
- Recurso
- Valor recomendado
- Nome do motor
- Hora da última atualização

O parâmetro track_counts do Amazon RDS está desativado

Descrição

Quando o parâmetro track_counts é desativado, o banco de dados não coleta as estatísticas de atividade do banco de dados. O autovacuum exige que essas estatísticas funcionem corretamente.

Recomendamos que você defina o parâmetro track_counts como 1

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

> **Note**
>
> Quando uma instância de banco de dados ou cluster de banco de dados é interrompido, você pode visualizar as recomendações do Amazon RDS Trusted Advisor por 3 a

5 dias. Depois de cinco dias, as recomendações não estão disponíveis emTrusted Advisor. Para visualizar as recomendações, abra o console do Amazon RDS e escolha Recomendações.
Se você excluir uma instância de banco de dados ou um cluster de banco de dados, as recomendações associadas a essas instâncias ou clusters não estarão disponíveis no Trusted Advisor console de gerenciamento do Amazon RDS.

ID da verificação

`c1qf5bt027`

Critérios de alerta

Amarelo: grupos de parâmetros do banco de dados têm o parâmetro track_counts desativado.

Recommended Action (Ação recomendada)

Defina o parâmetro track_counts como 1

Recursos adicionais

Quando o parâmetro track_counts é desativado, ele desativa a coleta de estatísticas de atividades do banco de dados. O daemon autovacuum requer as estatísticas coletadas para identificar as tabelas para autovacuum e autoanálise.

Para obter mais informações, consulte Estatísticas de tempo de execução do PostgreSQL no site de documentação do PostgreSQL.

Colunas do relatório

- Status
- Região
- Recurso
- Valor do parâmetro
- Valor recomendado
- Hora da última atualização

Registro em log de auditoria de clusters do Amazon Redshift

Descrição

Verifica se os clusters do Amazon Redshift têm o registro em log de auditoria do banco de dados ativado. O Amazon Redshift registra informações sobre conexões e atividades do usuário em seu banco de dados.

Você pode especificar o nome do bucket de registro em log do Amazon S3 desejado para corresponder ao parâmetro bucketNames de suas regras do AWS Config.

Para obter mais informações, consulte Registro em log da auditoria de banco de dados.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c18d2gz134`

Origem

`AWS Config Managed Rule: redshift-audit-logging-enabled`

Critérios de alerta

Amarelo: um cluster do Amazon Redshift tem o registro em log de auditoria do banco de dados desabilitado

Recommended Action (Ação recomendada)

Ative o registro em log e o monitoramento dos clusters do Amazon Redshift.

Para obter mais informações, consulte Configurar a auditoria usando o console.

Recursos adicionais

Registrar em log e monitorar no Amazon Redshift

Colunas do relatório

- Status

- Região
- Recurso
- Regra do AWS Config
- Parâmetros de entrada
- Hora da última atualização

Amazon S3 não tem as notificações de eventos habilitadas

Descrição

Verifica se as notificações de eventos do Amazon S3 estão habilitadas ou configuradas corretamente com o destino ou os tipos desejados.

O recurso de notificações de eventos do Amazon S3 envia notificações quando determinados eventos ocorrem no bucket do Amazon S3. O Amazon S3 pode enviar mensagens de notificação para filas do Amazon SQS, tópicos do Amazon SNS e funções do AWS Lambda.

Você pode especificar o destino e os tipos de eventos desejados usando os parâmetros destinationArn e eventTypes de suas regras do AWS Config.

Para obter mais informações, consulte Notificações de eventos do Amazon S3.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c18d2gz163`

Origem

`AWS Config Managed Rule: s3-event-notifications-enabled`

Critérios de alerta

Amarelo: o Amazon S3 não tem as notificações de eventos habilitadas ou não estão configuradas com a designação ou os tipos desejados.

Recommended Action (Ação recomendada)

Configure as notificações de eventos do Amazon S3 para eventos de objetos e buckets.

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

Colunas do relatório

- Status
- Região
- Recurso
- Regra do AWS Config
- Parâmetros de entrada
- Hora da última atualização

Tópicos do Amazon SNS não estão registrando em log o status da entrega de mensagens

Descrição

Verifica se os tópicos do Amazon SNS têm o registro em log do status da entrega de mensagens ativado.

Configure os tópicos do Amazon SNS para registrar em log o status da entrega de mensagens para ajudar a fornecer melhores insights operacionais. Por exemplo, o registro em log da entrega de mensagens verifica se uma mensagem foi entregue a um determinado endpoint do Amazon SNS. Além disso, ele também ajuda a identificar a resposta enviada pelo endpoint.

Para obter mais informações, consulte Status de entrega de mensagens do Amazon SNS.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c18d2gz121`

Origem

`AWS Config Managed Rule: sns-topic-message-delivery-notification-enabled`

Critérios de alerta

Amarelo: o registro em log do status da entrega de mensagens não está ativado para um tópico do Amazon SNS.

Recommended Action (Ação recomendada)

Ative o registro em log do status da entrega de mensagens para seus tópicos do SNS.

Para obter mais informações, consulte Configurar o registro em log do status de entrega usando o Console de Gerenciamento da AWS.

Colunas do relatório

- Status
- Região
- Recurso
- Regra do AWS Config
- Parâmetros de entrada
- Hora da última atualização

Amazon VPC sem logs de fluxo

Descrição

Verifica se os logs de fluxo da Amazon Virtual Private Cloud foram criados para uma VPC.

Você pode especificar o tipo de tráfego usando o parâmetro trafficType nas suas regras do AWS Config.

Para obter mais informações, consulte Como registrar tráfego IP em log com logs de fluxo da VPC.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c18d2gz122`

Origem

`AWS Config Managed Rule: vpc-flow-logs-enabled`

Critérios de alerta

Amarelo: as VPCs não têm logs de fluxo da Amazon VPC.

Recommended Action (Ação recomendada)

Crie logs de fluxo da VPC para cada uma de suas VPCs.

Para obter mais informações, consulte Criar um log de fluxo

Colunas do relatório

- Status
- Região
- Recurso
- Regra do AWS Config
- Parâmetros de entrada
- Hora da última atualização

Application Load Balancers e Classic Load Balancers sem logs de acesso habilitados

Descrição

Verifica se os Application Load Balancers e os Classic Load Balancers têm o registro de acesso habilitado.

O Elastic Load Balancing fornece logs de acesso que capturam informações detalhadas sobre as solicitações enviadas ao seu balanceador de carga. Cada log contém informações como a hora

em que a solicitação foi recebida, o endereço IP do cliente, latências, caminhos de solicitação e respostas do servidor. Você pode usar esses logs de acesso para analisar padrões de tráfego e solucionar problemas.

Os logs de acesso são um recurso opcional do Elastic Load Balancing que é desabilitado por padrão. Depois que os logs de acesso para seu balanceador de carga forem habilitados, o Elastic Load Balancing capturará os logs e os armazenará no bucket do Amazon S3 que você especificar.

Você pode especificar o log de acesso do bucket Amazon S3 que deseja verificar usando o BucketNames parâmetro s3 em suas regras. AWS Config

Para obter mais informações, consulte Access logs for your Application Load Balancer ou Logs de acesso do seu Classic Load Balancer.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c18d2gz167`

Origem

`AWS Config Managed Rule: elb-logging-enabled`

Critérios de alerta

Amarelo: o recurso de logs de acesso não está habilitado para um Application Load Balancer ou Classic Load Balancer.

Recommended Action (Ação recomendada)

Habilite os logs de acesso para os Application Load Balancers e os Classic Load Balancers.

Para obter mais informações, consulte Enable access logs for your Application Load Balancer ou Habilitar os logs de acesso do seu Classic Load Balancer.

Colunas do relatório

- Status

- Região
- Recurso
- Regra do AWS Config
- Parâmetros de entrada
- Hora da última atualização

Notificação de pilha do AWS CloudFormation

Descrição

Verifica se todas as suas pilhas do AWS CloudFormation usam o Amazon SNS para receber notificações quando ocorre um evento.

Você pode configurar essa verificação para procurar ARNs de tópicos específicos do Amazon SNS usando parâmetros em suas regras do AWS Config.

Para obter mais informações, consulte Configurar opções de pilha do AWS CloudFormation.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c18d2gz111`

Origem

`AWS Config Managed Rule: cloudformation-stack-notification-check`

Critérios de alerta

Amarelo: as notificações de eventos do Amazon SNS para suas pilhas do AWS CloudFormation não estão ativadas.

Recommended Action (Ação recomendada)

Certifique-se de que suas pilhas do AWS CloudFormation usem o Amazon SNS para receber notificações quando ocorrer um evento.

O monitoramento de eventos da pilha ajuda você a responder rapidamente a ações não autorizadas que podem alterar seu ambiente da AWS.

Recursos adicionais

Como posso receber um alerta por e-mail quando minha CloudFormation pilha da AWS entra no status ROLLBACK_IN_PROGRESS?

Colunas do relatório

- Status
- Região
- Recurso
- Regra do AWS Config
- Parâmetros de entrada
- Hora da última atualização

Registo em log de eventos de dados do AWS CloudTrail para objetos em um bucket S3

Descrição

Verifica se pelo menos uma trilha do AWS CloudTrail registra eventos de dados do Amazon S3 para todos os seus buckets do Amazon S3.

Para obter mais informações, consulte Registrar chamadas de API do Amazon S3 em log usando o AWS CloudTrail.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c18d2gz166`

Origem

```
AWS Config Managed Rule: cloudtrail-s3-dataevents-enabled
```

Critérios de alerta

Amarelo: o registro em log de eventos do AWS CloudTrail para buckets do Amazon S3 não está configurado

Recommended Action (Ação recomendada)

Ative o registro de CloudTrail eventos para buckets e objetos do Amazon S3 para rastrear solicitações de acesso ao bucket de destino.

Para obter mais informações, consulte Habilitar o registro de CloudTrail eventos para buckets e objetos do S3.

Colunas do relatório

- Status
- Região
- Recurso
- Regra do AWS Config
- Parâmetros de entrada
- Hora da última atualização

Registro em log do projeto do AWS CodeBuild

Descrição

Verifica se o ambiente do projeto do AWS CodeBuild usa registro em log. As opções de registro podem ser registros no Amazon CloudWatch Logs ou criadas em um bucket específico do Amazon S3, ou ambos. Habilitar o registro em um CodeBuild projeto pode oferecer vários benefícios, como depuração e auditoria.

Você pode especificar o nome do bucket Amazon S33 ou do grupo de CloudWatch registros para armazenar os registros, usando o parâmetro s3 BucketNames ou cloudWatchGroupNames em suas AWS Config regras.

Para obter mais informações, consulte Monitoramento do AWS CodeBuild.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c18d2gz113`

Origem

`AWS Config Managed Rule: codebuild-project-logging-enabled`

Critérios de alerta

Amarelo: o registro em log do projeto do AWS CodeBuild não está habilitado.

Recommended Action (Ação recomendada)

Certifique-se de que o registro em log esteja ativado em seu projeto do AWS CodeBuild. Essa verificação não pode ser excluída da visualização no console do AWS Trusted Advisor.

Para obter mais informações, consulte Registro em log e monitoramento de aplicações no AWS CodeBuild.

Colunas do relatório

- Status
- Região
- Recurso
- Regra do AWS Config
- Parâmetros de entrada
- Hora da última atualização

Monitoramento e reversão automática do AWS CodeDeploy habilitados

Descrição

Verifica se o grupo de implantação está configurado com reversão automática de implantação e monitoramento de implantação com alarmes anexados. Se algo der errado durante uma

implantação, ela será automaticamente revertida e sua aplicação permanecerá em um estado estável

Para obter mais informações, consulte Reimplantar e reverter uma implantação com CodeDeploy.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c18d2gz114`

Origem

`AWS Config Managed Rule: codedeploy-auto-rollback-monitor-enabled`

Critérios de alerta

Amarelo: a reversão automática da implantação e o monitoramento da implantação do AWS CodeDeploy não estão habilitados.

Recommended Action (Ação recomendada)

Configure um grupo de implantação ou uma implantação para reversão automática quando uma implantação falhar ou quando um limite de monitoramento especificado for atendido.

Configure o alarme para monitorar várias métricas, como uso de CPU, uso de memória ou tráfego de rede, durante o processo de implantação. Se alguma dessas métricas exceder determinados limites, os alarmes serão acionados e a implantação será interrompida ou revertida.

Para obter informações sobre como configurar reversões automáticas e alarmes para seus grupos de implantação, consulte Configure advanced options for a deployment group.

Recursos adicionais

O que CodeDeploy é

Colunas do relatório

- Status
- Região

- Recurso
- Regra do AWS Config
- Parâmetros de entrada
- Hora da última atualização

AWS CodeDeployO Lambda está usando all-at-once a configuração de implantação

Descrição

Verifica se o grupo AWS CodeDeploy de implantação da plataforma de AWS Lambda computação está usando a configuração all-at-once de implantação.

Para reduzir o risco de falhas na implantação de suas funções do Lambda CodeDeploy, é uma prática recomendada usar a configuração de implantação canária ou linear em vez da opção padrão, na qual todo o tráfego é transferido da função Lambda original para a função atualizada de uma só vez.

Para obter mais informações, consulte Versões da função do Lambda e Configuração de implantação.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c18d2gz115`

Origem

`AWS Config Managed Rule: codedeploy-lambda-allatonce-traffic-shift-disabled`

Critérios de alerta

Amarelo: a implantação do AWS CodeDeploy Lambda usa a configuração de all-at-once implantação para transferir todo o tráfego para as funções atualizadas do Lambda de uma só vez.

Recommended Action (Ação recomendada)

Use a configuração de implantação Canary ou Linear do grupo de CodeDeploy implantação para a plataforma de computação Lambda.

Recursos adicionais

Configuração de implantação

Colunas do relatório

- Status
- Região
- Recurso
- Regra do AWS Config
- Parâmetros de entrada
- Hora da última atualização

Os relatórios de integridade aprimorada do AWS Elastic Beanstalk não estão configurados

Descrição

Verifica se um ambiente do AWS Elastic Beanstalk está configurado para relatórios de integridade aprimorada.

Os relatórios de integridade aprimorada do Elastic Beanstalk fornecem métricas de desempenho detalhadas, como uso de CPU, uso de memória, tráfego de rede e informações de integridade da infraestrutura, como número de instâncias e status do balanceador de carga.

Para obter mais informações, consulte Monitoramento e relatórios de integridade aprimorada.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c18d2gz108`

Origem

`AWS Config Managed Rule: beanstalk-enhanced-health-reporting-enabled`

Critérios de alerta

Amarelo: o ambiente do Elastic Beanstalk não está configurado para relatórios de integridade aprimorada

Recommended Action (Ação recomendada)

Certifique-se de que um ambiente do Elastic Beanstalk esteja configurado para relatórios de integridade aprimorada.

Para obter mais informações, consulte Habilitar relatórios de integridade aprimorada do console do Elastic Beanstalk.

Recursos adicionais

- Habilitar relatórios de integridade aprimorada do Elastic Beanstalk
- Monitoramento e relatórios de integridade aprimorada

Colunas do relatório

- Status
- Região
- Recurso
- Regra do AWS Config
- Parâmetros de entrada
- Hora da última atualização

AWS Elastic Beanstalk com as atualizações gerenciadas da plataforma desabilitadas

Descrição

Verifica se as atualizações de plataforma gerenciadas nos ambientes e modelos de configuração do Elastic Beanstalk estão habilitadas.

O AWS Elastic Beanstalk lança regularmente atualizações da plataforma para fornecer correções, atualizações de software e novos recursos. Com as atualizações gerenciadas da plataforma, o

Elastic Beanstalk pode realizar automaticamente atualizações de plataforma para novos patches e versões secundárias da plataforma.

Você pode especificar o nível de atualização desejado nos UpdateLevelparâmetros de suas AWS Config regras.

Para obter mais informações, consulte Atualizar a versão de plataforma do ambiente Elastic Beanstalk.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c18d2gz177`

Origem

`AWS Config Managed Rule: elastic-beanstalk-managed-updates-enabled`

Critérios de alerta

Amarelo: as atualizações gerenciadas da plataforma do AWS Elastic Beanstalk não estão configuradas de nenhuma alguma, inclusive em um nível secundário ou de patch.

Recommended Action (Ação recomendada)

Habilite as atualizações gerenciadas de plataforma em seus ambientes do Elastic Beanstalk ou configure-as em um nível secundário ou de atualização.

Para obter mais informações, consulte Atualizações gerenciadas de plataforma.

Recursos adicionais

- Habilitar relatórios de integridade aprimorada do Elastic Beanstalk
- Monitoramento e relatórios de integridade aprimorada

Colunas do relatório

- Status
- Região

- Recurso
- Regra do AWS Config
- Parâmetros de entrada
- Hora da última atualização

A versão da plataforma do AWS Fargate não é a mais recente

Descrição

Verifica se o Amazon ECS está executando a versão mais recente da plataforma do AWS Fargate. A versão da plataforma do Fargate refere-se a um ambiente de runtime específico para a infraestrutura de tarefas do Fargate. Trata-se de uma combinação das versões do kernel e do runtime do contêiner. Novas versões da plataforma são lançadas à medida que o ambiente de runtime evolui. Por exemplo, se houver atualizações do kernel ou do sistema operacional, novos recursos, correções de erros ou atualizações de segurança.

Para obter mais informações, consulte Fargate task maintenance.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c18d2gz174`

Origem

`AWS Config Managed Rule: ecs-fargate-latest-platform-version`

Critérios de alerta

Amarelo: o Amazon ECS não está sendo executado na versão mais recente da plataforma do Fargate.

Recommended Action (Ação recomendada)

Atualize para a versão mais recente da plataforma do Fargate.

Para obter mais informações, consulte Fargate task maintenance.

Colunas do relatório

- Status
- Região
- Recurso
- Regra do AWS Config
- Parâmetros de entrada
- Hora da última atualização

Associação do Gerenciador de Estados do AWS Systems Manager em status de não conformidade

Descrição

Verifica se o status de conformidade da associação do AWS Systems Manager é COMPLIANT ou NON_COMPLIANT após a execução da associação na instância.

O Gerenciador de Estados, um recurso do AWS Systems Manager, é um serviço de gerenciamento de configuração seguro e escalável que automatiza o processo de manter os nós gerenciados e outros recursos da AWS em um estado definido por você. Uma associação do Gerenciador de Estados é uma configuração que você atribui aos seus recursos da AWS. A configuração define o estado que você deseja manter em seus recursos e, portanto, ajuda você a atingir a meta, como evitar desvios de configuração em suas instâncias do Amazon EC2.

Para obter mais informações, consulte Gerenciador de Estados do AWS Systems Manager.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c18d2gz147`

Origem

`AWS Config Managed Rule: ec2-managedinstance-association-compliance-status-check`

Critérios de alerta

Amarelo: o status da conformidade da associação do AWS Systems Manager é NON_COMPLIANT.

Recommended Action (Ação recomendada)

Valide o status das associações do Gerenciador de Estados e, em seguida, execute as ações necessárias para retornar o status para COMPLIANT.

Para obter mais informações, consulte Sobre o Gerenciador de Estados.

Recursos adicionais

Gerenciador de Estados do AWS Systems Manager

Colunas do relatório

- Status
- Região
- Recurso
- Regra do AWS Config
- Parâmetros de entrada
- Hora da última atualização

CloudTrail as trilhas não estão configuradas com o Amazon CloudWatch Logs

Descrição

Verifica se as AWS CloudTrail trilhas estão configuradas para enviar registros para o CloudWatch Logs.

Monitore os arquivos de CloudTrail log com o CloudWatch Logs para acionar uma resposta automática quando eventos críticos forem capturadosAWS CloudTrail.

Para obter mais informações, consulte Monitoramento de arquivos de CloudTrail log com CloudWatch registros.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c18d2gz164`

Origem

`AWS Config Managed Rule: cloud-trail-cloud-watch-logs-enabled`

Critérios de alerta

Amarelo: não AWS CloudTrail está configurado com a integração do CloudWatch Logs.

Recommended Action (Ação recomendada)

Configure CloudTrail trilhas para enviar eventos de registro para o CloudWatch Logs.

Para obter mais informações, consulte Criação de CloudWatch alarmes para CloudTrail eventos: exemplos.

Colunas do relatório

- Status
- Região
- Recurso
- Regra do AWS Config
- Parâmetros de entrada
- Hora da última atualização

A proteção contra exclusão do Elastic Load Balancing não está habilitada para balanceadores de carga

Descrição

Verifica se a proteção contra exclusão está habilitada para seus balanceadores de carga.

O Elastic Load Balancing oferece suporte à proteção contra exclusão para seus Application Load Balancers, Network Load Balancers e Gateway Load Balancers. Ative a proteção contra exclusão para evitar que seu balanceador de carga seja excluído acidentalmente. A proteção contra exclusão é desativada por padrão quando você cria um balanceador de carga. Se os balanceadores de carga fizerem parte de um ambiente de produção, considere a possibilidade de ativar a proteção contra exclusão.

Os logs de acesso são um recurso opcional do Elastic Load Balancing que é desabilitado por padrão. Depois que os logs de acesso para seu balanceador de carga forem habilitados, o Elastic Load Balancing capturará os logs e os armazenará no bucket do Amazon S3 que você especificar.

Para obter mais informações, consulte Application Load Balancer Deletion protection, Network Load Balancers Deletion protection ou Gateway Load Balancers Deletion protection.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c18d2gz168`

Origem

`AWS Config Managed Rule: elb-deletion-protection-enabled`

Critérios de alerta

Amarelo: a proteção contra exclusão não está habilitada para um balanceador de carga.

Recommended Action (Ação recomendada)

Ative a proteção contra exclusão para seus Application Load Balancers, Network Load Balancers e Gateway Load Balancers.

Para obter mais informações, consulte Application Load Balancer Deletion protection, Network Load Balancers Deletion protection ou Gateway Load Balancers Deletion protection.

Colunas do relatório

- Status
- Região
- Recurso
- Regra do AWS Config
- Parâmetros de entrada
- Hora da última atualização

Verificação da proteção contra exclusão do cluster de banco de dados do RDS

Descrição

Verifica se seus clusters de banco de dados do Amazon RDS têm a proteção contra exclusão habilitada.

Quando um cluster é configurado com proteção contra exclusão, o banco de dados não pode ser excluído por nenhum usuário.

A proteção contra exclusão está disponível para instâncias de banco de dados do Amazon Aurora e RDS para MySQL, do RDS para MariaDB, do RDS para Oracle, do RDS para PostgreSQL e do RDS para SQL Server em todas as regiões da AWS.

Para obter mais informações, consulte Proteção contra exclusão para clusters do Aurora.

ID da verificação

`c18d2gz160`

Origem

`AWS Config Managed Rule: rds-cluster-deletion-protection-enabled`

Critérios de alerta

Amarelo: você tem clusters de banco de dados do Amazon RDS que não têm a proteção contra exclusão habilitada.

Recommended Action (Ação recomendada)

Ative a proteção contra exclusão ao criar um cluster de banco de dados do Amazon RDS.

Você só pode excluir clusters que não tenham a proteção contra exclusão habilitada. Habilitar a proteção contra exclusão adiciona uma camada extra de proteção e evita a perda de dados devido à exclusão acidental ou não acidental de uma instância de banco de dados. A proteção contra exclusão também ajuda a atender aos requisitos de conformidade normativa e a garantir a continuidade dos negócios.

Para obter mais informações, consulte Proteção contra exclusão para clusters do Aurora.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

Recursos adicionais

Proteção contra exclusão para clusters do Aurora.

Colunas do relatório

- Status
- Região
- Recurso
- Regra do AWS Config
- Parâmetros de entrada
- Hora da última atualização

Verificação de atualização automática de versão secundária da instância de banco de dados do RDS

Descrição

Verifica se as instâncias de banco de dados do Amazon RDS têm atualizações automáticas de versões secundárias configuradas.

Ative as atualizações automáticas de versões secundárias para uma instância do Amazon RDS para garantir que o banco de dados esteja sempre executando a versão mais recente, segura

e estável. Pequenas atualizações fornecem atualizações de segurança, correções de erros, melhorias de desempenho e mantêm a compatibilidade com as aplicações existentes.

Para obter mais informações, consulte Atualizar a versão de mecanismo de uma instância de banco de dados.

> **Note**
>
> Os resultados dessa verificação são atualizados automaticamente várias vezes ao dia e as solicitações de atualização não são permitidas. Poderá levar algumas horas para que as alterações sejam exibidas. Não é possível excluir recursos dessa verificação.

ID da verificação

`c18d2gz155`

Origem

`AWS Config Managed Rule: rds-automatic-minor-version-upgrade-enabled`

Critérios de alerta

Amarelo: a instância de banco de dados do RDS não tem atualizações automáticas de versões secundárias ativadas.

Recommended Action (Ação recomendada)

Ative as atualizações automáticas de versões secundárias ao criar uma instância de banco de dados do Amazon RDS.

Quando você ativa a atualização de versão secundária, a versão do banco de dados será atualizada automaticamente se estiver executando uma versão secundária do mecanismo de BD que seja inferior à versão de atualização manual do mecanismo.

Colunas do relatório

- Status
- Região
- Recurso
- Regra do AWS Config
- Parâmetros de entrada
- Hora da última atualização

Registro de alterações para AWS Trusted Advisor

Consulte o tópico a seguir para ver as mudanças recentes nas Trusted Advisor verificações.

> **Note**
>
> Se você usar o Trusted Advisor console ou a AWS Support API, as verificações que foram removidas não aparecerão nos resultados das verificações. Se você usar qualquer uma das verificações removidas, como especificar o ID da verificação em uma operação de AWS Support API ou seu código, deverá remover essas verificações para evitar erros de chamada de API.

Para obter mais informações sobre as verificações disponíveis, consulte o Referência de verificação do AWS Trusted Advisor.

Nova verificação de tolerância a falhas

Trusted Advisor adicionou 1 verificação de tolerância a falhas em 29 de fevereiro de 2024:

- NLB - Recurso voltado para a Internet em sub-rede privada

Para obter mais informações, consulte Referência de verificação do AWS Trusted Advisor.

Tolerância a falhas e verificações de segurança atualizadas

Trusted Advisor adicionou 1 nova verificação de tolerância a falhas e alterou 1 tolerância a falhas existente e 1 verificação de segurança em 28 de março de 2024:

- Verificação AWS Resilience Hub de componente de aplicativo adicionada
- Funções atualizadas AWS Lambda habilitadas para VPC sem redundância Multi-AZ
- AWS Lambda Funções atualizadas usando tempos de execução obsoletos

Para obter mais informações, consulte Referência de verificação do AWS Trusted Advisor.

Nova verificação de tolerância a falhas

Trusted Advisor adicionou 1 verificação de tolerância a falhas em 31 de janeiro de 2024:

- AWS Direct Connect Resiliência de localização

Para obter mais informações, consulte Referência de verificação do AWS Trusted Advisor.

Verificação atualizada de tolerância a falhas

Trusted Advisor alterou 1 verificação de tolerância a falhas em 08 de janeiro de 2024:

- O parâmetro innodb_flush_log_at_trx_commit do Amazon RDS não é 1

Para obter mais informações, consulte Referência de verificação do AWS Trusted Advisor.

Verificação de segurança atualizada

Trusted Advisor alterou 1 Verificação de segurança em 21 de dezembro de 2023:

- AWS Lambda Funções usando tempos de execução obsoletos

Para obter mais informações, consulte Referência de verificação do AWS Trusted Advisor.

Novas verificações de segurança e desempenho

Trusted Advisor adicionou 2 novas verificações de segurança e 2 novas verificações de desempenho em 20 de dezembro de 2023:

- Clientes Amazon EFS que não usam data-in-transit criptografia
- Cluster de banco de dados Amazon Aurora subprovisionado para carga de trabalho de leitura
- Instância do Amazon RDS subprovisionada para capacidade do sistema
- Fim do suporte padrão para instâncias do Amazon EC2 com Ubuntu LTS

Para obter mais informações, consulte Referência de verificação do AWS Trusted Advisor.

Nova verificação de segurança

Trusted Advisor adicionou 1 nova verificação de segurança em 15 de dezembro de 2023:

- Registros CNAME incompatíveis do Amazon Route 53 apontando diretamente para buckets S3

Para obter mais informações, consulte Referência de verificação do AWS Trusted Advisor.

Novas verificações de tolerância a falhas e otimização de custos

Trusted Advisor adicionou 2 novas verificações de tolerância a falhas e 1 nova verificação de otimização de custos em 07 de dezembro de 2023:

- Clusters Single-AZ do Amazon DocumentDB
- Configuração de cancelamento de upload em várias partes incompleta do Amazon S3
- Driver do Amazon ECS AWS Logs em modo de bloqueio

Para obter mais informações, consulte Referência de verificação do AWS Trusted Advisor.

Novas verificações de tolerância a falhas

Trusted Advisor adicionou 3 novas verificações de tolerância a falhas em 17 de novembro de 2023:

- ALB Multi-AZ
- NLB Multi-AZ
- Interface VPC, endpoint, interfaces de rede em várias AZs

Para obter mais informações, consulte Referência de verificação do AWS Trusted Advisor.

Novas verificações para o Amazon RDS

Trusted Advisor adicionou 37 novas verificações para o Amazon RDS em 15 de novembro de 2023.

Para obter mais informações, consulte Referência de verificação do AWS Trusted Advisor.

Nova AWS Trusted Advisor API

AWS Trusted Advisor apresenta novas APIs para permitir que você acesse programaticamente as verificações, recomendações e recomendações priorizadas de melhores práticas do Trusted Advisor. Trusted Advisor As APIs permitem que você se Trusted Advisor integre programaticamente à sua ferramenta operacional preferida para automatizar e otimizar suas cargas de trabalho em grande escala. Disponíveis para clientes Business, Enterprise On-Ramp ou Enterprise Support, as novas APIs fornecem acesso a Trusted Advisor recomendações para sua conta ou para todas as contas vinculadas em uma conta pagante. Os clientes do Enterprise Support com acesso a

contas gerenciais ou de administrador delegado também podem recuperar programaticamente recomendações priorizadas em toda a organização.

As novas Trusted Advisor APIs substituirão as 3 funcionalidades oferecidas anteriormente pela AWS Support API (SAPI). A SAPI continuará oferecendo casos e outras informações de suporte.

Trusted Advisor As APIs geralmente estão disponíveis nas regiões Leste dos EUA (Ohio), Leste dos EUA (Norte da Virgínia), Oeste dos EUA (Oregon), Ásia-Pacífico (Seul), Ásia-Pacífico (Sydney) e Europa (Irlanda).

Para saber mais, visite a página AWS Trusted Advisor da API.

Trusted Advisor verifique a remoção

Trusted Advisor removeu as seguintes verificações em 9 de novembro de 2023.

Nome da verificação	Categoria da verificação	ID da verificação
Os volumes do EBS devem ser anexados às instâncias do EC2	Segurança	`Hs4Ma3G119`
Os buckets do S3 devem ter a criptografia no lado do servidor habilitada	Segurança	`Hs4Ma3G167`
CloudFront as distribuições devem ter a identidade de acesso de origem ativada	Segurança	`Hs4Ma3G195`

Integração de AWS Config cheques em Trusted Advisor

Trusted Advisor adicionou 64 novos cheques fornecidos AWS Config em 30 de outubro de 2023.

Para obter mais informações, consulte Exibir as verificações do AWS Trusted Advisor fornecidas pelo AWS Config.

Novas verificações de tolerância a falhas

Trusted Advisor adicionou as seguintes verificações em 12 de outubro de 2023.

- Amazon RDS ReplicaLag
- Amazon RDS FreeStorageSpace
- Amazon RDS DiskQueueDepth
- Amazon Route 53 Resolver Redundância da zona de disponibilidade do endpoint
- IPs disponíveis para ajuste de escala automático em sub-redes
- Agentes do Amazon MSK que hospedam muitas partições

Para obter mais informações, consulte a categoria de Tolerância a falhas.

Verificação de novos limites de serviço

Trusted Advisor adicionou a seguinte verificação em 17 de agosto de 2023.

- Uso do armazenamento de código Lambda

Para obter mais informações, consulte a categoria de Limites do serviço.

Nova verificação de tolerância a falhas

Trusted Advisor adicionou a seguinte verificação em 3 de agosto de 2023.

- AWS Lambda Sobre destinos de eventos de falha

Para obter mais informações, consulte a categoria de Tolerância a falhas.

Novas verificações de tolerância a falhas e performance

Trusted Advisor adicionou as seguintes verificações em 1º de junho de 2023.

- Redundância de destino sem montagem do Amazon EFS
- Otimização do modo throughput do Amazon EFS
- Redundância de zona de disponibilidade do ActiveMQ
- Redundância de zona de disponibilidade do RabbitMQ

Para obter mais informações, consulte as categorias Tolerância a falhas e Performance.

Novas verificações de tolerância a falhas

Trusted Advisor adicionou as seguintes verificações em 16 de maio de 2023.

- Independência da AZ do NAT Gateway
- Verificação de aplicação de AZ única

Para obter mais informações, consulte a categoria de Tolerância a falhas.

Novas verificações de tolerância a falhas

Trusted Advisor adicionou as seguintes verificações em 27 de abril de 2023.

- Número de Regiões da AWS em um conjunto de replicação do Incident Manager
- AWS Resilience Hub idade de avaliação

Para obter mais informações, consulte a categoria de Tolerância a falhas.

Expansão regional das verificações de tolerância a falhas do Amazon ECS

Trusted Advisor expandiu as seguintes verificações para outras regiões em 27 de abril de 2023. Trusted Advisor as verificações do Amazon ECS agora estão disponíveis em todas as regiões onde o Amazon ECS está geralmente disponível.

- Serviço do Amazon ECS usando uma única AZ
- Estratégia de posicionamento multi-AZ do Amazon ECS

As regiões expandidas incluem: África (Cidade do Cabo), Ásia-Pacífico (Hong Kong), Ásia-Pacífico (Hyderabad), Ásia-Pacífico (Jacarta), Ásia-Pacífico (Melbourne), Europa (Milão), Europa (Espanha), Europa (Zurique), Oriente Médio (Bahrein) e Oriente Médio (Emirados Árabes Unidos).

Novas verificações de tolerância a falhas

Trusted Advisor adicionou as seguintes verificações em 30 de março de 2023.

- Serviço do Amazon ECS usando uma única AZ
- Estratégia de posicionamento multi-AZ do Amazon ECS

Para obter mais informações, consulte a categoria de Tolerância a falhas.

Novas verificações de tolerância a falhas

Trusted Advisor adicionou as seguintes verificações em 15 de dezembro de 2022.

- AWS CloudHSM clusters executando instâncias do HSM em uma única AZ
- Clusters Amazon ElastiCache Multi-AZ
- Clusters multi-AZ do Amazon MemoryDB

Para receber resultados Trusted Advisor para seus clusters AWS CloudHSM ElastiCache, e MemoryDB, você deve ter clusters em suas zonas de disponibilidade. Para obter mais informações, consulte a seguinte documentação do :

- AWS CloudHSM Guia do usuário
- Guia do desenvolvedor do Amazon MemoryDB para Redis
- Guia do usuário do Amazon ElastiCache for Redis

Trusted Advisor atualizou as seguintes informações de verificação em 15 de dezembro de 2022.

- AWS Resilience Hub política violada — O nome do aplicativo foi atualizado para o nome do aplicativo
- AWS Resilience Hub pontuações de resiliência — Nome do aplicativo e Pontuação de resiliência do aplicativo foram atualizados para Nome do aplicativo e Pontuação de resiliência do aplicativo

Para obter mais informações, consulte a categoria de Tolerância a falhas.

Atualizações na Trusted Advisor integração com AWS Security Hub

Trusted Advisor fez a seguinte atualização em 17 de novembro de 2022.

Se você desabilitar o Security Hub ou AWS Config for an Região da AWS, Trusted Advisor agora removerá suas descobertas de controle Região da AWS em 7 a 9 dias. Anteriormente, o prazo para remover seus dados do Security Hub Trusted Advisor era de 90 dias.

Para obter mais informações, consulte as seguintes seções no tópico Solução de problemas:

- Desativei o Security Hub ou o AWS Config em uma região

- Meu controle está arquivado no Security Hub, mas ainda vejo as descobertas no Trusted Advisor

Novas verificações de tolerância a falhas para o AWS Resilience Hub

Trusted Advisor adicionou as seguintes verificações em 17 de novembro de 2022.

- AWS Resilience Hub política violada
- AWS Resilience Hub pontuações de resiliência

Você pode usar essas verificações para visualizar o status mais recente da política de resiliência e a pontuação de resiliência para suas aplicações. O Resilience Hub fornece um local central para definir, monitorar e gerenciar a resiliência e a disponibilidade de suas aplicações.

Para receber resultados Trusted Advisor para seus aplicativos do Resilience Hub, você deve implantar um AWS aplicativo e usar o Resilience Hub para rastrear a postura de resiliência do aplicativo. Para mais informações, consulte o Guia do usuário do AWS Resilience Hub.

Para receber resultados Trusted Advisor para seus clusters ElastiCache e MemoryDB, você deve ter clusters em suas zonas de disponibilidade. Para obter mais informações, consulte a seguinte documentação do :

- Guia do desenvolvedor do Amazon MemoryDB para Redis
- Guia do usuário do Amazon ElastiCache for Redis

Para obter mais informações, consulte a categoria de Tolerância a falhas.

Atualização para o Trusted Advisor console

Trusted Advisor adicionou a seguinte alteração em 16 de novembro de 2022.

O Trusted Advisor painel no console agora é Trusted Advisor Recomendações. A página Recomendações do Trusted Advisor ainda exibe os resultados da verificação e as verificações disponíveis para cada categoria de sua Conta da AWS.

Essa alteração de nome atualiza apenas o Trusted Advisor console. Você pode continuar usando o Trusted Advisor console e as Trusted Advisor operações na AWS Support API normalmente.

Para ter mais informações, consulte Conceitos básicos das recomendações do Trusted Advisor.

Novas verificações para o Amazon EC2

Trusted Advisor adicionou a seguinte verificação em 1º de setembro de 2022.

- Fim do suporte para instâncias do Amazon EC2 com o Microsoft Windows Server

Para obter mais informações, consulte a categoria de Segurança.

Verificações do Security Hub adicionadas ao Trusted Advisor

A partir de 23 de junho de 2022, Trusted Advisor só oferece suporte aos controles do Security Hub disponíveis até 7 de abril de 2022. Esta versão oferece suporte a todos os controles do padrão de segurança AWS Foundational Security Best Practices, exceto os controles na categoria: Recuperação > Resiliência. Para obter mais informações, consulte Visualizar os controles do AWS Security Hub no AWS Trusted Advisor.

Para obter uma lista dos controles, consulte AWS Foundational Security Best Practices controls no Guia do usuário do AWS Security Hub .

Cheques adicionados de AWS Compute Optimizer

Trusted Advisor adicionou as seguintes verificações em 4 de maio de 2022.

Nome da verificação	Categoria da verificação	ID da verificação
Volumes superprovisionados do Amazon EBS	Otimização de custo	`COr6dfpM03`
Volumes subprovisionados do Amazon EBS	Performance	`COr6dfpM04`
AWS Lambda funções superprovisionadas para o tamanho da memória	Otimização de custo	`COr6dfpM05`
AWS Lambda funções subprovisionadas para o tamanho da memória	Performance	`COr6dfpM06`

Você deve optar pelo Compute Optimizer Conta da AWS para que essas verificações possam receber dados de seus recursos do Lambda e do Amazon EBS. Para ter mais informações, consulte Optar por verificações do Trusted Advisor para o AWS Compute Optimizer.

Atualizações para a verificação de chaves de acesso expostas

Trusted Advisor atualizou a seguinte verificação em 25 de abril de 2022.

Nome da verificação	Categoria da verificação	ID da verificação
Exposed Access Keys	Segurança	`12Fnkpl8Y5`

Trusted Advisor agora atualiza essa verificação para você automaticamente. Essa verificação não pode ser atualizada manualmente no Trusted Advisor console ou na AWS Support API. Se seu aplicativo ou código atualizar essa verificação para você Conta da AWS, recomendamos que você a atualize para não atualizar mais essa verificação. Caso contrário, você receberá o erro `InvalidParameterValue`.

Todas as chaves de acesso que você excluiu antes dessa atualização não serão mais excluídas e aparecerão como recursos afetados. Você não pode excluir chaves de acesso dos resultados da verificação. Para obter mais informações, consulte Exposed Access Keys.

> **Note**
>
> Se você criou a sua Conta da AWS depois de 25 de abril de 2022, os resultados da verificação de Chaves de Acesso Expostas mostram inicialmente o ícone cinza ( ), mesmo para chaves de acesso não expostas. Isso significa que o Trusted Advisor não identificou nenhuma alteração na verificação.
> Se Trusted Advisor identificar um recurso em risco, o status muda para o ícone de ação recomendada ( ).
> Após corrigir ou excluir o recurso, o resultado da verificação mostrará o ícone de marca de seleção ( ).

Verificações atualizadas para AWS Direct Connect

Trusted Advisor atualizou as seguintes verificações em 29 de março de 2022.

Nome da verificação	Categoria da verificação	ID da verificação
AWS Direct Connect Redundância de conexão	Tolerância a falhas	`0t121N1Ty3`
AWS Direct Connect Redundância de localização	Tolerância a falhas	`8M012Ph3U5`
AWS Direct Connect Redundância de interface virtual	Tolerância a falhas	`4g3Nt5M1Th`

- O valor da coluna Região agora mostra o código da Região da AWS em vez do nome completo. Por exemplo, os recursos no Leste dos EUA (Norte da Virgínia) agora terão o valor de `us-east-1`.
- O valor da coluna Carimbo de data/hora agora aparece no formato RFC 3339, como`2022-03-30T01:02:27.000Z`.
- Os recursos que não tiverem problemas detectados agora aparecerão na tabela de verificação. Esses recursos terão um ícone de marca de seleção () ao lado deles.

  Anteriormente, somente os recursos que Trusted Advisor recomendavam que você investigasse apareciam na tabela. Esses recursos têm um ícone de aviso () ao lado deles.

AWS Security Hub controles adicionados ao AWS Trusted Advisor console

AWS Trusted Advisor adicionou 111 controles do Security Hub à categoria Segurança em 18 de janeiro de 2022.

Você pode ver suas descobertas sobre os controles do Security Hub a partir do padrão de segurança AWS Foundational Security Best Practices. Essa integração não inclui os controles que têm a Category: Recover > Resilience (Categoria: Recuperar > Resiliência).

Para obter mais informações sobre esse recurso, consulte Visualizar os controles do AWS Security Hub no AWS Trusted Advisor.

Novas verificações para o Amazon EC2 e o AWS Well-Architected

Trusted Advisor adicionou as seguintes verificações em 20 de dezembro de 2021.

- Consolidação de instâncias do Amazon EC2 para Microsoft SQL Server
- Instâncias do Amazon EC2 superprovisionadas para Microsoft SQL Server
- Fim do suporte para instâncias do Amazon EC2 com o Microsoft SQL Server
- Problemas de alto risco do AWS Well-Architected para otimização de custos
- Problemas de alto risco do AWS Well-Architected em relação à performance
- Problemas de alto risco do AWS Well-Architected em relação à segurança
- Problemas de alto risco do AWS Well-Architected em relação à confiabilidade

Para obter mais informações, consulte Referência da verificação do AWS Trusted Advisor.

Nome do cheque atualizado para o Amazon OpenSearch Service

Trusted Advisor atualizou o nome do Amazon OpenSearch Service Reserved Instance Optimization cheque em 8 de setembro de 2021.

As recomendações de verificação, categoria e ID são as mesmas.

Nome da verificação	Categoria da verificação	ID da verificação
Otimização de instâncias reservadas do Amazon OpenSearch Service	Otimização de custo	`7ujm6yhn5t`

> **Note**
>
> Se você usa Trusted Advisor CloudWatch métricas da Amazon, o nome da métrica para essa verificação também é atualizado. Para obter mais informações, consulte Criar alarmes do Amazon CloudWatch para monitorar métricas do AWS Trusted Advisor.

Verificações adicionadas para o armazenamento de volumes do Amazon Elastic Block Store

Trusted Advisor adicionou as seguintes verificações em 8 de junho de 2021.

Nome da verificação	Categoria da verificação	ID da verificação
Armazenamento de volumes SSD de uso geral (gp3) do EBS	Limites do serviço	`dH7RR0l6J3`
Armazenamento de volumes SSD de IOPS provisionadas (io2) do EBS	Limites do serviço	`gI7MM0l7J2`

Verificações adicionadas para AWS Lambda

Trusted Advisor adicionou as seguintes verificações em 8 de março de 2021.

Nome da verificação	Categoria da verificação	ID da verificação
AWS Lambda Funções com tempos limite excessivos	Otimização de custo	`L4dfs2Q3C3`
AWS Lambda Funções com altas taxas de erro	Otimização de custo	`L4dfs2Q3C2`
AWS Lambda Funções usando tempos de execução obsoletos	Segurança	`L4dfs2Q4C5`

Nome da verificação	Categoria da verificação	ID da verificação
AWS Lambda Funções habilitadas para VPC sem redundância Multi-AZ	Tolerância a falhas	`L4dfs2Q4C6`

Para obter mais informações sobre como usar essas verificações com o Lambda, consulte Exemplo de AWS Trusted Advisor fluxo de trabalho para ver as recomendações no Guia do AWS Lambda desenvolvedor.

Trusted Advisor verifique a remoção

Trusted Advisor removeu a seguinte verificação para o AWS GovCloud (US) Region em 8 de março de 2021.

Nome da verificação	Categoria da verificação	ID da verificação
Endereços de IP elástico do EC2	Limites do serviço	`aW9HH0l8J6`

Verificações atualizadas para o Amazon Elastic Block Store

Trusted Advisor atualizou a unidade do volume do Amazon EBS de gibibyte (GiB) para tebibyte (TiB) para as seguintes verificações em 5 de março de 2021.

> **Note**
>
> Se você usa Trusted Advisor CloudWatch métricas da Amazon, os nomes das métricas dessas cinco verificações também são atualizados. Para ter mais informações, consulte Criar alarmes do Amazon CloudWatch para monitorar métricas do AWS Trusted Advisor.

Nome da verificação	Categoria da verificação	ID da verificação	CloudWatch Métrica atualizada para ServiceLimit
Armazenamento de volume EBS de disco rígido frio (sc1)	Limites do serviço	`gH5CC0e3J9`	Armazenamento de volume (TiB) de disco rígido frio (sc1)
Armazenamento de volume EBS (gp2) de uso geral SSD	Limites do serviço	`dH7RR0l6J9`	Armazenamento de volume (gp2) de uso geral SSD (TiB)
Armazenamento de volume (padrão) magnético EBS	Limites do serviço	`cG7HH0l7J9`	Armazenamento de volume (padrão) magnético (TiB)
Armazenamento de volumes SSD de IOPS provisionadas (io1) do EBS	Limites do serviço	`gI7MM0l7J9`	Armazenamento (SSD) de IOPS provisionadas (TiB)
Armazenamento de volume HDD otimizados para throughput (st1) EBS	Limites do serviço	`wH7DD0l3J9`	Armazenamento de volume HDD otimizados para throughput (st1)

Trusted Advisor verifique a remoção

> **Note**
>
> Trusted Advisor removeu as seguintes verificações em 18 de novembro de 2020.

Verificações removidos em 18 de novembro de 2020	Categoria da verificação	ID da verificação
Serviço do EC2Config para instâncias do EC2 Windows	Tolerância a falhas	V77iOLlBqz
Versão do driver ENA para instâncias do EC2 Windows	Tolerância a falhas	TyfdMXG69d
Versão do driver NVMe para instâncias do EC2 Windows	Tolerância a falhas	yHAGQJV9K5
Versão do driver PV para instâncias do EC2 Windows	Tolerância a falhas	Wnwm9Il5bG
Volumes ativos do EBS	Limites do serviço	fH7LL0l7J9

O Amazon Elastic Block Store não tem mais um limite no número de volumes que você pode provisionar.

É possível monitorar suas instâncias do Amazon EC2 e verificar se elas estão atualizadas usando o Distribuidor do AWS Systems Manager, outras ferramentas de terceiros ou escrever seus próprios scripts para retornar informações de driver para o Windows Management Instrumentation (WMI).

Trusted Advisor verifique a remoção

Trusted Advisor removeu a seguinte verificação em 18 de fevereiro de 2020.

Nome da verificação	Categoria da verificação	ID da verificação
Service Limits	Performance	eW7HH0l7J9

Aplicativo AWS Support no Slack

Você pode usar o aplicativo AWS Support para gerenciar seus casos de suporte AWS no Slack. Você pode convidar os membros da sua equipe para canais de chat, responder às atualizações de casos e conversar diretamente com os atendentes de suporte. O aplicativo AWS Support ajuda você a gerenciar casos de suporte de forma rápida e direta no Slack.

É possível usar o aplicativo AWS Support para fazer o seguinte:

- Criar, atualizar, procurar e resolver casos de suporte nos canais do Slack
- Anexar arquivos aos casos de suporte
- Solicitar aumentos de cota do Service Quotas
- Compartilhar detalhes do caso de suporte com a sua equipe sem sair do canal do Slack
- Iniciar uma sessão de chat ao vivo com os atendentes de suporte

Quando você cria, atualiza ou resolve um caso de suporte no AWS Support App, o caso também é atualizado no AWS Support Center Console. Não é preciso fazer login no console do Support Center para gerenciar seus casos de suporte individualmente.

Observações

- Os tempos de resposta para os casos de suporte são os mesmos, independentemente de você ter criado o caso no Slack ou no console do Support Center.
- Você pode criar um caso de suporte para suporte de conta e faturamento, aumentos de cotas de serviço e suporte técnico.

Tópicos

- Pré-requisitos
- Autorizar um espaço de trabalho do Slack
- Como configurar um canal do Slack
- Como criar casos de suporte em um canal do Slack
- Como responder a casos de suporte no Slack

- Como entrar em uma sessão de chat ao vivo com o AWS Support
- Como procurar casos de suporte no Slack
- Como resolver um caso de suporte no Slack
- Como reabrir um caso de suporte no Slack
- Como solicitar um aumento de cota de serviço
- Como excluir uma configuração de canal do Slack do aplicativo AWS Support
- Como excluir uma configuração de espaço de trabalho do Slack no aplicativo AWS Support
- Aplicativo AWS Support nos comandos do Slack
- Visualizar correspondências do aplicativo AWS Support no AWS Support Center Console
- Como criar o aplicativo AWS Support em recursos do Slack com o AWS CloudFormation

Pré-requisitos

Você deve atender aos seguintes requisitos para usar o aplicativo AWS Support no Slack:

- Você tem um plano de suporte Business, Enterprise On-Ramp ou Enterprise. É possível encontrar seu plano de suporte no AWS Support Center Console ou na página Support plans (Planos de suporte). Para obter mais informações, consulte Comparar os planos do AWS Support.
- Você tem um espaço de trabalho e o canal do Slack para sua organização. É preciso que você seja um administrador do espaço de trabalho do Slack ou que tenha permissão para adicionar aplicativos a esse espaço de trabalho. Para obter mais informações, consulte a Slack Help Center (Central de ajuda do Slack).
- Faça login na Conta da AWS como um usuário ou perfil do AWS Identity and Access Management (IAM) com as permissões necessárias. Para obter mais informações, consulte Como gerenciar o acesso ao widget do aplicativo AWS Support.
- É preciso criar um perfil do IAM que tenha as permissões necessárias para executar as ações para você. O aplicativo AWS Support usa esse perfil para fazer chamadas de API para diferentes serviços. Para obter mais informações, consulte Como gerenciar o acesso ao aplicativo AWS Support.

Tópicos

- Como gerenciar o acesso ao widget do aplicativo AWS Support
- Como gerenciar o acesso ao aplicativo AWS Support

Como gerenciar o acesso ao widget do aplicativo AWS Support

Você pode anexar uma política do AWS Identity and Access Management (IAM) que conceda uma permissão de usuário do IAM para configurar o widget do aplicativo AWS Support no AWS Support Center Console.

Para obter mais informações sobre como acrescentar uma política a uma entidade do IAM, consulte Adding IAM identity permissions (console) [Adicionar permissões de identidade do IAM (console)] no Guia do usuário do IAM.

> **Note**
>
> Você também pode fazer login como usuário raiz na sua Conta da AWS, mas não recomendamos que faça isso. Para obter mais informações sobre o acesso do usuário raiz, consulte Safeguard your root user credentials and don't use them for everyday tasks (Proteja suas credenciais de usuário raiz e não as use para tarefas diárias) no Guia do usuário do IAM.

Exemplo de política do IAM

Você pode anexar a política a seguir a uma entidade, como um usuário ou grupo do IAM. Essa política permite que um usuário autorize um espaço de trabalho do Slack e configure os canais do Slack no console do Support Center.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "supportapp:GetSlackOauthParameters",
                "supportapp:RedeemSlackOauthCode",
                "supportapp:DescribeSlackChannels",
                "supportapp:ListSlackWorkspaceConfigurations",
                "supportapp:ListSlackChannelConfigurations",
                "supportapp:CreateSlackChannelConfiguration",
                "supportapp:DeleteSlackChannelConfiguration",
                "supportapp:DeleteSlackWorkspaceConfiguration",
                "supportapp:GetAccountAlias",
```

```
                "supportapp:PutAccountAlias",
                "supportapp:DeleteAccountAlias",
                "supportapp:UpdateSlackChannelConfiguration",
                "iam:ListRoles"
            ],
            "Resource": "*"
        }
    ]
}
```

Permissões necessárias para conectar a aplicação AWS Support ao Slack

A aplicação AWS Support inclui ações somente de permissão que não correspondem diretamente a uma operação de API. Essas ações são indicadas na Referência de autorização de serviço com [permission only].

A aplicação AWS Support usa as seguintes ações de API para se conectar ao Slack e, em seguida, lista seus canais públicos do Slack no AWS Support Center Console:

- `supportapp:GetSlackOauthParameters`
- `supportapp:RedeemSlackOauthCode`
- `supportapp:DescribeSlackChannels`

Essas ações de API não devem ser chamadas pelo código. Por isso, essas ações de API não são incluídas na AWS CLI e nos SDKs da AWS.

Como gerenciar o acesso ao aplicativo AWS Support

Após obter as permissões para o widget do aplicativo AWS Support, você também deve criar um perfil do IAM do AWS Identity and Access Management. Esse perfil executa ações de outros Serviços da AWS para você, como a API do AWS Support e o Service Quotas.

Em seguida, você anexa uma política do IAM a esse perfil para obter as permissões necessárias para concluir essas ações. Esse perfil é escolhido ao criar a configuração do seu canal do Slack no console do Support Center.

Os usuários do seu canal do Slack têm as mesmas permissões concedidas ao perfil do IAM. Por exemplo, se você especificar o acesso somente leitura aos seus casos de suporte, os usuários do seu canal do Slack poderão visualizar seus casos de suporte, mas não poderão atualizá-los.

> **Important**
>
> Quando você solicita um chat ao vivo com um atendente de suporte e escolhe um novo canal privado como sua preferência de canal de chat ao vivo, o AWS Support App cria um canal separado do Slack. Esse canal do Slack tem as mesmas permissões do canal em que você criou o caso ou iniciou o chat.
> Se você alterar o perfil ou a política do IAM, suas alterações se aplicarão ao canal configurado do Slack e a quaisquer novos canais de chat ao vivo do Slack que o aplicativo AWS Support criar para você.

Siga esses procedimentos para criar seu perfil e sua política do IAM.

Tópicos

- Use uma política gerenciada pela AWS ou crie uma política gerenciada pelo cliente
- Criar uma função do IAM
- Solução de problemas

Use uma política gerenciada pela AWS ou crie uma política gerenciada pelo cliente

Para conceder as permissões do perfil, você pode usar uma política gerenciada pela AWS ou uma política gerenciada pelo cliente.

> **Tip**
>
> Se não quiser criar uma política manualmente, recomendamos usar uma política gerenciada pela AWS e ignorar esse procedimento. As políticas gerenciadas têm, de forma automática, as permissões necessárias para o aplicativo AWS Support. Não é necessário atualizar as políticas manualmente. Para obter mais informações, consulte AWS políticas gerenciadas para AWS Support aplicativos no Slack.

Siga esse procedimento para criar uma política gerenciada pelo cliente para seu perfil. Esse procedimento usa o editor de política do JSON no console do IAM.

Criar uma política gerenciada pelo cliente para o AWS Support App

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, escolha Policies (Políticas).
3. Escolha Create policy (Criar política).
4. Escolha a guia JSON.
5. Insira seu JSON e, em seguida, substitua o JSON padrão no editor. Você pode usar o example policy (exemplo de política).
6. Escolha Next: Tags (Próximo: tags).
7. (Opcional) É possível usar tags como pares de chave-valor para adicionar metadados à política.
8. Escolha Next: Review (Próximo: revisar).
9. Na página Review policy (Revisar política), insira um Name (Nome), como *`AWSSupportAppRolePolicy`*, e uma Description (Descrição) (opcional).
10. Revise a página Summary (Resumo) para ver as permissões que a política permite e, em seguida, escolha Create policy (Criar política).

Essa política define as ações que o perfil pode realizar. Para obter mais informações, consulte a seção Creating IAM policies (console) [Como criar políticas do IAM (console)] no Guia do usuário do IAM.

Exemplo de política do IAM

Você pode anexar o exemplo de política a seguir ao seu perfil do IAM. Essa política permite que o perfil obtenha permissões completas para todas as ações necessárias para o aplicativo AWS Support. Depois de configurar um canal do Slack com o perfil, qualquer usuário em seu canal terá as mesmas permissões.

> **Note**
>
> Para obter uma lista das políticas gerenciadas pela AWS, consulte AWS políticas gerenciadas para AWS Support aplicativos no Slack.

Você pode atualizar a política para excluir uma permissão do aplicativo AWS Support.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "servicequotas:GetRequestedServiceQuotaChange",
                "servicequotas:GetServiceQuota",
                "servicequotas:RequestServiceQuotaIncrease",
                "support:AddAttachmentsToSet",
                "support:AddCommunicationToCase",
                "support:CreateCase",
                "support:DescribeCases",
                "support:DescribeCommunications",
                "support:DescribeSeverityLevels",
                "support:InitiateChatForCase",
                "support:ResolveCase"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {"iam:AWSServiceName": "servicequotas.amazonaws.com"}
            }
        }
    ]
}
```

Para obter as descrições de cada ação, consulte os seguintes tópicos em Service Authorization Reference (Referência de autorização do serviço):

- Ações, recursos e chaves de condição para o AWS Support
- Actions, resources, and condition keys for Service Quotas (Ações, recursos e chaves de condição para o Service Quotas)
- Ações, recursos e chaves de condição para o AWS Identity and Access Management

Criar uma função do IAM

Quando tiver a política, crie um perfil do IAM e anexe a política a esse perfil. Esse perfil é escolhido ao criar uma configuração de canal do Slack no console do Support Center.

Criar um perfil para o aplicativo AWS Support

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, escolha Roles (Funções) e Create role (Criar função).
3. Em Select trusted entity (Selecionar entidade confiável), escolha AWS service (Serviço da AWS).
4. Selecione AWS Support App.
5. Escolha Next: Permissions (Próximo: permissões).
6. Insira o nome da política. Você pode escolher a política gerenciada da AWS ou uma política gerenciada pelo cliente criada por você, como *AWSSupportAppRolePolicy*. Em seguida, marque a caixa de seleção ao lado da política.
7. Escolha Next: Tags (Próximo: tags).
8. (Opcional) Para adicionar metadados ao perfil, use tags como pares de chave-valor.
9. Escolha Next: Review (Próximo: revisar).
10. Em Role name (Nome do perfil), digite um nome, como *AWSSupportAppRole*.
11. (Opcional) Em Role description (Descrição da função), digite uma descrição para a função.
12. Revise a função e escolha Create role (Criar função). Agora você pode escolher esse perfil ao configurar um canal do Slack no console do Support Center. Consulte Como configurar um canal do Slack.

Para obter mais informações, consulte Criar um perfil para um serviço da AWS no Guia do usuário do IAM.

Solução de problemas

Consulte os tópicos a seguir para gerenciar o acesso ao aplicativo AWS Support.

Sumário

- Quero restringir determinados usuários em meu canal do Slack de ações específicas
- Quando configuro um canal do Slack, não vejo o perfil do IAM que criei

- Falta uma permissão para o meu perfil do IAM
- Um erro do Slack sinaliza que o meu perfil do IAM não é válido
- O aplicativo AWS Support diz que falta um perfil do IAM para o Service Quotas

Quero restringir determinados usuários em meu canal do Slack de ações específicas

Por padrão, os usuários do seu canal do Slack têm as mesmas permissões especificadas na política do IAM que você atribui ao perfil do IAM criado. Isso significa que qualquer pessoa no canal tem acesso de leitura ou gravação a seus casos de suporte, independentemente de ter ou não uma Conta da AWS ou um usuário do IAM.

Recomendamos seguir estas práticas recomendadas:

- Configure canais privados do Slack com o aplicativo AWS Support
- Convide para seu canal apenas usuários que precisem acessar seus casos de suporte
- Use uma política do IAM que tenha as permissões mínimas necessárias para o aplicativo AWS Support. Consulte AWS políticas gerenciadas para AWS Support aplicativos no Slack.

Quando configuro um canal do Slack, não vejo o perfil do IAM que criei

Se o seu perfil do IAM não aparecer na lista de perfis do IAM para o AWS Support App, isso significa que o perfil não tem o AWS Support App como uma entidade confiável ou que o perfil foi excluído. É possível atualizar um perfil existente ou criar um. Consulte Criar uma função do IAM.

Falta uma permissão para o meu perfil do IAM

O perfil do IAM criado para o seu canal do Slack precisa de permissões para realizar as ações que você deseja. Por exemplo, se você quiser que seus usuários no Slack criem casos de suporte, o perfil deve ter a permissão `support:CreateCase`. O aplicativo AWS Support assume esse perfil para realizar essas ações para você.

Se você receber uma mensagem de erro sobre a falta de permissão do aplicativo AWS Support, verifique se a política anexada ao seu perfil tem a permissão necessária.

Veja o Exemplo de política do IAM anterior.

Um erro do Slack sinaliza que o meu perfil do IAM não é válido

Verifique se você escolheu o perfil correto para a configuração do seu canal.

Para verificar o seu perfil

1. Faça login no AWS Support Center Console na página https://console.aws.amazon.com/support/app#/config.
2. Escolha o canal que você configurou com o aplicativo AWS Support.
3. Na seção Permissions (Permissões), encontre o nome do perfil do IAM que você escolheu.
   - Para alterar o perfil, escolha Edit (Editar), selecione outro perfil e, em seguida, Save (Salvar).
   - Para atualizar o perfil ou a política anexada ao perfil, faça login no IAM console (Console do IAM).

O aplicativo AWS Support diz que falta um perfil do IAM para o Service Quotas

É necessário ter o perfil `AWSServiceRoleForServiceQuotas` em sua conta para solicitar aumentos de cotas do Service Quotas. Se você receber uma mensagem de erro sobre a falta de um recurso, conclua uma das seguintes etapas:

- Para solicitar um aumento de cota, use o console do Service Quotas. Depois de fazer uma solicitação bem-sucedida, o Service Quotas cria esse perfil para você automaticamente. Em seguida, você poderá usar o aplicativo AWS Support para solicitar aumentos de cotas no Slack. Consulte Requesting a quota increase (Como solicitar um aumento de cota) para obter mais informações.
- Atualize a política do IAM que está anexada ao perfil. Com isso, o Service Quotas recebe a permissão do perfil. A seção a seguir no Exemplo de política do IAM permite que o aplicativo AWS Support crie o perfil do Service Quotas para você.

```
{
    "Effect": "Allow",
    "Action": "iam:CreateServiceLinkedRole",
    "Resource": "*",
    "Condition": {
        "StringEquals": {"iam:AWSServiceName": "servicequotas.amazonaws.com"}
     }
}
```

Caso exclua o perfil do IAM que configurou para o seu canal, você deve criar manualmente o perfil ou atualizar a política do IAM para permitir que o aplicativo AWS Support crie um para você.

Autorizar um espaço de trabalho do Slack

Depois de autorizar seu espaço de trabalho e conceder a permissão do aplicativo AWS Support para acessá-lo, é necessário um perfil do AWS Identity and Access Management (IAM) para sua Conta da AWS. O aplicativo AWS Support usa esse perfil para chamar as operações de API do AWS Support e do Service Quotas para você. Por exemplo, o aplicativo AWS Support usa o perfil para chamar a operação `CreateCase` para criar um caso de suporte para você no Slack.

Observações

- O canal do Slack herda as permissões do perfil do IAM. Isso significa que qualquer usuário no canal do Slack tem as mesmas permissões especificadas na política do IAM vinculada ao perfil.

  Por exemplo, se sua política do IAM permite que o perfil tenha permissões completas de leitura e gravação para seus casos de suporte, qualquer pessoa no seu canal do Slack poderá criar, atualizar e resolver seus casos de suporte. Se sua política do IAM conceder permissões somente leitura do perfil, os usuários do seu canal do Slack só terão permissões de leitura para seus casos de suporte.
- Recomendamos que você adicione os espaços de trabalho e canais do Slack necessários para gerenciar suas operações de suporte. Recomendamos que você configure canais privados e convide apenas usuários que sejam necessários.

Você deve autorizar cada espaço de trabalho do Slack que deseja usar para sua Conta da AWS. Se você tiver várias Contas da AWS, deve entrar em cada conta e repetir o procedimento a seguir para autorizar o espaço de trabalho. Se a sua conta pertence a uma das AWS Organizations, e você deseja autorizar várias contas, vá para Authorize multiple accounts (Autorizar várias contas).

Para autorizar o espaço de trabalho do Slack para sua Conta da AWS

1. Faça login no AWS Support Center Console e escolha Slack configuration (Configuração do Slack).
2. Na página Getting started (Começar), escolha Authorize workspace (Autorizar espaço de trabalho).
3. Caso ainda não tenha feito login no Slack, na página Sign in to your workspace (Fazer login em seu espaço de trabalho), insira seu nome do workspace e escolha Continue (Continuar).

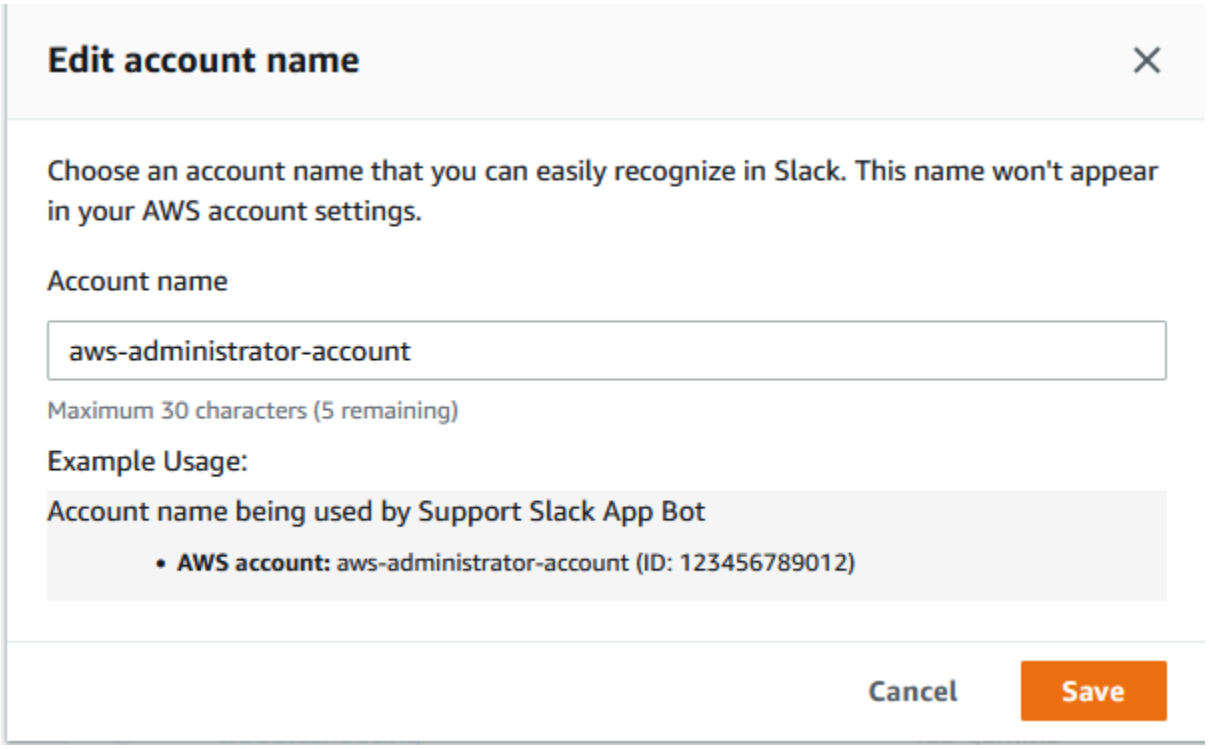
4. Na página O AWS Support está solicitando permissão para acessar o nome-do-seu-espaço-de-trabalho do Slack, escolha Permitir.

> **Note**
>
> Caso não consiga permitir que o Slack acesse seu espaço de trabalho, verifique se você tem permissões do administrador do Slack para adicionar o aplicativo AWS Support ao espaço de trabalho. Consulte Pré-requisitos.

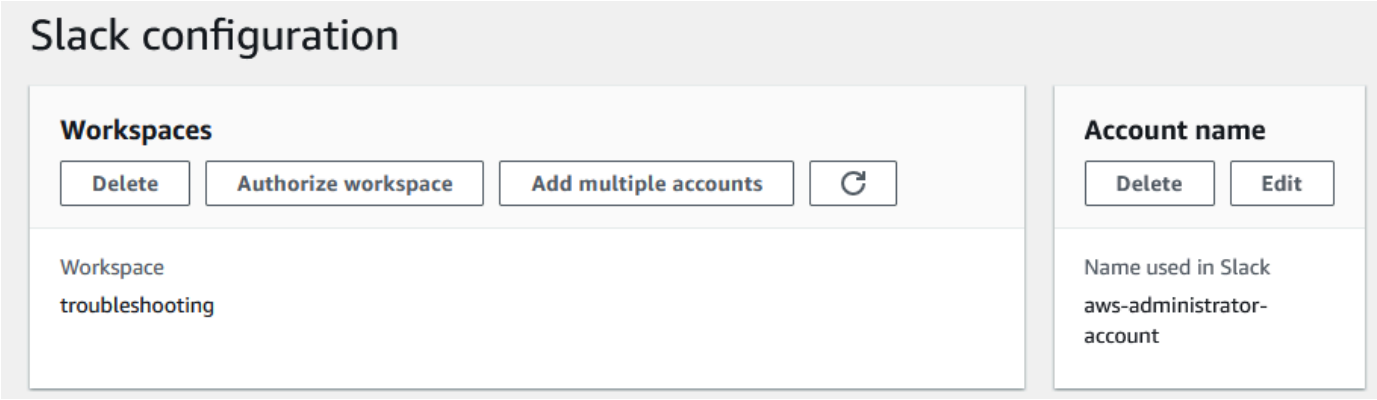
Na página Slack configuration (Configuração do Slack), o nome do seu espaço de trabalho aparece em Workspaces (Espaços de trablho).

5. (Opcional) Para adicionar mais espaços de trabalho, escolha Authorize workspace (Autorizar espaço de trabalho) e repita as etapas 3 e 4. Você pode adicionar até cinco espaços de trabalho à sua conta.
6. (Opcional) Por padrão, o número de ID da sua Conta da AWS aparece como o nome da conta em seu canal do Slack. Para alterar esse valor, em Account name (Nome da conta), escolha Edit (Editar), insira o nome da conta e selecione Save (Salvar).

> **Tip**
>
> Use um nome que você e a sua equipe possam reconhecer facilmente. O aplicativo AWS Support usa esse nome para identificar a sua conta no canal do Slack. É possível atualizá-lo a qualquer momento.



Seu espaço de trabalho e o nome da conta aparecem na página Slack configuration (Configuração do Slack).



Autorizar várias contas

Para autorizar várias Contas da AWS a usar espaços de trabalho do Slack, você pode usar o AWS CloudFormation ou o Terraform para criar seus recursos do AWS Support App.

Como configurar um canal do Slack

Depois de autorizar seu espaço de trabalho do Slack, é possível configurar seus canais do Slack para usar o aplicativo AWS Support.

O canal em que você convida e adiciona o aplicativo AWS Support é onde você pode criar, pesquisar e receber notificações de casos. Esse canal mostra atualizações de casos, como casos recém-criados ou resolvidos, correspondências adicionadas e detalhes compartilhados do caso.

O canal do Slack herda as permissões do perfil do IAM. Isso significa que qualquer usuário no canal do Slack tem as mesmas permissões especificadas na política do IAM vinculada ao perfil.

Por exemplo, se sua política do IAM permite que o perfil tenha permissões completas de leitura e gravação para seus casos de suporte, qualquer pessoa no seu canal do Slack poderá criar, atualizar e resolver seus casos de suporte. Se sua política do IAM conceder permissões somente leitura do perfil, os usuários do seu canal do Slack só terão permissões de leitura para seus casos de suporte.

Você pode adicionar até 20 canais para uma conta. Um canal do Slack pode ter até 100 Contas da AWS. Isso significa que apenas 100 contas podem adicionar o mesmo canal do Slack ao aplicativo AWS Support. Recomendamos que você adicione apenas as contas necessárias para gerenciar os casos de suporte da sua organização. Com isso, reduz-se o número de notificações que você recebe no canal, para que você e sua equipe tenham menos distrações.

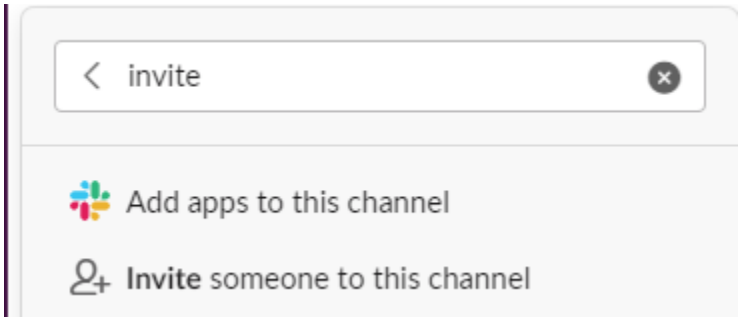
Cada Conta da AWS deve configurar um canal do Slack separadamente no aplicativo AWS Support. Dessa forma, o aplicativo AWS Support pode acessar os casos de suporte nessa Conta da AWS. Se outra Conta da AWS em sua organização já tiver convidado o aplicativo AWS Support do Slack, passe para a etapa 3.

> **Note**
>
> Você pode configurar canais que fazem parte do Slack Connect e canais compartilhados com vários espaços de trabalho. No entanto, somente o primeiro espaço de trabalho que configurou o canal compartilhado para uma Conta da AWS pode usar o AWS Support App. O AWS Support App retornará uma mensagem de erro se você tentar configurar o mesmo canal do Slack para outro espaço de trabalho.

Para configurar um canal do Slack

1. No seu aplicativo Slack, escolha o canal do Slack que você deseja usar com o aplicativo AWS Support.
2. Conclua as etapas a seguir para convidar o aplicativo AWS Support para o seu canal:

   a. Escolha o ícone + e insira `invite`. Quando solicitado, escolha Add apps to this channel (Adicionar aplicativos a este canal).

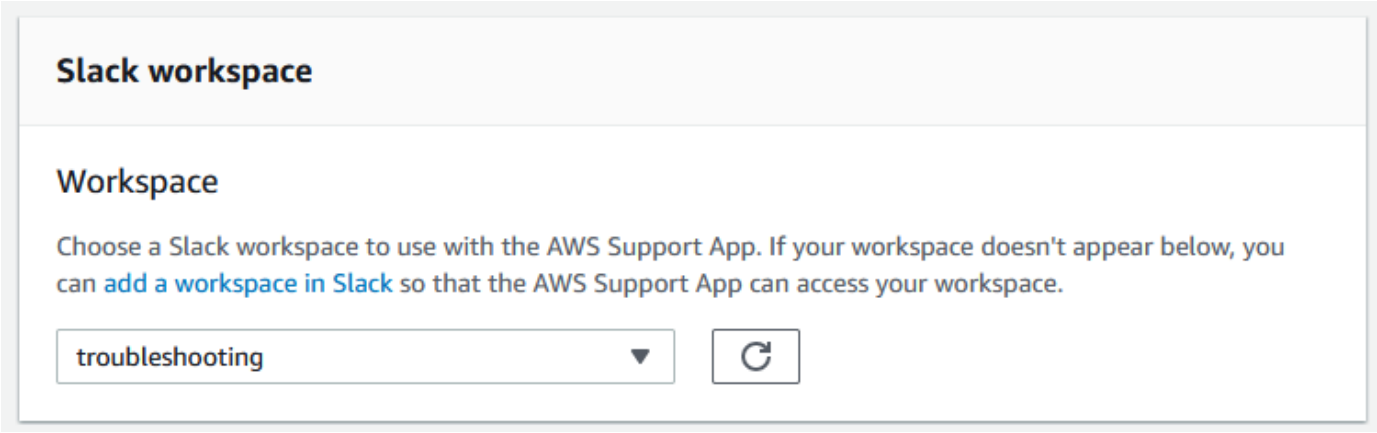
   

   b. Para pesquisar a aplicação, em Add apps to channelName (Adicionar aplicativos a channelName), insira AWS Support App.

   c. Escolha Add (Adicionar) ao lado de AWS Support App.

3. Faça login no Support Center Console e escolha Slack configuration (Configuração do Slack).
4. Escolha Add channel (Adicionar canal).
5. Na página Add channel (Adicionar canal), em Workspace (Espaço de trabalho), escolha o nome do espaço de trabalho que você autorizou anteriormente. Você pode escolher o ícone de atualização se o nome do espaço de trabalho não aparecer na lista.

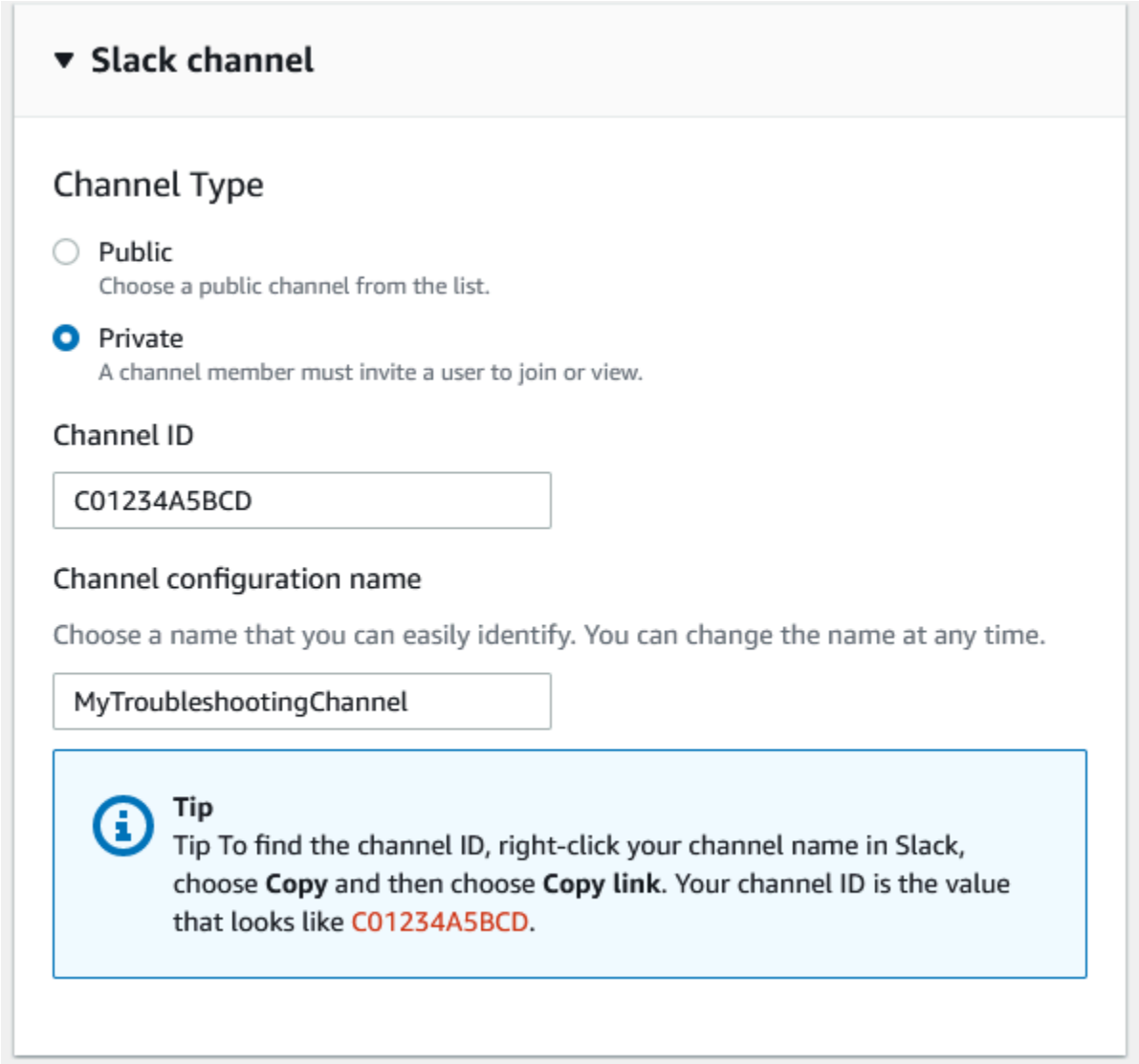


6. Em Slack channel (Canal do Slack), para Channel type (Tipo de canal), escolha uma das seguintes opções:
   - Public (Público) – Em Public channel (Canal público), escolha o canal do Slack para o qual você convidou o aplicativo AWS Support (etapa 2). Se o seu canal não aparecer na lista, escolha o ícone de atualização e tente novamente.
   - Private (Privado) – Em Channel ID (ID do canal), insira o ID ou o URL do canal do Slack para o qual você convidou o aplicativo AWS Support.

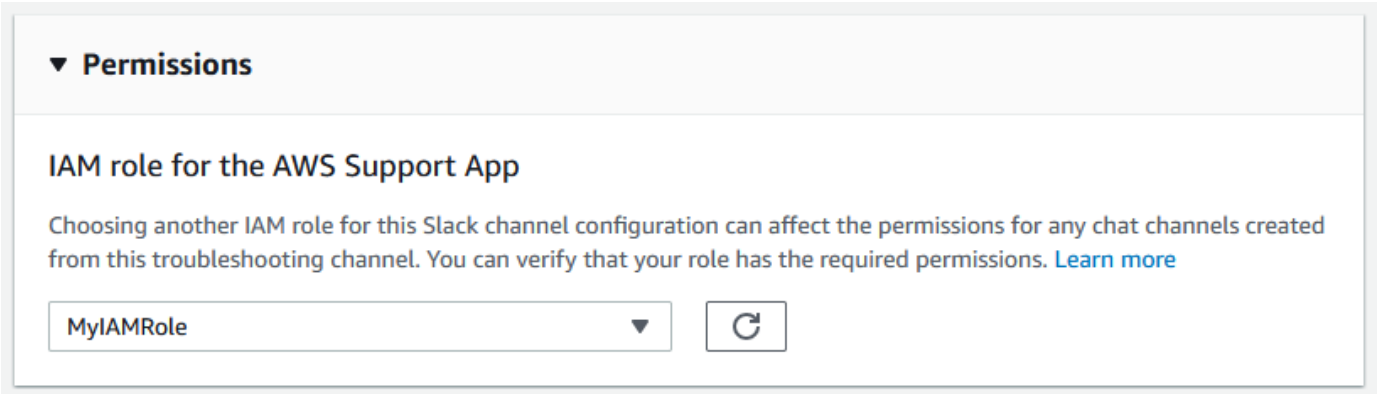
   > **Tip**
   >
   > Para encontrar o ID do canal, abra o menu de contexto (clique com o botão direito) para o nome do canal no Slack e selecione Copy (Copiar). Em seguida, escolha Copy link (Copiar link). O ID do canal é o valor parecido com `C01234A5BCD`.

7. Em Channel configuration name (Nome de configuração do canal), insira um nome que identifique facilmente a configuração do seu canal do Slack para o aplicativo AWS Support. Esse nome aparece somente em sua Conta da AWS e não aparece no Slack. Você pode renomear a configuração do seu canal posteriormente.

   O tipo de canal do Slack pode ser como o exemplo a seguir.



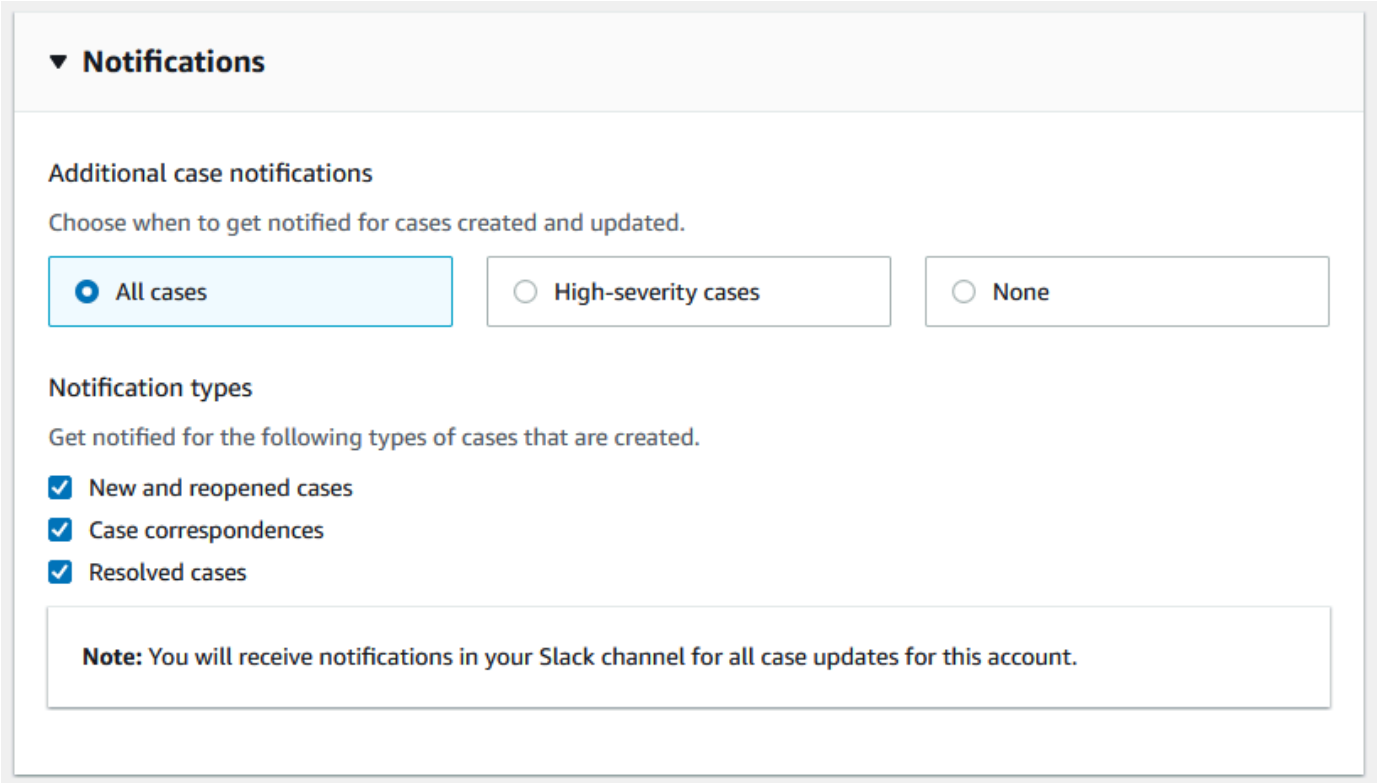
8. Em Permissões, para Perfil do IAM para o AWS Support App no Slack, escolha um perfil criado para o AWS Support App. Somente perfis que têm o aplicativo AWS Support como uma entidade confiável aparecem na lista.



> **Note**
>
> Se você não criou um perfil ou não encontra seu perfil na lista, consulte Como gerenciar o acesso ao aplicativo AWS Support.

9. Em Notifications (Notificações), especifique como receber notificações sobre os casos.
   - All cases (Todos os casos): receba notificações sobre todas as atualizações de casos.
   - High-severity cases (Casos de alta gravidade): receba notificações somente para casos que afetem um sistema de produção ou superior. Para obter mais informações, consulte Escolher uma gravidade.
   - None (Nenhum): não receba notificações sobre atualizações de casos.
10. (Opcional) Se você escolher All cases (Todos os casos) ou High-severity cases (Casos de alta gravidade), selecione pelo menos uma das opções a seguir:
    - New and reopened cases (Casos novos e reabertos)
    - Case correspondences (Correspondências de caso)
    - Resolved cases (Casos resolvidos)

    O canal a seguir recebe notificações de todas as atualizações de casos no Slack.



11. Revise sua configuração e escolha Add channel (Adicionar canal). Seu canal aparece na página Slack configuration (Configuração do Slack).

Atualizar a configuração do seu canal do Slack

Depois de configurar seu canal do Slack, você pode atualizá-lo posteriormente para alterar o perfil do IAM ou a notificação do caso.

Para atualizar a configuração do seu canal do Slack

1. Faça login no Support Center Console e escolha Slack configuration (Configuração do Slack).
2. Em Channels (Canais), escolha a configuração de canal que você deseja.
3. Na página ***channelName***, você pode realizar as tarefas a seguir:
   - Escolha Rename (Renomear) para atualizar o nome da configuração do seu canal. Esse nome só aparece em sua Conta da AWS e não aparecerá no Slack.
   - Escolha Delete (Excluir) para excluir a configuração do canal do aplicativo AWS Support. Consulte Como excluir uma configuração de canal do Slack do aplicativo AWS Support.
   - Escolha Open in Slack (Abrir no Slack) para abrir o canal do Slack no seu navegador.
   - Escolha Edit (Editar) para alterar o perfil do IAM ou as notificações.

Como criar casos de suporte em um canal do Slack

Depois de autorizar seu espaço de trabalho do Slack e adicionar um canal, você pode criar um caso de suporte em seu canal do Slack.

Criar um caso de suporte no Slack

1. Insira o seguinte comando em seu canal:

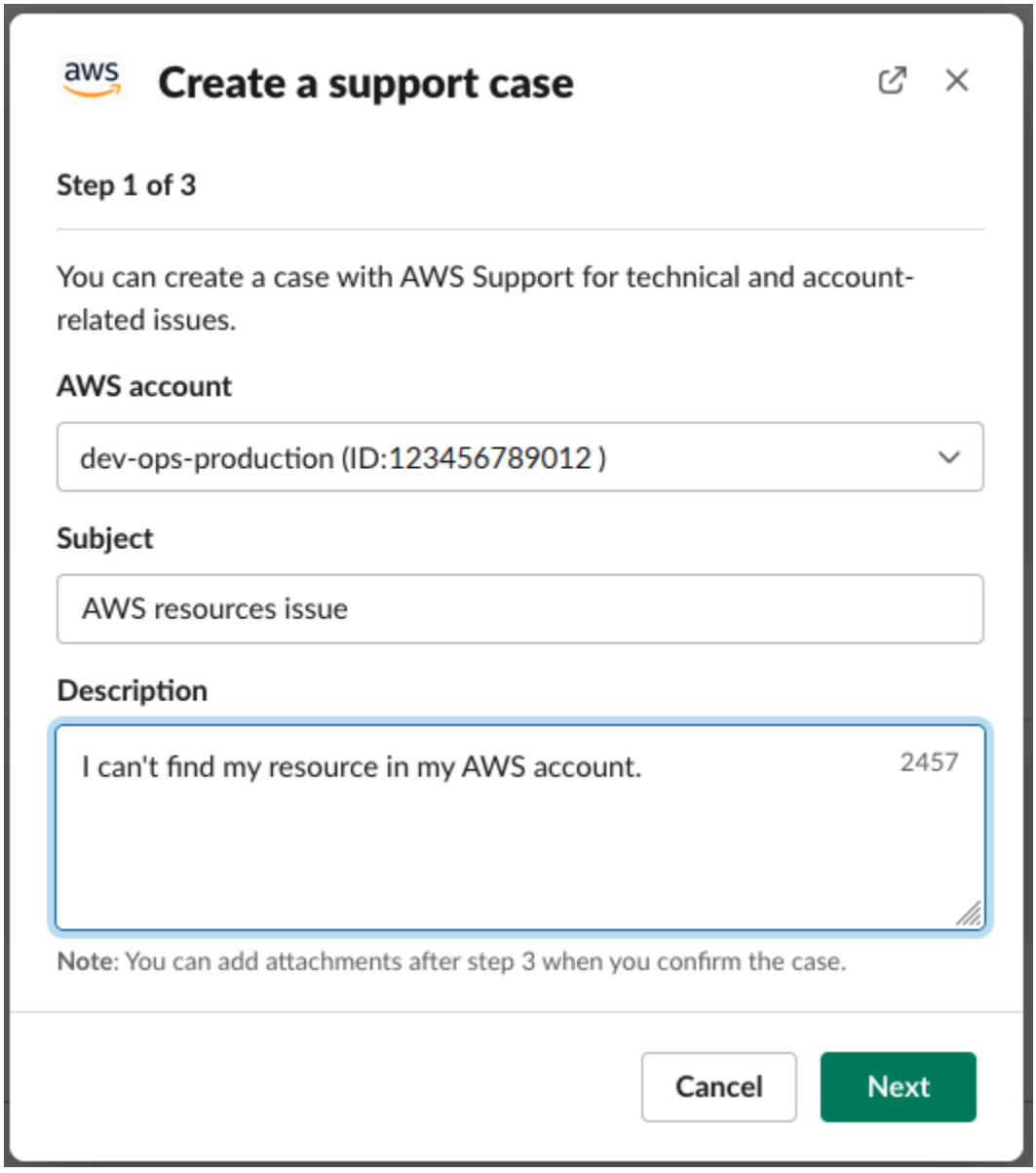
   ```
   /awssupport create
   ```

2. Na caixa de diálogo Create a support case (Criar um caso de suporte), faça o seguinte:

   a. Se você tiver configurado mais de uma conta para esse canal do Slack, escolha o ID de conta da Conta da AWS. Se você criou um nome de conta, esse valor aparece ao lado do ID da conta. Para obter mais informações, consulte Autorizar um espaço de trabalho do Slack.

   b. Para Subject (Assunto), insira um título para o caso de suporte.

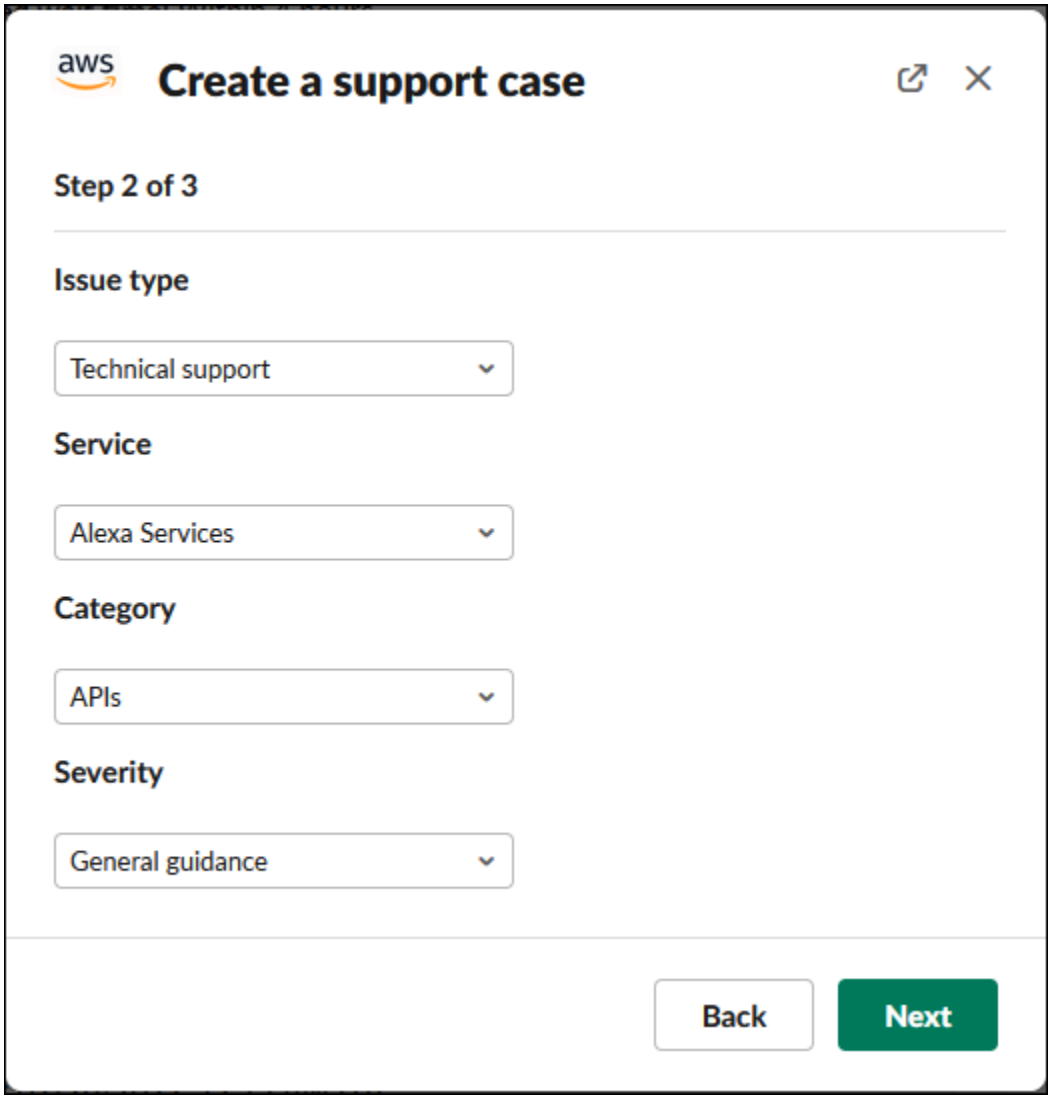
   c. Em Description (Descrição), descreva o seu caso de suporte. Forneça detalhes, por exemplo, como você está usando um AWS service (Serviço da AWS) e que etapas de solução de problemas você tentou.



3. Escolha Next (Próximo).
4. Na caixa de diálogo Create a support case (Criar um caso de suporte), especifique as seguintes opções:

   a. Escolha o Issue type (Tipo de problema).
   b. Selecione o Service (Serviço).
   c. Escolha a Category (Categoria).
   d. Escolha a Severity (Gravidade).
   e. Revise os detalhes do seu caso e escolha Next (Próximo).

   O exemplo a seguir mostra um caso de suporte técnico para serviços da Alexa.

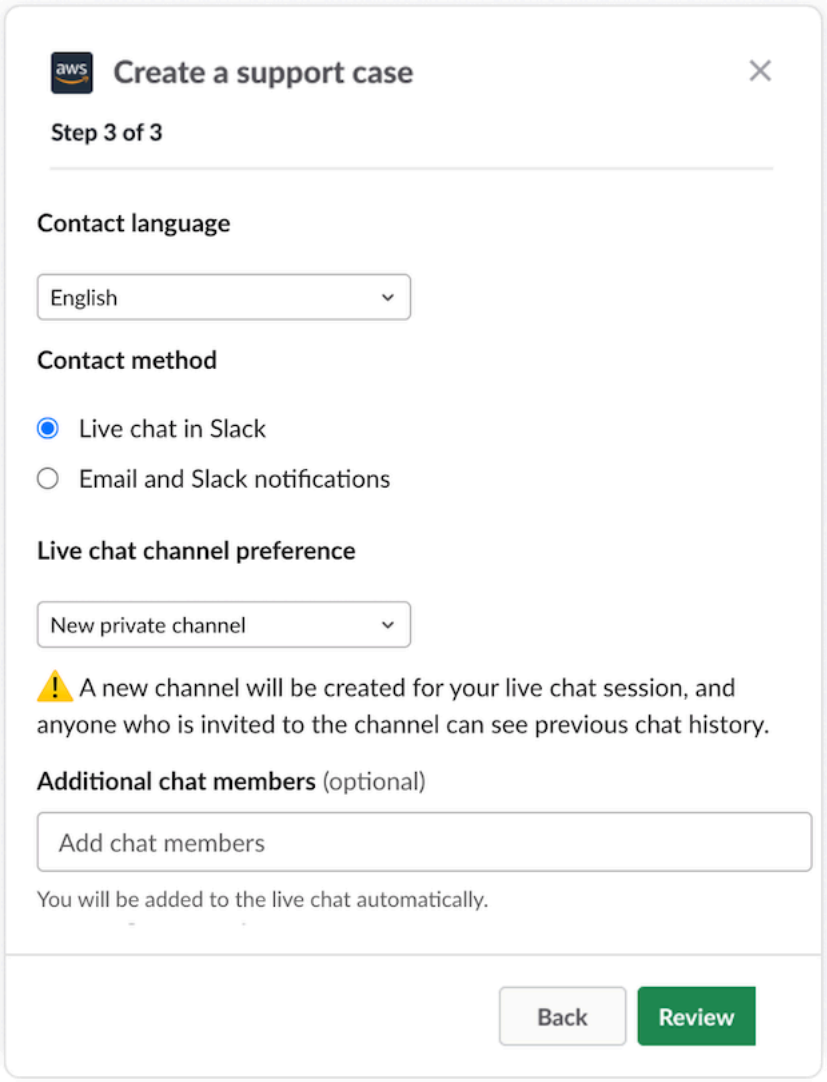


5. Em Contact language (Idioma de contato), escolha o idioma de sua preferência para o caso de suporte.

> **Note**
>
> O suporte ao idioma japonês não está disponível para chat ao vivo no Slack para casos de contas e faturamento.

6. Para Contact method (Método de contato), escolha Email and Slack notifications (Notificações por e-mail e Slack) ou Live chat in Slack (Chat ao vivo no Slack).

   O exemplo a seguir mostra como escolher um chat ao vivo no Slack.



a. Se você escolher Chat ao vivo no Slack, escolha Novo canal privado ou Canal atual como sua Preferência de canal de chat ao vivo. O Novo canal privado criará um canal privado separado para você conversar com o atendente do AWS Support, e o Canal atual usará um tópico no canal atual para você conversar com o atendente do AWS Support.

b. (Opcional) Caso escolha Live chat in Slack (Chat ao vivo no Slack), você pode inserir os nomes de outros membros do Slack. Para Novo canal privado, o AWS Support App adicionará automaticamente você e os membros selecionados ao novo canal. Para o Canal atual, o AWS Support App marcará automaticamente você e os membros selecionados no chat quando o atendente do AWS Support ingressar.

> **Important**
>
> - Recomendamos que você adicione apenas os membros do chat que deseja que tenham acesso aos detalhes do seu caso de suporte e ao histórico do chat.
> - Caso você inicie uma nova sessão de chat ao vivo para um caso de suporte existente, o AWS Support App usará o mesmo canal de chat ou thread usado para um chat ao vivo anterior. O AWS Support App também usa a mesma preferência de canal de chat ao vivo usada anteriormente.
> - A opção Canal atual só estará disponível se o chat for solicitado de um canal privado. Recomendamos que você use essa opção somente se quiser que todos os membros do canal tenham acesso ao seu chat.

7. (Opcional) Para Additional contacts to notify (Contatos adicionais para notificar), insira os endereços de e-mail que também receberão atualizações sobre esse caso de suporte. Você pode inserir até 10 endereços de e-mail.
8. Escolha Review (Revisar).
9. No canal do Slack, revise os detalhes do caso. Você pode fazer o seguinte:
   - Escolha Edit (Editar) para alterar os detalhes do caso.
   - Adicione um arquivo ao seu caso. Para fazer isso, siga estas etapas:
     a. Escolha Attach file (Anexar arquivo), selecione o ícone + no Slack e escolha Your computer (Seu computador).
     b. Navegue até o seu arquivo e escolha-o.
     c. Na caixa de diálogo Upload a file (Fazer upload de um arquivo), insira `@awssupport` e pressione o ícone

        para enviar mensagem.

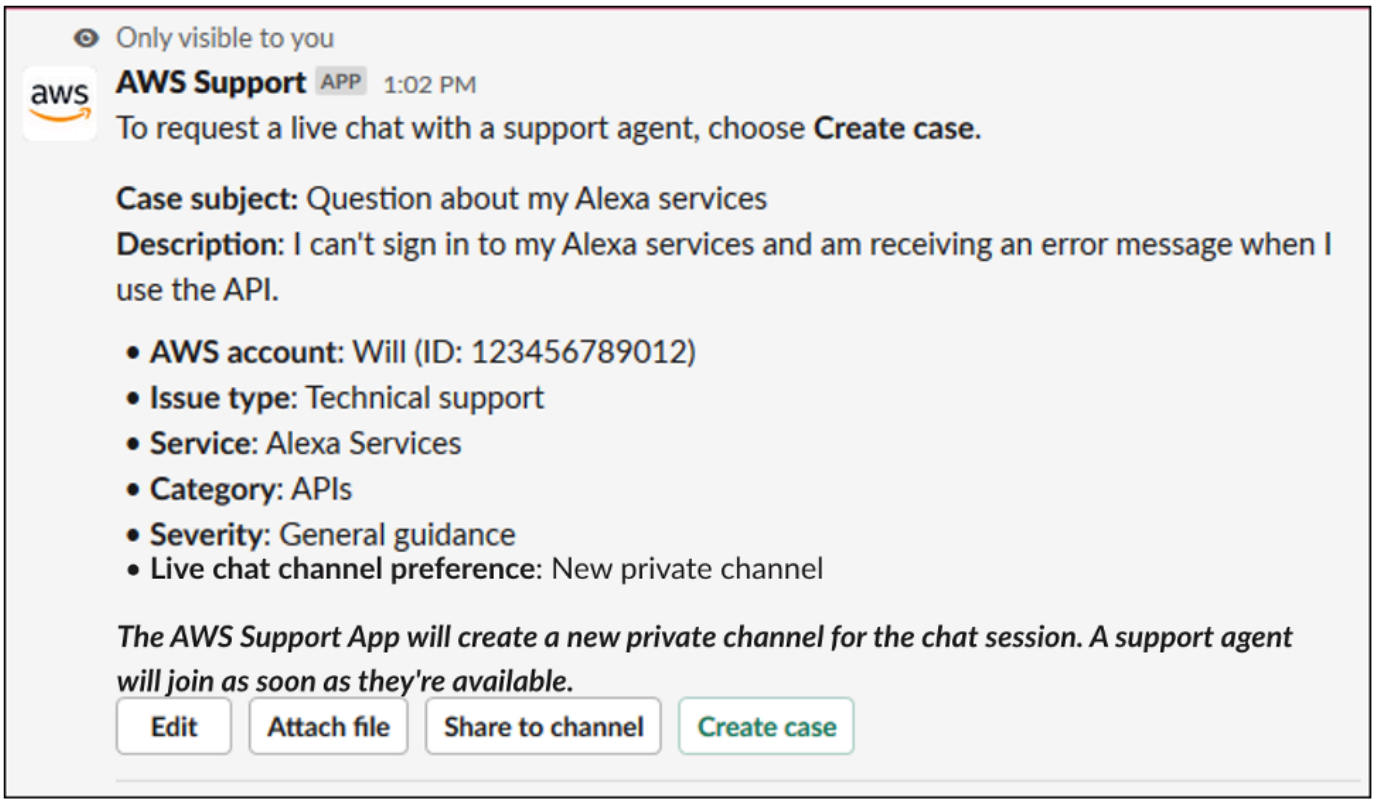
> **Observações**
>
> - É possível anexar até três arquivos. Cada arquivo pode ter até 5 MB.

- Se você anexar um arquivo ao seu caso de suporte, deverá enviar o caso dentro de 1 hora. Caso contrário, você deverá adicionar os arquivos novamente.

- Escolha Share to channel (Compartilhar com o canal) para compartilhar os detalhes do caso com outras pessoas no canal do Slack. Você pode usar essa opção para compartilhar os detalhes do caso com sua equipe antes de criá-lo.

10. Revise os detalhes do seu caso e escolha Create case (Criar caso).

    O exemplo a seguir mostra um caso de suporte técnico para serviços da Alexa.



    Depois que você criar um caso de suporte, poderá levar alguns minutos para que os detalhes do caso apareçam.

11. Quando seu caso de suporte for atualizado, você poderá escolher See details (Visualizar detalhes) para visualizar as informações do seu caso. Você pode, então, fazer o seguinte:

    - Escolha Share to channel (Compartilhar com o canal) para compartilhar os detalhes do caso com outras pessoas no canal do Slack.
    - Escolha Reply (Responder) para adicionar uma correspondência.
    - Escolha Resolve case (Resolver caso).

> **Note**
>
> Se você não optou por receber atualizações automáticas de casos no Slack, pode pesquisar o caso de suporte para encontrar a opção See details (Visualizar detalhes).

Como responder a casos de suporte no Slack

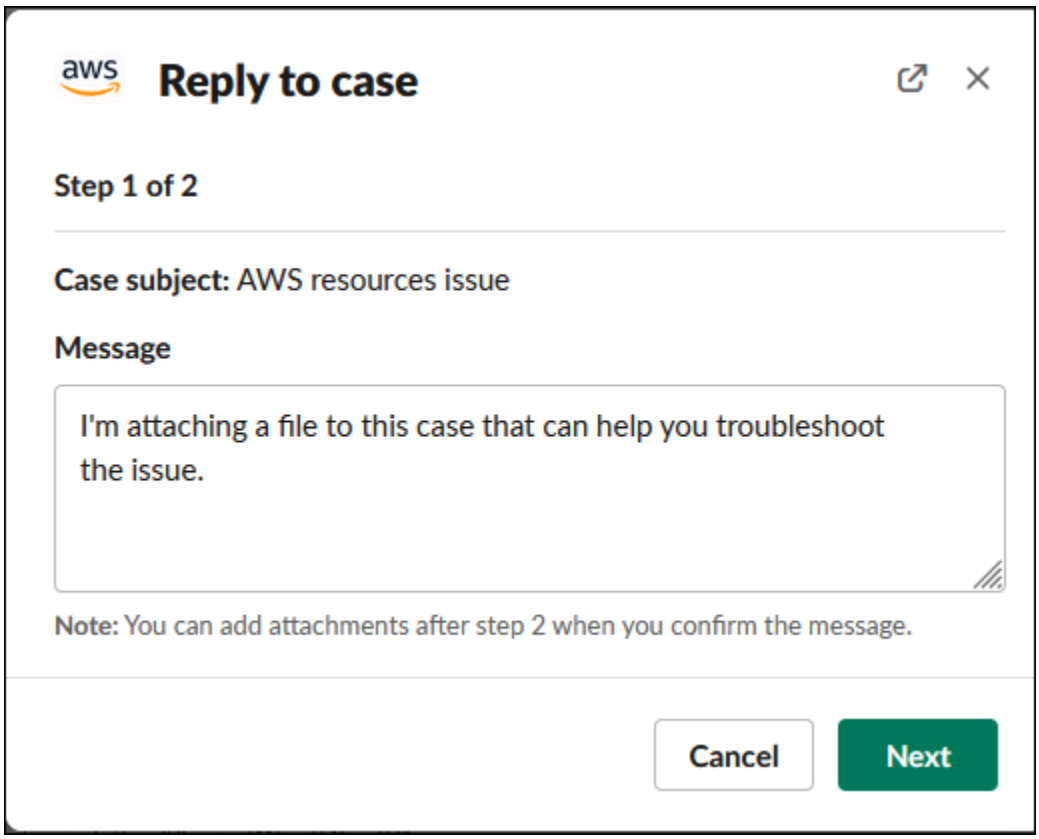
Você pode adicionar atualizações ao seu caso, como detalhes do caso e anexos, e responder ao atendente de suporte.

> **Note**
>
> - Você também pode usar o AWS Support Center Console para responder aos atendentes de suporte. Para obter mais informações, consulte Atualizar, resolver e reabrir um caso.
> - Você não pode adicionar correspondências a casos de canais de chat criados pelo AWS Support App. Os canais de bate-papo ao vivo só enviam mensagens aos agentes durante o bate-papo ao vivo.

Para responder a um caso de suporte no Slack

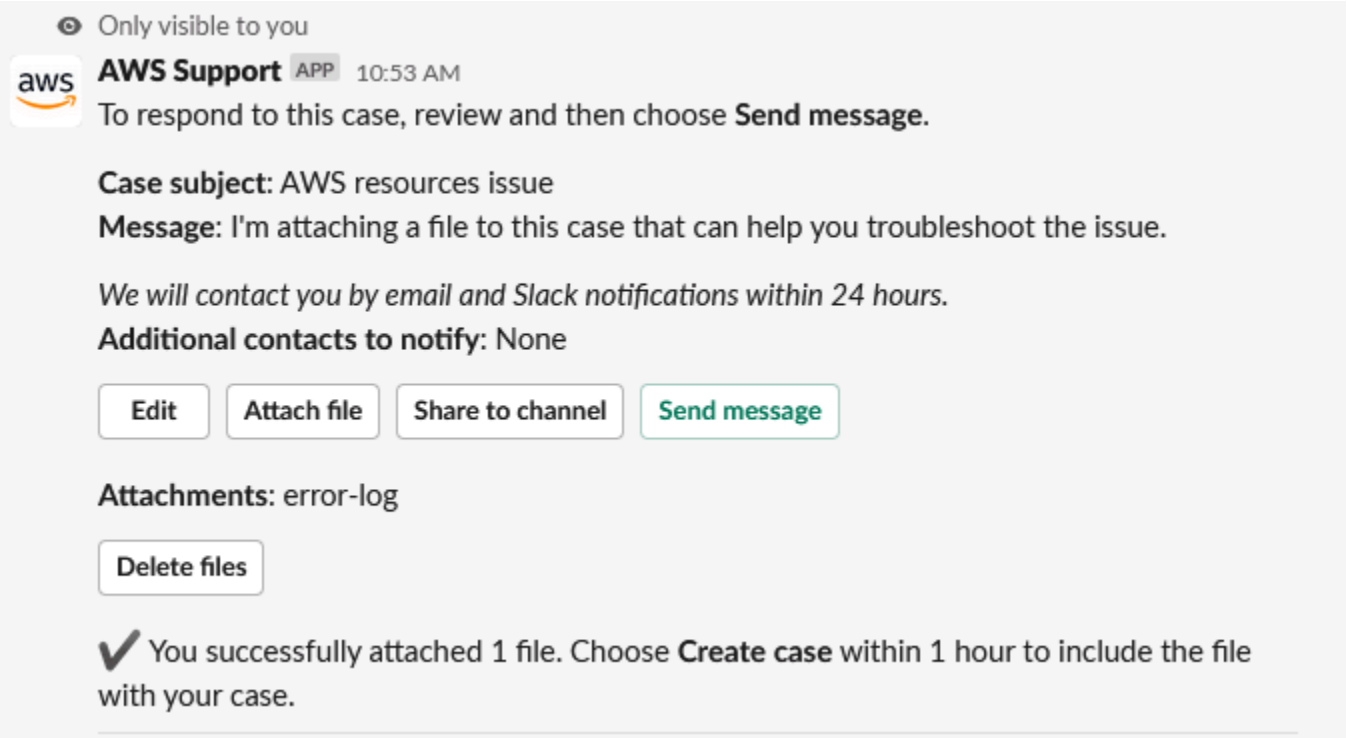
1. No seu canal do Slack, escolha o caso ao qual você quer responder. Você pode inserir `/awssupport search` para encontrar o seu caso de suporte.
2. Escolha See details (Visualizar detalhes) ao lado do caso que você deseja.
3. Na parte inferior dos detalhes de caso, escolha Reply (Responder).

4. Na caixa de diálogo Reply to case (Responder ao caso), insira uma breve descrição do problema no campo Message (Mensagem). Em seguida, escolha Next (Próximo).



5. Escolha seu método de contato. Os métodos de contato disponíveis dependem do tipo de caso e do plano de suporte.
6. (Opcional) Para Additional contacts to notify (Contatos adicionais para notificar), insira endereços de e-mail adicionais para os quais você deseja receber atualizações sobre esse caso de suporte. Você pode inserir até 10 endereços de e-mail.
7. Escolha Review (Revisar). Em seguida, você pode escolher se deseja editar sua resposta, anexar arquivos ou compartilhar no canal.
8. Quando você estiver pronto para responder, escolha Send message (Enviar mensagem).
9. (Opcional) Para ver a correspondência anterior do seu caso, escolha Previous correspondence (Correspondência anterior). Para visualizar as mensagens mais curtas, escolha Show full message (Mostrar mensagem completa).

Example : responder a um caso no Slack



Como entrar em uma sessão de chat ao vivo com o AWS Support

Quando você solicita um chat ao vivo para o seu caso, você escolhe usar um novo canal de chat ou um thread no canal atual para você e o atendente do AWS Support. Use esse canal de chat ou thread para se comunicar com o atendente de suporte e qualquer outro convidado do chat ao vivo.

Important

Qualquer pessoa que ingressar em um canal de chat ao vivo poderá ver os detalhes sobre o caso de suporte específico e o histórico do chat. Recomendamos que você adicione somente usuários que precisem de acesso aos seus casos de suporte. Qualquer membro de um canal ou thread de chat também pode participar de um chat ativo.

Note

Os canais de chat ao vivo ou threads também receberão notificações quando uma correspondência for adicionada ao caso fora da sessão de chat ao vivo. Isso ocorrerá antes, durante e depois de uma sessão de chat, para que você possa usar um canal de chat ou

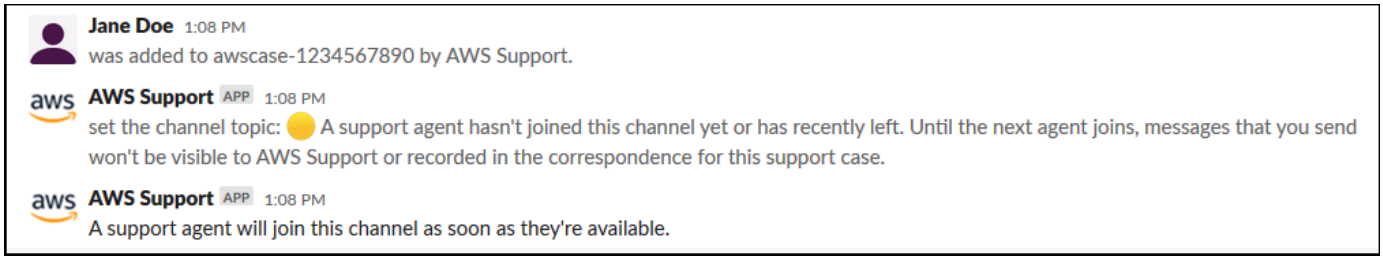
thread para monitorar todas as atualizações de um caso. Se você optar por usar um novo canal de chat, use o canal de configuração em que você convidou o AWS Support App para responder a essas correspondências.

Para participar de uma sessão de chat ao vivo com o AWS Support em um novo canal

1. No aplicativo Slack, navegue até o canal criado pelo aplicativo AWS Support. O nome do canal inclui o ID do seu caso de suporte, como *awscase-1234567890*.

   > **Note**
   >
   > O aplicativo AWS Support adiciona uma mensagem fixada ao canal de chat ao vivo que contém detalhes sobre o seu caso de suporte. Na mensagem fixada, você pode encerrar o chat ou resolver o caso. Todas as mensagens fixadas neste canal podem ser encontradas no nome do canal.

2. Quando o atendente de suporte entrar no canal, você poderá conversar sobre o seu caso de suporte. O atendente de suporte somente verá as mensagens nesse chat quando entrar no canal, e as mensagens não aparecerão na correspondência do seu caso.

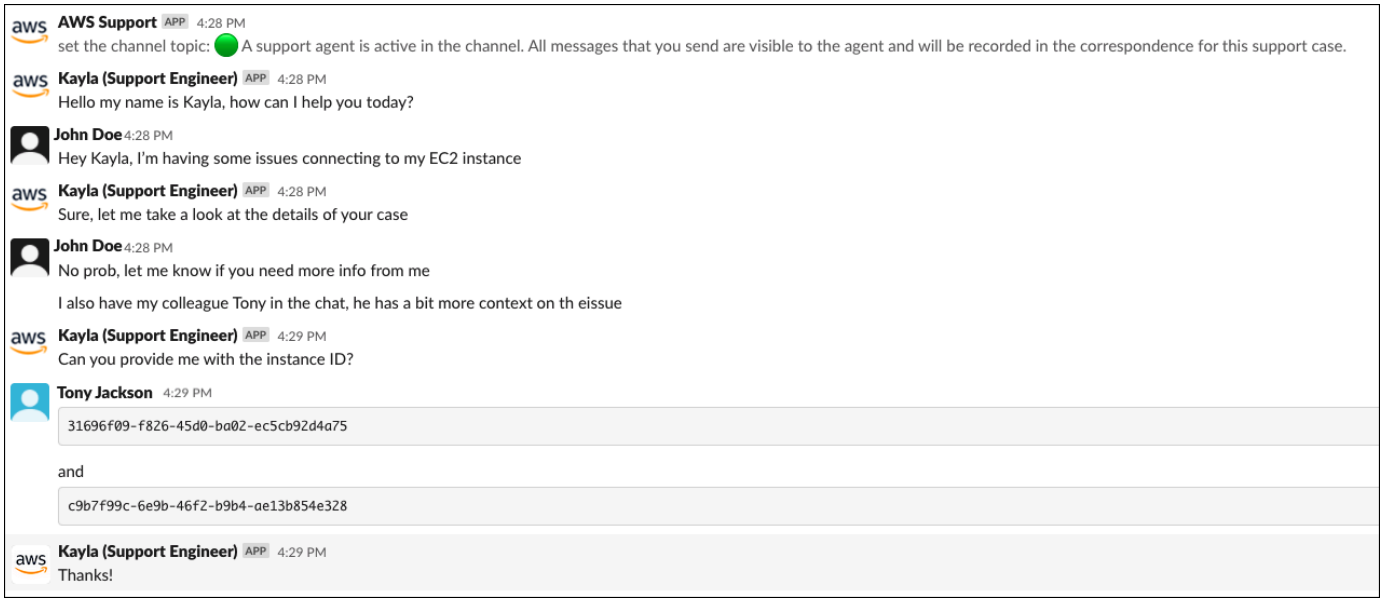
3. (Opcional) Adicione outros membros ao canal de chat. Por padrão, os canais de chat são privados.
4. Depois que o atendente de suporte entra no chat, o canal de chat fica ativo e o aplicativo AWS Support grava a conversa.

   Você pode conversar com o atendente sobre seu caso de suporte e enviar qualquer anexo de arquivo para o canal. O aplicativo AWS Support salva automaticamente seus arquivos e o log de chat na correspondência do seu caso.

> **Note**
>
> Ao conversar com um atendente de suporte, observe as seguintes diferenças no Slack para o aplicativo AWS Support:
>
> - Os atendentes de suporte não têm acesso a mensagens ou tópicos compartilhados. Para compartilhar texto de uma mensagem ou conversa, insira o texto como uma nova mensagem.
> - Se você editar ou excluir uma mensagem, o atendente ainda verá a mensagem original. Você deve inserir sua nova mensagem de novo para mostrar a revisão.

Example : sessão de chat ao vivo

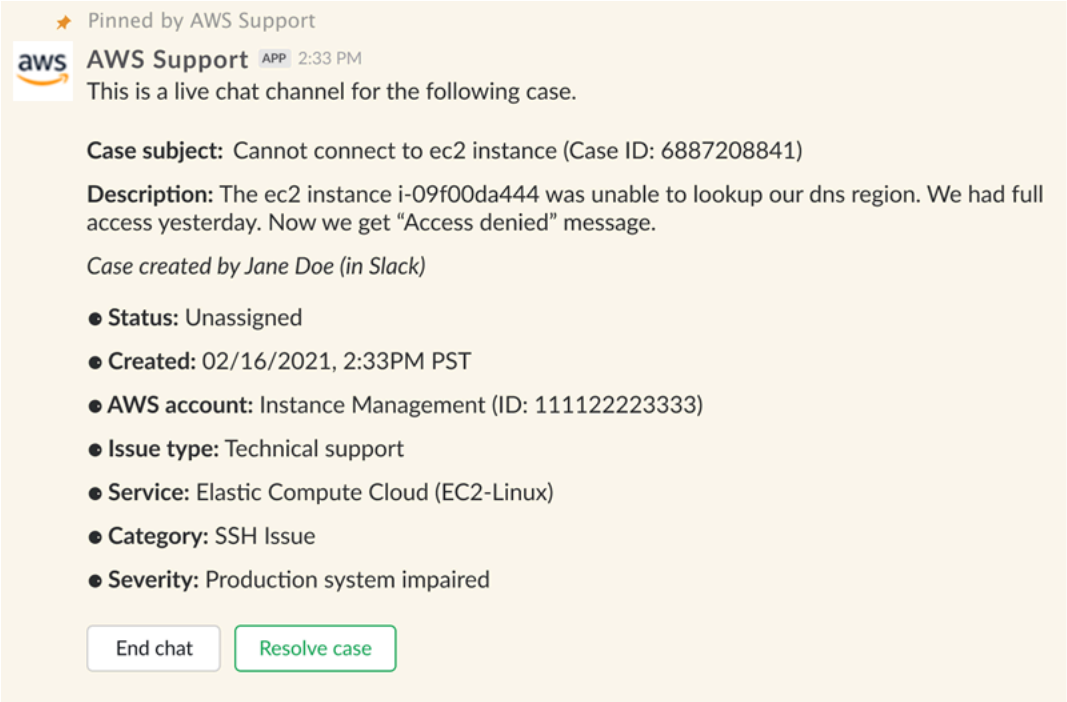
A seguir está um exemplo de uma sessão de chat ao vivo com um atendente de suporte para corrigir um problema de conectividade de duas instâncias do Amazon Elastic Compute Cloud (Amazon EC2).



5. (Opcional) Para interromper o chat ao vivo, escolha End chat (Encerrar chat). O atendente de suporte sai do canal e o aplicativo AWS Support para de gravar o chat ao vivo. O histórico de chat estará anexado à correspondência do caso para esse caso de suporte.
6. Se o problema for resolvido, você pode selecionar Resolve case (Resolver caso) na mensagem fixada ou digitar `/awssupport resolve`.

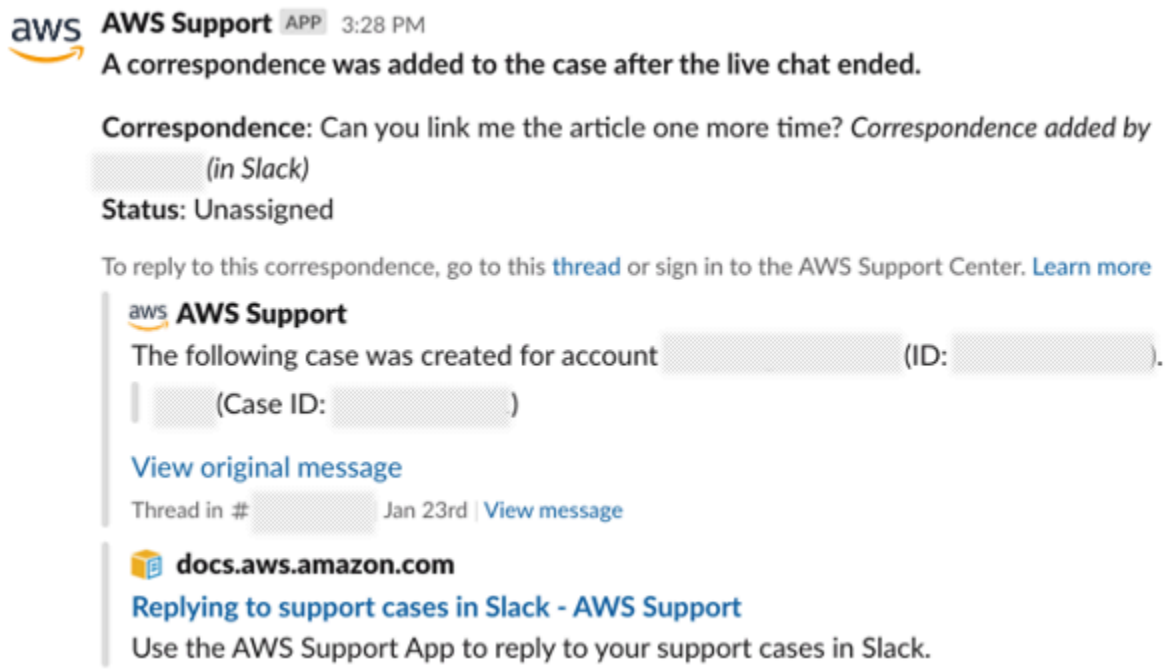
Example : encerrar um chat ao vivo

A mensagem fixada a seguir mostra os detalhes do caso sobre uma instância do Amazon EC2. É possível encontrar as mensagens fixadas abaixo do nome do canal do Slack.



Example : notificação por correspondência no canal de bate-papo

Veja a seguir um exemplo de um canal de bate-papo ao vivo recebendo uma notificação quando outro colaborador adiciona uma atualização após o término do bate-papo.

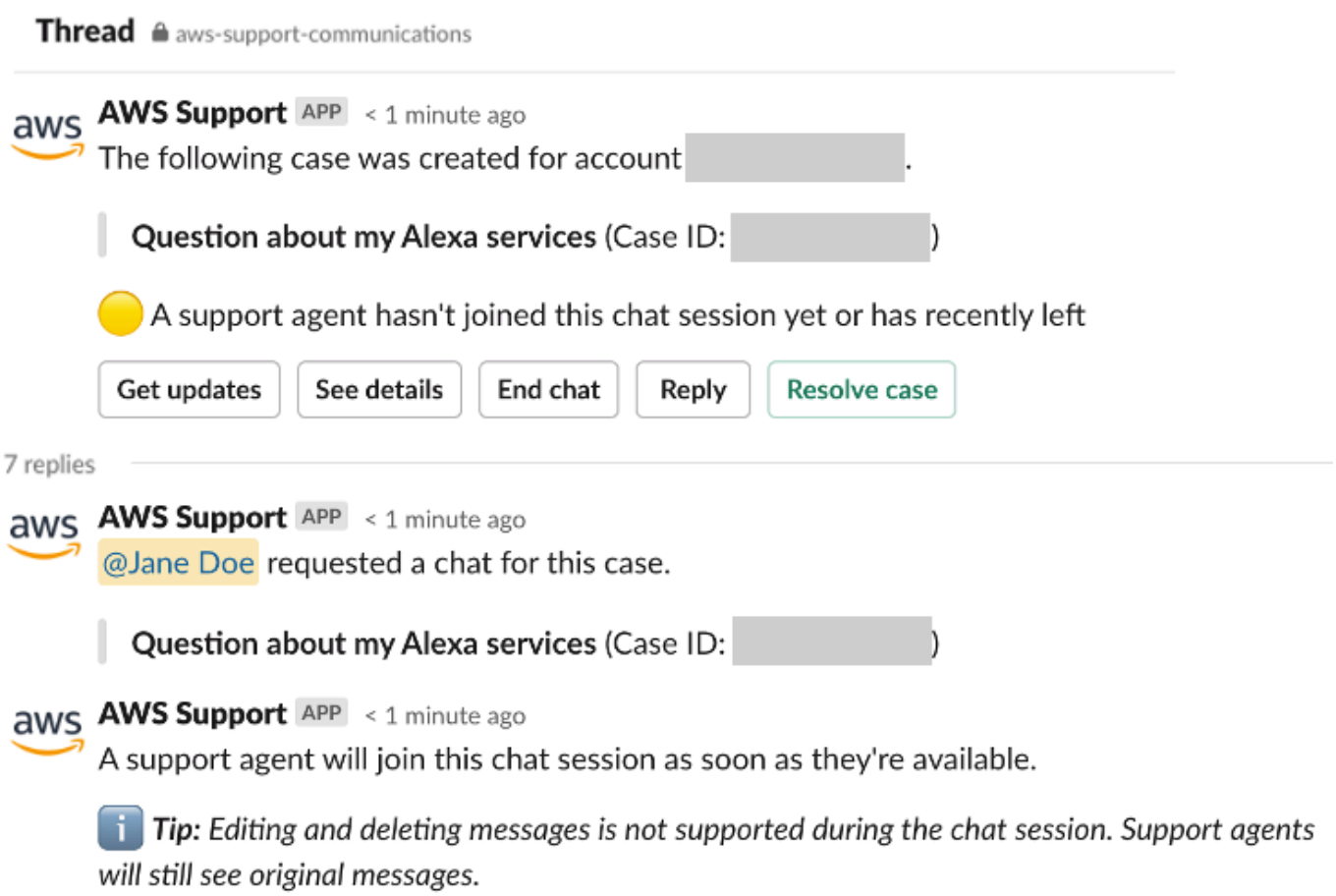


A notificação indicará o status do bate-papo (solicitado, em andamento ou encerrado) e se a correspondência foi adicionada por um agente ou por outro colaborador. O aplicativo de Support também tentará se conectar ao tópico ou canal original do Slack em que esse bate-papo foi solicitado. Você pode responder a esse caso a partir desse canal ou de qualquer outro canal com acesso a esse caso.

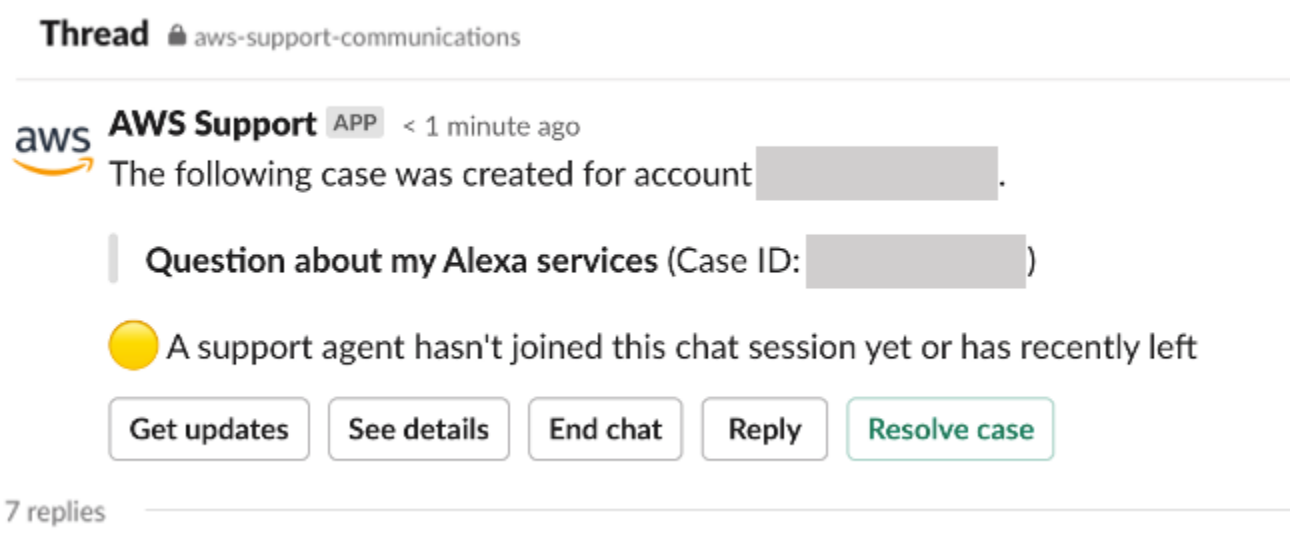
Para participar de uma sessão de chat ao vivo com o AWS Support em um canal atual

1. Na aplicação Slack, navegue até o thread no canal atual que o AWS Support App usa para o chat. Na maioria dos casos, esse será o thread iniciado quando o caso for criado pela primeira vez.
2. Quando o atendente de suporte entrar no thread, você poderá conversar sobre o seu caso de suporte. O atendente de suporte somente verá as mensagens nesse thread quando ingressar no thread, e as mensagens não aparecerão na correspondência do seu caso quando o chat for encerrado.

> **Note**
>
> As mensagens enviadas para esse canal fora do thread de chat nunca serão vistas pelo AWS Support, mesmo quando o chat estiver ativo.



3. (Opcional) Marque outros membros do canal para notificá-los no thread do chat.
4. Depois que o atendente de suporte ingressa no chat, o thread de chat fica ativo e o AWS Support App grava a conversa. Semelhante à nova opção de canal de chat, você pode conversar com o atendente sobre o seu caso de suporte e carregar qualquer arquivo anexado ao thread. O aplicativo AWS Support salva automaticamente seus arquivos e o log de chat na correspondência do seu caso.
5. (Opcional) Para interromper o chat ao vivo, escolha Encerrar chat na mensagem inicial desse thread. O atendente de suporte sai do thread e o AWS Support App para de gravar o chat ao vivo. O histórico de chat estará anexado à correspondência do caso para esse caso de suporte.
6. Se o problema for resolvido, você poderá selecionar Resolver caso na mensagem inicial desse thread.



Como procurar casos de suporte no Slack

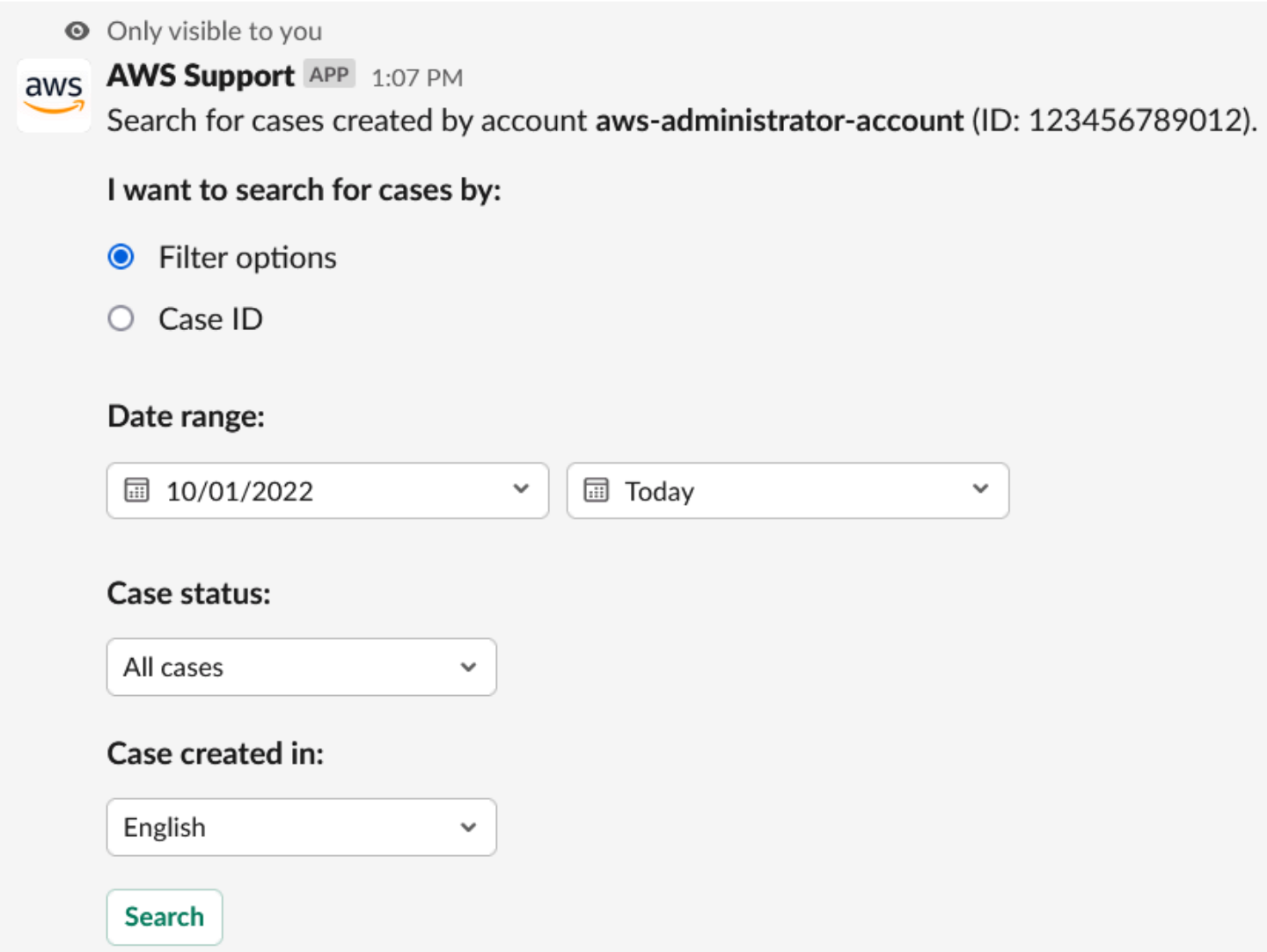
Em seu canal do Slack, é possível procurar casos de suporte da sua Conta da AWS e de outras contas que configuraram o mesmo canal e espaço de trabalho. Por exemplo, se a sua conta (123456789012) e a conta de seu colega de trabalho (111122223333) tiverem configurado o mesmo espaço de trabalho e canais no AWS Support Center Console, vocês poderão usar o AWS Support App para pesquisar e atualizar os casos de suporte um do outro.

Para filtrar seus resultados de pesquisa, use as opções a seguir:

- ID da conta
- ID do caso
- Status do caso
- Idioma de contato
- Intervalo de datas

Example : procurar casos no Slack

O exemplo a seguir mostra como pesquisar por Filter options (Opções de filtro) para uma única conta especificando o intervalo de datas, o status do caso e o idioma do contato.



Para procurar um caso de suporte no Slack

1. No canal do Slack, insira o seguinte comando:

   ```
   /awssupport search
   ```

2. Para a opção I want to search for cases by: (Quero pesquisar casos por:), escolha uma destas opções:

   A. Filter options (Opções de filtro): você pode filtrar casos com as seguintes opções:

   - Conta da AWS: esta lista só será exibida se você tiver várias contas nesse canal.
   - Date range (Intervalo de datas): a data em que o caso foi criado.
   - Case status (Status do caso): escolha o status do caso, como All open cases (Todos os casos abertos) ou Resolved (Resolvido).

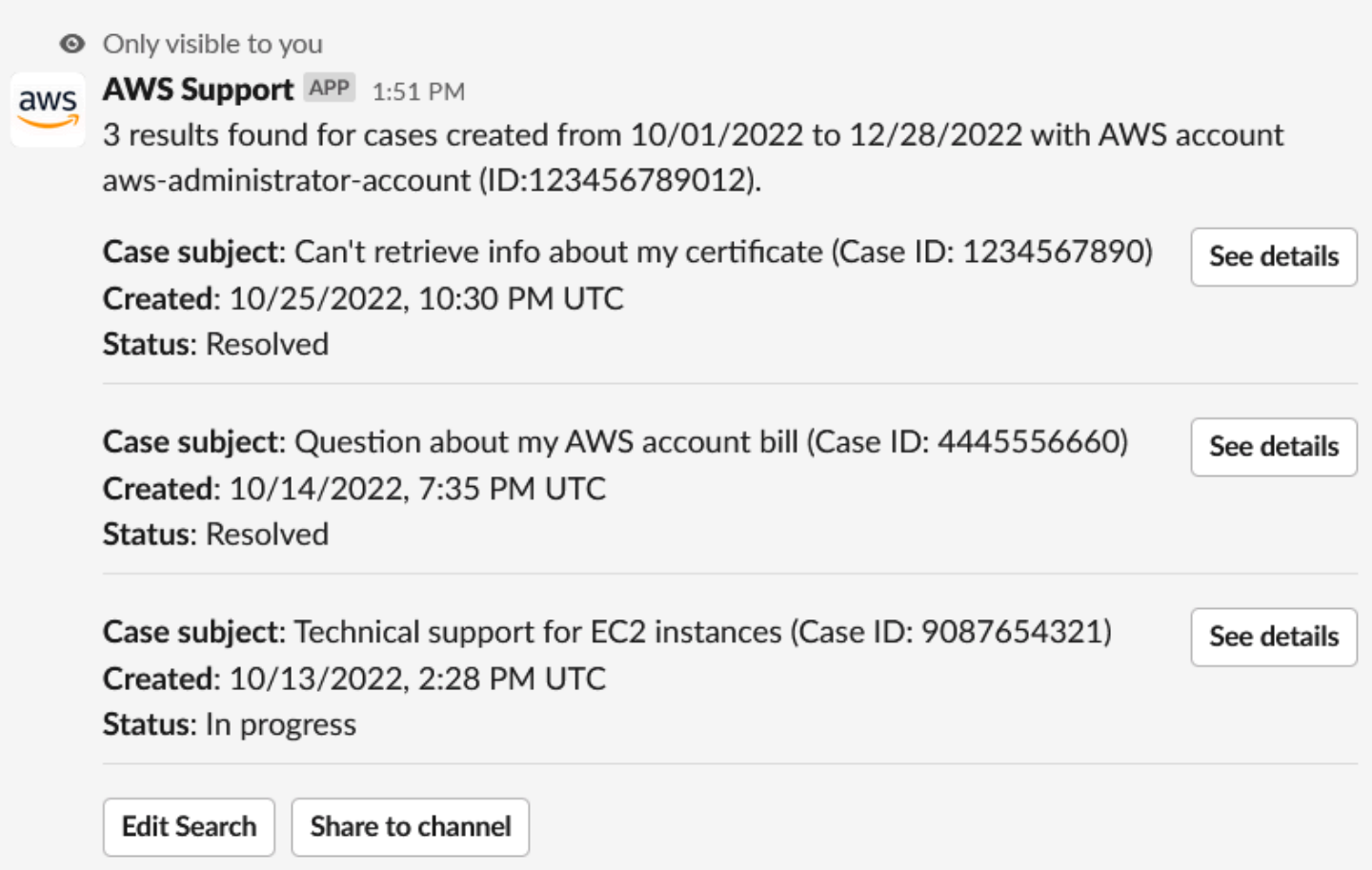
- Case created in (Caso criado em): o idioma de contato do caso.

B. Case ID (ID do caso): insira o ID do caso. Você só pode inserir um ID de caso por vez. Se você tiver várias contas no canal, escolha a Conta da AWS para pesquisar o caso.

3. Escolha Pesquisar. Os resultados da pesquisa são exibidos no Slack.

Usar os resultados da pesquisa

O exemplo a seguir retorna três casos de suporte de uma Conta da AWS.



Depois de receber os resultados da pesquisa, você pode fazer o seguinte:

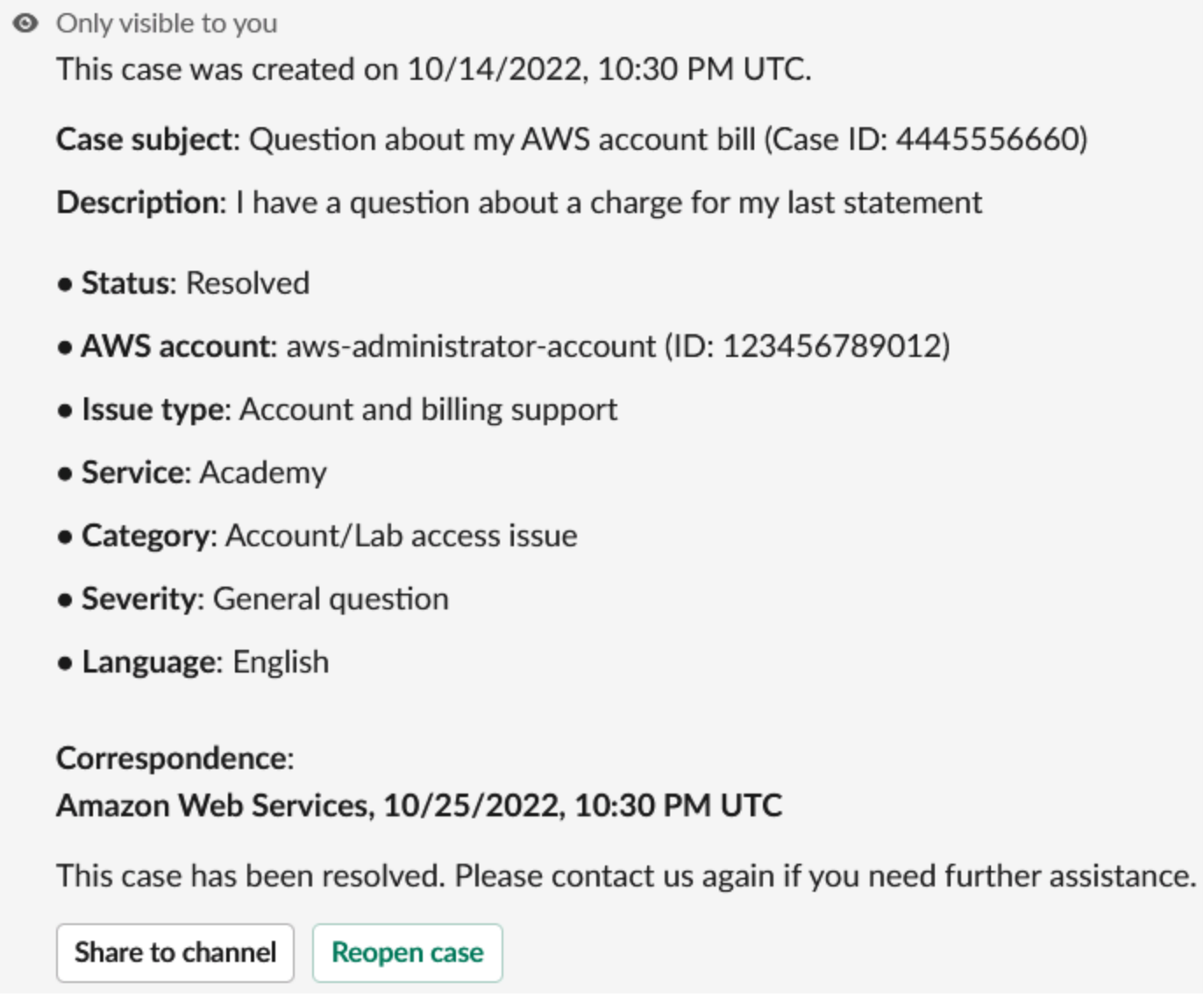
Para usar seus resultados de pesquisa

1. Escolha Edit Search (Editar pesquisa) para alterar opções de filtro ou ID do caso anteriores.
2. Escolha Share to channel (Compartilhar com o canal) para compartilhar os resultados da pesquisa com o canal.

3. Escolha See details (Visualizar detalhes) para obter mais informações sobre um caso. É possível escolher Show full message (Mostrar mensagem completa) para visualizar o restante da correspondência mais recente.
4. Se você pesquisou por Filter options (Opções de filtro), os resultados da pesquisa podem retornar vários casos. Escolha Next 5 results (5 resultados seguintes) ou Previous 5 results (5 resultados anteriores) para ver os 5 casos seguintes ou os 5 casos anteriores.

Example : caso de suporte resolvido

O exemplo a seguir mostra um caso de suporte resolvido de um problema de conta e faturamento depois de escolher See details (Ver detalhes).

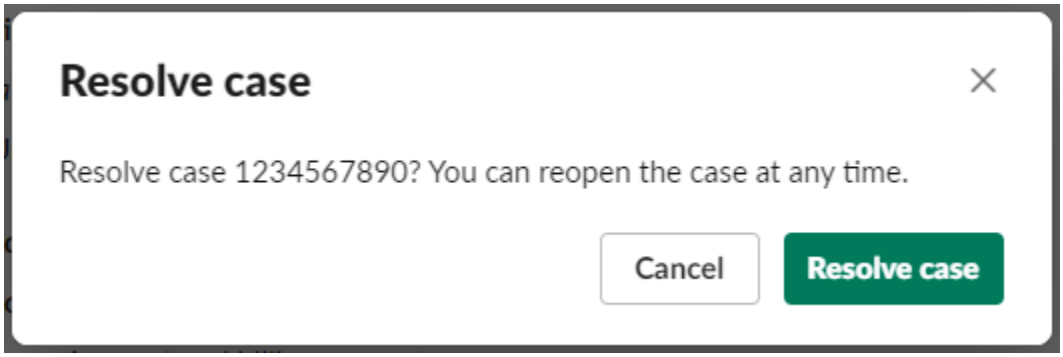


Como resolver um caso de suporte no Slack

Se você não precisar mais do seu caso de suporte ou tiver corrigido o problema, poderá resolver um caso de suporte diretamente no Slack. Assim, o caso também é resolvido no AWS Support Center Console. Depois de resolver um caso, você pode reabri-lo posteriormente.

Para resolver um caso de suporte no Slack

1. No seu canal do Slack, navegue até o caso de suporte. Consulte Como procurar casos de suporte no Slack.
2. Escolha See details (Visualizar detalhes) para o caso.
3. Escolha Resolve case (Resolver caso).
4. Na caixa de diálogo Resolve case (Resolver caso), escolha Resolve case (Resolver caso). Você pode reabrir um caso no canal do Slack ou no console do Support Center.

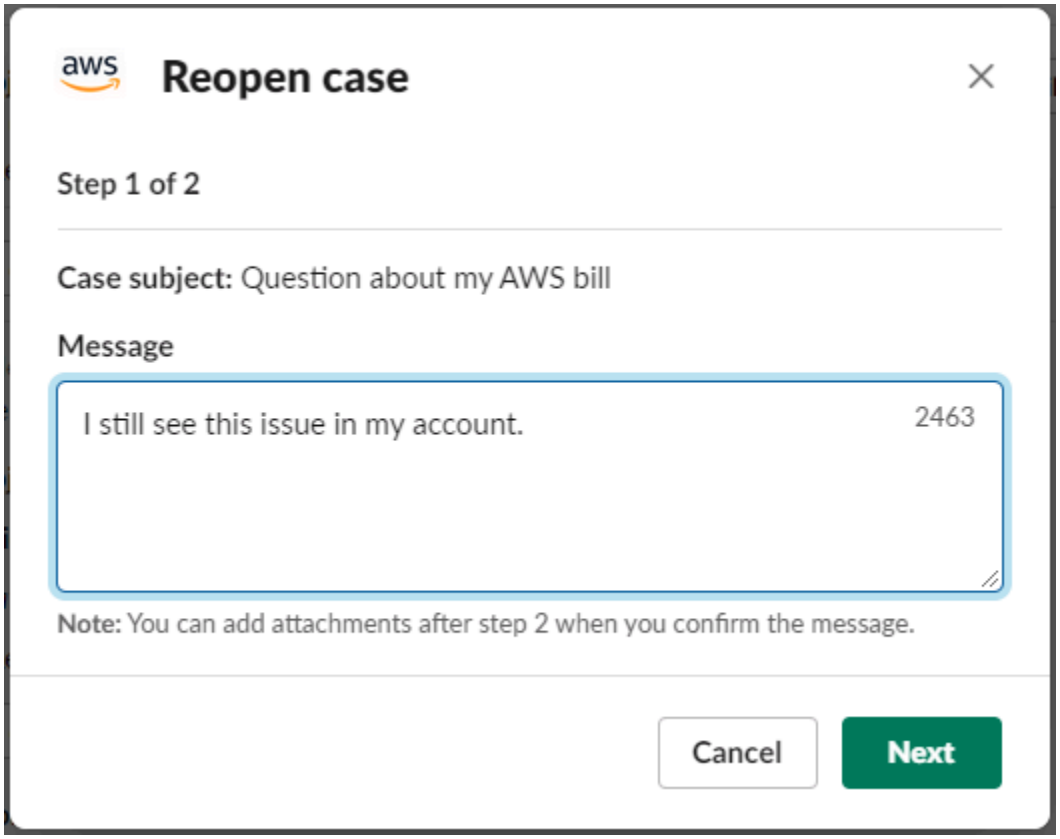


Como reabrir um caso de suporte no Slack

Depois de resolver um caso de suporte, você pode reabri-lo no Slack.

Para reabrir um caso de suporte no Slack

1. Encontre o caso de suporte para reabrir no Slack. Consulte Como procurar casos de suporte no Slack.
2. Escolha See details (Visualizar detalhes).
3. Selecione Reopen case (Reabrir caso).
4. Na caixa de diálogo Reopen case (Reabrir caso), insira uma breve descrição do problema no campo Message (Mensagem).
5. Escolha Next (Próximo).



6. (Opcional) Insira contatos adicionais.
7. Escolha Review (Revisar).
8. Revise os detalhes do seu caso e escolha Send message (Enviar mensagem). O seu caso reabre. Se você solicitou um novo chat ao vivo com um atendente de suporte, o Slack utilizará o mesmo canal de chat ou thread usado para um chat ao vivo anterior. Se você solicitou um chat ao vivo em um novo canal e ainda não o obteve, será aberto um novo canal de chat. Se você solicitou um chat ao vivo no canal atual e ainda não o obteve, será usado outro thread no canal atual.

Como solicitar um aumento de cota de serviço

Você pode solicitar aumentos de cota de serviço para sua conta no seu canal do Slack.

Para solicitar aumentos de cota de serviço

1. No canal do Slack, insira o seguinte comando:

   ```
   /awssupport quota
   ```

2. Na caixa de diálogo Increase service quota (Aumentar cota de serviço), insira as seguintes informações:

    a. Selecione a Conta da AWS.

    b. Selecione a Região da AWS.

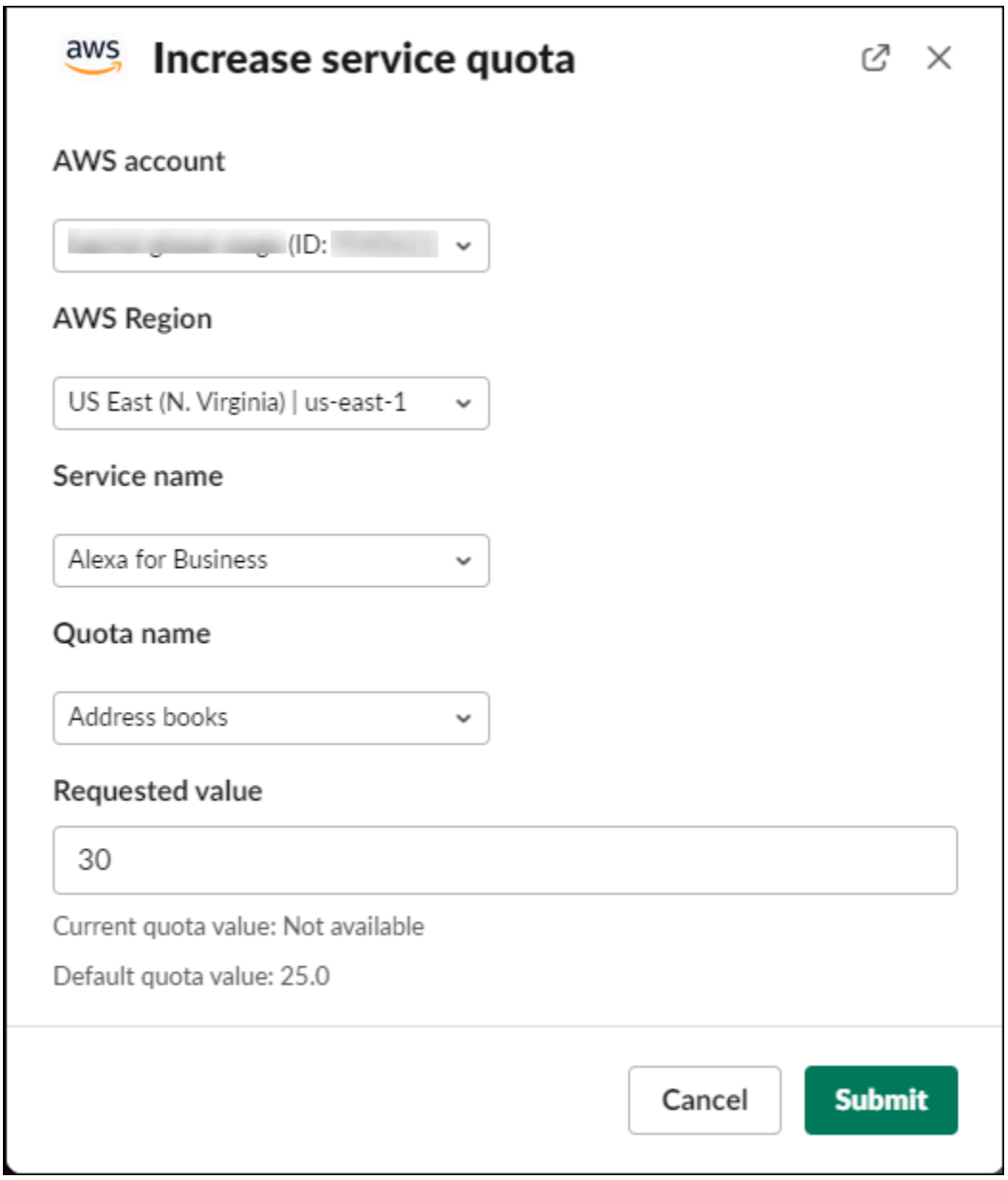
    c. Selecione o Service name (Nome do serviço).

    d. Escolha o Quota name (Nome da cota).

    e. Insira o Requested value (Valor solicitado) para o aumento da cota. Você deve inserir um valor maior do que a cota padrão.

3. Selecione Submit (Enviar).

Example : aumento da cota do Alexa for Business



Você também pode ver suas solicitações no console do Service Quotas. Para obter mais informações, consulte Requesting a quota increase (Como solicitar um aumento de cota) no Service Quotas User Guide (Guia do usuário do Service Quotas).

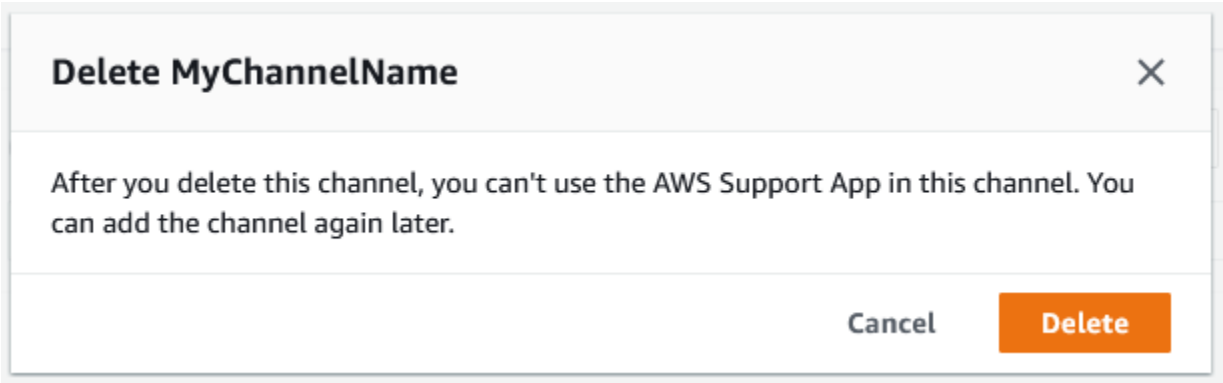
Como excluir uma configuração de canal do Slack do aplicativo AWS Support

Você pode excluir uma configuração de canal do aplicativo AWS Support caso não precise dele. Essa ação só exclui o canal do aplicativo AWS Support e do AWS Support Center Console. Seu canal não foi excluído do Slack.

É possível adicionar até 20 canais em sua Conta da AWS. Se você já atingiu essa cota, exclua um canal antes de adicionar outro.

Para excluir uma configuração de canal do Slack

1. Faça login no Support Center Console e escolha Slack configuration (Configuração do Slack).
2. Na página Slack configuration (Configuração do Slack), em Channels (Canais), escolha o nome do canal e, em seguida, selecione Delete (Excluir).
3. Na caixa de diálogo Delete channel name (Excluir nome do canal), escolha Delete (Excluir). Você pode adicionar esse canal ao aplicativo AWS Support depois.



Como excluir uma configuração de espaço de trabalho do Slack no aplicativo AWS Support

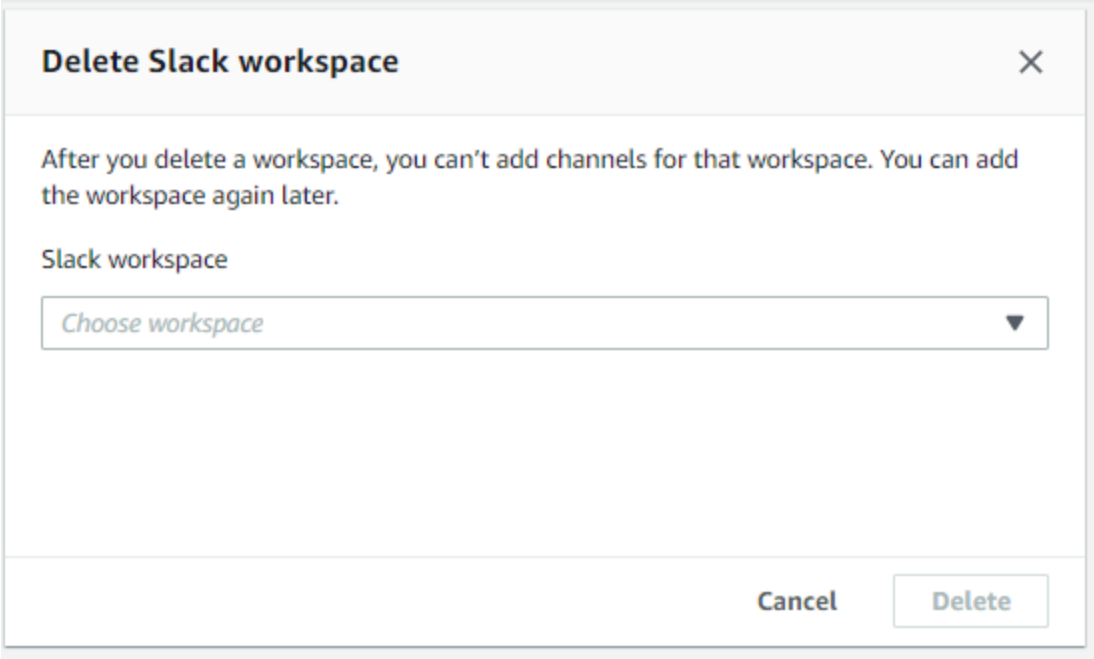
Você pode excluir uma configuração de espaço de trabalho do aplicativo AWS Support caso não precise dele. Essa ação exclui somente o espaço de trabalho do aplicativo AWS Support e do AWS Support Center Console. O seu espaço de trabalho não é excluído do Slack.

É possível adicionar até 5 espaços de trabalho em sua Conta da AWS. Se você já atingiu essa cota, exclua um espaço de trabalho do Slack antes de adicionar outro.

> **Note**
>
> Se você adicionou canais desse espaço de trabalho no aplicativo AWS Support, deve primeiro excluir esses canais antes de excluir o espaço de trabalho. Consulte Como excluir uma configuração de canal do Slack do aplicativo AWS Support.

Para excluir uma configuração de espaço de trabalho do Slack

1. Faça login no AWS Support Center Console e escolha Slack configuration (Configuração do Slack).
2. Na página Slack configuration (Configuração do Slack), em Slack workspaces (Espaços de trabalho do Slack), escolha Delete a workspace (Excluir um espaço de trabalho).
3. Na caixa de diálogo Delete Slack workspace (Excluir espaço de trabalho do Slack), escolha o nome do espaço de trabalho e selecione Delete (Excluir). Você pode adicionar o espaço de trabalho à sua Conta da AWS depois.



Aplicativo AWS Support nos comandos do Slack

Comandos do canal do Slack

Você pode inserir os comandos a seguir no canal do Slack em que convidou o aplicativo AWS Support. Esse nome de canal do Slack também aparece como um canal configurado no AWS Support Center Console.

`/awssupport create` ou `/awssupport create-case`

Crie um caso de suporte.

`/awssupport search` ou `/awssupport search-case`

Procure casos. Você pode procurar casos de suporte para as Contas da AWS que configurou no aplicativo AWS Support para o mesmo canal do Slack.

`/awssupport quota` ou `/awssupport service-quota-increase`

Solicite um aumento de cota de serviço.

Comandos do canal de chat ao vivo

Você pode inserir os comandos a seguir no canal de chat ao vivo. Este é o canal que o AWS Support App criará para você caso escolha um novo canal para conversar com o AWS Support. Os canais de chat incluem seu ID de caso de suporte, como *`awscase-1234567890`*.

> **Note**
>
> Os comandos a seguir não estão disponíveis ao usar um tópico no canal atual para um chat ao vivo. Em vez disso, use os botões anexados à mensagem inicial do tópico para encerrar um chat, convidar um novo atendente ou resolver o caso.

`/awssupport endchat`

Remova o atendente de suporte e encerre a sessão de chat ao vivo.

`/awssupport invite`

Convide um novo atendente de suporte para esse canal.

`/awssupport resolve`

Resolva esse caso de suporte.

Visualizar correspondências do aplicativo AWS Support no AWS Support Center Console

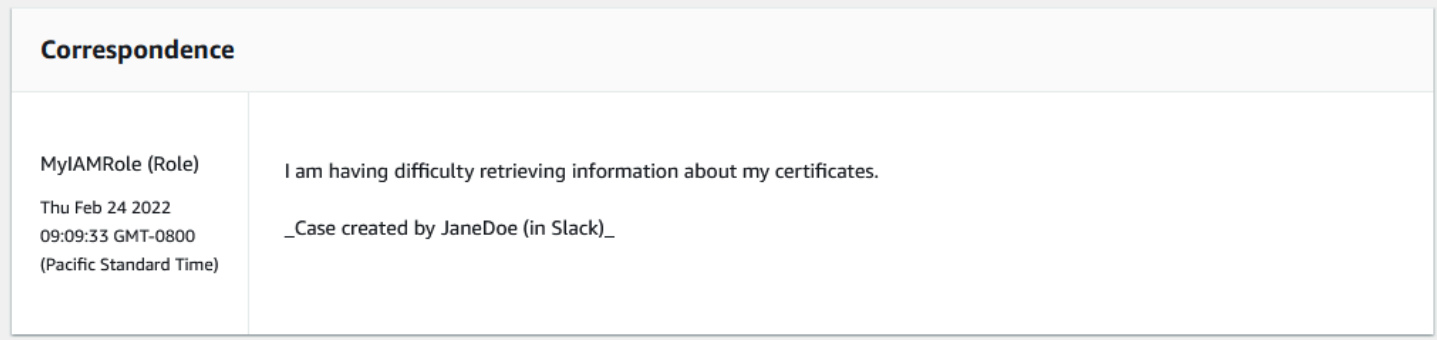
Ao criar, atualizar ou resolver casos de suporte para sua conta no canal do Slack, você também pode fazer login no console do Support Center para visualizar seus casos. Você pode visualizar as correspondências do caso para determinar se o caso foi atualizado no canal do Slack, ver o histórico de conversas com um atendente de suporte e encontrar qualquer anexo que você tenha enviado do Slack.

Para visualizar as correspondências de casos do Slack

1. Faça login no AWS Support Center Console para acessar sua conta.
2. Escolha seu caso de suporte.
3. Em Correspondence (Correspondência), você pode visualizar se o caso foi criado e atualizado no canal do Slack.

Example : caso de suporte

Na captura de tela a seguir, Maria Silva reabriu um caso de suporte no Slack. Essa correspondência aparece para o caso de suporte no console do Support Center.



Como criar o aplicativo AWS Support em recursos do Slack com o AWS CloudFormation

O aplicativo AWS Support no Slack está integrado ao AWS CloudFormation, um serviço que ajuda você a modelar e configurar seus recursos da AWS para que possa gastar menos tempo criando e gerenciando seus recursos e infraestrutura. Você cria um modelo que descreve todos os recursos da AWS desejados (como seu AccountAlias e SlackChannelConfiguration), e o AWS CloudFormation provisiona e configura esses recursos para você.

Ao usar o AWS CloudFormation, você poderá reutilizar seu modelo para configurar seus recursos do aplicativo AWS Support de forma repetida e consistente. Descreva seus recursos uma vez e depois provisione os mesmos recursos repetidamente em várias regiões e Contas da AWS.

Aplicativo AWS Support e modelos do AWS CloudFormation

Para provisionar e configurar recursos para o AWS Support App e serviços relacionados, é necessário entender os modelos do AWS CloudFormation. Os modelos são arquivos de texto formatados em JSON ou YAML. Esses modelos descrevem os recursos que você deseja provisionar nas suas pilhas do AWS CloudFormation. Se você não estiver familiarizado com JSON ou YAML, poderá usar o AWS CloudFormation Designer para ajudá-lo a começar a usar os modelos do AWS CloudFormation. Para obter mais informações, consulte O que é o Designer? (O que é o AWS CloudFormation Designer) no Manual do usuário do AWS CloudFormation.

O aplicativo AWS Support ajuda na criação de seu AccountAlias e SlackChannelConfiguration no AWS CloudFormation. Para obter mais informações, incluindo exemplos de modelos JSON e YAML para os recursos AccountAlias e SlackChannelConfiguration, consulte AWS Support App resource type reference no Guia do usuário do AWS CloudFormation.

Criar recursos de configuração do Slack para a organização

Você pode usar modelos do CloudFormation para criar os recursos necessários para o AWS Support App. Se você for a conta de gerenciamento de sua organização, você poderá usar os modelos para criar esses recursos para suas contas-membro no AWS Organizations.

Por exemplo, é possível usar um modelo para criar a mesma configuração de espaço de trabalho do Slack para todas as contas na organização, mas depois usar modelos separados para criar diferentes configurações de canais do Slack para Contas da AWS específicas ou unidades

organizacionais (UOs). Você também pode usar um modelo para criar uma configuração de espaço de trabalho do Slack para que as contas-membro possam configurar os canais do Slack que desejam para suas Contas da AWS.

É possível escolher se deseja usar os modelos do CloudFormation ou não. Caso não use modelos do CloudFormation, você poderá concluir as seguintes etapas manuais em vez disso:

- Crie os recursos do AWS Support App no AWS Support Center Console.
- Crie um caso de suporte no AWS Support para autorizar várias contas a usar o AWS Support App.
- Chame a operação da API RegisterSlackWorkspaceForOrganization para registrar um espaço de trabalho do Slack para sua conta. A pilha do CloudFormation chama essa operação de API para você.

Siga estes procedimentos para carregar o modelo do CloudFormation para sua organização. Você pode usar os modelos de exemplo da página de referência dos tipos de recursos do AWS Support App.

Os modelos dizem ao CloudFormation para criar os seguintes recursos:

- Uma configuração de canal do Slack.
- Uma configuração de espaço de trabalho do Slack.
- Um perfil do IAM com o nome `AWSSupportSlackAppCFNRole`. A política AWSSupportAppFullAccess gerenciada pela AWS é anexada.

Sumário

- Atualizar seus modelos do CloudFormation para o Slack
- Criar uma pilha para a conta de gerenciamento
- Criar um conjunto de pilhas para a organização

Atualizar seus modelos do CloudFormation para o Slack

Para começar, use os modelos a seguir para criar sua pilha. É necessário substituir os modelos por valores válidos para seu espaço de trabalho e canal do Slack.

> **Note**
>
> Não recomendamos usar o modelo para criar um recurso AccountAlias para sua organização. O recurso AccountAlias identifica de forma exclusiva uma Conta da AWS no AWS Support App. Suas contas-membro podem inserir um nome de conta no console da central de suporte. Para obter mais informações, consulte Autorizar um espaço de trabalho do Slack.

Atualize seus modelos do CloudFormation para o Slack

1. Se você for a conta de gerenciamento de uma organização, você deverá autorizar manualmente um espaço de trabalho do Slack para sua conta antes que suas contas-membro possam usar o CloudFormation para criar os recursos. Caso ainda não tenha feito isso, consulte Autorizar um espaço de trabalho do Slack.
2. Na página de referência de tipos de recursos do AWS Support App, copie o modelo JSON ou YAML para o recurso que você deseja.
3. Em um editor de texto, cole o modelo em um novo arquivo.
4. No modelo, especifique os parâmetros desejados. No mínimo, substitua os valores destes campos:

   - `TeamId` por seu ID de espaço de trabalho do Slack
   - `ChannelId` pelo ID do canal Slack
   - `ChannelName` por um nome para identificar a configuração do canal do Slack

   > **Tip**
   >
   > Para encontrar o espaço de trabalho e os IDs do canal, abra seu canal do Slack em um navegador. No URL, seu ID do espaço de trabalho é o primeiro identificador e o ID do canal é o segundo. Por exemplo, em https://app.slack.com/client/T012ABCDEFG/C01234A5BCD, T012ABCDEFG é o ID do espaço de trabalho e C01234A5BCD é o ID do canal.

5. Salve o arquivo como JSON ou YAML.

Criar uma pilha para a conta de gerenciamento

Em seguida, é necessário criar uma pilha para a conta de gerenciamento na organização. Essa etapa chama a operação de API RegisterSlackWorkspaceForOrganization para você e autoriza o espaço de trabalho com o Slack.

> **Note**
>
> Recomendamos carregar o modelo de configuração do espaço de trabalho do Slack que você atualizou no procedimento anterior para a conta de gerenciamento. Não é necessário carregar o modelo de configuração do canal do Slack, a menos que também esteja configurando a conta de gerenciamento para usar o AWS Support App.

Crie uma pilha para a conta de gerenciamento

1. Faça login no AWS Management Console ao usar a conta de gerenciamento de sua organização.
2. Abra o console do AWS CloudFormation em https://console.aws.amazon.com/cloudformation.
3. Se você ainda não tiver feito isso, em Region selector (Seletor de regiões), escolha uma das seguintes Regiões da AWS:
   - Europa (Frankfurt)
   - Europa (Irlanda)
   - Europa (Londres)
   - Leste dos EUA (N. da Virgínia)
   - Leste dos EUA (Ohio)
   - Oeste dos EUA (Oregon)
   - Ásia-Pacífico (Singapura)
   - Ásia-Pacífico (Tóquio)
   - Canadá (Central)
4. Siga o procedimento abaixo para criar uma pilha. Para obter mais informações, consulte Criar uma pilha no console do AWS CloudFormation.

   Depois de criar a pilha do CloudFormation com sucesso, você pode usar o mesmo modelo para criar um conjunto de pilhas para sua organização.

Criar um conjunto de pilhas para a organização

Em seguida, use o mesmo modelo para a configuração do espaço de trabalho do Slack para criar um conjunto de pilhas com permissões `service-managed`. É possível usar conjuntos de pilhas para criar a pilha para toda a organização ou especificar as UOs desejadas. Para obter mais informações, consulte Criar um conjunto de pilhas.

Esse procedimento também chama a operação de API RegisterSlackWorkspaceForOrganization para você. Essa operação de API autoriza o espaço de trabalho com o Slack para as contas-membro.

Para criar um conjunto de pilhas para a organização

1. Faça login no AWS Management Console ao usar a conta de gerenciamento de sua organização.
2. Abra o console do AWS CloudFormation em https://console.aws.amazon.com/cloudformation.
3. Caso ainda não tenha feito isso, em Region selector (Seletor de regiões), escolha a mesma Região da AWS usada no procedimento anterior.
4. No painel de navegação, escolha StackSets.
5. Escolha Create StackSet (Criar StackSet).
6. Na página Choose a template (Escolha um modelo), mantenha as opções padrão para as seguintes opções:
   - Em Permissions (Permissões), mantenha Service-managed permissions (Permissões gerenciadas pelo serviço).
   - Em Prerequisite - Prepare template (Pré-requisito: preparar modelo), mantenha Template is ready (O modelo está pronto).
7. Em Specify template (Especificar modelo), selecione Upload a template file (Carregar um arquivo de modelo) e depois Choose file (Escolher arquivo).
8. Escolha seu arquivo e escolha Next (Próximo).
9. Na página Specify StackSet (Especificar StackSet), digite o nome da pilha, como **`support-app-slack-workspace`**, insira uma descrição e escolha Next (Próximo).
10. Na página Configure StackSet options (Configurar opções do StackSet), mantenha os padrões e selecione Next (Próximo).

11. Na página Set deployment options (Definir opções de implantação), em Add stacks to stack set (Adicionar pilhas ao conjunto de pilhas), mantenha a opção padrão Deploy new stacks (Implantar novas pilhas).
12. Para Deployment targets (Metas de implantação), escolha se deseja criar a pilha para toda a organização ou UOs específicas. Se escolher uma UO, insira o ID da UO.
13. Em Specify regions (Especificar regiões), insira somente uma das seguintes Regiões da AWS:

    - Europa (Frankfurt)
    - Europa (Irlanda)
    - Europa (Londres)
    - Leste dos EUA (N. da Virgínia)
    - Leste dos EUA (Ohio)
    - Oeste dos EUA (Oregon)
    - Ásia-Pacífico (Singapura)
    - Ásia-Pacífico (Tóquio)
    - Canadá (Central)

    Observações:

    - Para otimizar seu fluxo de trabalho, recomendamos usar a mesma Região da AWS escolhida na Etapa 3.
    - Escolher mais de uma Região da AWS pode causar conflitos na criação de sua pilha.

14. Em Deployment options (Opções de implantação), em Failure tolerance - optional (Tolerância a falhas - opcional), insira o número de contas em que as pilhas podem falhar antes que o CloudFormation interrompa a operação. Recomendamos inserir o número de contas que deseja adicionar, menos uma. Por exemplo, se sua UO especificada tiver dez contas-membro, insira 9. Isso significa que, mesmo que a operação do CloudFormation falhe nove vezes, pelo menos uma conta será bem-sucedida.
15. Escolha Next (Próximo).
16. Na página Review (Revisar), reveja suas opções e escolha Submit (Enviar). É possível verificar o status de sua pilha na guia Stack instances (Instâncias da pilha).

17. (Opcional) Repita esse procedimento para carregar um modelo para a configuração de um canal do Slack. O modelo de exemplo também cria o perfil do IAM e anexa uma política gerenciada pela AWS. Essa função tem as permissões necessárias para acessar outros serviços por você. Para obter mais informações, consulte Como gerenciar o acesso ao aplicativo AWS Support.

    Se você não criar um conjunto de pilhas para criar a configuração do canal do Slack, suas contas-membro poderão configurar manualmente o canal do Slack. Para obter mais informações, consulte Como configurar um canal do Slack.

Depois que o CloudFormation cria as pilhas, cada conta-membro pode acessar o console da Central de suporte e encontrar seus espaços de trabalho e canais do Slack configurados. Elas podem então usar o AWS Support App para sua Conta da AWS. Consulte Como criar casos de suporte em um canal do Slack.

> **Tip**
>
> Caso precise carregar um novo modelo, recomendamos usar a mesma Região da AWS especificada anteriormente.

Saiba mais sobre o CloudFormation

Para saber mais sobre o CloudFormation, consulte os seguintes recursos:

- AWS CloudFormation
- Manual do usuário do AWS CloudFormation
- AWS CloudFormation Referência da API
- Guia do usuário da interface de linha de comando do AWS CloudFormation

Criar recursos do AWS Support App ao usar o Terraform

Também é possível usar o Terraform para criar os recursos do AWS Support App para sua Conta da AWS. O Terraform é uma ferramenta de infraestrutura como código que pode ser usada para suas aplicações em nuvem. Você pode usar o Terraform para criar recursos do AWS Support App em vez de implantar uma pilha do CloudFormation em uma conta.

Depois de instalar o Terraform, é possível especificar os recursos do AWS Support App que deseja. O Terraform chama a operação de API RegisterSlackWorkspaceForOrganization para registrar um espaço de trabalho do Slack para você e cria seus recursos. Em seguida, você pode fazer login no console da Central de suporte e encontrar seus espaços de trabalho e canais do Slack configurados.

Observações

- Se você for a conta de gerenciamento de uma organização, é necessário autorizar manualmente um espaço de trabalho do Slack para sua conta antes que suas contas-membro possam usar o Terraform para criar os recursos. Caso ainda não tenha feito isso, consulte Autorizar um espaço de trabalho do Slack.
- Ao contrário dos conjuntos de pilhas do CloudFormation, não é possível usar o Terraform para criar os recursos do AWS Support App para uma UO de sua organização.
- Você também encontra o histórico de eventos dessas atualizações no Terraform no AWS CloudTrail. O `eventSource` desses eventos será `cloudcontrolapi.amazonaws.com` e `supportapp.amazonaws.com`. Para obter mais informações, consulte Como fazer registro em log no aplicativo AWS Support nas chamadas de API do Slack com o AWS CloudTrail.

Saiba mais

Para saber mais sobre o Terraform, consulte os tópicos a seguir:

- Instalação do Terraform
- Tutorial do Terraform: criar uma infraestrutura para a AWS
- `awscc_support_app_account_alias`
- `awscc_supportapp_slack_workspace_configuration`
- `awscc_supportapp_slack_channel_configuration`

Segurança em AWS Support

A segurança na nuvem AWS é a maior prioridade. Como AWS cliente, você se beneficia de uma arquitetura de data center e rede criada para atender aos requisitos das organizações mais sensíveis à segurança.

A segurança é uma responsabilidade compartilhada entre você AWS e você. O modelo de responsabilidade compartilhada descreve isso como segurança da nuvem e segurança na nuvem:

- Segurança da nuvem — AWS é responsável por proteger a infraestrutura que executa AWS os serviços na AWS nuvem. AWS também fornece serviços que você pode usar com segurança. Auditores terceirizados testam e verificam regularmente a eficácia de nossa segurança como parte dos programas de AWS conformidade dos programas de . Para saber mais sobre os programas de conformidade que se aplicam AWS Support, consulte AWS serviços no escopo do programa de conformidade .
- Segurança na nuvem — Sua responsabilidade é determinada pelo AWS serviço que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da empresa e as leis e regulamentos aplicáveis.

Esta documentação ajuda você a entender como aplicar o modelo de responsabilidade compartilhada ao usar AWS Support. Os tópicos a seguir mostram como configurar para atender AWS Support aos seus objetivos de segurança e conformidade. Você também aprende a usar outros Amazon Web Services que ajudam você a monitorar e proteger seus AWS Support recursos.

Tópicos

- Proteção de dados em AWS Support
- Segurança para seus AWS Support casos
- Gerenciamento de identidade e acesso para AWS Support
- Resposta a incidentes
- Registro e monitoramento em AWS Support e AWS Trusted Advisor
- Validação de conformidade para AWS Support
- Resiliência em AWS Support
- Segurança da infraestrutura em AWS Support
- Análise de configuração e vulnerabilidade em AWS Support

Proteção de dados em AWS Support

O modelo de responsabilidade AWS compartilhada modelo se aplica à proteção de dados em AWS Support. Conforme descrito neste modelo, AWS é responsável por proteger a infraestrutura global que executa todos os Nuvem AWS. Você é responsável por manter o controle sobre seu conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para ter mais informações sobre a privacidade de dados, consulte as Perguntas frequentes sobre privacidade de dados. Para ter mais informações sobre a proteção de dados na Europa, consulte a postagem do blog AWS Shared Responsibility Model and GDPR no Blog de segurança da AWS .

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS as credenciais e configure usuários individuais com AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use uma autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com os recursos. AWS Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure a API e o registro de atividades do usuário com AWS CloudTrail.
- Use soluções de AWS criptografia, juntamente com todos os controles de segurança padrão Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sigilosos armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-2 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para ter mais informações sobre endpoints do FIPS, consulte Federal Information Processing Standard (FIPS) 140-2.

É altamente recomendável que nunca sejam colocadas informações de identificação confidenciais, como endereços de e-mail dos seus clientes, em marcações ou campos de formato livre, como um campo Nome. Isso inclui quando você trabalha com AWS Support ou Serviços da AWS usa o console, a API ou AWS os SDKs. AWS CLI Quaisquer dados inseridos em tags ou campos de texto de formato livre usados para nomes podem ser usados para logs de faturamento ou de diagnóstico.

Se você fornecer um URL para um servidor externo, recomendamos fortemente que não sejam incluídas informações de credenciais no URL para validar a solicitação a esse servidor.

Segurança para seus AWS Support casos

Ao criar um caso de suporte, você é o proprietário das informações que você inclui no seu caso de suporte. AWS não acessa seus Conta da AWS dados sem sua permissão. AWS não compartilha suas informações com terceiros.

Ao criar um caso de suporte, observe o seguinte:

- AWS Support usa as permissões definidas na função `AWSServiceRoleForSupport` vinculada ao serviço para ligar para outras pessoas Serviços da AWS que solucionam problemas do cliente para você. Para obter mais informações, consulte Usando funções vinculadas a serviços AWS Support e políticas AWS gerenciadas:. AWSSupportServiceRolePolicy
- Você pode ver as chamadas de API AWS Support que ocorreram em seu Conta da AWS. Por exemplo, você pode visualizar as informações de log quando alguém em sua conta cria ou resolve um caso de suporte. Para obter mais informações, consulte Logging AWS Support API call with AWS CloudTrail.
- Você pode usar a AWS Support API para chamar a `DescribeCases` API. Essa API retorna informações do caso de suporte, como o ID do caso, a data de criação e resolução e as correspondências com o atendente de suporte. É possível visualizar os detalhes do caso por até 12 meses após a sua abertura. Para obter mais informações, consulte DescribeCasesa Referência AWS Support da API.
- Seus casos de suporte seguem a Validação de conformidade para o AWS Support.
- Quando você cria um caso de suporte, AWS não obtém acesso à sua conta. Se necessário, os atendentes de suporte usam uma ferramenta de compartilhamento de tela para visualizar a sua tela remotamente e identificar e solucionar problemas. Essa ferramenta é somente para visualização. O AWS Support não pode agir por você durante a sessão de compartilhamento de tela. Você deve consentir para que haja o compartilhamento de uma tela com o atendente de suporte. Para obter mais informações, consulte as Perguntas frequentes do AWS Support.
- Você pode alterar seu AWS Support plano para obter a ajuda necessária para sua conta. Para obter mais informações, consulte Comparar AWS Support planos e Alterar seu AWS Support plano.

Gerenciamento de identidade e acesso para AWS Support

AWS Identity and Access Management (IAM) é uma ferramenta AWS service (Serviço da AWS) que ajuda o administrador a controlar com segurança o acesso aos AWS recursos. Os administradores do IAM controlam quem pode ser autenticado (conectado) e autorizado (tem permissões) a usar AWS Support os recursos. O IAM é um AWS service (Serviço da AWS) que você pode usar sem custo adicional.

Tópicos

- Público
- Autenticando com identidades
- Gerenciamento do acesso usando políticas
- Como AWS Support funciona com o IAM
- AWS Support exemplos de políticas baseadas em identidade
- Usar funções vinculadas a serviços
- AWS políticas gerenciadas para AWS Support
- Gerencie o acesso ao AWS Support Centro
- Gerencie o acesso aos AWS Support planos
- Gerencie o acesso ao AWS Trusted Advisor
- Políticas de controle de serviço de exemplo para o AWS Trusted Advisor
- Solução de problemas AWS Support de identidade e acesso

Público

A forma como você usa AWS Identity and Access Management (IAM) difere, dependendo do trabalho que você faz AWS Support.

Usuário do serviço — Se você usar o AWS Support serviço para realizar seu trabalho, seu administrador fornecerá as credenciais e as permissões de que você precisa. À medida que você usa mais AWS Support recursos para fazer seu trabalho, talvez precise de permissões adicionais. Entender como o acesso é gerenciado pode ajudá-lo a solicitar as permissões corretas ao seu administrador. Se não for possível acessar um recurso no AWS Support, consulte Solução de problemas AWS Support de identidade e acesso.

Administrador de serviços — Se você é responsável pelos AWS Support recursos da sua empresa, provavelmente tem acesso total AWS Support a. É seu trabalho determinar quais AWS Support recursos e recursos seus usuários do serviço devem acessar. Assim, você deve enviar solicitações ao administrador do IAM para alterar as permissões dos usuários de seu serviço. Revise as informações nesta página para entender os Introdução ao IAM. Para saber mais sobre como sua empresa pode usar o IAM com AWS Support, consulteComo AWS Support funciona com o IAM.

Administrador do IAM:Se você for um administrador do IAM, talvez queira saber detalhes sobre como pode gravar políticas para gerenciar o acesso ao AWS Support. Para ver exemplos de políticas AWS Support baseadas em identidade que você pode usar no IAM, consulte. AWS Support exemplos de políticas baseadas em identidade

Autenticando com identidades

A autenticação é como você faz login AWS usando suas credenciais de identidade. Você deve estar autenticado (conectado AWS) como o Usuário raiz da conta da AWS, como usuário do IAM ou assumindo uma função do IAM.

Você pode entrar AWS como uma identidade federada usando credenciais fornecidas por meio de uma fonte de identidade. AWS IAM Identity Center Usuários (IAM Identity Center), a autenticação de login único da sua empresa e suas credenciais do Google ou do Facebook são exemplos de identidades federadas. Quando você faz login como uma identidade federada, o administrador já configurou anteriormente a federação de identidades usando perfis do IAM. Ao acessar AWS usando a federação, você está assumindo indiretamente uma função.

Dependendo do tipo de usuário que você é, você pode entrar no AWS Management Console ou no portal de AWS acesso. Para obter mais informações sobre como fazer login em AWS, consulte Como fazer login Conta da AWS no Guia do Início de Sessão da AWS usuário.

Se você acessar AWS programaticamente, AWS fornece um kit de desenvolvimento de software (SDK) e uma interface de linha de comando (CLI) para assinar criptograficamente suas solicitações usando suas credenciais. Se você não usa AWS ferramentas, você mesmo deve assinar as solicitações. Para obter mais informações sobre como usar o método recomendado para assinar solicitações por conta própria, consulte Assinatura de solicitações de AWS API no Guia do usuário do IAM.

Independentemente do método de autenticação usado, também pode ser exigido que você forneça informações adicionais de segurança. Por exemplo, AWS recomenda que você use a autenticação multifator (MFA) para aumentar a segurança da sua conta. Para saber mais, consulte Autenticação

multifator no Guia AWS IAM Identity Center do usuário. Usar a autenticação multifator (MFA) na AWS no Guia do usuário do IAM.

AWS usuário raiz da conta

Ao criar uma Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos Serviços da AWS os recursos da conta. Essa identidade é chamada de usuário Conta da AWS raiz e é acessada fazendo login com o endereço de e-mail e a senha que você usou 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 pode 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.

Grupos e usuários do IAM

Um usuário do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas para uma única pessoa ou aplicativo. Sempre que possível, recomendamos depender de 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, recomendamos alternar as chaves de acesso. Para mais informações, consulte Alterne 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 atribuir 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 Quando criar um usuário do IAM (em vez de um perfil) no Guia do usuário do IAM.

Perfis do IAM

Uma função do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas. Ele é semelhante a um usuário do IAM, mas não está associado a uma pessoa específica. Você

pode assumir temporariamente uma função do IAM no AWS Management Console trocando de funções. Você pode assumir uma função chamando uma operação de AWS API AWS CLI ou usando uma URL personalizada. Para mais informações sobre métodos para o uso de perfis, consulte Usar perfis do IAM 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, você pode 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 pelo mesmo. Para mais informações sobre perfis para federação, consulte Criar um perfil para um provedor de identidades de terceiros no Guia do usuário do IAM. Se você usar o IAM Identity Center, configure um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o IAM Identity Center 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 assumir 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, com alguns Serviços da AWS, você pode anexar uma política diretamente a um recurso (em vez de usar uma função como proxy). Para saber a diferença entre funções e políticas baseadas em recurso para acesso entre contas, consulte Como os perfis do IAM diferem das políticas baseadas em recurso 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 do principal de chamada, usando um perfil de serviço ou um perfil vinculado ao serviço.
  - Sessões de acesso direto (FAS) — Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado o principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter

permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Encaminhar sessões de acesso.

- Perfil de serviço: um perfil de serviço é um perfil do IAM que um serviço assume para realizar 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 no Guia do usuário do IAM.
- Função vinculada ao serviço — Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode assumir o perfil para executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não pode editar as permissões para perfis vinculados ao serviço.

- Aplicativos em execução no Amazon EC2 — Você pode usar uma função do IAM para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma instância do EC2 e fazendo AWS CLI solicitações de API. AWS É preferível fazer isso a armazenar chaves de acesso na instância do EC2. Para atribuir uma AWS função a uma instância do EC2 e disponibilizá-la para todos os seus aplicativos, você cria um perfil de instância anexado à instância. Um perfil de instância contém o perfil e permite que os programas em execução na instância do EC2 obtenham credenciais temporárias. Para obter mais informações, consulte Usar uma função do IAM para conceder permissões a aplicações em execução nas instâncias do Amazon EC2 no Guia do usuário do IAM.

Para saber se deseja usar os perfis do IAM, consulte Quando criar um perfil do IAM (em vez de um usuário) no Guia do usuário do IAM.

Gerenciamento do acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política é um objeto AWS que, quando associada a uma identidade ou recurso, define suas permissões. AWS avalia essas políticas quando um principal (usuário, usuário raiz ou sessão de função) faz uma solicitação. As permissões nas políticas determinam se a solicitação será permitida ou negada. A maioria das políticas é armazenada AWS como documentos JSON. Para 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 políticas AWS JSON 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 funções não têm permissões. Para conceder aos usuários permissão para executar ações nos recursos de que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM a 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 função da AWS Management Console AWS CLI, da ou da AWS API.

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 funções podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Criação de política do IAM no Guia do usuário do IAM.

As políticas baseadas em identidade podem ser categorizadas ainda mais 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 autônomas que você pode associar a vários usuários, grupos e funções em seu Conta da AWS. As políticas AWS gerenciadas incluem políticas gerenciadas 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.

Outros tipos de política

AWS oferece suporte a tipos de políticas adicionais 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 atributo 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 e dos seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou a função no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para 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 (OU) em. AWS Organizations AWS Organizations é um serviço para agrupar e gerenciar centralmente vários Contas da AWS que sua empresa possui. Se você habilitar todos os atributos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as contas. O SCP limita as permissões para entidades nas contas dos membros, incluindo cada uma Usuário raiz da conta da AWS. Para mais informações sobre Organizações e SCPs, consulte Como os SCPs funcionam no AWS Organizations Guia do Usuário.
- 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 recurso. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para 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 AWS determinar se uma solicitação deve ser permitida quando vários tipos de políticas estão envolvidos, consulte Lógica de avaliação de políticas no Guia do usuário do IAM.

Como AWS Support funciona com o IAM

Antes de usar o IAM para gerenciar o acesso AWS Support, você deve entender quais recursos do IAM estão disponíveis para uso AWS Support. Para ter uma visão de alto nível de como AWS Support e outros AWS serviços funcionam com o IAM, consulte AWS os serviços que funcionam com o IAM no Guia do usuário do IAM.

Para obter informações sobre como gerenciar o acesso para AWS Support usar o IAM, consulte Gerenciar acesso para AWS Support.

Tópicos

- Políticas baseadas em identidade do AWS Support

- AWS Support Funções do IAM

Políticas baseadas em identidade do AWS Support

Com as políticas baseadas em identidade do IAM, é possível especificar as ações e os recursos que são permitidos ou negados, bem como as condições sob as quais as ações são permitidas ou negadas. O AWS Support oferece suporte a ações específicas. Para saber mais sobre os elementos usados em uma política JSON, consulte Referência de elementos de política JSON do IAM no Manual do usuário do IAM.

Ações

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao 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 você pode usar para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome da operação de AWS API associada. Existem algumas exceções, como ações somente de permissão, que não têm uma operação de API correspondente. Há também algumas operações que 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.

As ações políticas AWS Support usam o seguinte prefixo antes da ação:`support:`. Por exemplo, para conceder permissão a alguém para executar uma instância do Amazon EC2 com a operação da API `RunInstances` do Amazon EC2, inclua a ação `ec2:RunInstances` na política da pessoa. As declarações de política devem incluir um elemento `Action` ou AWS Support . O `NotAction` define seu próprio conjunto de ações que descrevem as tarefas que podem ser executadas com esse serviço.

Para especificar várias ações em uma única instrução, separe-as com vírgulas, como segue:

```
"Action": [
      "ec2:action1",
      "ec2:action2"
```

Você também pode especificar várias ações usando caracteres curinga (*). Por exemplo, para especificar todas as ações que começam com a palavra `Describe`, inclua a seguinte ação:

```
"Action": "ec2:Describe*"
```

Para ver uma lista de AWS Support ações, consulte Ações definidas por AWS Support no Guia do usuário do IAM.

Exemplos

Para ver exemplos de políticas AWS Support baseadas em identidade, consulte. AWS Support exemplos de políticas baseadas em identidade

AWS Support Funções do IAM

Uma função do IAM é uma entidade dentro da sua AWS conta que tem permissões específicas.

Usando credenciais temporárias com AWS Support

É possível usar credenciais temporárias para fazer login com federação, assumir um perfil do IAM ou assumir um perfil entre contas. Você obtém credenciais de segurança temporárias chamando operações de AWS STS API, como AssumeRoleou GetFederationToken.

AWS Support suporta o uso de credenciais temporárias.

Perfis vinculados ao serviço

As funções vinculadas ao serviço permitem que AWS os serviços acessem recursos em outros serviços para concluir uma ação em seu nome. Os perfis vinculados a serviço aparecem na sua conta do IAM e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não pode editar as permissões para perfis vinculados a serviço.

AWS Support suporta funções vinculadas a serviços. Para obter detalhes sobre como criar ou gerenciar funções AWS Support vinculadas a serviços, consulte. Usar perfis vinculados ao serviço do AWS Support

Perfis de serviço

Esse atributo permite que um serviço assuma um perfil de serviço em seu nome. O perfil permite que o serviço acesse recursos em outros serviços para concluir uma ação em seu nome. Os perfis de serviço aparecem em sua conta do IAM e são de propriedade da conta. Isso indica que um administrador do IAM pode alterar as permissões para essa função. Porém, fazer isso pode alterar a funcionalidade do serviço.

AWS Support suporta funções de serviço.

AWS Support exemplos de políticas baseadas em identidade

Por padrão, os usuários e os perfis do IAM não têm permissão para criar ou modificar recursos do AWS Support . Eles também não podem realizar tarefas usando a AWS API AWS Management Console AWS CLI, ou. Um administrador do IAM deve criar políticas do IAM que concedam aos usuários e perfis permissão para executarem operações de API específicas nos recursos especificados de que precisam. O administrador deve anexar essas políticas aos usuários ou grupos do IAM que exigem essas permissões.

Para saber como criar uma política baseada em identidade do IAM utilizando esses exemplos de documentos de política JSON, consulte Criar políticas na guia JSON no Guia do usuário do IAM.

Tópicos

- Práticas recomendadas de políticas
- Usar o console do AWS Support
- Permitir que os usuários visualizem suas próprias permissões

Práticas recomendadas de políticas

As políticas baseadas em identidade são muito eficientes. Eles determinam se alguém pode criar, acessar ou excluir AWS Support recursos em sua conta. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece a usar políticas AWS gerenciadas — Para começar a usar AWS Support rapidamente, use políticas AWS gerenciadas para dar a seus funcionários as permissões de que precisam. Essas políticas já estão disponíveis em sua conta e são mantidas e atualizadas pela AWS. Para obter mais informações, consulte Comece a usar permissões com políticas AWS gerenciadas no Guia do usuário do IAM.
- Conceder privilégio mínimo: ao criar políticas personalizadas, conceda apenas as permissões necessárias para executar uma tarefa. Comece com um conjunto mínimo de permissões e conceda permissões adicionais conforme necessário. Fazer isso é mais seguro do que começar com permissões que são muito lenientes e tentar restringi-las superiormente. Para obter mais informações, consulte Conceder privilégio mínimo no Guia do usuário do IAM.
- Habilitar o MFA para operações confidenciais: para segurança adicional, exija que os usuários do IAM usem a autenticação multifator (MFA) para acessar recursos ou operações de API

confidenciais. Para obter mais informações, consulte Usar autenticação multifator (MFA) AWS no Guia do usuário do IAM.

- Usar condições de política para segurança adicional: na medida do possível, defina as condições sob as quais suas políticas baseadas em identidade permitem o acesso a um recurso. Por exemplo, você pode gravar condições para especificar um intervalo de endereços IP permitidos do qual a solicitação deve partir. Você também pode escrever condições para permitir somente solicitações em uma data especificada ou período ou para exigir o uso de SSL ou MFA. Para obter mais informações, consulte Elementos de política JSON do IAM: condição no Guia do usuário do IAM.

Usar o console do AWS Support

Para acessar o AWS Support console, você deve ter um conjunto mínimo de permissões. Essas permissões devem permitir que você liste e visualize detalhes sobre os AWS Support recursos em sua AWS conta. Se você criar uma política baseada em identidade que seja mais restritiva que as permissões mínimas necessárias, o console não funcionará como pretendido para entidades (usuários ou perfis do IAM) com essa política.

Para garantir que essas entidades ainda possam usar o AWS Support console, anexe também a seguinte política AWS gerenciada às entidades. Para obter mais informações, consulte Adição de permissões a um usuário no Guia do usuário do IAM.

Você não precisa permitir permissões mínimas do console para usuários que estão fazendo chamadas somente para a API AWS CLI ou para a AWS API. Em vez disso, permita o acesso somente às ações que correspondem à operação da API que você está tentando executar.

Permitir que os usuários visualizem suas próprias permissões

Este exemplo mostra como você pode criar uma política que permite que os usuários do IAM visualizem as políticas gerenciadas e em linha anexadas a sua identidade de usuário. Essa política inclui permissões para concluir essa ação no console ou programaticamente usando a API AWS CLI ou AWS .

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
```

```
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Usar funções vinculadas a serviços

AWS Support e AWS Trusted Advisor use funções vinculadas ao serviço AWS Identity and Access Management (IAM). Uma função vinculada ao serviço é uma função exclusiva do IAM vinculada diretamente a e. AWS Support Trusted Advisor Em cada caso, a função vinculada ao serviço é uma função predefinida. Essa função inclui todas as permissões necessárias AWS Support ou Trusted Advisor necessárias para ligar para outros AWS serviços em seu nome. Os tópicos a seguir explicam o que as funções vinculadas a serviços fazem e como trabalhar com elas em e. AWS Support Trusted Advisor

Tópicos

- Usar perfis vinculados ao serviço do AWS Support
- Usar perfis vinculados ao serviço do Trusted Advisor

Usar perfis vinculados ao serviço do AWS Support

AWS Support as ferramentas coletam informações sobre seus AWS recursos por meio de chamadas de API para fornecer atendimento ao cliente e suporte técnico. Para aumentar a transparência e a auditabilidade das atividades de suporte, AWS Support usa uma função vinculada ao serviço AWS Identity and Access Management (IAM).

A função `AWSServiceRoleForSupport` vinculada ao serviço é uma função exclusiva do IAM vinculada diretamente a. AWS Support Essa função vinculada ao serviço é predefinida e inclui as permissões AWS Support necessárias para chamar outros AWS serviços em seu nome.

A função vinculada ao serviço `AWSServiceRoleForSupport` confia no serviço `support.amazonaws.com` para presumir a função.

Para fornecer esses serviços, as permissões predefinidas da função dão AWS Support acesso aos metadados do recurso, não aos dados do cliente. Somente AWS Support ferramentas podem assumir essa função, que existe na sua AWS conta.

Editamos os campos que podem conter dados do cliente. Por exemplo, os `Output` campos `Input` e do GetExecutionHistorypara a chamada de AWS Step Functions API não estão visíveis para AWS Support. Nós usamos AWS KMS keys para criptografar campos confidenciais. Esses campos são editados na resposta da API e não são visíveis para AWS Support os agentes.

> **Note**
>
> AWS Trusted Advisor usa uma função separada vinculada ao serviço do IAM para acessar AWS recursos da sua conta e fornecer recomendações e verificações de melhores práticas. Para ter mais informações, consulte Usar perfis vinculados ao serviço do Trusted Advisor.

A função `AWSServiceRoleForSupport` vinculada ao serviço permite que todas as chamadas de AWS Support API sejam visíveis para os clientes por meio de. AWS CloudTrail Isso ajuda nos requisitos de monitoramento e auditoria, pois fornece uma maneira transparente de entender as ações que são AWS Support executadas em seu nome. Para obter informações sobre CloudTrail, consulte o Guia AWS CloudTrail do usuário.

Permissões de função vinculada ao serviço AWS Support

Essa função usa a política `AWSSupportServiceRolePolicy` AWS gerenciada. Essa política gerenciada é anexada à função e permite à permissão da função realizar ações em seu nome.

Essas ações incluem o seguinte:

- Cobrança, serviços administrativos, de suporte e outros serviços AWS ao cliente — o atendimento ao cliente usa as permissões concedidas pela política gerenciada para realizar vários serviços como parte do seu plano de suporte. Isso inclui investigar e responder a perguntas sobre contas e cobrança, fornecendo apoio administrativo para a sua conta, aumentando as cotas de serviço e oferecendo suporte adicional ao cliente.
- Processamento de atributos de serviço e dados de uso da sua AWS conta — AWS Support pode usar as permissões concedidas pela política gerenciada para acessar os atributos do serviço e os dados de uso AWS da sua conta. Essa política permite AWS Support fornecer suporte técnico, administrativo e de cobrança para sua conta. Atributos de serviço incluem seus identificadores de recurso de conta, tags de metadados, funções e permissões. Os dados de uso incluem o uso de políticas, estatísticas e análises.
- Manter a integridade operacional de sua conta e de seus recursos — AWS Support usa ferramentas automatizadas para realizar ações relacionadas ao suporte operacional e técnico.

Para obter mais informações sobre os serviços e ações permitidos, consulte a AWSSupportServiceRolePolicy no console do IAM.

> **Note**
>
> AWS Support atualiza automaticamente a `AWSSupportServiceRolePolicy` política uma vez por mês para adicionar permissões para novos AWS serviços e ações.

Para ter mais informações, consulte AWS políticas gerenciadas para AWS Support.

Criação de uma função vinculada ao serviço para AWS Support

Você não precisa criar manualmente a função `AWSServiceRoleForSupport`. Quando você cria uma AWS conta, essa função é criada e configurada automaticamente para você.

> **Important**
>
> Se você usou AWS Support antes de começar a oferecer suporte a funções vinculadas a serviços, então AWS criou a `AWSServiceRoleForSupport` função em sua conta. Para obter mais informações, consulte Uma nova função apareceu na minha conta do IAM.

Editando e excluindo uma função vinculada ao serviço para AWS Support

É possível usar o IAM para editar a descrição da função vinculada ao serviço `AWSServiceRoleForSupport`. Para ter mais informações, consulte Editar um perfil vinculado ao serviço no Guia do usuário do IAM.

A `AWSServiceRoleForSupport` função é necessária AWS Support para fornecer suporte administrativo, operacional e técnico para sua conta. Como resultado, essa função não pode ser excluída por meio do console do IAM, da API ou AWS Command Line Interface (AWS CLI). Isso protege sua conta da AWS pois você não consegue remover por engano as permissões necessárias para serviços de suporte de administração.

Para obter mais informações sobre a função `AWSServiceRoleForSupport` ou seus usuários, entre em contato com o AWS Support.

Usar perfis vinculados ao serviço do Trusted Advisor

AWS Trusted Advisor usa a função vinculada ao serviço AWS Identity and Access Management (IAM). Uma função vinculada ao serviço é uma função exclusiva do IAM vinculada diretamente a. AWS Trusted Advisor As funções vinculadas ao serviço são predefinidas por Trusted Advisor, e incluem todas as permissões que o serviço exige para chamar outros AWS serviços em seu nome. Trusted Advisor usa essa função para verificar seu uso AWS e fornecer recomendações para melhorar seu AWS ambiente. Por exemplo, Trusted Advisor analisa o uso da instância do Amazon Elastic Compute Cloud (Amazon EC2) para ajudá-lo a reduzir custos, aumentar o desempenho, tolerar falhas e melhorar a segurança.

> **Note**
>
> AWS Support usa uma função separada vinculada ao serviço do IAM para acessar os recursos da sua conta e fornecer serviços administrativos, de faturamento e de suporte. Para obter mais informações, consulte Usar perfis vinculados ao serviço do AWS Support.

Para obter informações sobre outros produtos que oferecem suporte a funções vinculadas aos serviços, consulte Produtos da AWS que funcionam com o IAM. Procure os serviços que têm Yes (Sim) na coluna Função vinculada ao serviço. Escolha um Sim com um link para visualizar a documentação da função vinculada a esse serviço.

Tópicos

- Permissões de função vinculada ao serviço Trusted Advisor
- Gerenciar permissões para funções vinculadas ao serviço
- Crie uma função vinculada ao serviço para o Trusted Advisor
- Editar uma função vinculada ao serviço para o Trusted Advisor
- Excluir uma função vinculada ao serviço para o Trusted Advisor

Permissões de função vinculada ao serviço Trusted Advisor

Trusted Advisor usa duas funções vinculadas ao serviço:

- AWSServiceRoleForTrustedAdvisor— Essa função confia no Trusted Advisor serviço para assumir a função de acessar AWS os serviços em seu nome. A política de permissões de função permite acesso Trusted Advisor somente de leitura a todos AWS os recursos. Essa função simplifica o início da sua AWS conta, pois você não precisa adicionar as permissões necessárias para o. Trusted Advisor Quando você abre uma AWS conta, Trusted Advisor cria essa função para você. As permissões definidas incluem a política de confiança e a política de permissões. Não é possível anexar a política de permissões a nenhuma outra entidade do IAM.

  Para obter mais informações sobre a política anexada, consulte AWSTrustedAdvisorServiceRolePolicy.
- AWSServiceRoleForTrustedAdvisorReporting - Essa função confia no Trusted Advisor para assumir a função para o recurso de visualização organizacional. Essa função é ativada Trusted Advisor como um serviço confiável em sua AWS Organizations organização. Trusted Advisor cria essa função para você quando você ativa a visualização organizacional.

  Para obter mais informações sobre a política anexada, consulte AWSTrustedAdvisorReportingServiceRolePolicy.

  Você pode usar a visualização organizacional para criar relatórios para resultados de Trusted Advisor verificação de todas as contas em sua organização. Para obter mais informações sobre esse recurso, consulte Visualização organizacional para AWS Trusted Advisor.

Gerenciar permissões para funções vinculadas ao serviço

Você deve configurar permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua uma função vinculada a serviço. Os exemplos a seguir usam a função vinculada ao serviço do `AWSServiceRoleForTrustedAdvisor`.

Example : Permitir que uma entidade do IAM crie a função vinculada ao serviço do **`AWSServiceRoleForTrustedAdvisor`**

Essa etapa é necessária somente se a Trusted Advisor conta estiver desativada, a função vinculada ao serviço for excluída e o usuário precisar recriar a função para reativá-la. Trusted Advisor

É possível adicionar a instrução a seguir à política de permissões para que a entidade do IAM crie a função vinculada ao serviço.

```
{
    "Effect": "Allow",
    "Action": [
        "iam:CreateServiceLinkedRole",
        "iam:PutRolePolicy"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/trustedadvisor.amazonaws.com/
AWSServiceRoleForTrustedAdvisor*",
    "Condition": {"StringLike": {"iam:AWSServiceName": "trustedadvisor.amazonaws.com"}}
}
```

Example : Permitir que uma entidade do IAM edite a descrição da função vinculada ao serviço **`AWSServiceRoleForTrustedAdvisor`**

Você só pode editar a descrição da função do `AWSServiceRoleForTrustedAdvisor`. É possível adicionar a instrução a seguir à política de permissões para que a entidade do IAM edite a descrição de uma função vinculada ao serviço.

```
{
    "Effect": "Allow",
    "Action": [
        "iam:UpdateRoleDescription"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/trustedadvisor.amazonaws.com/
AWSServiceRoleForTrustedAdvisor*",
    "Condition": {"StringLike": {"iam:AWSServiceName": "trustedadvisor.amazonaws.com"}}
}
```

Example : Permitir que uma entidade do IAM exclua a função vinculada ao serviço **`AWSServiceRoleForTrustedAdvisor`**

É possível adicionar a instrução a seguir à política de permissões para que a entidade do IAM exclua uma função vinculada ao serviço.

```
{
    "Effect": "Allow",
    "Action": [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/trustedadvisor.amazonaws.com/
AWSServiceRoleForTrustedAdvisor*",
    "Condition": {"StringLike": {"iam:AWSServiceName": "trustedadvisor.amazonaws.com"}}
}
```

Você também pode usar uma política AWS gerenciada AdministratorAccess, como, para fornecer acesso total Trusted Advisor a.

Crie uma função vinculada ao serviço para o Trusted Advisor

Você não precisa criar manualmente a função vinculada a serviço `AWSServiceRoleForTrustedAdvisor`. Quando você abre uma AWS conta, Trusted Advisor cria a função vinculada ao serviço para você.

> **Important**
>
> Se você estava usando o Trusted Advisor serviço antes de ele começar a oferecer suporte a funções vinculadas ao serviço, então Trusted Advisor já criou a `AWSServiceRoleForTrustedAdvisor` função em sua conta. Para saber mais, consulte Uma nova função apareceu na minha conta do IAM no Manual do usuário do IAM.

Se a sua conta não tiver nenhuma função vinculada ao serviço `AWSServiceRoleForTrustedAdvisor`, o Trusted Advisor não funcionará como esperado. Isso pode acontecer se alguém desabilitar sua conta do Trusted Advisor e, em seguida, excluir a função vinculada ao serviço. Nesse caso, é possível usar o IAM para criar a função vinculada ao serviço `AWSServiceRoleForTrustedAdvisor` e, em seguida, habilitar o Trusted Advisor de novo.

Para ativar Trusted Advisor (console)

1. Use o console do IAM ou AWS CLI a API do IAM para criar uma função vinculada ao serviço para. Trusted Advisor Para obter mais informações, consulte Criar uma função vinculada ao serviço.

2. Faça login no e AWS Management Console, em seguida, navegue até o Trusted Advisor console emhttps://console.aws.amazon.com/trustedadvisor.

   O banner de status Disabled Trusted Advisor (Trusted Advisor desabilitado) é exibido no console.
3. Escolha Ativar Trusted Advisor função no banner de status. Se o `AWSServiceRoleForTrustedAdvisor` não for detectado, o banner de status desabilitado permanecerá.

Editar uma função vinculada ao serviço para o Trusted Advisor

Não é possível alterar o nome da função, pois várias entidades podem fazer referência a ela. No entanto, você pode usar o console do IAM ou a API do IAM para editar a descrição da função. AWS CLI Para obter mais informações, consulte Editar uma função vinculada a serviço no Guia do usuário do IAM.

Excluir uma função vinculada ao serviço para o Trusted Advisor

Se você não precisar usar os recursos ou serviços do Trusted Advisor, você pode excluir a `AWSServiceRoleForTrustedAdvisor` função. Você deve desabilitar Trusted Advisor antes de excluir essa função vinculada ao serviço. Isso evita que você remova permissões necessárias pelas operações do Trusted Advisor . Ao desativar Trusted Advisor, você desativa todos os recursos do serviço, incluindo o processamento e as notificações off-line. Além disso, se você desativar Trusted Advisor a conta de um membro, a conta de pagante separada também será afetada, o que significa que você não receberá Trusted Advisor cheques que identifiquem formas de economizar custos. Não é possível acessar o console do Trusted Advisor . Chamadas de API para Trusted Advisor retornar um erro de acesso negado.

Você deve recriar a função `AWSServiceRoleForTrustedAdvisor` vinculada à conta antes de habilitar novamente o Trusted Advisor.

Você deve primeiro desabilitar Trusted Advisor no console antes de excluir a função `AWSServiceRoleForTrustedAdvisor` vinculada ao serviço.

Para desativar Trusted Advisor

1. Faça login no AWS Management Console e navegue até o Trusted Advisor console emhttps://console.aws.amazon.com/trustedadvisor.
2. No painel de navegação, escolha Preferences.

3. Na seção Service Linked Role Permissions (Permissões de função vinculada ao serviço), escolha Disable Trusted Advisor (Desativar &SERVICENAME;).
4. Na caixa de diálogo de confirmação, confirme se você deseja desabilitar o , escolhendo OK Trusted Advisor.

Depois que você desabilitar Trusted Advisor, todas as Trusted Advisor funcionalidades serão desativadas e o Trusted Advisor console exibirá somente o banner de status desativado.

Em seguida, você pode usar o console do IAM AWS CLI, o ou a API do IAM para excluir a função Trusted Advisor vinculada ao serviço chamada. `AWSServiceRoleForTrustedAdvisor` Para obter mais informações, consulte Excluir um perfil vinculado ao serviço no Guia do usuário do IAM.

AWS políticas gerenciadas para AWS Support

Uma política AWS gerenciada é uma política autônoma criada e administrada por AWS. AWS as políticas gerenciadas são projetadas para fornecer permissões para muitos casos de uso comuns, para que você possa começar a atribuir permissões a usuários, grupos e funções.

Lembre-se de que as políticas AWS gerenciadas podem não conceder permissões de privilégio mínimo para seus casos de uso específicos porque elas estão disponíveis para uso de todos os AWS clientes. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo cliente específicas para seus casos de uso.

Você não pode alterar as permissões definidas nas políticas AWS gerenciadas. Se AWS atualizar as permissões definidas em uma política AWS gerenciada, a atualização afetará todas as identidades principais (usuários, grupos e funções) às quais a política está anexada. AWS é mais provável que atualize uma política AWS gerenciada quando uma nova AWS service (Serviço da AWS) for lançada ou novas operações de API forem disponibilizadas para serviços existentes.

Para mais informações, consulte Políticas gerenciadas pela AWS no Manual do usuário do IAM.

Tópicos

- AWS políticas gerenciadas para AWS Support
- AWS políticas gerenciadas para AWS Support aplicativos no Slack
- AWS políticas gerenciadas para AWS Trusted Advisor
- AWS políticas gerenciadas para AWS Support planos

AWS políticas gerenciadas para AWS Support

AWS Support tem as seguintes políticas gerenciadas.

Sumário

- AWS política gerenciada: AWSSupportServiceRolePolicy
- AWS Support atualizações nas políticas AWS gerenciadas
- Alterações de permissão do AWSSupportServiceRolePolicy

AWS política gerenciada: AWSSupportServiceRolePolicy

AWS Support usa a política AWSSupportServiceRolePolicy AWS gerenciada. Essa política gerenciada é anexada à função vinculada ao serviço do `AWSServiceRoleForSupport`. A política permite que a função vinculada ao serviço realize ações em seu nome. Não é possível anexar essa política a suas entidades do IAM. Para obter mais informações, consulte Permissões de função vinculada ao serviço AWS Support.

Para obter uma lista de alterações na política, consulte AWS Support atualizações nas políticas AWS gerenciadas e Alterações de permissão do AWSSupportServiceRolePolicy.

AWS Support atualizações nas políticas AWS gerenciadas

Veja detalhes sobre as atualizações das políticas AWS gerenciadas AWS Support desde que esses serviços começaram a rastrear essas alterações. Para obter alertas automáticos sobre alterações feitas nesta página, inscreva-se no feed RSS na página Histórico do documento.

A tabela a seguir descreve atualizações importantes nas políticas AWS Support gerenciadas desde 17 de fevereiro de 2022.

AWS Support

Alteração	Descrição	Data
AWSSupportServiceRolePolicy: atualizar para uma política existente	Foram adicionadas 17 novas permissões aos seguintes serviços para realizar ações	22 de março de 2024

Alteração	Descrição	Data
	que ajudam a soluciona r problemas de clientes relacionados ao faturamen to, suporte administrativo e técnico: • Amazon CloudWatch Network Monitor — Para solucionar problemas relacionados ao serviço Network Monitor. • Amazon CloudWatch Logs — Para depurar problemas relacionados ao Amazon CloudWatch Logs. • Amazon Managed Streaming para Apache Kafka — Para depurar problemas relacionados ao Amazon Managed Streaming para Apache Kafka. • Amazon Managed Service para Prometheus — Para solucionar problemas relacionados ao Amazon Managed Service para Prometheus.	

Alteração	Descrição	Data
AWSSupportServiceRolePolicy: atualização para uma política existente	Foram adicionadas 63 novas permissões aos seguintes serviços para realizar ações que ajudem a solucionar problemas de clientes relacionados ao faturamento, suporte administrativo e técnico: • AWS Salas limpas — Para solucionar problemas relacionados às salas AWS limpas. • CodeConnections — Para solucionar problemas relacionados a. CodeConnections • Amazon EKS — Para depurar problemas relacionados ao Amazon EKS. • Image Builder — Para depurar problemas relacionados ao Image Builder. • Amazon Inspector2 — Para solucionar problemas relacionados ao Amazon Inspector2. • Amazon Inspector Scan — Para depurar problemas relacionados ao Amazon Inspector Scan.	17 de janeiro de 2024

Alteração	Descrição	Data
	• Amazon CloudWatch Logs — Para solucionar problemas relacionados ao Amazon CloudWatch Logs. • AWS Outposts — Para solucionar problemas relacionados ao AWS Outposts. • Amazon RDS: para depurar problemas relativos ao Amazon RDS. • AWS IAM Identity Center — Para solucionar problemas relacionados a. AWS IAM Identity Center • Amazon S3 Express — Para depurar problemas relacionados ao Amazon S3 Express. • AWS Trusted Advisor — Para solucionar problemas relacionados a. AWS Trusted Advisor	

Alteração	Descrição	Data
AWSSupportServiceRolePolicy: atualização para uma política existente	Foram adicionadas 126 novas permissões aos seguintes serviços para realizar ações que ajudam a solucionar problemas de clientes relacionados ao faturamento, suporte administrativo e técnico: • AWS Direct Connect — Para solucionar problemas relacionados ao AWS Direct Connect serviço. • Amazon SageMaker — Para solucionar problemas relacionados ao SageMaker serviço da Amazon. • Amazon AppStream — Para depurar problemas relacionados à Amazon AppStream. • Explorador de recursos da AWS — Para depurar problemas relacionados ao Explorador de recursos da AWS. • Amazon Redshift serverless — Para solucionar problemas relacionados ao Amazon Redshift serverless. • Amazon ElastiCache — Para depurar problemas	6 de dez de 2023

Alteração	Descrição	Data
	relacionados à Amazon ElastiCache. • Amazon Comprehend: para solucionar problemas relacionados ao Amazon Comprehend. • Amazon EC2 — Para solucionar problemas relacionados ao Amazon EC2. • Amazon Elastic Kubernetes Service — Para depurar problemas relacionados ao Amazon Elastic Kubernetes Service. • AWS Elastic Disaster Recovery — Para solucionar problemas relacionados a. AWS Elastic Disaster Recovery • AWS AppSync — Para depurar problemas relacionados a. AWS AppSync • Amazon CloudWatch Logs — Para solucionar problemas relacionados ao Amazon CloudWatch Logs. • AWS Health — Para depurar problemas relacionados ao AWS Health Serviço.	

Alteração	Descrição	Data
	• Amazon Connect — Para depurar problemas relacionados ao Amazon Connect. • AWS Snowball — Para solucionar problemas relacionados a. AWS Snowball • AWS Health Criação de imagens — Para solucionar problemas relacionados à AWS Health geração de imagens.	

Alteração	Descrição	Data
AWSSupportServiceRolePolicy: atualização para uma política existente	Adição de 163 novas permissões aos seguintes serviços para a execução de ações que ajudam a solucionar problemas do cliente relacionados a suporte técnico, administrativo e faturamento: • Amazon CloudFront — Para solucionar problemas relacionados ao CloudFront serviço. • Amazon EC2: para solucionar problemas relativos ao serviço do Amazon EC2. • Amazon AppStream — Para depurar problemas relacionados à Amazon AppStream. • AWS WAF — Para depurar problemas relacionados ao AWS Web Application Firewall. • Amazon Connect: para solucionar problemas relativos ao Amazon Connect. • AWS IoT — Para depurar problemas relacionados ao AWS IoT. • Amazon Route 53: para solucionar problemas	27 de outubro de 2023

Alteração	Descrição	Data
	relativos ao Amazon Route 53. • AWS Acesso verificado — Para solucionar problemas relacionados ao serviço de acesso AWS verificado. • Amazon Simple Email Service: para depurar problemas relativos ao Amazon Simple Email Service. • AWS Elastic Beanstalk — Para solucionar problemas relacionados a. AWS Elastic Beanstalk • Amazon DynamoDB: para depurar problemas relativos ao Amazon DynamoDB. • AWS EC2 Image Builder — Para solucionar problemas relacionados ao EC2 Image AWS Builder. • AWS Outposts — Para depurar problemas relacionados ao AWS Outposts Serviço. • AWS Glue — Para depurar problemas relacionados ao AWS Glue. • AWS Directory Service — Para solucionar problemas relacionados a. AWS Directory Service	

Alteração	Descrição	Data
	• AWS Elastic Disaster Recovery — Para solucionar problemas relacionados a. AWS Elastic Disaster Recovery • AWS Step Functions — Para depurar problemas relacionados a. AWS Step Functions • Amazon EMR: para solucionar problemas relativos ao Amazon EMR. • Amazon Relational Database Service: para solucionar problemas relativos ao Amazon Relational Database Service. • Amazon EC2 Systems Manager: para depurar problemas relativos ao Amazon EC2 Systems Manager.	

Alteração	Descrição	Data
AWSSupportServiceRolePolicy: atualização para uma política existente	Adição de 176 novas permissões aos seguintes serviços para a execução de ações que ajudam a solucionar problemas do cliente relacionados a suporte técnico, administrativo e faturamento: • AWS Glue — Para solucionar problemas relacionados ao serviço AWS Glue • Amazon EMR: para solucionar problemas relativos ao serviço do Amazon EMR. • Amazon Security Lake: para depurar problemas relativos ao Amazon Security Lake. • AWS Systems Manager — Para depurar problemas relacionados ao serviço Systems Manager. • Amazon Verified Permissions: para solucionar problemas relativos às Amazon Verified Permissions. • AWS IAM Access Analyzer — Para depurar problemas relacionados ao serviço IAM Access Analyzer.	28 de agosto de 2023

Alteração	Descrição	Data
	• AWS Backup — Para solucionar problemas relacionados a. AWS Backup • AWS Database Migration Service — Para solucionar problemas relacionados ao serviço DMS. • Amazon DynamoDB: para depurar problemas relativos ao Dynamo DB. • Amazon Elastic Container Registry (Amazon ECR): para solucionar problemas relativos ao Amazon Elastic Container Registry (Amazon ECR). • Amazon Elastic Container Service: para depurar problemas relativos ao Amazon Elastic Container Service. • Amazon Elastic Kubernetes Service: para solucionar problemas relativos ao Amazon Elastic Kubernetes Service. • Amazon EMR Sem Servidor: para depurar problemas relativos ao serviço do Amazon EMR Sem servidor.	

Alteração	Descrição	Data
	• AWS Identity and Access Management — Para solucionar problemas relacionados a. AWS Identity and Access Management • AWS Firewall de Rede — Para solucionar problemas relacionados ao Firewall AWS de Rede. • AWS HealthOmics — Para depurar problemas relacionados a. AWS HealthOmics • Amazon QuickSight — Para depurar problemas relacionados à Amazon QuickSight. • Amazon Relational Database Service: para solucionar problemas relativos ao Amazon Relational Database Service. • Amazon Redshift: para solucionar problemas relativos ao Amazon Redshift. • Amazon Redshift sem servidor: para depurar problemas relativos ao Amazon Redshift sem servidor.	

Alteração	Descrição	Data
	• Amazon SageMaker — Para depurar problemas relacionados à Amazon SageMaker.	

Alteração	Descrição	Data
AWSSupportServiceRolePolicy: atualização para uma política existente	Adição de 141 novas permissões aos seguintes serviços para a execução de ações que ajudam a solucionar problemas do cliente relacionados a suporte técnico, administrativo e faturamento: • Lambda: para solucionar problemas relativos ao serviço do Lambda. • Amazon Lex: para solucionar problemas relativos ao serviço do Amazon Lex. • AWS Transferência — Para depurar problemas relacionados ao serviço de transferência. • AWS Amplify — Para depurar problemas relacionados ao serviço Amplify. • Amazon EventBridge Pipes — Para solucionar problemas de permissões e cobrança relacionados ao Pipes. • Amazon EventBridge — Para depurar problemas relacionados à Amazon EventBridge • Amazon CloudWatch Logs — Para solucionar	26 de junho de 2023

Alteração	Descrição	Data
	problemas relacionados ao Amazon CloudWatch Logs. • AWS Systems Manager — Para solucionar problemas relacionados ao Systems Manager. • Amazon CloudWatch — Para depurar problemas relacionados a. CloudWatch • Amazon ElastiCache — Para solucionar problemas relacionados à Amazon ElastiCache. • Amazon Athena: para depurar problemas relativos ao Athena. • AWS Elastic Disaster Recovery — Para soluciona r problemas relacionados ao Elastic Disaster Recovery. • Amazon CloudWatc h — Para solucionar problemas de configuração da Amazon. CloudWatch • Amazon EC2: para depurar problemas relativos ao serviço do EC2. • AWS Certificate Manager — Para solucionar problemas relacionados ao Certificate Manager. • Amazon EventBridge Scheduler — Para soluciona	

Alteração	Descrição	Data
	r problemas relacionados ao EventBridge Scheduler. • Amazon OpenSearch Service — Para solucionar problemas relacionados a. OpenSearch • Amazon EventBridge Schemas — Para depurar problemas relacionados a EventBridge esquemas. • AWS Notificações do usuário — Para solucionar problemas relacionados às notificações do usuário. • Amazon CloudWatch Application Insights — Para solucionar problemas relacionados ao CloudWatch Application Insights. • Amazon DynamoDB: para solucionar problemas relativos ao DynamoDB. • Clusters elásticos do Amazon DocumentDB: para solucionar problemas relativos aos clusters elásticos do Amazon DocumentDB.	

Alteração	Descrição	Data
AWSSupportServiceRolePolicy: atualização para uma política existente	Adição de 53 novas permissões aos seguintes serviços para a execução de ações que ajudam a solucionar problemas do cliente referentes a suporte técnico, administrativo e faturamento: • Ajuste de escala automático: para solucionar problemas relativos ao serviço de ajuste de escala automático. • Amazon CloudWatch — Para solucionar problemas relacionados à Amazon CloudWatch. • AWS Compute Optimizer — Para solucionar problemas relacionados ao Compute Optimizer. • Amazon CloudWatch Evidently — Para solucionar problemas relacionados ao Evidently. • EC2 Image Builder: para solucionar problemas relativos ao serviço do Image Builder. • AWS IoT TwinMaker — Para solucionar problemas relacionados a. AWS IoT TwinMaker	2 de maio de 2023

Alteração	Descrição	Data
	• Amazon CloudWatch Logs — Para solucionar problemas relacionados ao Amazon CloudWatch Logs. • Amazon Pinpoint: para solucionar problemas relacionados ao Amazon Pinpoint. • AWS Link do OAM — Para depurar problemas relacionados aos recursos do OAM. • AWS Outposts — Para solucionar problemas relacionados a. AWS Outposts • Amazon RDS: para depurar problemas relativos ao Amazon RDS. • Explorador de recursos da AWS — Para solucionar problemas relacionados ao Resource Explorer. • Amazon CloudWatch RUM — Para solucionar problemas de configuração dos recursos do serviço RUM. • Amazon SNS: para solucionar problemas relativos ao Amazon SNS. • Amazon CloudWatc h Synthetics — Para	

Alteração	Descrição	Data
	solucionar problemas relacionados a Synthetics. CloudWatch	

Alteração	Descrição	Data
AWSSupportServiceRolePolicy: atualização para uma política existente	Adição de 52 novas permissões aos seguintes serviços para a execução de ações que ajudam a solucionar problemas do cliente relacionados a suporte técnico, administrativo e faturamento: • AWS Backup gateway — Para solucionar problemas relacionados ao gateway de Backup. • Amazon S3: para depurar problemas relativos ao Amazon S3. • AWS Application Migration Service — Para solucionar problemas relacionados ao Serviço de Migração de Aplicativos. • AWS Salas limpas — Para depurar problemas relacionados às salas AWS limpas; • AWS Systems Manager para SAP — Para solucionar problemas relacionados ao AWS Systems Manager SAP. • Amazon VPC Lattice: para depurar problemas relativos ao Amazon VPC Lattice.	16 de março de 2023

Alteração	Descrição	Data
AWSSupportServiceRolePolicy: atualização para uma política existente	Adição de 220 novas permissões aos seguintes serviços para a execução de ações que ajudam a solucionar problemas do cliente relacionados a suporte técnico, administrativo e de faturamento: • Amazon Athena — AWS Support Para permitir o desenvolvimento de ferramentas que possam ser usadas para ajudar os clientes com suas dúvidas relacionadas ao Athena. • Amazon Chime: para solucionar problemas relacionados ao Amazon Chime. • Amazon CloudWatch Internet Monitor — Para depurar problemas relacionados ao Internet Monitor. • Amazon Comprehend: para solucionar problemas relacionados ao Amazon Comprehend. • Amazon Elastic Compute Cloud: para depurar problemas relacionados ao Transit Gateway Connect e aos recursos de multicast.	10 de janeiro de 2023

Alteração	Descrição	Data
	• Amazon EventBridge Pipes — Para solucionar problemas relacionados ao EventBridge Pipes. • Amazon Interactive Video Service — Para permitir AWS Support a consulta de recursos do Amazon IVS para solucionar problemas de clientes. • Amazon FSx — Para permitir o desenvolvimento de ferramentas AWS Support para apoiar a importação e exportaçã o para um repositório de dados Amazon FSx. • Amazon GameLift — Para solucionar problemas relacionados à Amazon GameLift. • AWS Glue: para solucionar problemas relacionados ao AWS Glue Data Quality. • Amazon Kinesis Video Streams: para solucionar problemas relacionados ao Kinesis Video Streams. • Amazon Managed Service for Prometheus: para solucionar problemas relacionados ao Amazon Managed Service for Prometheus.	

Alteração	Descrição	Data
	• Amazon Managed Streaming for Apache Kafka: para solucionar problemas relacionados ao Amazon MSK Connect. • AWS Network Manager — Para solucionar problemas relacionados ao Network Manager. • Amazon Nimble Studio: para depurar problemas relacionados ao Nimble Studio. • Amazon Personalize: para depurar problemas relacionados ao Amazon Personalize. • Amazon Pinpoint: para solucionar problemas relacionados ao Amazon Pinpoint. • AWS HealthOmics — Para solucionar problemas relacionados a. HealthOmics • Amazon Transcribe: para depurar problemas relacionados ao Amazon Transcribe.	

Alteração	Descrição	Data
AWSSupportServiceRolePolicy: atualização para uma política existente	Adição de 47 novas permissões aos seguintes serviços para a execução de ações que ajudam a solucionar problemas do cliente relacionados a suporte técnico, administrativo e de faturamento: • AWS Application Migration Service — Para solucionar problemas de replicação e lançamento. • AWS CloudFormation ganchos — AWS Support Para permitir o desenvolvimento de ferramentas de automação que possam ajudar a resolver problemas. • Amazon Elastic Kubernetes Service: para solucionar problemas referentes ao Amazon EKS. • AWS IoT FleetWise: para solucionar problemas relativos ao AWS IoT FleetWise. • AWS Mainframe Modernization — Para depurar problemas relacionados à modernização do mainframe. • AWS Outposts — Para ajudar a AWS Support obter	4 de outubro de 2022

Alteração	Descrição	Data
	uma lista de hosts e ativos dedicados. • AWS Private 5G: para solucionar problemas relativos ao Private 5G. • AWS Tiros: para depurar problemas relacionados ao Tiros.	

Alteração	Descrição	Data
AWSSupportServiceRolePolicy: atualização para uma política existente	Adição de 46 novas permissões aos seguintes serviços para a execução de ações que ajudam a solucionar problemas do cliente relacionados a suporte técnico, administrativo e de faturamento: • Amazon Managed Streaming for Apache Kafka: para solucionar problemas referentes ao Amazon MSK. • AWS DataSync — Para solucionar problemas relacionados a. DataSync • AWS Elastic Disaster Recovery — Para solucionar problemas de replicação e lançamento. • Amazon GameSparks — Para solucionar problemas relacionados a. GameSparks • AWS IoT TwinMaker — Para depurar problemas relacionados a. AWS IoT TwinMaker • AWS Lambda — Para visualizar a configuração de um URL de função para solucionar problemas.	17 de agosto de 2022

Alteração	Descrição	Data
	• Amazon Lookout for Equipment: para solucionar problemas referentes ao Lookout for Equipment. • Amazon Route 53 e Amazon Route 53 Resolver — Para obter configurações de resolvedor que AWS Support possam verificar o comportamento da resolução de DNS de uma VPC.	

Alteração	Descrição	Data
AWSSupportServiceRolePolicy: atualização para uma política existente	Adição de novas permissões aos seguintes serviços para a execução de ações que ajudam a solucionar problemas do cliente relacionados a suporte técnico, administrativo e de faturamento: • Amazon CloudWatch Logs — Para ajudar a solucionar problemas relacionados aos CloudWatch registros. • Amazon Interactive Video Service — Para ajudar a AWS Support verificar os recursos existentes do Amazon IVS para casos de suporte relacionados a fraudes ou contas comprometidas. • Amazon Inspector: para solucionar problemas relacionados ao Amazon Inspector. Permissões removidas para serviços, como a Amazon WorkLink. A Amazon WorkLink foi descontinuada em 19 de abril de 2022.	23 de junho de 2022

Alteração	Descrição	Data
AWSSupportServiceRolePolicy: atualização para uma política existente	Adição de 25 novas permissões aos seguintes serviços para a execução de ações que ajudam a solucionar problemas do cliente relacionados a suporte técnico, administrativo e de faturamento: • AWS Amplify UI Builder — Para solucionar problemas relacionados à geração de componentes e temas. • Amazon AppStream — Para solucionar problemas recuperando recursos para recursos lançados recentemente. • AWS Backup — Para solucionar problemas relacionados às tarefas de backup. • AWS CloudFormation — Para realizar diagnósticos sobre problemas relacionados ao IAM, extensão e controle de versão. • Amazon Kinesis: para solucionar problemas relacionados ao Kinesis. • AWS Transfer Family — Para solucionar problemas	27 de abril de 2022

Alteração	Descrição	Data
	relacionados ao Transfer Family.	

Alteração	Descrição	Data

AWSSupportServiceRolePolicy: atualização para uma política existente	Adição de 54 novas permissões aos seguintes serviços para executar ações que ajudam a solucionar problemas do cliente relacionados ao suporte técnico, administrativo e de faturamento:
	• Amazon Elastic Compute Cloud
	  • Solucionar problemas relacionados ao cliente e listas prefixadas gerenciadas pela AWS.
	  • Solucionar problemas referentes ao Gerenciador de endereços IP da Amazon VPC (IPAM).
	• AWS Network Manager — Para solucionar problemas relacionados ao Network Manager.
	• Savings Plans – Obter metadados sobre compromissos pendentes de Savings Plans.
	• AWS Serverless Application Repository — Melhorar e apoiar as ações de resposta como parte da pesquisa e resolução de casos de suporte.
	• Amazon WorkSpaces Web — Para depurar e soluciona
		14 de março de 2022

Alteração	Descrição	Data
	r problemas com serviços WorkSpaces da Web.	

Alteração	Descrição	Data
AWSSupportServiceRolePolicy: atualização para uma política existente	Adição de 74 novas permissões aos seguintes serviços para executar ações que ajudam a solucionar problemas do cliente relacionados ao suporte técnico, administrativo e de faturamento: • AWS Application Migration Service — Para oferecer suporte à replicação sem agente no Serviço de Migração de Aplicativos. • AWS CloudFormation — Para realizar diagnósticos sobre problemas relacionados ao IAM, à extensão e ao controle de versão. • Amazon CloudWatch Logs — Para validar políticas de recursos. • Lixeira do Amazon EC2: para obter metadados sobre as regras de retenção da lixeira. • AWS Elastic Disaster Recovery — Solucionar problemas de replicação e lançamento nas contas dos clientes. • Amazon FSx: para visualizar a descrição dos snapshots do Amazon FSx.	17 de fevereiro de 2022

Alteração	Descrição	Data
	• Amazon Lightsail: para visualizar detalhes de metadados e configurações para buckets do Lightsail. • Amazon Macie: para visualizar configurações do Macie, como trabalhos de classificação, identificadores de dados personalizados, expressões regulares e descobertas. • Amazon S3: para coletar metadados e configurações para buckets do Amazon S3. • AWS Storage Gateway — Visualizar metadados sobre as políticas de criação automática de fitas dos clientes. • Balanceamento de carga elástico: para exibir a descrição dos limites de recursos ao usar o console do Service Quotas. Para obter mais informaçõ es, consulte Alterações de permissão do AWSSupport ServiceRolePolicy.	
Publicação do log de alteraçõe s	Registro de alterações das políticas AWS Support gerenciadas.	17 de fevereiro de 2022

Alterações de permissão do AWSSupportServiceRolePolicy

A maioria das permissões foi adicionada AWS Support para `AWSSupportServiceRolePolicy` permitir a chamada de uma operação de API com o mesmo nome. No entanto, algumas operações de API exigem permissões com um nome diferente.

A tabela a seguir lista somente as operações de API que exigem permissões com um nome diferente. Esta tabela descreve essas diferenças a partir de 17 de fevereiro de 2022.

Data	Nome da operação da API	Permissões do IAM necessárias
Adição de permissões em 17 de fevereiro de 2022	`s3.GetBucketAnalyticsConfiguration` `s3.ListBucketAnalyticsConfiguration`	`s3:GetAnalyticsConfiguration`
	`s3.GetBucketNotificationConfiguration`	`s3:GetBucketNotification`
	`s3.GetBucketEncryption`	`s3:GetEncryptionConfiguration`
	`s3.GetBucketIntelligentTieringConfiguration` `s3.ListBucketIntelligentTieringConfiguration`	`s3:GetIntelligentTieringConfiguration`
	`s3.GetBucketInventoryConfiguration` `s3.ListBucketInventoryConfiguration`	`s3:GetInventoryConfiguration`
	`s3.GetBucketLifecycleConfiguration`	`s3:GetLifecycleConfiguration`

Data	Nome da operação da API	Permissões do IAM necessári as
	s3.GetBucketMetric sConfiguration s3.ListBucketMetri csConfiguration	s3:GetMetricsConfi guration
	s3.GetBucketReplic ation	s3:GetReplicationC onfiguration
	s3.HeadBucket s3.ListObjects	s3:ListBucket
	s3.ListBuckets	s3:ListAllMyBuckets
	s3.ListMultipartUp loads	s3:ListBucketMulti partUploads
	s3.ListObjectVersi ons	s3:ListBucketVersi ons
	s3.ListParts	s3:ListMultipartUp loadParts

AWS políticas gerenciadas para AWS Support aplicativos no Slack

> **Note**
>
> Para acessar e visualizar casos de suporte no AWS Support Center Console, consulteGerencie o acesso ao AWS Support Centro.

AWS Support O aplicativo tem as seguintes políticas gerenciadas.

Sumário

- AWS política gerenciada: AWSSupportAppFullAccess

- AWS política gerenciada: AWSSupportAppReadOnlyAccess
- AWS Support Atualizações de aplicativos para políticas AWS gerenciadas

AWS política gerenciada: AWSSupportAppFullAccess

Você pode usar a política gerenciada pelo AWSSupportAppFullAccess para conceder ao perfil do IAM as permissões para as configurações do seu canal do Slack. Também é possível anexar a política do AWSSupportAppFullAccess às suas entidades do IAM.

Para obter mais informações, consulte Aplicativo AWS Support no Slack.

Essa política concede permissões que permitem que a entidade execute AWS Support, Service Quotas e ações do IAM para o AWS Support aplicativo.

Detalhes de permissão

Esta política inclui as seguintes permissões:

- `servicequotas`: descreve suas cotas e solicitações de serviço existentes e cria aumentos de cotas de serviço para sua conta.
- `support`: cria, atualiza e resolve seus casos de suporte. Atualiza e descreve informações sobre seus casos, como anexos de arquivos, correspondências e níveis de gravidade. Inicia sessões de chat ao vivo com um atendente de suporte.
- `iam`: cria um perfil vinculado ao serviço para o Service Quotas.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "servicequotas:GetRequestedServiceQuotaChange",
                "servicequotas:GetServiceQuota",
                "servicequotas:RequestServiceQuotaIncrease",
```

```
                "support:AddAttachmentsToSet",
                "support:AddCommunicationToCase",
                "support:CreateCase",
                "support:DescribeCases",
                "support:DescribeCommunications",
                "support:DescribeSeverityLevels",
                "support:InitiateChatForCase",
                "support:ResolveCase"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {"iam:AWSServiceName": "servicequotas.amazonaws.com"}
            }
        }
    ]
}
```

Para obter mais informações, consulte Como gerenciar o acesso ao aplicativo AWS Support.

AWS política gerenciada: AWSSupportAppReadOnlyAccess

A AWSSupportAppReadOnlyAccesspolítica concede permissões que permitem que a entidade execute ações do AWS Support aplicativo somente para leitura. Para obter mais informações, consulte Aplicativo AWS Support no Slack.

Detalhes de permissão

Esta política inclui as seguintes permissões:

- `support`: descreve os detalhes do caso de suporte e as comunicações adicionadas aos casos de suporte.

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "support:DescribeCases",
                "support:DescribeCommunications"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS Support Atualizações de aplicativos para políticas AWS gerenciadas

Veja detalhes sobre as atualizações das políticas AWS gerenciadas do AWS Support App desde que esse serviço começou a rastrear essas alterações. Para obter alertas automáticos sobre alterações feitas nesta página, inscreva-se no feed RSS na página Histórico do documento.

A tabela a seguir descreve atualizações importantes nas políticas gerenciadas de AWS Support aplicativos desde 17 de agosto de 2022.

AWS Support Aplicativo

Alteração	Descrição	Data
AWSSupportAppFullAccesse AWSSupportAppReadOnlyAccess Novas políticas AWS gerenciadas para o AWS Support aplicativo	Você pode usar essas políticas para o perfil do IAM definido para a configuração do seu canal do Slack. Para obter mais informaçõ es, consulte Como gerenciar o acesso ao aplicativo AWS Support.	19 de agosto de 2022
Publicação do log de alteraçõe s	Registro de alterações das políticas gerenciadas pelo AWS Support aplicativo.	19 de agosto de 2022

AWS políticas gerenciadas para AWS Trusted Advisor

Trusted Advisor tem as seguintes políticas AWS gerenciadas.

Sumário

- AWS política gerenciada: AWSTrustedAdvisorPriorityFullAccess
- AWS política gerenciada: AWSTrustedAdvisorPriorityReadOnlyAccess
- Política gerenciada da AWS : AWSTrustedAdvisorServiceRolePolicy
- AWS política gerenciada: AWSTrustedAdvisorReportingServiceRolePolicy
- Atualizações do Trusted Advisor para políticas gerenciadas pela AWS

AWS política gerenciada: AWSTrustedAdvisorPriorityFullAccess

A AWSTrustedAdvisorPriorityFullAccesspolítica concede acesso total ao Trusted Advisor Priority. Essa política também permite que o usuário adicione Trusted Advisor como um serviço confiável AWS Organizations e especifique as contas de administrador delegado para o Trusted Advisor Priority.

Detalhes da permissão

Na primeira declaração, a política inclui as seguintes permissões para `trustedadvisor`:

- Descreve a sua conta e a sua organização.
- Descreve os riscos identificados pelo Trusted Advisor Priority. As permissões permitem que você baixe e atualize o status de risco.
- Descreve suas configurações para notificações Trusted Advisor prioritárias por e-mail. As permissões permitem que você configure as notificações por e-mail e as desative para os seus administradores delegados.
- Configura Trusted Advisor para que sua conta possa ser ativada AWS Organizations.

Na segunda declaração, a política inclui as seguintes permissões para `organizations`:

- Descreve sua Trusted Advisor conta e sua organização.
- Lista as Serviços da AWS que você habilitou para usar Organizations.

Na terceira declaração, a política inclui as seguintes permissões para `organizations`:

- Lista os administradores delegados para Trusted Advisor Prioridade.
- Ativa e desativa o acesso confiável com o Organizations.

Na quarta declaração, a política inclui as seguintes permissões para `iam`:

- Cria o perfil vinculado ao serviço `AWSServiceRoleForTrustedAdvisorReporting`.

Na quinta declaração, a política inclui as seguintes permissões para `organizations`:

- Permite que você registre e cancele o registro de administradores delegados para o Trusted Advisor Priority.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "AWSTrustedAdvisorPriorityFullAccess",
   "Effect": "Allow",
   "Action": [
    "trustedadvisor:DescribeAccount*",
    "trustedadvisor:DescribeOrganization",
    "trustedadvisor:DescribeRisk*",
    "trustedadvisor:DownloadRisk",
    "trustedadvisor:UpdateRiskStatus",
    "trustedadvisor:DescribeNotificationConfigurations",
    "trustedadvisor:UpdateNotificationConfigurations",
    "trustedadvisor:DeleteNotificationConfigurationForDelegatedAdmin",
    "trustedadvisor:SetOrganizationAccess"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AllowAccessForOrganization",
   "Effect": "Allow",
   "Action": [
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization",
    "organizations:ListAWSServiceAccessForOrganization"
   ],
   "Resource": "*"
```

```
  },
  {
   "Sid": "AllowListDelegatedAdministrators",
   "Effect": "Allow",
   "Action": [
    "organizations:ListDelegatedAdministrators",
    "organizations:EnableAWSServiceAccess",
    "organizations:DisableAWSServiceAccess"
   ],
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "organizations:ServicePrincipal": [
      "reporting.trustedadvisor.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "AllowCreateServiceLinkedRole",
   "Effect": "Allow",
   "Action": "iam:CreateServiceLinkedRole",
   "Resource": "arn:aws:iam::*:role/aws-service-role/
reporting.trustedadvisor.amazonaws.com/AWSServiceRoleForTrustedAdvisorReporting",
   "Condition": {
    "StringLike": {
     "iam:AWSServiceName": "reporting.trustedadvisor.amazonaws.com"
    }
   }
  },
  {
   "Sid": "AllowRegisterDelegatedAdministrators",
   "Effect": "Allow",
   "Action": [
    "organizations:RegisterDelegatedAdministrator",
    "organizations:DeregisterDelegatedAdministrator"
   ],
   "Resource": "arn:aws:organizations::*:*",
   "Condition": {
    "StringEquals": {
     "organizations:ServicePrincipal": [
      "reporting.trustedadvisor.amazonaws.com"
     ]
    }
```

```
    }
   }
  ]
}
```

AWS política gerenciada: AWSTrustedAdvisorPriorityReadOnlyAccess

A AWSTrustedAdvisorPriorityReadOnlyAccesspolítica concede permissões somente de leitura à Trusted Advisor Priority, incluindo permissão para visualizar as contas de administrador delegado.

Detalhes da permissão

Na primeira declaração, a política inclui as seguintes permissões para `trustedadvisor`:

- Descreve sua Trusted Advisor conta e sua organização.
- Descreve os riscos identificados pelo Trusted Advisor Priority e permite que você os baixe.
- Descreve as configurações das notificações Trusted Advisor prioritárias por e-mail.

Na segunda e terceira declarações, a política inclui as seguintes permissões para `organizations`:

- Descreve sua organização com o Organizations.
- Lista as Serviços da AWS que você habilitou para usar Organizations.
- Lista os administradores delegados para Priority Trusted Advisor

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "AWSTrustedAdvisorPriorityReadOnlyAccess",
   "Effect": "Allow",
   "Action": [
    "trustedadvisor:DescribeAccount*",
    "trustedadvisor:DescribeOrganization",
    "trustedadvisor:DescribeRisk*",
    "trustedadvisor:DownloadRisk",
    "trustedadvisor:DescribeNotificationConfigurations"
   ],
   "Resource": "*"
  },
  {
```

```
    "Sid": "AllowAccessForOrganization",
    "Effect": "Allow",
    "Action": [
     "organizations:DescribeOrganization",
     "organizations:ListAWSServiceAccessForOrganization"
    ],
    "Resource": "*"
   },
   {
    "Sid": "AllowListDelegatedAdministrators",
    "Effect": "Allow",
    "Action": [
     "organizations:ListDelegatedAdministrators"
    ],
    "Resource": "*",
    "Condition": {
     "StringEquals": {
      "organizations:ServicePrincipal": [
       "reporting.trustedadvisor.amazonaws.com"
      ]
     }
    }
   }
  ]
}
```

Política gerenciada da AWS : AWSTrustedAdvisorServiceRolePolicy

Esta política é anexada à função vinculada ao serviço `AWSServiceRoleForTrustedAdvisor`. Isso permite que o perfil vinculado ao serviço execute ações em seu nome. Não é possível anexar a política AWSTrustedAdvisorServiceRolePolicy às suas entidades do AWS Identity and Access Management (IAM). Para obter mais informações, consulte Usar perfis vinculados ao serviço do Trusted Advisor.

Essa política concede permissões administrativas que permitem que o perfil vinculado ao serviço acesse os Serviços da AWS. Essas permissões permitem que as verificações avaliem sua conta. Trusted Advisor

Detalhes das permissões

Esta política inclui as seguintes permissões:

- `Auto Scaling` - Descreve cotas e recursos da conta do Amazon EC2 Auto Scaling
- `cloudformation`— Descreve AWS CloudFormation (CloudFormation) cotas e pilhas de contas
- `cloudfront`— Descreve as CloudFront distribuições da Amazon
- `cloudtrail`— Descreve AWS CloudTrail (CloudTrail) trilhas
- `dynamodb` - Descreve cotas e recursos da conta do Amazon DynamoDB
- `ec2` - Descreve cotas e recursos da conta do Amazon Elastic Compute Cloud (Amazon EC2)
- `elasticloadbalancing`: descreve as cotas e recursos da conta do Elastic Load Balancing (ELB)
- `iam` - Obtém recursos do IAM, como credenciais, política de senha e certificados
- `kinesis` - Descreve cotas de contas do Amazon Kinesis (Kinesis)
- `rds` - Descrever recursos do Amazon Relational Database Service (Amazon RDS)
- `redshift` - Descreve os recursos do Amazon Redshift
- `route53` - Descreve cotas e recursos da conta do Amazon Route 53
- `s3` - Descreve recursos do Amazon Simple Storage Service (Amazon S3)
- `ses` - Faz o Amazon Simple Email Service (Amazon SES) enviar cotas
- `sqs` - Lista as filas do Amazon Simple Queue Service (Amazon SQS)
- `cloudwatch`— Obtém estatísticas métricas da Amazon CloudWatch CloudWatch Events (Events)
- `ce` - Obtém recomendações do Serviço Cost Explorer (Cost Explorer)
- `route53resolver`— Obtém endpoints e recursos do Amazon Route 53 Resolver Resolver
- `kafka`: obtém o Amazon Managed Streaming para os recursos do Apache Kafka
- `ecs`— Obtém recursos do Amazon ECS
- `outposts`— Obtém AWS Outposts recursos

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
```

```
                "autoscaling:DescribeAccountLimits",
                "autoscaling:DescribeAutoScalingGroups",
                "autoscaling:DescribeLaunchConfigurations",
                "ce:GetReservationPurchaseRecommendation",
                "ce:GetSavingsPlansPurchaseRecommendation",
                "cloudformation:DescribeAccountLimits",
                "cloudformation:DescribeStacks",
                "cloudformation:ListStacks",
                "cloudfront:ListDistributions",
                "cloudtrail:DescribeTrails",
                "cloudtrail:GetTrailStatus",
                "cloudtrail:GetTrail",
                "cloudtrail:ListTrails",
                "cloudtrail:GetEventSelectors",
                "cloudwatch:GetMetricStatistics",
                "dynamodb:DescribeLimits",
                "dynamodb:DescribeTable",
                "dynamodb:ListTables",
                "ec2:DescribeAddresses",
                "ec2:DescribeReservedInstances",
                "ec2:DescribeInstances",
                "ec2:DescribeVpcs",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeImages",
                "ec2:DescribeVolumes",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeRegions",
                "ec2:DescribeReservedInstancesOfferings",
                "ec2:DescribeSnapshots",
                "ec2:DescribeVpnConnections",
                "ec2:DescribeVpnGateways",
                "ec2:DescribeLaunchTemplateVersions",
                "ecs:DescribeTaskDefinition",
                "ecs:ListTaskDefinitions"
                "elasticloadbalancing:DescribeAccountLimits",
                "elasticloadbalancing:DescribeInstanceHealth",
                "elasticloadbalancing:DescribeLoadBalancerAttributes",
                "elasticloadbalancing:DescribeLoadBalancerPolicies",
                "elasticloadbalancing:DescribeLoadBalancerPolicyTypes",
                "elasticloadbalancing:DescribeLoadBalancers",
                "elasticloadbalancing:DescribeTargetGroups",
                "iam:GenerateCredentialReport",
                "iam:GetAccountPasswordPolicy",
```

```
                "iam:GetAccountSummary",
                "iam:GetCredentialReport",
                "iam:GetServerCertificate",
                "iam:ListServerCertificates",
                "kinesis:DescribeLimits",
                "kafka:ListClustersV2",
                "kafka:ListNodes",
                "outposts:GetOutpost",
                "outposts:ListAssets",
                "outposts:ListOutposts",
                "rds:DescribeAccountAttributes",
                "rds:DescribeDBClusters",
                "rds:DescribeDBEngineVersions",
                "rds:DescribeDBInstances",
                "rds:DescribeDBParameterGroups",
                "rds:DescribeDBParameters",
                "rds:DescribeDBSecurityGroups",
                "rds:DescribeDBSnapshots",
                "rds:DescribeDBSubnetGroups",
                "rds:DescribeEngineDefaultParameters",
                "rds:DescribeEvents",
                "rds:DescribeOptionGroupOptions",
                "rds:DescribeOptionGroups",
                "rds:DescribeOrderableDBInstanceOptions",
                "rds:DescribeReservedDBInstances",
                "rds:DescribeReservedDBInstancesOfferings",
                "rds:ListTagsForResource",
                "redshift:DescribeClusters",
                "redshift:DescribeReservedNodeOfferings",
                "redshift:DescribeReservedNodes",
                "route53:GetAccountLimit",
                "route53:GetHealthCheck",
                "route53:GetHostedZone",
                "route53:ListHealthChecks",
                "route53:ListHostedZones",
                "route53:ListHostedZonesByName",
                "route53:ListResourceRecordSets",
                "route53resolver:ListResolverEndpoints",
                "route53resolver:ListResolverEndpointIpAddresses",
                "s3:GetAccountPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketLocation",
```

```
                "s3:GetBucketLogging",
                "s3:GetBucketVersioning",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetLifecycleConfiguration",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "ses:GetSendQuota",
                "sqs:ListQueues"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS política gerenciada: AWSTrustedAdvisorReportingServiceRolePolicy

Essa política é anexada à função `AWSServiceRoleForTrustedAdvisorReporting` vinculada ao serviço que permite realizar ações Trusted Advisor para o recurso de visão organizacional. Não é possível anexar o AWSTrustedAdvisorReportingServiceRolePolicy às suas entidades do IAM. Para ter mais informações, consulte Usar perfis vinculados ao serviço do Trusted Advisor.

Essa política concede permissões administrativas que permitem que a função vinculada ao serviço execute ações AWS Organizations .

Detalhes das permissões

Esta política inclui as seguintes permissões:

- `organizations` - Descreve sua organização e lista o acesso ao serviço, contas, pais, filhos e unidades organizacionais

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:ListAWSServiceAccessForOrganization",
```

```
                "organizations:ListAccounts",
                "organizations:ListAccountsForParent",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListChildren",
                "organizations:ListParents",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Atualizações do Trusted Advisor para políticas gerenciadas pela AWS

Veja detalhes sobre as atualizações das políticas AWS gerenciadas para AWS Support e Trusted Advisor desde que esses serviços começaram a monitorar essas alterações. Para obter alertas automáticos sobre alterações feitas nesta página, inscreva-se no feed RSS na página Histórico do documento.

A tabela a seguir descreve atualizações importantes nas políticas Trusted Advisor gerenciadas desde 10 de agosto de 2021.

Trusted Advisor

Alteração	Descrição	Data
AWSTrustedAdvisorServiceRolePolicy Atualização de uma política existente.	Trusted Advisor adicionou novas ações para conceder o `cloudtrail:GetTrail` `cloudtrail:ListTrails` `cloudtrail:GetEventSelectors` `outposts:GetOutpost` , `outposts:ListAssets` e `outposts:`	18 de janeiro de 2024

Alteração	Descrição	Data
	`ListOutposts` permissões.	
AWSTrustedAdvisorPriorityFullAccess Atualização de uma política existente.	Trusted Advisor atualizou a política `AWSTrustedAdvisorPriorityFullAccess` AWS gerenciada para incluir IDs de declaração.	6 de dezembro de 2023
AWSTrustedAdvisorPriorityReadOnlyAccess Atualização de uma política existente.	Trusted Advisor atualizou a política `AWSTrustedAdvisorPriorityReadOnlyAccess` AWS gerenciada para incluir IDs de declaração.	6 de dezembro de 2023
AWSTrustedAdvisorServiceRolePolicy: atualização para uma política existente	Trusted Advisor adicionou novas ações para conceder `ec2:DescribeRegions` `s3:GetLifecycleConfiguration` `ecs:DescribeTaskDefinition` as `ecs:ListTaskDefinitions` permissões e.	9 de novembro de 2023

Alteração	Descrição	Data
AWSTrustedAdvisorServiceRolePolicy: atualização para uma política existente	Trusted Advisor adicionou novas ações do IAM `route53resolver:ListResolverEndpoints` , `route53resolver:ListResolverEndpointIpAddresses` `ec2:DescribeSubnets` , `kafka:ListClustersV2` e `kafka:ListNodes` para integrar novas verificações de resiliência.	14 de setembro de 2023
AWSTrustedAdvisorReportingServiceRolePolicy V2 da política gerenciada anexada à função vinculada ao Trusted Advisor `AWSServiceRoleForTrustedAdvisorReporting` serviço	Atualize a política AWS gerenciada para V2 para a função vinculada ao Trusted Advisor `AWSServiceRoleForTrustedAdvisorReporting` serviço. A V2 adicionará mais uma ação `organizations:ListDelegatedAdministrators` do IAM	28 de fevereiro de 2023
AWSTrustedAdvisorPriorityFullAccess e AWSTrustedAdvisorPriorityReadOnlyAccess Novas políticas AWS gerenciadas para o Trusted Advisor	Trusted Advisor adicionou duas novas políticas gerenciadas que você pode usar para controlar o acesso ao Trusted Advisor Priority.	17 de agosto de 2022

Alteração	Descrição	Data
AWSTrustedAdvisorServiceRolePolicy: atualização para uma política existente	Trusted Advisor adicionou novas ações para conceder `DescribeTargetGroups` as `GetAccountPublicAccessBlock` permissões e. `DescribeTargetGroup` é necessário para a permissão Auto Scaling Group Health Check (Verificação de integridade do grupo do Auto Scaling) para recuperar balanceadores de carga não clássicos anexados a um grupo do Auto Scaling. `GetAccountPublicAccessBlock` é necessário para a permissão Amazon S3 Bucket Permissions (Permissões do bucket do Amazon S3) para recuperar as configurações de acesso público de bloqueio para um Conta da AWS.	10 de agosto de 2021
Publicação do log de alterações	Trusted Advisor começou a rastrear as mudanças em suas políticas AWS gerenciadas.	10 de agosto de 2021

AWS políticas gerenciadas para AWS Support planos

AWS Support O Plans tem as seguintes políticas gerenciadas.

Sumário

- AWS política gerenciada: AWSSupportPlansFullAccess
- AWS política gerenciada: AWSSupportPlansReadOnlyAccess
- AWS Support Planeja atualizações nas políticas AWS gerenciadas

AWS política gerenciada: AWSSupportPlansFullAccess

AWS Support Os planos usam a política AWSSupportPlansFullAccess AWS gerenciada. A entidade do IAM usa essa política para concluir as seguintes ações dos planos de suporte para você:

- Veja seu plano de suporte para seu Conta da AWS
- Visualizar detalhes sobre o status de uma solicitação para alterar seu plano de suporte
- Altere o plano de suporte para seu Conta da AWS
- Crie cronogramas de planos de suporte para seu Conta da AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "supportplans:GetSupportPlan",
                "supportplans:GetSupportPlanUpdateStatus",
                "supportplans:StartSupportPlanUpdate",
                "supportplans:CreateSupportPlanSchedule"
            ],
            "Resource": "*"
        }
    ]
}
```

Para obter uma lista de alterações nas políticas, consulte AWS Support Planeja atualizações nas políticas AWS gerenciadas.

AWS política gerenciada: AWSSupportPlansReadOnlyAccess

AWS Support Os planos usam a política AWSSupportPlansReadOnlyAccess AWS gerenciada. A entidade do IAM usa essa política para concluir as seguintes ações de planos de suporte somente leitura para você:

- Veja seu plano de suporte para seu Conta da AWS
- Visualizar detalhes sobre o status de uma solicitação para alterar seu plano de suporte

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "supportplans:GetSupportPlan",
                "supportplans:GetSupportPlanUpdateStatus"
            ],
            "Resource": "*"
        }
    ]
}
```

Para obter uma lista de alterações nas políticas, consulte AWS Support Planeja atualizações nas políticas AWS gerenciadas.

AWS Support Planeja atualizações nas políticas AWS gerenciadas

Veja detalhes sobre as atualizações das políticas AWS gerenciadas dos Support Plans desde que esses serviços começaram a monitorar essas mudanças. Para obter alertas automáticos sobre alterações feitas nesta página, inscreva-se no feed RSS na página Histórico do documento.

A tabela a seguir descreve as atualizações importantes nas políticas gerenciadas pelos planos de suporte desde 29 de setembro de 2022.

AWS Support

Alteração	Descrição	Data
AWSSupportPlansFullAccess - Atualização em uma política existente	Adicione a ação `CreateSupportPlanSchedule` à política gerenciada da `AWSSupportPlansFullAccess` .	8 de maio de 2023
Publicação do log de alterações	Altere o log das políticas gerenciadas pelos planos de suporte.	29 de setembro de 2022

Gerencie o acesso ao AWS Support Centro

Você deve ter permissões para acessar a Central de Suporte e Abrir um caso de suporte.

É possível usar uma das opções a seguir para acessar a Central de Suporte:

- Use o endereço de e-mail e a senha associados à sua AWS conta. Essa identidade é chamada de usuário raiz da AWS conta.
- Uso AWS Identity and Access Management (IAM).

Se você tiver um plano Business, Enterprise On-Ramp ou Enterprise Support, também poderá usar a AWS Support API para acessar AWS Support e Trusted Advisor operar programaticamente. Para obter mais informações, consulte a AWS Support Referência da API.

> **Note**
>
> Se você não conseguir fazer login na Central de Suporte, use a página Entre em contato conosco, É possível usar esta página para obter ajuda com problemas de cobrança e conta.

AWS conta

Você pode entrar AWS Management Console e acessar o Support Center usando o endereço de e-mail e a senha da sua AWS conta. Essa identidade é chamada de usuário raiz da AWS

conta. No entanto, recomendamos não usar o usuário rai para suas tarefas diárias, nem mesmo as administrativas. Em vez disso, recomendamos usar o IAM, o que permite controlar quem pode executar determinadas tarefas na conta.

AWS ações de apoio

Você pode realizar as seguintes AWS Support ações no console. Você também pode especificar essas AWS Support ações em uma política do IAM para permitir ou negar ações específicas.

> **Note**
>
> Se você negar qualquer uma das ações abaixo em suas políticas do IAM, isso poderá resultar em um comportamento não intencional no Support Center ao criar ou interagir com um caso de suporte.

Ação	Descrição
`DescribeSupportLevel`	Concede permissão para retornar o nível de suporte de um identificador de conta da AWS . Isso é usado internamente pelo AWS Support Center para identificar seu nível de suporte.
`InitiateCallForCase`	Concede permissão para iniciar uma chamada no AWS Support Center. Isso é usado internamente pelo AWS Support Center para iniciar uma chamada em seu nome.
`InitiateChatForCase`	Concede permissão para iniciar uma chamada no AWS Support Center. Isso é usado internamente pelo AWS Support Center para iniciar um bate-papo em seu nome.
`RateCaseCommunication`	Concede permissão para avaliar a comunicaç ão de um AWS Support caso.
`DescribeCaseAttributes`	Concede permissão para que os serviços secundários leiam os atributos do caso do

Ação	Descrição
	AWS Support . Isso é usado internamente pelo AWS Support Center para obter atributos marcados em seu caso.
`DescribeIssueTypes`	Concede permissão para retornar tipos de problemas para casos do AWS Support . Isso é usado internamente pelo AWS Support Center para obter os tipos de problemas disponíveis para sua conta.
`SearchForCases`	Concede permissão para retornar uma lista de AWS Support casos que corresponda às entradas fornecidas. Isso é usado internamente pelo AWS Support Center para encontrar casos pesquisados.
`PutCaseAttributes`	Concede permissão para permitir que serviços secundários anexem atributos aos AWS Support casos. Isso é usado internamente pelo AWS Support Center para adicionar tags operacionais aos seus AWS Support casos.

IAM

Por padrão, os usuários do IAM não podem acessar a Central de Suporte. É possível usar o IAM para criar usuários ou grupos individuais. Em seguida, você anexa políticas do IAM a essas entidades, para que elas tenham permissão para realizar ações e acessar recursos, como abrir casos do Support Center e usar a AWS Support API.

Depois de criar usuários do IAM, será possível fornecer a esses usuários senhas individuais e uma página de login específica da conta. Eles podem então entrar na sua AWS conta e trabalhar no Support Center. Os usuários do IAM que têm AWS Support acesso podem ver todos os casos criados para a conta.

Para obter mais informações, consulte Como os usuários do IAM fazem login na sua AWS conta no Guia do usuário do IAM.

A maneira mais fácil de conceder permissões é anexar a política AWS gerenciada AWSSupportAccessao usuário, grupo ou função. AWS Support permite permissões em nível de ação para controlar o acesso a operações específicas AWS Support . AWS Support não fornece acesso em nível de recurso, então o `Resource` elemento está sempre definido como. * Não é possível permitir ou negar o acesso a casos de suporte específicos.

Example : Permitir acesso a todas as AWS Support ações

A política AWS gerenciada AWSSupportAccessconcede acesso a um usuário do IAM AWS Support a. Um usuário do IAM com essa política pode acessar todas as AWS Support operações e recursos.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": ["support:*"],
            "Resource": "*"
        }
    ]
}
```

Para obter mais informações sobre como anexar a política do `AWSSupportAccess` para suas entidades, consulte Adicionar permissões de identidade do IAM (console) noManual do usuário do IAM.

Example : Permitir acesso a todas as ações, exceto à ResolveCase ação

Também é possível criar políticas gerenciadas pelo cliente no IAM para especificar quais ações permitir ou negar. A declaração de política a seguir permite que um usuário do IAM execute todas as ações AWS Support , exceto resolver um caso.

```
{
   "Version": "2012-10-17",
   "Statement": [
   {
      "Effect": "Allow",
      "Action": "support:*",
      "Resource": "*"
   },
   {
       "Effect": "Deny",
```

```
        "Action": "support:ResolveCase",
        "Resource": "*"
    }]
}
```

Para obter mais informações sobre como criar uma política do IAM gerenciada pelo cliente, consulte Criar políticas do IAM (console) no Manual do usuário do IAM.

Se o usuário ou grupo já tiver uma política, você poderá adicionar a declaração AWS Support de política específica a essa política.

> **Important**
>
> - Se não conseguir visualizar casos na Central de Suporte, verifique se você tem as permissões necessárias. Talvez seja necessário entrar em contato com o administrador do IAM. Para obter mais informações, consulte Gerenciamento de identidade e acesso para AWS Support.

Acesso a AWS Trusted Advisor

No AWS Management Console, um namespace `trustedadvisor` do IAM separado controla o acesso a. Trusted Advisor Na AWS Support API, o namespace `support` do IAM controla o acesso a. Trusted Advisor Para ter mais informações, consulte Gerencie o acesso ao AWS Trusted Advisor.

Gerencie o acesso aos AWS Support planos

Tópicos

- Permissões para o console de planos de suporte
- Ações de planos de suporte
- Exemplos de políticas do IAM para planos de suporte
- Solução de problemas

Permissões para o console de planos de suporte

Para acessar o console dos planos de suporte, o usuário deve ter um conjunto mínimo de permissões. Essas permissões devem possibilitar que o usuário liste e visualize detalhes sobre os recursos dos planos de suporte em sua Conta da AWS.

Você pode criar uma política AWS Identity and Access Management (IAM) com o `supportplans` namespace. É possível usar essa política para especificar permissões para ações e recursos.

Ao criar uma política, é possível especificar o namespace do serviço para permitir ou negar uma ação. O namespace dos planos de suporte é `supportplans`.

Você pode usar políticas AWS gerenciadas e anexá-las às suas entidades do IAM. Para obter mais informações, consulte AWS políticas gerenciadas para AWS Support planos.

Ações de planos de suporte

É possível executar as ações a seguir dos planos de suporte no console. Também é possível especificar essas ações dos planos de suporte em uma política do IAM para permitir ou negar ações específicas.

Ação	Descrição
`GetSupportPlan`	Concede permissão para visualizar detalhes sobre o plano de suporte atual para esta Conta da AWS.
`GetSupportPlanUpdateStatus`	Concede permissão para visualizar detalhes sobre o status de uma solicitação de atualizaç ão de um plano de suporte.
`StartSupportPlanUpdate`	Concede permissão para iniciar a solicitação de atualização do plano de suporte para esta Conta da AWS.
`CreateSupportPlanSchedule`	Concede permissão para criar agendamentos de planos de suporte para esta Conta da AWS.

Exemplos de políticas do IAM para planos de suporte

Você pode usar os exemplos a seguir de políticas para gerenciar o acesso aos planos de suporte.

Acesso total aos planos de suporte

A política a seguir permite o acesso total dos usuários aos planos de suporte.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "supportplans:*",
            "Resource": "*"
        }
    ]
}
```

Acesso somente leitura aos planos de suporte

A política a seguir permite que os usuários tenham acesso somente leitura aos planos de suporte.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "supportplans:Get*",
            "Resource": "*"
        }
    ]
}
```

Negar acesso aos planos de suporte

A política a seguir não permite o acesso dos usuários aos planos de suporte.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "supportplans:*",
            "Resource": "*"
        }
    ]
}
```

Solução de problemas

Consulte os tópicos a seguir para gerenciar o acesso aos planos de suporte.

Quando tento visualizar ou alterar meu plano de suporte, o console dos planos do Supporte informa que não tenho a permissão **`GetSupportPlan`**

Os usuário do IAM devem ter as permissões necessárias para acessar o console dos planos do Support. Você pode atualizar sua política do IAM para incluir a permissão ausente ou usar uma política gerenciada pela AWS , como AWSSupportPlansFullAccess ou AWSSupportPlansReadOnlyAccess. Para ter mais informações, consulte AWS políticas gerenciadas para AWS Support planos.

Caso não tenha acesso para atualizar suas políticas do IAM, entre em contato com o administrador da sua Conta da AWS .

Informações relacionadas

Para obter mais informações, consulte os seguintes tópicos no Guia do usuário do IAM:

- Testar as políticas do IAM com o simulador de políticas do IAM
- Solução de problemas de mensagens de erro de acesso negado

Eu tenho as permissões corretas dos planos do Support, mas continuo recebendo o mesmo erro

Se você Conta da AWS for uma conta de membro que faz parte AWS Organizations, talvez seja necessário atualizar a política de controle de serviços (SCP). As SCPs são um tipo de política que gerencia as permissões em uma organização.

Como os planos do Support são um serviço global, as políticas que restringem as Regiões da AWS podem impedir que as contas-membro visualizem ou alterem seu plano de suporte. Para permitir serviços globais para sua organização, como o IAM e os planos do Support, é necessário adicionar o serviço à lista de exclusão em qualquer SCP aplicável. Isso significa que as contas da organização podem acessar esses serviços, mesmo que o SCP negue um especificado. Região da AWS

Para adicionar planos do Support como exceção, insira `"supportplans:*"` na lista `"NotAction"` na SCP.

```
"supportplans:*",
```

Sua SCP pode ser exibida como o seguinte trecho de política.

Example : SCP que permite o acesso a planos de suporte em uma organização

```
{ "Version":  "2012-10-17",
   "Statement": [
     { "Sid":  "GRREGIONDENY",
       "Effect":  "Deny",
       "NotAction": [
         "aws-portal:*",
         "budgets:*",
         "chime:*"
         "iam:*",
         "supportplans:*",
         ....
```

Caso tenha uma conta-membro e não consiga atualizar a SCP, fale com o administrador da Conta da AWS . Talvez a conta de gerenciamento precise atualizar a SCP para que todas as contas-membro possam acessar os planos de suporte.

Notas para AWS Control Tower

- Se sua organização usa um SCP com AWS Control Tower, você pode atualizar o Negar acesso AWS com base no Região da AWS controle solicitado (comumente chamado de controle de negação de região).
- Se você atualizar o SCP AWS Control Tower para permitir`supportplans`, reparar o desvio removerá sua atualização do SCP. Para obter mais informações, consulte Detectar e resolver o drift in AWS Control Tower.

Informações relacionadas

Para obter mais informações, consulte os tópicos a seguir.

- Políticas de controle de serviço (SCPs) no Guia do usuário do AWS Organizations .
- Configure the Region deny control (Configurar o controle de negação de região) no Guia do usuário do AWS Control Tower
- Negar acesso a AWS com base no solicitado Região da AWS no Guia AWS Control Tower do usuário

Gerencie o acesso ao AWS Trusted Advisor

Você pode acessar AWS Trusted Advisor a partir do AWS Management Console. Todos Contas da AWS têm acesso a algumas Trusted Advisor verificações básicas. Se você tiver um plano de suporte Business, Enterprise On-Ramp ou Enterprise, será possível acessar todas as verificações. Para obter mais informações, consulte Referência de verificação do AWS Trusted Advisor.

Você pode usar AWS Identity and Access Management (IAM) para controlar o acesso Trusted Advisor a.

Tópicos

- Permissões para o console do Trusted Advisor
- Trusted Advisor ações
- Exemplos de política do IAM
- Consulte também

Permissões para o console do Trusted Advisor

Para acessar o Trusted Advisor console, o usuário deve ter um conjunto mínimo de permissões. Essas permissões devem permitir que o usuário liste e visualize detalhes sobre os Trusted Advisor recursos em seu Conta da AWS.

É possível usar as seguintes opções para controlar o acesso ao Trusted Advisor:

- Use o recurso de filtro de tags do Trusted Advisor console. O usuário ou a função deve ter permissões associadas às tags.

  Você pode usar políticas AWS gerenciadas ou políticas personalizadas para atribuir permissões por tags. Para obter mais informações, consulte Controlar o acesso a/para usuários e funções do IAM usando tags.
- Crie uma política do IAM com o namespace `trustedadvisor`. É possível usar essa política para especificar permissões para ações e recursos.

Ao criar uma política, é possível especificar o namespace do serviço para permitir ou negar uma ação. O namespace para Trusted Advisor é. `trustedadvisor` No entanto, você não pode usar o `trustedadvisor` namespace para permitir ou negar operações de Trusted Advisor API na AWS Support API. Em vez disso, use o namespace `support` para AWS Support .

> **Note**
>
> Se você tiver permissões para a AWS SupportAPI, o Trusted Advisor widget no AWS Management Console mostra uma visão resumida dos seus Trusted Advisor resultados. Para ver seus resultados no Trusted Advisor console, você deve ter permissão para o `trustedadvisor` namespace.

Trusted Advisor ações

Você pode realizar as seguintes Trusted Advisor ações no console. Você também pode especificar essas Trusted Advisor ações em uma política do IAM para permitir ou negar ações específicas.

Ação	Descrição
`DescribeAccount`	Concede permissão para visualizar o AWS Support plano e várias Trusted Advisor p referências.
`DescribeAccountAccess`	Concede permissão para ver se o Conta da AWS foi ativado ou desativado Trusted Advisor.
`DescribeCheckItems`	Concede permissão para visualizar detalhes dos itens de verificação.
`DescribeCheckRefreshStatuses`	Concede permissão para visualizar os status de atualização para verificações do Trusted Advisor .
`DescribeCheckSummaries`	Concede permissão para visualizar resumos de Trusted Advisor cheques.
`DescribeChecks`	Concede permissão para visualizar os detalhes dos Trusted Advisor cheques.
`DescribeNotificationPreferences`	Concede permissão para visualizar as preferências de notificação para a conta da AWS .

Ação	Descrição
`ExcludeCheckItems`	Concede permissão para excluir recomendações para verificações do Trusted Advisor .
`IncludeCheckItems`	Concede permissão para incluir recomendações para verificações do Trusted Advisor .
`RefreshCheck`	Concede permissão para atualizar um Trusted Advisor cheque.
`SetAccountAccess`	Concede permissão para ativar ou desativar Trusted Advisor a conta.
`UpdateNotificationPreferences`	Concede permissão para atualizar as preferências de notificação do Trusted Advisor.
`DescribeCheckStatusHistoryChanges`	Concede permissão para visualizar os resultados e os status alterados das verificações nos últimos 30 dias.

Trusted Advisor ações para visão organizacional

As Trusted Advisor ações a seguir são para o recurso de visualização organizacional. Para obter mais informações, consulte Visualização organizacional para AWS Trusted Advisor.

Ação	Descrição
`DescribeOrganization`	Concede permissão para ver se Conta da AWS ele atende aos requisitos para ativar o recurso de visualização organizacional.
`DescribeOrganizationAccounts`	Concede permissão para visualizar as AWS contas vinculadas que estão na organização.
`DescribeReports`	Concede permissão para visualizar detalhes para relatórios de visualização organizacional,

Ação	Descrição
	como o nome do relatório, o runtime, a data de criação, o status e o formato
`DescribeServiceMetadata`	Concede permissão para visualizar informaçõ es sobre relatórios de exibição organizacional, como categorias de verificação Regiões da AWS, nomes de cheques e status de recursos.
`GenerateReport`	Concede permissão para criar um relatório para Trusted Advisor cheques em sua organização.
`ListAccountsForParent`	Concede permissão para visualizar, no Trusted Advisor console, todas as contas em uma AWS organização que estão contidas em uma unidade raiz ou organizacional (OU).
`ListOrganizationalUnitsForParent`	Concede permissão para visualizar, no Trusted Advisor console, todas as unidades organizac ionais (OUs) em uma unidade organizacional principal ou raiz.
`ListRoots`	Concede permissão para visualizar, no Trusted Advisor console, todas as raízes definidas em uma AWS organização.
`SetOrganizationAccess`	Concede permissão para ativar o recurso de visualização organizacional para Trusted Advisor.

Trusted Advisor Ações prioritárias

Se você tiver a Trusted Advisor Prioridade ativada para sua conta, poderá realizar as seguintes Trusted Advisor ações no console. Você também pode adicionar essas ações do Trusted Advisor em uma política do IAM para permitir ou negar ações específicas. Para obter mais informações, consulte Exemplos de políticas do IAM para o Trusted Advisor Priority.

> **Note**
>
> Os riscos que aparecem em Trusted Advisor Prioridade são recomendações que seu gerente técnico de contas (TAM) identificou para sua conta. As recomendações de um serviço, como um Trusted Advisor cheque, são criadas automaticamente para você. As recomendações do seu TAM são criadas manualmente. Em seguida, seu TAM envia essas recomendações para que elas apareçam em Trusted Advisor Prioridade para sua conta.

Para obter mais informações, consulte Conceitos básicos do AWS Trusted Advisor Priority.

Ação	Descrição
`DescribeRisks`	Concede permissão para visualizar riscos em Trusted Advisor Prioridade.
`DescribeRisk`	Concede permissão para visualizar os detalhes do risco em Trusted Advisor Prioridade.
`DescribeRiskResources`	Concede permissão para exibir recursos afetados para um risco no Trusted Advisor Priority.
`DownloadRisk`	Concede permissão para baixar um arquivo que contém detalhes sobre o risco em Trusted Advisor Prioridade.
`UpdateRiskStatus`	Concede permissão para atualizar o status do risco no Trusted Advisor Priority.
`DescribeNotificationConfigurations`	Concede permissão para obter suas preferências de notificação por e-mail para Trusted Advisor Priority.
`UpdateNotificationConfigurations`	Concede permissão para criar ou atualizar as preferências de notificação por e-mail do Trusted Advisor Priority.

Ação	Descrição
`DeleteNotificationConfigurationForDelegatedAdmin`	Concede permissão à conta de gerenciamento da organização para excluir as preferências de notificação por e-mail de uma conta de administrador delegado do Trusted Advisor Priority.

Trusted Advisor Engajar ações

Se você tiver o Trusted Advisor Engage ativado para sua conta, poderá realizar as seguintes Trusted Advisor ações no console. Você também pode adicionar essas Trusted Advisor ações em uma política do IAM para permitir ou negar ações específicas. Para obter mais informações, consulteExemplos de políticas do IAM para o Trusted Advisor Engage.

Para obter mais informações, consulte Comece a usar o AWS Trusted Advisor Engage (versão pré-visualização).

Ação	Descrição
`CreateEngagement`	Concede permissão para criar um engajamento no Trusted Advisor Engage.
`CreateEngagementAttachment`	Concede permissão para criar um anexo de engajamento no Trusted Advisor Engage.
`CreateEngagementCommunication`	Concede permissão para criar uma comunicação de engajamento no Trusted Advisor Engage.
`GetEngagement`	Concede permissão para visualizar um engajamento no Trusted Advisor Engage.
`GetEngagementAttachment`	Concede permissão para visualizar um anexo de engajamento no Trusted Advisor Engage.

Ação	Descrição
`GetEngagementType`	Concede permissão para visualizar um tipo específico de engajamento no Trusted Advisor Engage.
`ListEngagementCommunications`	Concede permissão para visualizar todas as comunicações de uma interação no Trusted Advisor Engage.
`ListEngagements`	Concede permissão para visualizar todos os engajamentos no Trusted Advisor Engage.
`ListEngagementTypes`	Concede permissão para visualizar todos os tipos de engajamento no Trusted Advisor Engage.
`UpdateEngagement`	Concede permissão para atualizar os detalhes de um engajamento no Trusted Advisor Engage.
`UpdateEngagementStatus`	Concede permissão para atualizar o status de um engajamento no Trusted Advisor Engage.

Exemplos de política do IAM

As políticas a seguir mostram como permitir e negar acesso ao Trusted Advisor. É possível usar uma das políticas a seguir para criar uma política gerenciada pelo cliente no console do IAM. Por exemplo, é possível copiar uma política de exemplo e colá-la na Guia JSON do console do IAM. Em seguida, é possível anexar a política a um usuário, grupo ou função do IAM.

Para obter mais informações sobre como criar uma política do IAM, consulte Criar políticas do IAM (console) no Manual do usuário do IAM.

Exemplos

- Acesso total ao Trusted Advisor
- Acesso somente leitura ao Trusted Advisor
- Negar acesso a Trusted Advisor

- Permitir e negar ações específicas
- Controle o acesso às operações AWS Support da API para Trusted Advisor
- Exemplos de políticas do IAM para o Trusted Advisor Priority
- Exemplos de políticas do IAM para o Trusted Advisor Engage.

Acesso total ao Trusted Advisor

A política a seguir permite que os usuários visualizem e realizem todas as ações em todas as Trusted Advisor verificações no Trusted Advisor console.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "trustedadvisor:*",
            "Resource": "*"
        }
    ]
}
```

Acesso somente leitura ao Trusted Advisor

A política a seguir permite que os usuários tenham acesso somente de leitura ao Trusted Advisor console. Os usuários não podem fazer alterações, como verificações de atualização ou alterar preferências de notificação.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "trustedadvisor:Describe*",
                "trustedadvisor:Get*",
                "trustedadvisor:List*"
            ],
            "Resource": "*"
        }
    ]
```

```
}
```

Negar acesso a Trusted Advisor

A política a seguir não permite que os usuários visualizem ou realizem Trusted Advisor verificações no Trusted Advisor console.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "trustedadvisor:*",
            "Resource": "*"
        }
    ]
}
```

Permitir e negar ações específicas

A política a seguir permite que os usuários visualizem todas as Trusted Advisor verificações no Trusted Advisor console, mas não permite que eles atualizem nenhuma verificação.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "trustedadvisor:*",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": "trustedadvisor:RefreshCheck",
            "Resource": "*"
        }
    ]
}
```

Controle o acesso às operações AWS Support da API para Trusted Advisor

No AWS Management Console, um namespace `trustedadvisor` do IAM separado controla o acesso a. Trusted Advisor Você não pode usar o `trustedadvisor` namespace para permitir ou negar operações de Trusted Advisor API na AWS Support API. Em vez disso, use o namespace `support`. Você precisa ter permissões na AWS Support API para fazer chamadas Trusted Advisor programaticamente.

Por exemplo, se você quiser chamar a RefreshTrustedAdvisorCheckoperação, deverá ter permissões para essa ação na política.

Example : permitir somente operações de Trusted Advisor API

A política a seguir permite que os usuários acessem as operações da AWS Support API Trusted Advisor, mas não o resto das operações da AWS Support API. Por exemplo, os usuários podem usar a API para exibir e atualizar verificações. Eles não podem criar, visualizar, atualizar ou resolver AWS Support casos.

Você pode usar essa política para chamar as operações da Trusted Advisor API de forma programática, mas não pode usar essa política para visualizar ou atualizar as verificações no console. Trusted Advisor

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "support:DescribeTrustedAdvisorCheckRefreshStatuses",
                "support:DescribeTrustedAdvisorCheckResult",
                "support:DescribeTrustedAdvisorChecks",
                "support:DescribeTrustedAdvisorCheckSummaries",
                "support:RefreshTrustedAdvisorCheck",
                "trustedadvisor:Describe*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "support:AddAttachmentsToSet",
```

```
                "support:AddCommunicationToCase",
                "support:CreateCase",
                "support:DescribeAttachment",
                "support:DescribeCases",
                "support:DescribeCommunications",
                "support:DescribeServices",
                "support:DescribeSeverityLevels",
                "support:ResolveCase"
            ],
            "Resource": "*"
        }
    ]
}
```

Para obter mais informações sobre como o IAM funciona com AWS Support e Trusted Advisor, consulteAções.

Exemplos de políticas do IAM para o Trusted Advisor Priority

Você pode usar as seguintes políticas AWS gerenciadas para controlar o acesso à Trusted Advisor Prioridade. Para obter mais informações, consulte AWS políticas gerenciadas para AWS Trusted Advisor e Conceitos básicos do AWS Trusted Advisor Priority.

Exemplos de políticas do IAM para o Trusted Advisor Engage.

> **Note**
>
> Trusted Advisor O Engage está em versão prévia e atualmente não tem nenhuma política AWS gerenciada. É possível usar uma das políticas a seguir para criar uma política gerenciada pelo cliente no console do IAM.

Um exemplo de política que concede acesso de leitura e gravação no Trusted Advisor Engage:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "trustedadvisor:CreateEngagement*",
```

```
                "trustedadvisor:DescribeAccount*",
                "trustedadvisor:GetEngagement*",
                "trustedadvisor:ListEngagement*",
                "trustedadvisor:UpdateEngagement*"
            ],
            "Resource": "*"
        }
    ]
}
```

Um exemplo de política que concede acesso somente para leitura no Engage: Trusted Advisor

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "trustedadvisor:DescribeAccount*",
                "trustedadvisor:GetEngagement*",
                "trustedadvisor:ListEngagement*"
            ],
            "Resource": "*"
        }
    ]
}
```

Um exemplo de política que concede acesso de leitura e gravação no Trusted Advisor Engage e a capacidade de habilitar acesso confiável a Trusted Advisor:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:ListAWSServiceAccessForOrganization",
                "trustedadvisor:CreateEngagement*",
                "trustedadvisor:DescribeAccount*",
                "trustedadvisor:DescribeOrganization",
                "trustedadvisor:GetEngagement*",
                "trustedadvisor:ListEngagement*",
```

```
                "trustedadvisor:SetOrganizationAccess",
                "trustedadvisor:UpdateEngagement*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:DisableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "organizations:ServicePrincipal": [
                        "reporting.trustedadvisor.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/
reporting.trustedadvisor.amazonaws.com/AWSServiceRoleForTrustedAdvisorReporting",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "reporting.trustedadvisor.amazonaws.com"
                }
            }
        }
    ]
}
```

Consulte também

Para obter mais informações sobre Trusted Advisor permissões, consulte os seguintes recursos:

- Ações definidas pelo AWS Trusted Advisor no Manual do usuário do IAM.
- Controlar o acesso ao console do Trusted Advisor

Políticas de controle de serviço de exemplo para o AWS Trusted Advisor

AWS Trusted Advisor suporta políticas de controle de serviços (SCPs). SCPs são políticas que você anexa a elementos em uma organização para gerenciar permissões dentro dessa organização. Um SCP se aplica a todas as AWS contas do elemento ao qual você anexa o SCP. As SCPs oferecem controle central sobre as permissões máximas disponíveis para todas as contas da organização. Eles podem ajudar você a garantir que suas AWS contas permaneçam dentro das diretrizes de controle de acesso da sua organização. Para obter mais informações, consulte Políticas de controle de serviço no Guia do usuário do AWS Organizations .

Tópicos

- Pré-requisitos
- Políticas de controle de serviço de exemplo

Pré-requisitos

Para usar os SCPs, você deve fazer o seguinte:

- Ativar todos os recursos em sua organização. Para obter mais informações, consulte Habilitar todos os atributos na sua organização no Manual do usuário do AWS Organizations .
- Habilitar SCPs para uso na sua organização. Para obter mais informações, consulte Habilitar e desabilitar tipos de política no Guia do usuário do AWS Organizations .
- Crie as SCPs de que você precisa. Para obter mais informações sobre a criação de SCPs, consulte Criar, atualizar e excluir políticas de controle de serviço no Guia do usuário do AWS Organizations .

Políticas de controle de serviço de exemplo

Os exemplos a seguir mostram como você pode controlar vários aspectos do compartilhamento de recursos em uma organização.

Example : Impeça que os usuários criem ou editem engajamentos no Engage Trusted Advisor

A SCP a seguir impede que os usuários criem novas interações ou editem as interações existentes.

```
{
  "Version": "2012-10-17",
  "Statement": [
```

```
    {
      "Effect": "Deny",
      "Action": [
        "trustedadvisor:CreateEngagement",
        "trustedadvisor:UpdateEngagement*"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Example : negue Trusted Advisor engajamento e acesso Trusted Advisor prioritário

O SCP a seguir impede que os usuários acessem ou realizem qualquer ação no Trusted Advisor Engage e no Trusted Advisor Priority.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "trustedadvisor:ListEngagement*",
        "trustedadvisor:GetEngagement*",
        "trustedadvisor:CreateEngagement*",
        "trustedadvisor:UpdateEngagement*",
        "trustedadvisor:DescribeRisk*",
        "trustedadvisor:UpdateRisk*",
        "trustedadvisor:DownloadRisk"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Solução de problemas AWS Support de identidade e acesso

Use as informações a seguir para ajudá-lo a diagnosticar e corrigir problemas comuns que você pode encontrar ao trabalhar com AWS Support um IAM.

Tópicos

- Não estou autorizado a realizar iam: PassRole
- Quero visualizar minhas chaves de acesso
- Sou administrador e quero permitir que outras pessoas acessem AWS Support
- Quero permitir que pessoas fora da minha AWS conta acessem meus AWS Support recursos

Não estou autorizado a realizar iam: PassRole

Se você receber uma mensagem de erro informando que não está autorizado a executar a ação `iam:PassRole`, as suas políticas devem ser atualizadas para permitir que você passe uma função para o AWS Support.

Alguns Serviços da AWS permitem que você passe uma função existente para esse serviço em vez de criar uma nova função de serviço ou uma função vinculada ao serviço. Para fazê-lo, você deve ter permissões para passar o perfil para o serviço.

O exemplo de erro a seguir ocorre quando uma usuária do IAM chamada `marymajor` tenta utilizar o console para executar uma ação no AWS Support. 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 precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

Quero visualizar minhas chaves de acesso

Depois de criar suas chaves de acesso de usuário do IAM, é possível visualizar seu ID da chave de acesso a qualquer momento. No entanto, você não pode visualizar sua chave de acesso secreta novamente. Se você perder sua chave secreta, crie um novo par de chaves de acesso.

As chaves de acesso consistem em duas partes: um ID de chave de acesso (por exemplo, `AKIAIOSFODNN7EXAMPLE`) e uma chave de acesso secreta (por exemplo, `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`). Como um nome de usuário e uma senha, você deve usar o

ID da chave de acesso e a chave de acesso secreta em conjunto para autenticar suas solicitações. Gerencie suas chaves de acesso de forma tão segura quanto você gerencia seu nome de usuário e sua senha.

> **Important**
>
> Não forneça as chaves de acesso a terceiros, mesmo que seja para ajudar a encontrar o ID de usuário canônico. Ao fazer isso, você pode dar a alguém acesso permanente ao seu Conta da AWS.

Ao criar um par de chaves de acesso, você é solicitado a guardar o ID da chave de acesso e a chave de acesso secreta em um local seguro. A chave de acesso secreta só está disponível no momento em que é criada. Se você perder sua chave de acesso secreta, será necessário adicionar novas chaves de acesso para seu usuário do IAM. Você pode ter no máximo duas chaves de acesso. Se você já tiver duas, você deverá excluir um par de chaves para poder criar um novo. Para visualizar as instruções, consulte Gerenciar chaves de acesso no Guia do usuário do IAM.

Sou administrador e quero permitir que outras pessoas acessem AWS Support

Para permitir que outras pessoas acessem AWS Support, você deve criar uma entidade do IAM (usuário ou função) para a pessoa ou o aplicativo que precisa de acesso. Elas usarão as credenciais dessa entidade para acessar a AWS. Você deve anexar uma política à entidade que concede a eles as permissões corretas no AWS Support.

Para começar a usar imediatamente, consulte Criar os primeiros usuário e grupo delegados pelo IAM no Guia do usuário do IAM.

Quero permitir que pessoas fora da minha AWS conta acessem meus AWS Support recursos

Você pode criar uma função que os usuários de outras contas ou pessoas fora da sua organização podem usar para acessar seus recursos. Você pode especificar quem é confiável para assumir o perfil. Para serviços que oferecem suporte a 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 é AWS Support compatível com esses recursos, consulteComo AWS Support funciona com o IAM.

- Para saber como fornecer acesso aos seus recursos em todos os Contas da AWS que você possui, consulte Como fornecer acesso a um usuário do IAM em outro Conta da AWS que você possui no Guia do usuário do IAM.
- Para saber como fornecer acesso aos seus recursos a terceiros Contas da AWS, consulte Como fornecer acesso Contas da AWS 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 usar perfis e políticas baseadas em recursos para acesso entre contas, consulte Como os perfis do IAM diferem de políticas baseadas em recursos no Guia do usuário do IAM.

Resposta a incidentes

A resposta a incidentes AWS Support é uma AWS responsabilidade. AWS tem uma política e um programa formais e documentados que regem a resposta a incidentes. Para obter mais informações, consulte o whitepaper Apresentando a resposta a incidentes de AWS segurança.

Use as seguintes opções para se informar sobre problemas operacionais:

- Veja problemas AWS operacionais com amplo impacto no AWS Service Health Dashboard. Por exemplo, eventos que afetam um serviço ou uma região que não é específico(a) para sua conta.
- Visualize os problemas operacionais das contas individuais no AWS Health Dashboard. Por exemplo, eventos que afetam serviços ou recursos em sua conta. Para obter mais informações, consulte Conceitos básicos do AWS Health Dashboard no Manual do usuário do AWS Health .

Registro e monitoramento em AWS Support e AWS Trusted Advisor

O monitoramento é uma parte importante da manutenção da confiabilidade, disponibilidade e desempenho de AWS Support suas outras AWS soluções. AWS Trusted Advisor AWS fornece as seguintes ferramentas de monitoramento para observar AWS Support e AWS Trusted Advisor relatar quando algo está errado e tomar medidas quando apropriado:

- A Amazon CloudWatch monitora seus AWS recursos e os aplicativos nos quais você executa AWS em tempo real. É possível coletar e rastrear métricas, criar painéis personalizados e definir

alarmes que o notificam ou que realizam ações quando uma métrica especificada atinge um limite definido. Por exemplo, você pode CloudWatch monitorar o uso da CPU ou outras métricas de suas instâncias do Amazon Elastic Compute Cloud (Amazon EC2) e iniciar automaticamente novas instâncias quando necessário. Para obter mais informações, consulte o Guia CloudWatch do usuário da Amazon.

- A Amazon EventBridge fornece um fluxo quase em tempo real de eventos do sistema que descrevem mudanças nos AWS recursos. EventBridge permite a computação automatizada baseada em eventos, pois você pode escrever regras que observam determinados eventos e acionam ações automatizadas em outros AWS serviços quando esses eventos acontecem. Para obter mais informações, consulte o Guia EventBridge do usuário da Amazon.
- AWS CloudTrailcaptura chamadas de API e eventos relacionados feitos por ou em nome de sua AWS conta e entrega os arquivos de log para um bucket do Amazon Simple Storage Service (Amazon S3) especificado por você. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem a partir do qual as chamadas foram feitas e quando elas ocorreram. Para mais informações, consulte o Guia do usuário do AWS CloudTrail.

Para obter mais informações, consulte Monitorar e registrar em log para o AWS Support e Monitorar e registrar em log para o AWS Trusted Advisor.

Validação de conformidade para AWS Support

Para saber se um AWS service (Serviço da AWS) está dentro do escopo de programas de conformidade específicos, consulte Serviços da AWS Escopo por Programa de Conformidade Serviços da AWS e escolha o programa de conformidade em que você está interessado. Para obter informações gerais, consulte Programas de AWS conformidade Programas AWS de .

Você pode baixar relatórios de auditoria de terceiros usando AWS Artifact. Para obter mais informações, consulte Baixar relatórios em AWS Artifact .

Sua responsabilidade de conformidade ao usar Serviços da AWS é determinada pela confidencialidade de seus dados, pelos objetivos de conformidade de sua empresa e pelas leis e regulamentações aplicáveis. AWS fornece os seguintes recursos para ajudar na conformidade:

- Guias de início rápido sobre segurança e conformidade — Esses guias de implantação discutem considerações arquitetônicas e fornecem etapas para a implantação de ambientes básicos AWS focados em segurança e conformidade.

- Arquitetura para segurança e conformidade com a HIPAA na Amazon Web Services — Este whitepaper descreve como as empresas podem usar AWS para criar aplicativos qualificados para a HIPAA.

> **Note**
>
> Nem todos Serviços da AWS são elegíveis para a HIPAA. Para obter mais informações, consulte a Referência dos serviços qualificados pela HIPAA.

- AWS Recursos de https://aws.amazon.com/compliance/resources/ de conformidade — Essa coleção de pastas de trabalho e guias pode ser aplicada ao seu setor e local.
- AWS Guias de conformidade do cliente — Entenda o modelo de responsabilidade compartilhada sob a ótica da conformidade. Os guias resumem as melhores práticas de proteção Serviços da AWS e mapeiam as diretrizes para controles de segurança em várias estruturas (incluindo o Instituto Nacional de Padrões e Tecnologia (NIST), o Conselho de Padrões de Segurança do Setor de Cartões de Pagamento (PCI) e a Organização Internacional de Padronização (ISO)).
- Avaliação de recursos com regras no Guia do AWS Config desenvolvedor — O AWS Config serviço avalia o quão bem suas configurações de recursos estão em conformidade com as práticas internas, as diretrizes e os regulamentos do setor.
- AWS Security Hub— Isso AWS service (Serviço da AWS) fornece uma visão abrangente do seu estado de segurança interno AWS. O Security Hub usa controles de segurança para avaliar os recursos da AWS e verificar a conformidade com os padrões e as práticas recomendadas do setor de segurança. Para obter uma lista dos serviços e controles aceitos, consulte a Referência de controles do Security Hub.
- AWS Audit Manager— Isso AWS service (Serviço da AWS) ajuda você a auditar continuamente seu AWS uso para simplificar a forma como você gerencia o risco e a conformidade com as regulamentações e os padrões do setor.

Resiliência em AWS Support

A infraestrutura AWS global é construída em torno de AWS regiões e zonas de disponibilidade. AWS As regiões fornecem várias zonas de disponibilidade fisicamente separadas e isoladas, conectadas a redes de baixa latência, alta taxa de transferência e alta redundância. Com as zonas de disponibilidade, é possível projetar e operar aplicações e bancos de dados que automaticamente executam o failover entre as zonas sem interrupção. As zonas de disponibilidade são mais altamente

disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de datacenter tradicionais.

Para obter mais informações sobre AWS regiões e zonas de disponibilidade, consulte infraestrutura AWS global.

Segurança da infraestrutura em AWS Support

Como serviço gerenciado, AWS Support é protegido pelos procedimentos AWS globais de segurança de rede descritos no whitepaper Amazon Web Services: Visão geral dos processos de segurança.

Você usa chamadas de API AWS publicadas para acessar AWS Support pela rede. Os clientes devem oferecer suporte a Transport Layer Security (TLS) 1.0 ou posterior. Recomendamos TLS 1.2 ou posterior. Os clientes também devem ter suporte a conjuntos de criptografia com perfect forward secrecy (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, as solicitações devem ser assinadas utilizando um ID da chave de acesso e uma chave de acesso secreta associada a uma entidade principal do IAM. Ou é possível usar o AWS Security Token Service (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

Análise de configuração e vulnerabilidade em AWS Support

For AWS Trusted Advisor, AWS lida com tarefas básicas de segurança, como sistema operacional (SO) convidado e aplicação de patches em bancos de dados, configuração de firewall e recuperação de desastres.

A configuração e os controles de TI são uma responsabilidade compartilhada entre você AWS e você, nosso cliente. Para obter mais informações, consulte o modelo de responsabilidade AWS compartilhada.

Exemplos de código para AWS Support usar AWS SDKs

Os exemplos de código a seguir mostram como usar AWS Support com um kit AWS de desenvolvimento de software (SDK).

Ações são trechos de código de programas maiores e devem ser executadas em contexto. Embora as ações mostrem como chamar funções de serviço específicas, é possível ver as ações contextualizadas em seus devidos cenários e exemplos entre serviços.

Cenários são exemplos de código que mostram como realizar uma tarefa específica chamando várias funções dentro do mesmo serviço.

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsar o AWS Support com um SDK da AWS. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Conceitos básicos

Olá AWS Support

O exemplo de código a seguir mostra como começar a usar o AWS Support.

.NET

AWS SDK for .NET

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

```
using Amazon.AWSSupport;
using Microsoft.Extensions.DependencyInjection;
using Microsoft.Extensions.Hosting;

public static class HelloSupport
{
    static async Task Main(string[] args)
    {
```

```
        // Use the AWS .NET Core Setup package to set up dependency injection for
 the AWS Support service.
        // Use your AWS profile name, or leave it blank to use the default
 profile.
        // You must have one of the following AWS Support plans: Business,
 Enterprise On-Ramp, or Enterprise. Otherwise, an exception will be thrown.
        using var host = Host.CreateDefaultBuilder(args)
            .ConfigureServices((_, services) =>
                services.AddAWSService<IAmazonAWSSupport>()
            ).Build();

        // Now the client is available for injection.
        var supportClient =
 host.Services.GetRequiredService<IAmazonAWSSupport>();

        // You can use await and any of the async methods to get a response.
        var response = await supportClient.DescribeServicesAsync();
        Console.WriteLine($"\tHello AWS Support! There are
 {response.Services.Count} services available.");
    }
}
```

- Para obter detalhes da API, consulte DescribeServicesa Referência AWS SDK for .NET da API.

Java

SDK para Java 2.x

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.support.SupportClient;
import software.amazon.awssdk.services.support.model.Category;
import software.amazon.awssdk.services.support.model.DescribeServicesRequest;
import software.amazon.awssdk.services.support.model.DescribeServicesResponse;
```

```
import software.amazon.awssdk.services.support.model.Service;
import software.amazon.awssdk.services.support.model.SupportException;
import java.util.ArrayList;
import java.util.List;

/**
 * Before running this Java (v2) code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 *
 * In addition, you must have the AWS Business Support Plan to use the AWS
 * Support Java API. For more information, see:
 *
 * https://aws.amazon.com/premiumsupport/plans/
 *
 * This Java example performs the following task:
 *
 * 1. Gets and displays available services.
 *
 *
 * NOTE: To see multiple operations, see SupportScenario.
 */

public class HelloSupport {
    public static void main(String[] args) {
        Region region = Region.US_WEST_2;
        SupportClient supportClient = SupportClient.builder()
                .region(region)
                .build();

        System.out.println("***** Step 1. Get and display available services.");
        displayServices(supportClient);
    }

    // Return a List that contains a Service name and Category name.
    public static void displayServices(SupportClient supportClient) {
        try {
            DescribeServicesRequest servicesRequest =
 DescribeServicesRequest.builder()
                    .language("en")
```

```
                    .build();

            DescribeServicesResponse response =
 supportClient.describeServices(servicesRequest);
            List<Service> services = response.services();

            System.out.println("Get the first 10 services");
            int index = 1;
            for (Service service : services) {
                if (index == 11)
                    break;

                System.out.println("The Service name is: " + service.name());

                // Display the Categories for this service.
                List<Category> categories = service.categories();
                for (Category cat : categories) {
                    System.out.println("The category name is: " + cat.name());
                }
                index++;
            }

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }
}
```

- Para obter detalhes da API, consulte DescribeServicesa Referência AWS SDK for Java 2.x da API.

JavaScript

SDK para JavaScript (v3)

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

Invoque `main()` para executar o exemplo.

```
import {
  DescribeServicesCommand,
  SupportClient,
} from "@aws-sdk/client-support";

// Change the value of 'region' to your preferred AWS Region.
const client = new SupportClient({ region: "us-east-1" });

const getServiceCount = async () => {
  try {
    const { services } = await client.send(new DescribeServicesCommand({}));
    return services.length;
  } catch (err) {
    if (err.name === "SubscriptionRequiredException") {
      throw new Error(
        "You must be subscribed to the AWS Support plan to use this feature.",
      );
    } else {
      throw err;
    }
  }
};

export const main = async () => {
  try {
    const count = await getServiceCount();
    console.log(`Hello, AWS Support! There are ${count} services available.`);
  } catch (err) {
    console.error("Failed to get service count: ", err.message);
  }
};
```

- Para obter detalhes da API, consulte DescribeServicesa Referência AWS SDK for JavaScript da API.

Kotlin

SDK for Kotlin

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

```
/**
Before running this Kotlin code example, set up your development environment,
including your credentials.

For more information, see the following documentation topic:
https://docs.aws.amazon.com/sdk-for-kotlin/latest/developer-guide/setup.html

In addition, you must have the AWS Business Support Plan to use the AWS Support
 Java API. For more information, see:

https://aws.amazon.com/premiumsupport/plans/

This Kotlin example performs the following task:

1. Gets and displays available services.
 */

suspend fun main() {
    displaySomeServices()
}

// Return a List that contains a Service name and Category name.
suspend fun displaySomeServices() {
    val servicesRequest = DescribeServicesRequest {
        language = "en"
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeServices(servicesRequest)
        println("Get the first 10 services")
        var index = 1
```

```
        response.services?.forEach { service ->
            if (index == 11) {
                return@forEach
            }

            println("The Service name is: " + service.name)

            // Get the categories for this service.
            service.categories?.forEach { cat ->
                println("The category name is ${cat.name}")
                index++
            }
        }
    }
}
```

- Para obter detalhes da API, consulte a DescribeServicesreferência da API AWS SDK for Kotlin.

Python

SDK para Python (Boto3)

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

```
import logging
import boto3
from botocore.exceptions import ClientError

logger = logging.getLogger(__name__)


def hello_support(support_client):
    """
    Use the AWS SDK for Python (Boto3) to create an AWS Support client and count
```

```
    the available services in your account.
    This example uses the default settings specified in your shared credentials
    and config files.

    :param support_client: A Boto3 Support Client object.
    """
    try:
        print("Hello, AWS Support! Let's count the available Support services:")
        response = support_client.describe_services()
        print(f"There are {len(response['services'])} services available.")
    except ClientError as err:
        if err.response["Error"]["Code"] == "SubscriptionRequiredException":
            logger.info(
                "You must have a Business, Enterprise On-Ramp, or Enterprise
 Support "
                "plan to use the AWS Support API. \n\tPlease upgrade your
 subscription to run these "
                "examples."
            )
        else:
            logger.error(
                "Couldn't count services. Here's why: %s: %s",
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise


if __name__ == "__main__":
    hello_support(boto3.client("support"))
```

- Para obter detalhes da API, consulte a DescribeServicesReferência da API AWS SDK for Python (Boto3).

Exemplos de código

- Ações para AWS Support usar AWS SDKs
  - Use AddAttachmentsToSet com um AWS SDK ou uma ferramenta de linha de comando
  - Use AddCommunicationToCase com um AWS SDK ou uma ferramenta de linha de comando
  - Use CreateCase com um AWS SDK ou uma ferramenta de linha de comando

- Use DescribeAttachment com um AWS SDK ou uma ferramenta de linha de comando
- Use DescribeCases com um AWS SDK ou uma ferramenta de linha de comando
- Use DescribeCommunications com um AWS SDK ou uma ferramenta de linha de comando
- Use DescribeServices com um AWS SDK ou uma ferramenta de linha de comando
- Use DescribeSeverityLevels com um AWS SDK ou uma ferramenta de linha de comando
- Use DescribeTrustedAdvisorCheckRefreshStatuses com um AWS SDK ou uma ferramenta de linha de comando
- Use DescribeTrustedAdvisorCheckResult com um AWS SDK ou uma ferramenta de linha de comando
- Use DescribeTrustedAdvisorCheckSummaries com um AWS SDK ou uma ferramenta de linha de comando
- Use DescribeTrustedAdvisorChecks com um AWS SDK ou uma ferramenta de linha de comando
- Use RefreshTrustedAdvisorCheck com um AWS SDK ou uma ferramenta de linha de comando
- Use ResolveCase com um AWS SDK ou uma ferramenta de linha de comando

- Cenários para AWS Support usar AWS SDKs
  - Comece a usar AWS Support casos usando um AWS SDK

Ações para AWS Support usar AWS SDKs

Os exemplos de código a seguir demonstram como realizar AWS Support ações individuais com AWS SDKs. Esses trechos chamam a AWS Support API e são trechos de código de programas maiores que devem ser executados em contexto. Cada exemplo inclui um link para GitHub, onde você pode encontrar instruções para configurar e executar o código.

Os exemplos a seguir incluem apenas as ações mais utilizadas. Para obter uma lista completa, consulte a Referência de APIs do AWS Support.

Exemplos

- Use AddAttachmentsToSet com um AWS SDK ou uma ferramenta de linha de comando
- Use AddCommunicationToCase com um AWS SDK ou uma ferramenta de linha de comando
- Use CreateCase com um AWS SDK ou uma ferramenta de linha de comando
- Use DescribeAttachment com um AWS SDK ou uma ferramenta de linha de comando

- Use DescribeCases com um AWS SDK ou uma ferramenta de linha de comando
- Use DescribeCommunications com um AWS SDK ou uma ferramenta de linha de comando
- Use DescribeServices com um AWS SDK ou uma ferramenta de linha de comando
- Use DescribeSeverityLevels com um AWS SDK ou uma ferramenta de linha de comando
- Use DescribeTrustedAdvisorCheckRefreshStatuses com um AWS SDK ou uma ferramenta de linha de comando
- Use DescribeTrustedAdvisorCheckResult com um AWS SDK ou uma ferramenta de linha de comando
- Use DescribeTrustedAdvisorCheckSummaries com um AWS SDK ou uma ferramenta de linha de comando
- Use DescribeTrustedAdvisorChecks com um AWS SDK ou uma ferramenta de linha de comando
- Use RefreshTrustedAdvisorCheck com um AWS SDK ou uma ferramenta de linha de comando
- Use ResolveCase com um AWS SDK ou uma ferramenta de linha de comando

Use **`AddAttachmentsToSet`** com um AWS SDK ou uma ferramenta de linha de comando

Os exemplos de código a seguir mostram como usar`AddAttachmentsToSet`.

Exemplos de ações são trechos de código de programas maiores e devem ser executados em contexto. É possível ver essa ação no contexto no seguinte exemplo de código:

- Conceitos básicos de casos

.NET

AWS SDK for .NET

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

```
    /// <summary>
    /// Add an attachment to a set, or create a new attachment set if one does
not exist.
    /// </summary>
    /// <param name="data">The data for the attachment.</param>
    /// <param name="fileName">The file name for the attachment.</param>
    /// <param name="attachmentSetId">Optional setId for the attachment. Creates
a new attachment set if empty.</param>
    /// <returns>The setId of the attachment.</returns>
    public async Task<string> AddAttachmentToSet(MemoryStream data, string
fileName, string? attachmentSetId = null)
    {
        var response = await _amazonSupport.AddAttachmentsToSetAsync(
            new AddAttachmentsToSetRequest
            {
                AttachmentSetId = attachmentSetId,
                Attachments = new List<Attachment>
                {
                    new Attachment
                    {
                        Data = data,
                        FileName = fileName
                    }
                }
            });
        return response.AttachmentSetId;
    }
```

- Para obter detalhes da API, consulte AddAttachmentsToSeta Referência AWS SDK for .NET da API.

Java

SDK para Java 2.x

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

```
   public static String addAttachment(SupportClient supportClient, String
fileAttachment) {
       try {
           File myFile = new File(fileAttachment);
           InputStream sourceStream = new FileInputStream(myFile);
           SdkBytes sourceBytes = SdkBytes.fromInputStream(sourceStream);

           Attachment attachment = Attachment.builder()
                   .fileName(myFile.getName())
                   .data(sourceBytes)
                   .build();

           AddAttachmentsToSetRequest setRequest =
AddAttachmentsToSetRequest.builder()
                   .attachments(attachment)
                   .build();

           AddAttachmentsToSetResponse response =
supportClient.addAttachmentsToSet(setRequest);
           return response.attachmentSetId();

       } catch (SupportException | FileNotFoundException e) {
           System.out.println(e.getLocalizedMessage());
           System.exit(1);
       }
       return "";
   }
```

- Para obter detalhes da API, consulte AddAttachmentsToSeta Referência AWS SDK for Java 2.x da API.

JavaScript

SDK para JavaScript (v3)

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

```
import { AddAttachmentsToSetCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

export const main = async () => {
  try {
    // Create a new attachment set or add attachments to an existing set.
    // Provide an 'attachmentSetId' value to add attachments to an existing set.
    // Use AddCommunicationToCase or CreateCase to associate an attachment set
 with a support case.
    const response = await client.send(
      new AddAttachmentsToSetCommand({
        // You can add up to three attachments per set. The size limit is 5 MB
 per attachment.
        attachments: [
          {
            fileName: "example.txt",
            data: new TextEncoder().encode("some example text"),
          },
        ],
      }),
    );
    // Use this ID in AddCommunicationToCase or CreateCase.
    console.log(response.attachmentSetId);
    return response;
  } catch (err) {
    console.error(err);
  }
};
```

- Para obter detalhes da API, consulte AddAttachmentsToSeta Referência AWS SDK for JavaScript da API.

Kotlin

SDK for Kotlin

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

```
suspend fun addAttachment(fileAttachment: String): String? {
    val myFile = File(fileAttachment)
    val sourceBytes = (File(fileAttachment).readBytes())
    val attachmentVal = Attachment {
        fileName = myFile.name
        data = sourceBytes
    }

    val setRequest = AddAttachmentsToSetRequest {
        attachments = listOf(attachmentVal)
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.addAttachmentsToSet(setRequest)
        return response.attachmentSetId
    }
}
```

- Para obter detalhes da API, consulte a AddAttachmentsToSetreferência da API AWS SDK for Kotlin.

Python

SDK para Python (Boto3)

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def add_attachment_to_set(self):
        """
        Add an attachment to a set, or create a new attachment set if one does
 not exist.

        :return: The attachment set ID.
        """
        try:
            response = self.support_client.add_attachments_to_set(
                attachments=[
                    {
                        "fileName": "attachment_file.txt",
                        "data": b"This is a sample file for attachment to a
 support case.",
                    }
                ]
            )
            new_set_id = response["attachmentSetId"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
 Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
 subscription to run these "
```

```
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't add attachment. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return new_set_id
```

- Para obter detalhes da API, consulte a AddAttachmentsToSetReferência da API AWS SDK for Python (Boto3).

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsar o AWS Support com um SDK da AWS. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **`AddCommunicationToCase`** com um AWS SDK ou uma ferramenta de linha de comando

Os exemplos de código a seguir mostram como usar`AddCommunicationToCase`.

Exemplos de ações são trechos de código de programas maiores e devem ser executados em contexto. É possível ver essa ação no contexto no seguinte exemplo de código:

- Conceitos básicos de casos

.NET

AWS SDK for .NET

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

```
    /// <summary>
    /// Add communication to a case, including optional attachment set ID and CC
 email addresses.
    /// </summary>
    /// <param name="caseId">Id for the support case.</param>
    /// <param name="body">Body text of the communication.</param>
    /// <param name="attachmentSetId">Optional Id for an attachment set.</param>
    /// <param name="ccEmailAddresses">Optional list of CC email addresses.</
param>
    /// <returns>True if successful.</returns>
    public async Task<bool> AddCommunicationToCase(string caseId, string body,
        string? attachmentSetId = null, List<string>? ccEmailAddresses = null)
    {
        var response = await _amazonSupport.AddCommunicationToCaseAsync(
            new AddCommunicationToCaseRequest()
            {
                CaseId = caseId,
                CommunicationBody = body,
                AttachmentSetId = attachmentSetId,
                CcEmailAddresses = ccEmailAddresses
            });
        return response.Result;
    }
```

- Para obter detalhes da API, consulte AddCommunicationToCasea Referência AWS SDK for .NET da API.

Java

SDK para Java 2.x

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

```
   public static void addAttachSupportCase(SupportClient supportClient, String
caseId, String attachmentSetId) {
       try {
           AddCommunicationToCaseRequest caseRequest =
AddCommunicationToCaseRequest.builder()
                   .caseId(caseId)
                   .attachmentSetId(attachmentSetId)
                   .communicationBody("Please refer to attachment for details.")
                   .build();

           AddCommunicationToCaseResponse response =
supportClient.addCommunicationToCase(caseRequest);
           if (response.result())
               System.out.println("You have successfully added a communication
to an AWS Support case");
           else
               System.out.println("There was an error adding the communication
to an AWS Support case");

       } catch (SupportException e) {
           System.out.println(e.getLocalizedMessage());
           System.exit(1);
       }
   }
```

- Para obter detalhes da API, consulte AddCommunicationToCasea Referência AWS SDK for Java 2.x da API.

JavaScript

SDK para JavaScript (v3)

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

```
import { AddCommunicationToCaseCommand } from "@aws-sdk/client-support";
```

```
import { client } from "../libs/client.js";

export const main = async () => {
  let attachmentSetId;

  try {
    // Add a communication to a case.
    const response = await client.send(
      new AddCommunicationToCaseCommand({
        communicationBody: "Adding an attachment.",
        // Set value to an existing support case id.
        caseId: "CASE_ID",
        // Optional. Set value to an existing attachment set id to add
 attachments to the case.
        attachmentSetId,
      }),
    );
    console.log(response);
    return response;
  } catch (err) {
    console.error(err);
  }
};
```

- Para obter detalhes da API, consulte AddCommunicationToCasea Referência AWS SDK for JavaScript da API.

Kotlin

SDK for Kotlin

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

```
suspend fun addAttachSupportCase(caseIdVal: String?, attachmentSetIdVal: String?)
 {
    val caseRequest = AddCommunicationToCaseRequest {
```

```
        caseId = caseIdVal
        attachmentSetId = attachmentSetIdVal
        communicationBody = "Please refer to attachment for details."
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.addCommunicationToCase(caseRequest)
        if (response.result) {
            println("You have successfully added a communication to an AWS
 Support case")
        } else {
            println("There was an error adding the communication to an AWS
 Support case")
        }
    }
}
```

- Para obter detalhes da API, consulte a AddCommunicationToCasereferência da API AWS SDK for Kotlin.

Python

SDK para Python (Boto3)

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
```

```
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def add_communication_to_case(self, attachment_set_id, case_id):
        """
        Add a communication and an attachment set to a case.

        :param attachment_set_id: The ID of an existing attachment set.
        :param case_id: The ID of the case.
        """
        try:
            self.support_client.add_communication_to_case(
                caseId=case_id,
                communicationBody="This is an example communication added to a
support case.",
                attachmentSetId=attachment_set_id,
            )
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't add communication. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
```

- Para obter detalhes da API, consulte a AddCommunicationToCaseReferência da API AWS SDK for Python (Boto3).

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsar o AWS Support com um SDK da AWS. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use `CreateCase` com um AWS SDK ou uma ferramenta de linha de comando

Os exemplos de código a seguir mostram como usar`CreateCase`.

Exemplos de ações são trechos de código de programas maiores e devem ser executados em contexto. É possível ver essa ação no contexto no seguinte exemplo de código:

- Conceitos básicos de casos

.NET

AWS SDK for .NET

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

```
   /// <summary>
   /// Create a new support case.
   /// </summary>
   /// <param name="serviceCode">Service code for the new case.</param>
   /// <param name="categoryCode">Category for the new case.</param>
   /// <param name="severityCode">Severity code for the new case.</param>
   /// <param name="subject">Subject of the new case.</param>
   /// <param name="body">Body text of the new case.</param>
   /// <param name="language">Optional language support for your case.
   /// Currently Chinese (“zh”), English ("en"), Japanese ("ja") and Korean
(“ko”) are supported.</param>
   /// <param name="attachmentSetId">Optional Id for an attachment set for the
new case.</param>
   /// <param name="issueType">Optional issue type for the new case. Options are
"customer-service" or "technical".</param>
```

```
    /// <returns>The caseId of the new support case.</returns>
    public async Task<string> CreateCase(string serviceCode, string categoryCode,
 string severityCode, string subject,
        string body, string language = "en", string? attachmentSetId = null,
 string issueType = "customer-service")
    {
        var response = await _amazonSupport.CreateCaseAsync(
            new CreateCaseRequest()
            {
                ServiceCode = serviceCode,
                CategoryCode = categoryCode,
                SeverityCode = severityCode,
                Subject = subject,
                Language = language,
                AttachmentSetId = attachmentSetId,
                IssueType = issueType,
                CommunicationBody = body
            });
        return response.CaseId;
    }
```

- Para obter detalhes da API, consulte CreateCasea Referência AWS SDK for .NET da API.

CLI

AWS CLI

Como criar um caso

O `create-case` exemplo a seguir cria um caso de suporte para sua AWS conta.

```
aws support create-case \
    --category-code "using-aws" \
    --cc-email-addresses "myemail@example.com" \
    --communication-body "I want to learn more about an AWS service." \
    --issue-type "technical" \
    --language "en" \
    --service-code "general-info" \
    --severity-code "low" \
    --subject "Question about my account"
```

Saída:

```
{
    "caseId": "case-12345678910-2013-c4c1d2bf33c5cf47"
}
```

Para obter mais informações, consulte Case management no Guia do usuário do AWS Support.

- Para obter detalhes da API, consulte CreateCasena Referência de AWS CLI Comandos.

Java

SDK para Java 2.x

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

```
   public static String createSupportCase(SupportClient supportClient,
List<String> sevCatList, String sevLevel) {
       try {
           String serviceCode = sevCatList.get(0);
           String caseCat = sevCatList.get(1);
           CreateCaseRequest caseRequest = CreateCaseRequest.builder()
                   .categoryCode(caseCat.toLowerCase())
                   .serviceCode(serviceCode.toLowerCase())
                   .severityCode(sevLevel.toLowerCase())
                   .communicationBody("Test issue with " +
serviceCode.toLowerCase())
                   .subject("Test case, please ignore")
                   .language("en")
                   .issueType("technical")
                   .build();

           CreateCaseResponse response = supportClient.createCase(caseRequest);
           return response.caseId();

       } catch (SupportException e) {
           System.out.println(e.getLocalizedMessage());
```

```
            System.exit(1);
        }
        return "";
    }
```

- Para obter detalhes da API, consulte CreateCasea Referência AWS SDK for Java 2.x da API.

JavaScript

SDK para JavaScript (v3)

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

```
import { CreateCaseCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

export const main = async () => {
  try {
    // Create a new case and log the case id.
    // Important: This creates a real support case in your account.
    const response = await client.send(
      new CreateCaseCommand({
        // The subject line of the case.
        subject: "IGNORE: Test case",
        // Use DescribeServices to find available service codes for each service.
        serviceCode: "service-quicksight-end-user",
        // Use DescribeSecurityLevels to find available severity codes for your
 support plan.
        severityCode: "low",
        // Use DescribeServices to find available category codes for each
 service.
        categoryCode: "end-user-support",
        // The main description of the support case.
        communicationBody: "This is a test. Please ignore.",
```

```
      }),
    );
    console.log(response.caseId);
    return response;
  } catch (err) {
    console.error(err);
  }
};
```

- Para obter detalhes da API, consulte CreateCasea Referência AWS SDK for JavaScript da API.

Kotlin

SDK for Kotlin

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

```
suspend fun createSupportCase(sevCatListVal: List<String>, sevLevelVal: String):
 String? {
    val serCode = sevCatListVal[0]
    val caseCategory = sevCatListVal[1]
    val caseRequest = CreateCaseRequest {
        categoryCode = caseCategory.lowercase(Locale.getDefault())
        serviceCode = serCode.lowercase(Locale.getDefault())
        severityCode = sevLevelVal.lowercase(Locale.getDefault())
        communicationBody = "Test issue with
 ${serCode.lowercase(Locale.getDefault())}"
        subject = "Test case, please ignore"
        language = "en"
        issueType = "technical"
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.createCase(caseRequest)
        return response.caseId
```

```
    }
}
```

- Para obter detalhes da API, consulte a CreateCasereferência da API AWS SDK for Kotlin.

PowerShell

Ferramentas para PowerShell

Exemplo 1: Cria um novo caso no AWS Support Center. Os valores dos CategoryCode parâmetros - ServiceCode e - podem ser obtidos usando o cmdlet Get-asaService. O valor do SeverityCode parâmetro - pode ser obtido usando o cmdlet Get-ASASeverityLevel . O valor do IssueType parâmetro - pode ser “atendimento ao cliente” ou “técnico”. Se for bem-sucedido, o número do caso de AWS Support será exibido. Por padrão, o caso será tratado em inglês. Para usar o japonês, adicione o parâmetro -Language “ja”. Os CommunicationBody parâmetros -ServiceCode, -CategoryCode, -Assunto e - são obrigatórios.

```
New-ASACase -ServiceCode "amazon-cloudfront" -CategoryCode "APIs" -SeverityCode
 "low" -Subject "subject text" -CommunicationBody "description of the case" -
CcEmailAddress @("email1@domain.com", "email2@domain.com") -IssueType "technical"
```

- Para obter detalhes da API, consulte CreateCaseem Referência de AWS Tools for PowerShell cmdlet.

Python

SDK para Python (Boto3)

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
```

```
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def create_case(self, service, category, severity):
        """
        Create a new support case.

        :param service: The service to use for the new case.
        :param category: The category to use for the new case.
        :param severity: The severity to use for the new case.
        :return: The caseId of the new case.
        """
        try:
            response = self.support_client.create_case(
                subject="Example case for testing, ignore.",
                serviceCode=service["code"],
                severityCode=severity["code"],
                categoryCode=category["code"],
                communicationBody="Example support case body.",
                language="en",
                issueType="customer-service",
            )
            case_id = response["caseId"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
```

```
                logger.error(
                    "Couldn't create case. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return case_id
```

- Para obter detalhes da API, consulte a CreateCaseReferência da API AWS SDK for Python (Boto3).

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsar o AWS Support com um SDK da AWS. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **`DescribeAttachment`** com um AWS SDK ou uma ferramenta de linha de comando

Os exemplos de código a seguir mostram como usar`DescribeAttachment`.

Exemplos de ações são trechos de código de programas maiores e devem ser executados em contexto. É possível ver essa ação no contexto no seguinte exemplo de código:

- Conceitos básicos de casos

.NET

AWS SDK for .NET

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

```
    /// <summary>
    /// Get description of a specific attachment.
    /// </summary>
    /// <param name="attachmentId">Id of the attachment, usually fetched by
 describing the communications of a case.</param>
    /// <returns>The attachment object.</returns>
    public async Task<Attachment> DescribeAttachment(string attachmentId)
    {
        var response = await _amazonSupport.DescribeAttachmentAsync(
            new DescribeAttachmentRequest()
            {
                AttachmentId = attachmentId
            });
        return response.Attachment;
    }
```

- Para obter detalhes da API, consulte DescribeAttachmenta Referência AWS SDK for .NET da API.

CLI

AWS CLI

Como descrever um anexo

O exemplo de `describe-attachment` a seguir retorna informações sobre o anexo com o ID especificado.

```
aws support describe-attachment \
    --attachment-id "attachment-KBnjRNrePd9D6Jx0-Mm00xZuDEaL2JAj_0-
gJv9qqDooTipsz3V1Nb19rCfkZneeQeDPgp8X1iVJyHH7UuhZDdNeqGoduZsPrAhyMakqlc60-
iJjL5HqyYGiT1FG8EXAMPLE"
```

Saída:

```
{
    "attachment": {
        "fileName": "troubleshoot-screenshot.png",
        "data": "base64-blob"
```

```
    }
}
```

Para obter mais informações, consulte Case management no Guia do usuário do AWS Support.

- Para obter detalhes da API, consulte DescribeAttachmentna Referência de AWS CLI Comandos.

Java

SDK para Java 2.x

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

```
   public static void describeAttachment(SupportClient supportClient, String
attachId) {
       try {
           DescribeAttachmentRequest attachmentRequest =
DescribeAttachmentRequest.builder()
                   .attachmentId(attachId)
                   .build();

           DescribeAttachmentResponse response =
supportClient.describeAttachment(attachmentRequest);
           System.out.println("The name of the file is " +
response.attachment().fileName());

       } catch (SupportException e) {
           System.out.println(e.getLocalizedMessage());
           System.exit(1);
       }
   }
```

- Para obter detalhes da API, consulte DescribeAttachmenta Referência AWS SDK for Java 2.x da API.

JavaScript

SDK para JavaScript (v3)

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

```
import { DescribeAttachmentCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

export const main = async () => {
  try {
    // Get the metadata and content of an attachment.
    const response = await client.send(
      new DescribeAttachmentCommand({
        // Set value to an existing attachment id.
        // Use DescribeCommunications or DescribeCases to find an attachment id.
        attachmentId: "ATTACHMENT_ID",
      }),
    );
    console.log(response.attachment?.fileName);
    return response;
  } catch (err) {
    console.error(err);
  }
};
```

- Para obter detalhes da API, consulte DescribeAttachmenta Referência AWS SDK for JavaScript da API.

Kotlin

SDK for Kotlin

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

```
suspend fun describeAttachment(attachId: String?) {
    val attachmentRequest = DescribeAttachmentRequest {
        attachmentId = attachId
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeAttachment(attachmentRequest)
        println("The name of the file is ${response.attachment?.fileName}")
    }
}
```

- Para obter detalhes da API, consulte a DescribeAttachmentreferência da API AWS SDK for Kotlin.

Python

SDK para Python (Boto3)

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
```

```
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def describe_attachment(self, attachment_id):
        """
        Get information about an attachment by its attachmentID.

        :param attachment_id: The ID of the attachment.
        :return: The name of the attached file.
        """
        try:
            response = self.support_client.describe_attachment(
                attachmentId=attachment_id
            )
            attached_file = response["attachment"]["fileName"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't get attachment description. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return attached_file
```

- Para obter detalhes da API, consulte a DescribeAttachmentReferência da API AWS SDK for Python (Boto3).

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsar o AWS Support com um SDK da AWS. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use `DescribeCases` com um AWS SDK ou uma ferramenta de linha de comando

Os exemplos de código a seguir mostram como usar`DescribeCases`.

Exemplos de ações são trechos de código de programas maiores e devem ser executados em contexto. É possível ver essa ação no contexto no seguinte exemplo de código:

- Conceitos básicos de casos

.NET

AWS SDK for .NET

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

```
    /// <summary>
    /// Get case details for a list of case ids, optionally with date filters.
    /// </summary>
    /// <param name="caseIds">The list of case IDs.</param>
    /// <param name="displayId">Optional display ID.</param>
    /// <param name="includeCommunication">True to include communication.
Defaults to true.</param>
    /// <param name="includeResolvedCases">True to include resolved cases.
Defaults to false.</param>
```

```
    /// <param name="afterTime">The optional start date for a filtered search.</
param>
    /// <param name="beforeTime">The optional end date for a filtered search.</
param>
    /// <param name="language">Optional language support for your case.
    /// Currently Chinese (“zh”), English ("en"), Japanese ("ja") and Korean
 (“ko”) are supported.</param>
    /// <returns>A list of CaseDetails.</returns>
    public async Task<List<CaseDetails>> DescribeCases(List<string> caseIds,
 string? displayId = null, bool includeCommunication = true,
        bool includeResolvedCases = false, DateTime? afterTime = null, DateTime?
 beforeTime = null,
        string language = "en")
    {
        var results = new List<CaseDetails>();
        var paginateCases = _amazonSupport.Paginators.DescribeCases(
            new DescribeCasesRequest()
            {
                CaseIdList = caseIds,
                DisplayId = displayId,
                IncludeCommunications = includeCommunication,
                IncludeResolvedCases = includeResolvedCases,
                AfterTime = afterTime?.ToString("s"),
                BeforeTime = beforeTime?.ToString("s"),
                Language = language
            });
        // Get the entire list using the paginator.
        await foreach (var cases in paginateCases.Cases)
        {
            results.Add(cases);
        }
        return results;
    }
```

- Para obter detalhes da API, consulte DescribeCasesa Referência AWS SDK for .NET da API.

CLI

AWS CLI

Como descrever um caso

O `describe-cases` exemplo a seguir retorna informações sobre o caso de suporte especificado em sua AWS conta.

```
aws support describe-cases \
    --display-id "1234567890" \
    --after-time "2020-03-23T21:31:47.774Z" \
    --include-resolved-cases \
    --language "en" \
    --no-include-communications \
    --max-item 1
```

Saída:

```
{
    "cases": [
        {
            "status": "resolved",
            "ccEmailAddresses": [],
            "timeCreated": "2020-03-23T21:31:47.774Z",
            "caseId": "case-12345678910-2013-c4c1d2bf33c5cf47",
            "severityCode": "low",
            "language": "en",
            "categoryCode": "using-aws",
            "serviceCode": "general-info",
            "submittedBy": "myemail@example.com",
            "displayId": "1234567890",
            "subject": "Question about my account"
        }
    ]
}
```

Para obter mais informações, consulte Case management no Guia do usuário do AWS Support.

- Para obter detalhes da API, consulte DescribeCasesna Referência de AWS CLI Comandos.

Java

SDK para Java 2.x

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

```
   public static void getOpenCase(SupportClient supportClient) {
       try {
           // Specify the start and end time.
           Instant now = Instant.now();
           java.time.LocalDate.now();
           Instant yesterday = now.minus(1, ChronoUnit.DAYS);

           DescribeCasesRequest describeCasesRequest =
DescribeCasesRequest.builder()
                   .maxResults(20)
                   .afterTime(yesterday.toString())
                   .beforeTime(now.toString())
                   .build();

           DescribeCasesResponse response =
supportClient.describeCases(describeCasesRequest);
           List<CaseDetails> cases = response.cases();
           for (CaseDetails sinCase : cases) {
               System.out.println("The case status is " + sinCase.status());
               System.out.println("The case Id is " + sinCase.caseId());
               System.out.println("The case subject is " + sinCase.subject());
           }

       } catch (SupportException e) {
           System.out.println(e.getLocalizedMessage());
           System.exit(1);
       }
   }
```

- Para obter detalhes da API, consulte DescribeCasesa Referência AWS SDK for Java 2.x da API.

JavaScript

SDK para JavaScript (v3)

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

```
import { DescribeCasesCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

export const main = async () => {
  try {
    // Get all of the unresolved cases in your account.
    // Filter or expand results by providing parameters to the
 DescribeCasesCommand. Refer
    // to the TypeScript definition and the API doc for more information on
 possible parameters.
    // https://docs.aws.amazon.com/AWSJavaScriptSDK/v3/latest/clients/client-
support/interfaces/describecasescommandinput.html
    const response = await client.send(new DescribeCasesCommand({}));
    const caseIds = response.cases.map((supportCase) => supportCase.caseId);
    console.log(caseIds);
    return response;
  } catch (err) {
    console.error(err);
  }
};
```

- Para obter detalhes da API, consulte DescribeCasesa Referência AWS SDK for JavaScript da API.

Kotlin

SDK for Kotlin

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

```
suspend fun getOpenCase() {
    // Specify the start and end time.
    val now = Instant.now()
    LocalDate.now()
    val yesterday = now.minus(1, ChronoUnit.DAYS)
    val describeCasesRequest = DescribeCasesRequest {
        maxResults = 20
        afterTime = yesterday.toString()
        beforeTime = now.toString()
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeCases(describeCasesRequest)
        response.cases?.forEach { sinCase ->
            println("The case status is ${sinCase.status}")
            println("The case Id is ${sinCase.caseId}")
            println("The case subject is ${sinCase.subject}")
        }
    }
}
```

- Para obter detalhes da API, consulte a DescribeCasesreferência da API AWS SDK for Kotlin.

PowerShell

Ferramentas para PowerShell

Exemplo 1: retorna os detalhes de todos os casos de suporte.

```
Get-ASACase
```

Exemplo 2: retorna os detalhes de todos os casos de suporte desde a data e a hora especificadas.

```
Get-ASACase -AfterTime "2013-09-10T03:06Z"
```

Exemplo 3: retorna os detalhes dos primeiros 10 casos de suporte, incluindo aqueles que foram resolvidos.

```
Get-ASACase -MaxResult 10 -IncludeResolvedCases $true
```

Exemplo 4: retorna os detalhes do único caso de suporte especificado.

```
Get-ASACase -CaseIdList "case-12345678910-2013-c4c1d2bf33c5cf47"
```

Exemplo 5: retorna os detalhes dos casos de suporte especificados.

```
Get-ASACase -CaseIdList @("case-12345678910-2013-c4c1d2bf33c5cf47",
 "case-18929034710-2011-c4fdeabf33c5cf47")
```

Exemplo 6: retorna todos os casos de suporte usando paginação manual. As caixas são recuperadas em lotes de 20.

```
$nextToken = $null
do {
  Get-ASACase -NextToken $nextToken -MaxResult 20
  $nextToken = $AWSHistory.LastServiceResponse.NextToken
} while ($nextToken -ne $null)
```

- Para obter detalhes da API, consulte DescribeCasesem Referência de AWS Tools for PowerShell cmdlet.

Python

SDK para Python (Boto3)

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def describe_cases(self, after_time, before_time, resolved):
        """
        Describe support cases over a period of time, optionally filtering
        by status.

        :param after_time: The start time to include for cases.
        :param before_time: The end time to include for cases.
        :param resolved: True to include resolved cases in the results,
            otherwise results are open cases.
        :return: The final status of the case.
        """
        try:
            cases = []
            paginator = self.support_client.get_paginator("describe_cases")
```

```
            for page in paginator.paginate(
                afterTime=after_time,
                beforeTime=before_time,
                includeResolvedCases=resolved,
                language="en",
            ):
                cases += page["cases"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't describe cases. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            if resolved:
                cases = filter(lambda case: case["status"] == "resolved", cases)
            return cases
```

- Para obter detalhes da API, consulte a DescribeCasesReferência da API AWS SDK for Python (Boto3).

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsar o AWS Support com um SDK da AWS. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **`DescribeCommunications`** com um AWS SDK ou uma ferramenta de linha de comando

Os exemplos de código a seguir mostram como usar`DescribeCommunications`.

Exemplos de ações são trechos de código de programas maiores e devem ser executados em contexto. É possível ver essa ação no contexto no seguinte exemplo de código:

- Conceitos básicos de casos

.NET

AWS SDK for .NET

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

```
    /// <summary>
    /// Describe the communications for a case, optionally with a date filter.
    /// </summary>
    /// <param name="caseId">The ID of the support case.</param>
    /// <param name="afterTime">The optional start date for a filtered search.</
param>
    /// <param name="beforeTime">The optional end date for a filtered search.</
param>
    /// <returns>The list of communications for the case.</returns>
    public async Task<List<Communication>> DescribeCommunications(string caseId,
 DateTime? afterTime = null, DateTime? beforeTime = null)
    {
        var results = new List<Communication>();
        var paginateCommunications =
 _amazonSupport.Paginators.DescribeCommunications(
            new DescribeCommunicationsRequest()
            {
                CaseId = caseId,
                AfterTime = afterTime?.ToString("s"),
                BeforeTime = beforeTime?.ToString("s")
            });
        // Get the entire list using the paginator.
        await foreach (var communications in
 paginateCommunications.Communications)
        {
```

```
            results.Add(communications);
        }
        return results;
    }
```

- Para obter detalhes da API, consulte DescribeCommunicationsa Referência AWS SDK for .NET da API.

CLI

AWS CLI

Como descrever a comunicação mais recente de um caso

O `describe-communications` exemplo a seguir retorna a comunicação mais recente para o caso de suporte especificado em sua AWS conta.

```
aws support describe-communications \
    --case-id "case-12345678910-2013-c4c1d2bf33c5cf47" \
    --after-time "2020-03-23T21:31:47.774Z" \
    --max-item 1
```

Saída:

```
{
    "communications": [
        {
            "body": "I want to learn more about an AWS service.",
            "attachmentSet": [],
            "caseId": "case-12345678910-2013-c4c1d2bf33c5cf47",
            "timeCreated": "2020-05-12T23:12:35.000Z",
            "submittedBy": "Amazon Web Services"
        }
    ],
    "NextToken":
 "eyJuZXh0VG9rZW4iOiBudWxsLCAiYm90b190cnVuY2F0ZV9hbW91bnQEXAMPLE=="
}
```

Para obter mais informações, consulte Case management no Guia do usuário do AWS Support.

- Para obter detalhes da API, consulte DescribeCommunicationsna Referência de AWS CLI Comandos.

Java

SDK para Java 2.x

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

```
   public static String listCommunications(SupportClient supportClient, String
caseId) {
       try {
           String attachId = null;
           DescribeCommunicationsRequest communicationsRequest =
DescribeCommunicationsRequest.builder()
                   .caseId(caseId)
                   .maxResults(10)
                   .build();

           DescribeCommunicationsResponse response =
supportClient.describeCommunications(communicationsRequest);
           List<Communication> communications = response.communications();
           for (Communication comm : communications) {
               System.out.println("the body is: " + comm.body());

               // Get the attachment id value.
               List<AttachmentDetails> attachments = comm.attachmentSet();
               for (AttachmentDetails detail : attachments) {
                   attachId = detail.attachmentId();
               }
           }
           return attachId;

       } catch (SupportException e) {
           System.out.println(e.getLocalizedMessage());
           System.exit(1);
       }
```

```
        return "";
    }
```

- Para obter detalhes da API, consulte DescribeCommunicationsa Referência AWS SDK for Java 2.x da API.

JavaScript

SDK para JavaScript (v3)

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

```
import { DescribeCommunicationsCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

export const main = async () => {
  try {
    // Get all communications for the support case.
    // Filter results by providing parameters to the
 DescribeCommunicationsCommand. Refer
    // to the TypeScript definition and the API doc for more information on
 possible parameters.
    // https://docs.aws.amazon.com/AWSJavaScriptSDK/v3/latest/clients/client-
support/interfaces/describecommunicationscommandinput.html
    const response = await client.send(
      new DescribeCommunicationsCommand({
        // Set value to an existing case id.
        caseId: "CASE_ID",
      }),
    );
    const text = response.communications.map((item) => item.body).join("\n");
    console.log(text);
    return response;
  } catch (err) {
    console.error(err);
```

```
  }
};
```

- Para obter detalhes da API, consulte DescribeCommunicationsa Referência AWS SDK for JavaScript da API.

Kotlin

SDK for Kotlin

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

```
suspend fun listCommunications(caseIdVal: String?): String? {
    val communicationsRequest = DescribeCommunicationsRequest {
        caseId = caseIdVal
        maxResults = 10
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response =
 supportClient.describeCommunications(communicationsRequest)
        response.communications?.forEach { comm ->
            println("the body is: " + comm.body)
            comm.attachmentSet?.forEach { detail ->
                return detail.attachmentId
            }
        }
    }
    return ""
}
```

- Para obter detalhes da API, consulte a DescribeCommunicationsreferência da API AWS SDK for Kotlin.

PowerShell

Ferramentas para PowerShell

Exemplo 1: Retorna todas as comunicações do caso especificado.

```
Get-ASACommunication -CaseId "case-12345678910-2013-c4c1d2bf33c5cf47"
```

Exemplo 2: retorna todas as comunicações desde a meia-noite UTC de 1º de janeiro de 2012 para o caso especificado.

```
Get-ASACommunication -CaseId "case-12345678910-2013-c4c1d2bf33c5cf47" -AfterTime
 "2012-01-10T00:00Z"
```

Exemplo 3: retorna todas as comunicações desde a meia-noite UTC de 1º de janeiro de 2012 para o caso especificado, usando paginação manual. As comunicações são recuperadas em lotes de 20.

```
$nextToken = $null
do {
  Get-ASACommunication -CaseId "case-12345678910-2013-c4c1d2bf33c5cf47" -
NextToken $nextToken -MaxResult 20
  $nextToken = $AWSHistory.LastServiceResponse.NextToken
} while ($nextToken -ne $null)
```

- Para obter detalhes da API, consulte DescribeCommunicationsem Referência de AWS Tools for PowerShell cmdlet.

Python

SDK para Python (Boto3)

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

```
class SupportWrapper:
    """Encapsulates Support actions."""
```

```
    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def describe_all_case_communications(self, case_id):
        """
        Describe all the communications for a case using a paginator.

        :param case_id: The ID of the case.
        :return: The communications for the case.
        """
        try:
            communications = []
            paginator =
self.support_client.get_paginator("describe_communications")
            for page in paginator.paginate(caseId=case_id):
                communications += page["communications"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't describe communications. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
```

```
                raise
        else:
            return communications
```

- Para obter detalhes da API, consulte a DescribeCommunicationsReferência da API AWS SDK for Python (Boto3).

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsar o AWS Support com um SDK da AWS. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **`DescribeServices`** com um AWS SDK ou uma ferramenta de linha de comando

Os exemplos de código a seguir mostram como usar`DescribeServices`.

Exemplos de ações são trechos de código de programas maiores e devem ser executados em contexto. É possível ver essa ação no contexto no seguinte exemplo de código:

- Conceitos básicos de casos

.NET

AWS SDK for .NET

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

```
/// <summary>
/// Get the descriptions of AWS services.
/// </summary>
/// <param name="name">Optional language for services.
```

```
    /// Currently Chinese (“zh”), English ("en"), Japanese ("ja") and Korean
 (“ko”) are supported.</param>
    /// <returns>The list of AWS service descriptions.</returns>
    public async Task<List<Service>> DescribeServices(string language = "en")
    {
        var response = await _amazonSupport.DescribeServicesAsync(
            new DescribeServicesRequest()
            {
                Language = language
            });
        return response.Services;
    }
```

- Para obter detalhes da API, consulte DescribeServicesa Referência AWS SDK for .NET da API.

CLI

AWS CLI

Para listar AWS serviços e categorias de serviços

O exemplo de `describe-services` a seguir lista as categorias de serviço disponíveis para a solicitação de informações gerais.

```
aws support describe-services \
    --service-code-list "general-info"
```

Saída:

```
{
    "services": [
        {
            "code": "general-info",
            "name": "General Info and Getting Started",
            "categories": [
                {
                    "code": "charges",
                    "name": "How Will I Be Charged?"
```

```
                },
                {
                    "code": "gdpr-queries",
                    "name": "Data Privacy Query"
                },
                {
                    "code": "reserved-instances",
                    "name": "Reserved Instances"
                },
                {
                    "code": "resource",
                    "name": "Where is my Resource?"
                },
                {
                    "code": "using-aws",
                    "name": "Using AWS & Services"
                },
                {
                    "code": "free-tier",
                    "name": "Free Tier"
                },
                {
                    "code": "security-and-compliance",
                    "name": "Security & Compliance"
                },
                {
                    "code": "account-structure",
                    "name": "Account Structure"
                }
            ]
        }
    ]
}
```

Para obter mais informações, consulte Case management no Guia do usuário do AWS Support.

- Para obter detalhes da API, consulte DescribeServicesna Referência de AWS CLI Comandos.

Java

SDK para Java 2.x

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

```
   // Return a List that contains a Service name and Category name.
   public static List<String> displayServices(SupportClient supportClient) {
       try {
           DescribeServicesRequest servicesRequest =
DescribeServicesRequest.builder()
                   .language("en")
                   .build();

           DescribeServicesResponse response =
supportClient.describeServices(servicesRequest);
           String serviceCode = null;
           String catName = null;
           List<String> sevCatList = new ArrayList<>();
           List<Service> services = response.services();

           System.out.println("Get the first 10 services");
           int index = 1;
           for (Service service : services) {
               if (index == 11)
                   break;

               System.out.println("The Service name is: " + service.name());
               if (service.name().compareTo("Account") == 0)
                   serviceCode = service.code();

               // Get the Categories for this service.
               List<Category> categories = service.categories();
               for (Category cat : categories) {
                   System.out.println("The category name is: " + cat.name());
                   if (cat.name().compareTo("Security") == 0)
                       catName = cat.name();
               }
```

```
                index++;
            }

            // Push the two values to the list.
            sevCatList.add(serviceCode);
            sevCatList.add(catName);
            return sevCatList;

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return null;
    }
```

- Para obter detalhes da API, consulte DescribeServicesa Referência AWS SDK for Java 2.x da API.

Kotlin

SDK for Kotlin

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

```
// Return a List that contains a Service name and Category name.
suspend fun displayServices(): List<String> {
    var serviceCode = ""
    var catName = ""
    val sevCatList = mutableListOf<String>()
    val servicesRequest = DescribeServicesRequest {
        language = "en"
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeServices(servicesRequest)
        println("Get the first 10 services")
```

```
        var index = 1

        response.services?.forEach { service ->
            if (index == 11) {
                return@forEach
            }

            println("The Service name is ${service.name}")
            if (service.name == "Account") {
                serviceCode = service.code.toString()
            }

            // Get the categories for this service.
            service.categories?.forEach { cat ->
                println("The category name is ${cat.name}")
                if (cat.name == "Security") {
                    catName = cat.name!!
                }
            }
            index++
        }
    }

    // Push the two values to the list.
    serviceCode.let { sevCatList.add(it) }
    catName.let { sevCatList.add(it) }
    return sevCatList
}
```

- Para obter detalhes da API, consulte a DescribeServicesreferência da API AWS SDK for Kotlin.

PowerShell

Ferramentas para PowerShell

Exemplo 1: Retorna todos os códigos de serviço, nomes e categorias disponíveis.

```
Get-ASAService
```

Exemplo 2: retorna o nome e as categorias do serviço com o código especificado.

```
Get-ASAService -ServiceCodeList "amazon-cloudfront"
```

Exemplo 3: Retorna o nome e as categorias dos códigos de serviço especificados.

```
Get-ASAService -ServiceCodeList @("amazon-cloudfront", "amazon-cloudwatch")
```

Exemplo 4: retorna o nome e as categorias (em japonês) dos códigos de serviço especificados. Atualmente, os códigos de idioma inglês (“en”) e japonês (“ja”) são suportados.

```
Get-ASAService -ServiceCodeList @("amazon-cloudfront", "amazon-cloudwatch") -
Language "ja"
```

- Para obter detalhes da API, consulte DescribeServicesem Referência de AWS Tools for PowerShell cmdlet.

Python

SDK para Python (Boto3)

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
```

```
        support_client = boto3.client("support")
        return cls(support_client)


    def describe_services(self, language):
        """
        Get the descriptions of AWS services available for support for a
language.

        :param language: The language for support services.
        Currently, only "en" (English) and "ja" (Japanese) are supported.
        :return: The list of AWS service descriptions.
        """
        try:
            response = self.support_client.describe_services(language=language)
            services = response["services"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't get Support services for language %s. Here's why:
%s: %s",
                    language,
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return services
```

- Para obter detalhes da API, consulte a DescribeServicesReferência da API AWS SDK for Python (Boto3).

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsar o AWS Support com um SDK da AWS. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **`DescribeSeverityLevels`** com um AWS SDK ou uma ferramenta de linha de comando

Os exemplos de código a seguir mostram como usar`DescribeSeverityLevels`.

Exemplos de ações são trechos de código de programas maiores e devem ser executados em contexto. É possível ver essa ação no contexto no seguinte exemplo de código:

- Conceitos básicos de casos

.NET

AWS SDK for .NET

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

```
   /// <summary>
   /// Get the descriptions of support severity levels.
   /// </summary>
   /// <param name="name">Optional language for severity levels.
   /// Currently Chinese (“zh”), English ("en"), Japanese ("ja") and Korean
(“ko”) are supported.</param>
   /// <returns>The list of support severity levels.</returns>
   public async Task<List<SeverityLevel>> DescribeSeverityLevels(string language
= "en")
   {
       var response = await _amazonSupport.DescribeSeverityLevelsAsync(
           new DescribeSeverityLevelsRequest()
           {
               Language = language
           });
```

```
        return response.SeverityLevels;
    }
```

- Para obter detalhes da API, consulte DescribeSeverityLevelsa Referência AWS SDK for .NET da API.

CLI

AWS CLI

Como listar os níveis de gravidade disponíveis

O exemplo de `describe-severity-levels` a seguir lista os níveis de gravidade disponíveis para um caso de suporte.

```
aws support describe-severity-levels
```

Saída:

```
{
    "severityLevels": [
        {
            "code": "low",
            "name": "Low"
        },
        {
            "code": "normal",
            "name": "Normal"
        },
        {
            "code": "high",
            "name": "High"
        },
        {
            "code": "urgent",
            "name": "Urgent"
        },
        {
            "code": "critical",
```

```
            "name": "Critical"
        }
    ]
}
```

Para obter mais informações, consulte Choosing a severity no Guia do usuário do AWS Support.

- Para obter detalhes da API, consulte DescribeSeverityLevelsna Referência de AWS CLI Comandos.

Java

SDK para Java 2.x

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

```
   public static String displaySevLevels(SupportClient supportClient) {
       try {
           DescribeSeverityLevelsRequest severityLevelsRequest =
DescribeSeverityLevelsRequest.builder()
                   .language("en")
                   .build();

           DescribeSeverityLevelsResponse response =
supportClient.describeSeverityLevels(severityLevelsRequest);
           List<SeverityLevel> severityLevels = response.severityLevels();
           String levelName = null;
           for (SeverityLevel sevLevel : severityLevels) {
               System.out.println("The severity level name is: " +
sevLevel.name());
               if (sevLevel.name().compareTo("High") == 0)
                   levelName = sevLevel.name();
           }
           return levelName;

       } catch (SupportException e) {
```

```
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return "";
    }
```

- Para obter detalhes da API, consulte DescribeSeverityLevelsa Referência AWS SDK for Java 2.x da API.

JavaScript

SDK para JavaScript (v3)

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

```
import { DescribeSeverityLevelsCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

export const main = async () => {
  try {
    // Get the list of severity levels.
    // The available values depend on the support plan for the account.
    const response = await client.send(new DescribeSeverityLevelsCommand({}));
    console.log(response.severityLevels);
    return response;
  } catch (err) {
    console.error(err);
  }
};
```

- Para obter detalhes da API, consulte DescribeSeverityLevelsa Referência AWS SDK for JavaScript da API.

Kotlin

SDK for Kotlin

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

```
suspend fun displaySevLevels(): String {
    var levelName = ""
    val severityLevelsRequest = DescribeSeverityLevelsRequest {
        language = "en"
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response =
 supportClient.describeSeverityLevels(severityLevelsRequest)
        response.severityLevels?.forEach { sevLevel ->
            println("The severity level name is: ${sevLevel.name}")
            if (sevLevel.name == "High") {
                levelName = sevLevel.name!!
            }
        }
        return levelName
    }
}
```

- Para obter detalhes da API, consulte a DescribeSeverityLevelsreferência da API AWS SDK for Kotlin.

PowerShell

Ferramentas para PowerShell

Exemplo 1: Retorna a lista de níveis de severidade que podem ser atribuídos a um caso de AWS Support.

```
Get-ASASeverityLevel
```

Exemplo 2: Retorna a lista de níveis de severidade que podem ser atribuídos a um caso de AWS Support. Os nomes dos níveis são retornados em japonês.

```
Get-ASASeverityLevel -Language "ja"
```

- Para obter detalhes da API, consulte DescribeSeverityLevelsem Referência de AWS Tools for PowerShell cmdlet.

Python

SDK para Python (Boto3)

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def describe_severity_levels(self, language):
        """
```

```
        Get the descriptions of available severity levels for support cases for a
language.

        :param language: The language for support severity levels.
        Currently, only "en" (English) and "ja" (Japanese) are supported.
        :return: The list of severity levels.
        """
        try:
            response =
self.support_client.describe_severity_levels(language=language)
            severity_levels = response["severityLevels"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't get severity levels for language %s. Here's why:
%s: %s",
                    language,
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return severity_levels
```

- Para obter detalhes da API, consulte a DescribeSeverityLevelsReferência da API AWS SDK for Python (Boto3).

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsar o AWS Support com um SDK da AWS. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **DescribeTrustedAdvisorCheckRefreshStatuses** com um AWS SDK ou uma ferramenta de linha de comando

Os exemplos de código a seguir mostram como usar`DescribeTrustedAdvisorCheckRefreshStatuses`.

CLI

AWS CLI

Para listar os status de atualização das verificações do AWS Trusted Advisor

O `describe-trusted-advisor-check-refresh-statuses` exemplo a seguir lista os status de atualização de duas verificações do Trusted Advisor: Amazon S3 Bucket Permissions e IAM Use.

```
aws support describe-trusted-advisor-check-refresh-statuses \
    --check-id "Pfx0RwqBli" "zXCkfM1nI3"
```

Saída:

```
{
    "statuses": [
        {
            "checkId": "Pfx0RwqBli",
            "status": "none",
            "millisUntilNextRefreshable": 0
        },
        {
            "checkId": "zXCkfM1nI3",
            "status": "none",
            "millisUntilNextRefreshable": 0
        }
    ]
}
```

Para obter mais informações, consulte AWS Trusted Advisor no AWS Support User Guide.

- Para obter detalhes da API, consulte DescribeTrustedAdvisorCheckRefreshStatusesna Referência de AWS CLI Comandos.

PowerShell

Ferramentas para PowerShell

Exemplo 1: retorna o status atual das solicitações de atualização para as verificações especificadas. O Request-ASA TrustedAdvisorCheckRefresh pode ser usado para solicitar que as informações de status das verificações sejam atualizadas.

```
Get-ASATrustedAdvisorCheckRefreshStatus -CheckId @("checkid1", "checkid2")
```

- Para obter detalhes da API, consulte DescribeTrustedAdvisorCheckRefreshStatusesem Referência de AWS Tools for PowerShell cmdlet.

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsar o AWS Support com um SDK da AWS. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **`DescribeTrustedAdvisorCheckResult`** com um AWS SDK ou uma ferramenta de linha de comando

Os exemplos de código a seguir mostram como usar`DescribeTrustedAdvisorCheckResult`.

CLI

AWS CLI

Para listar os resultados de uma verificação do AWS Trusted Advisor

O `describe-trusted-advisor-check-result` exemplo a seguir lista os resultados da verificação de uso do IAM.

```
aws support describe-trusted-advisor-check-result \
    --check-id "zXCkfM1nI3"
```

Saída:

```
{
    "result": {
        "checkId": "zXCkfM1nI3",
        "timestamp": "2020-05-13T21:38:05Z",
```

```
        "status": "ok",
        "resourcesSummary": {
            "resourcesProcessed": 1,
            "resourcesFlagged": 0,
            "resourcesIgnored": 0,
            "resourcesSuppressed": 0
        },
        "categorySpecificSummary": {
            "costOptimizing": {
                "estimatedMonthlySavings": 0.0,
                "estimatedPercentMonthlySavings": 0.0
            }
        },
        "flaggedResources": [
            {
                "status": "ok",
                "resourceId": "47DEQpj8HBSa-_TImW-5JCeuQeRkm5NMpJWZEXAMPLE",
                "isSuppressed": false
            }
        ]
    }
}
```

Para obter mais informações, consulte AWS Trusted Advisor no AWS Support User Guide.

- Para obter detalhes da API, consulte DescribeTrustedAdvisorCheckResultna Referência de AWS CLI Comandos.

PowerShell

Ferramentas para PowerShell

Exemplo 1: Retorna os resultados de uma verificação do Trusted Advisor. A lista de verificações disponíveis do Trusted Advisor pode ser obtida usando o TrustedAdvisorChecks Get-ASA. A saída é o status geral da verificação, a data e hora em que a verificação foi executada pela última vez e o ID de verificação exclusivo da verificação específica. Para que os resultados sejam exibidos em japonês, adicione o parâmetro -Language “ja”.

```
Get-ASATrustedAdvisorCheckResult -CheckId "checkid1"
```

- Para obter detalhes da API, consulte DescribeTrustedAdvisorCheckResultem Referência de AWS Tools for PowerShell cmdlet.

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsar o AWS Support com um SDK da AWS. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **`DescribeTrustedAdvisorCheckSummaries`** com um AWS SDK ou uma ferramenta de linha de comando

Os exemplos de código a seguir mostram como usar`DescribeTrustedAdvisorCheckSummaries`.

CLI

AWS CLI

Para listar os resumos das verificações do AWS Trusted Advisor

O `describe-trusted-advisor-check-summaries` exemplo a seguir lista os resultados de duas verificações do Trusted Advisor: Amazon S3 Bucket Permissions e IAM Use.

```
aws support describe-trusted-advisor-check-summaries \
    --check-ids "Pfx0RwqBli" "zXCkfM1nI3"
```

Saída:

```
{
    "summaries": [
        {
            "checkId": "Pfx0RwqBli",
            "timestamp": "2020-05-13T21:38:12Z",
            "status": "ok",
            "hasFlaggedResources": true,
            "resourcesSummary": {
                "resourcesProcessed": 44,
                "resourcesFlagged": 0,
                "resourcesIgnored": 0,
                "resourcesSuppressed": 0
            },
            "categorySpecificSummary": {
                "costOptimizing": {
                    "estimatedMonthlySavings": 0.0,
                    "estimatedPercentMonthlySavings": 0.0
```

```
                }
            }
        },
        {
            "checkId": "zXCkfM1nI3",
            "timestamp": "2020-05-13T21:38:05Z",
            "status": "ok",
            "hasFlaggedResources": true,
            "resourcesSummary": {
                "resourcesProcessed": 1,
                "resourcesFlagged": 0,
                "resourcesIgnored": 0,
                "resourcesSuppressed": 0
            },
            "categorySpecificSummary": {
                "costOptimizing": {
                    "estimatedMonthlySavings": 0.0,
                    "estimatedPercentMonthlySavings": 0.0
                }
            }
        }
    ]
}
```

Para obter mais informações, consulte AWS Trusted Advisor no AWS Support User Guide.

- Para obter detalhes da API, consulte DescribeTrustedAdvisorCheckSummariesna Referência de AWS CLI Comandos.

PowerShell

Ferramentas para PowerShell

Exemplo 1: Retorna o resumo mais recente da verificação especificada do Trusted Advisor.

```
Get-ASATrustedAdvisorCheckSummary -CheckId "checkid1"
```

Exemplo 2: Retorna os resumos mais recentes das verificações especificadas do Trusted Advisor.

```
Get-ASATrustedAdvisorCheckSummary -CheckId @("checkid1", "checkid2")
```

- Para obter detalhes da API, consulte DescribeTrustedAdvisorCheckSummariesem Referência de AWS Tools for PowerShell cmdlet.

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsar o AWS Support com um SDK da AWS. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **`DescribeTrustedAdvisorChecks`** com um AWS SDK ou uma ferramenta de linha de comando

Os exemplos de código a seguir mostram como usar`DescribeTrustedAdvisorChecks`.

CLI

AWS CLI

Para listar as verificações disponíveis do AWS Trusted Advisor

O `describe-trusted-advisor-checks` exemplo a seguir lista os cheques do Trusted Advisor disponíveis em sua AWS conta. Essas informações incluem o nome, ID, descrição, categoria e metadados do cheque. Observe que a saída é reduzida para facilitar a leitura.

```
aws support describe-trusted-advisor-checks \
    --language "en"
```

Saída:

```
{
    "checks": [
        {
            "id": "zXCkfM1nI3",
            "name": "IAM Use",
            "description": "Checks for your use of AWS Identity and Access
 Management (IAM). You can use IAM to create users, groups, and roles in
 AWS, and you can use permissions to control access to AWS resources. \n<br>
\n<br>\n<b>Alert Criteria</b><br>\nYellow: No IAM users have been created
 for this account.\n<br>\n<br>\n<b>Recommended Action</b><br>\nCreate one or
 more IAM users and groups in your account. You can then create additional
 users whose permissions are limited to perform specific tasks in your AWS
 environment. For more information, see <a href=\"https://docs.aws.amazon.com/
```

```
IAM/latest/UserGuide/IAMGettingStarted.html\" target=\"_blank\">Getting
 Started</a>. \n<br><br>\n<b>Additional Resources</b><br>\n<a href=\"https://
docs.aws.amazon.com/IAM/latest/UserGuide/IAM_Introduction.html\" target=\"_blank
\">What Is IAM?</a>",
            "category": "security",
            "metadata": []
        }
    ]
}
```

Para obter mais informações, consulte AWS Trusted Advisor no AWS Support User Guide.

- Para obter detalhes da API, consulte DescribeTrustedAdvisorChecksna Referência de AWS CLI Comandos.

PowerShell

Ferramentas para PowerShell

Exemplo 1: Retorna a coleção de cheques do Trusted Advisor. Você deve especificar o parâmetro Language, que pode aceitar “en” para saída em inglês ou “ja” para saída em japonês.

```
Get-ASATrustedAdvisorCheck -Language "en"
```

- Para obter detalhes da API, consulte DescribeTrustedAdvisorChecksem Referência de AWS Tools for PowerShell cmdlet.

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsar o AWS Support com um SDK da AWS. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **`RefreshTrustedAdvisorCheck`** com um AWS SDK ou uma ferramenta de linha de comando

Os exemplos de código a seguir mostram como usar`RefreshTrustedAdvisorCheck`.

CLI

AWS CLI

Para atualizar uma verificação do AWS Trusted Advisor

O `refresh-trusted-advisor-check` exemplo a seguir atualiza o cheque do Amazon S3 Bucket Permissions Trusted Advisor em AWS sua conta.

```
aws support refresh-trusted-advisor-check \
    --check-id "Pfx0RwqBli"
```

Saída:

```
{
    "status": {
        "checkId": "Pfx0RwqBli",
        "status": "enqueued",
        "millisUntilNextRefreshable": 3599992
    }
}
```

Para obter mais informações, consulte AWS Trusted Advisor no AWS Support User Guide.

- Para obter detalhes da API, consulte RefreshTrustedAdvisorCheckna Referência de AWS CLI Comandos.

PowerShell

Ferramentas para PowerShell

Exemplo 1: Solicita uma atualização para a verificação especificada do Trusted Advisor.

```
Request-ASATrustedAdvisorCheckRefresh -CheckId "checkid1"
```

- Para obter detalhes da API, consulte RefreshTrustedAdvisorCheckem Referência de AWS Tools for PowerShell cmdlet.

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsar o AWS Support com um SDK da AWS. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **`ResolveCase`** com um AWS SDK ou uma ferramenta de linha de comando

Os exemplos de código a seguir mostram como usar`ResolveCase`.

Exemplos de ações são trechos de código de programas maiores e devem ser executados em contexto. É possível ver essa ação no contexto no seguinte exemplo de código:

- Conceitos básicos de casos

.NET

AWS SDK for .NET

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

```
/// <summary>
/// Resolve a support case by caseId.
/// </summary>
/// <param name="caseId">Id for the support case.</param>
/// <returns>The final status of the case after resolving.</returns>
public async Task<string> ResolveCase(string caseId)
{
    var response = await _amazonSupport.ResolveCaseAsync(
        new ResolveCaseRequest()
        {
            CaseId = caseId
        });
    return response.FinalCaseStatus;
}
```

- Para obter detalhes da API, consulte ResolveCasea Referência AWS SDK for .NET da API.

CLI

AWS CLI

Como solucionar um caso de suporte

O `resolve-case` exemplo a seguir resolve um caso de suporte em sua AWS conta.

```
aws support resolve-case \
    --case-id "case-12345678910-2013-c4c1d2bf33c5cf47"
```

Saída:

```
{
    "finalCaseStatus": "resolved",
    "initialCaseStatus": "work-in-progress"
}
```

Para obter mais informações, consulte Case management no Guia do usuário do AWS Support.

- Para obter detalhes da API, consulte ResolveCasena Referência de AWS CLI Comandos.

Java

SDK para Java 2.x

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

```
   public static void resolveSupportCase(SupportClient supportClient, String
caseId) {
       try {
           ResolveCaseRequest caseRequest = ResolveCaseRequest.builder()
                   .caseId(caseId)
                   .build();
```

```
            ResolveCaseResponse response =
 supportClient.resolveCase(caseRequest);
            System.out.println("The status of case " + caseId + " is " +
 response.finalCaseStatus());

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }
```

- Para obter detalhes da API, consulte ResolveCasea Referência AWS SDK for Java 2.x da API.

JavaScript

SDK para JavaScript (v3)

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

```
import { ResolveCaseCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

const main = async () => {
  try {
    const response = await client.send(
      new ResolveCaseCommand({
        caseId: "CASE_ID",
      }),
    );

    console.log(response.finalCaseStatus);
    return response;
  } catch (err) {
    console.error(err);
```

```
  }
};
```

- Para obter detalhes da API, consulte ResolveCasea Referência AWS SDK for JavaScript da API.

Kotlin

SDK for Kotlin

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

```
suspend fun resolveSupportCase(caseIdVal: String) {
    val caseRequest = ResolveCaseRequest {
        caseId = caseIdVal
    }
    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.resolveCase(caseRequest)
        println("The status of case $caseIdVal is ${response.finalCaseStatus}")
    }
}
```

- Para obter detalhes da API, consulte a ResolveCasereferência da API AWS SDK for Kotlin.

PowerShell

Ferramentas para PowerShell

Exemplo 1: retorna o estado inicial do caso especificado e o estado atual após a conclusão da chamada para resolvê-lo.

```
Resolve-ASACase -CaseId "case-12345678910-2013-c4c1d2bf33c5cf47"
```

- Para obter detalhes da API, consulte ResolveCaseem Referência de AWS Tools for PowerShell cmdlet.

Python

SDK para Python (Boto3)

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def resolve_case(self, case_id):
        """
        Resolve a support case by its caseId.

        :param case_id: The ID of the case to resolve.
        :return: The final status of the case.
        """
        try:
            response = self.support_client.resolve_case(caseId=case_id)
            final_status = response["finalCaseStatus"]
```

```
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't resolve case. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return final_status
```

- Para obter detalhes da API, consulte a ResolveCaseReferência da API AWS SDK for Python (Boto3).

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsar o AWS Support com um SDK da AWS. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Cenários para AWS Support usar AWS SDKs

Os exemplos de código a seguir mostram como implementar cenários comuns AWS Support com AWS SDKs. Esses cenários mostram como realizar tarefas específicas chamando várias funções internas AWS Support. Cada cenário inclui um link para GitHub, onde você pode encontrar instruções sobre como configurar e executar o código.

Exemplos

- Comece a usar AWS Support casos usando um AWS SDK

Comece a usar AWS Support casos usando um AWS SDK

Os exemplos de código a seguir mostram como:

- Obtenha e exiba os serviços disponíveis e os níveis de gravidade dos casos.
- Crie um caso de suporte usando um serviço, uma categoria e um nível de gravidade selecionados.
- Obtenha e exiba uma lista de casos em aberto para o dia atual.
- Adicione um conjunto de anexos e uma comunicação ao novo caso.
- Descreva o novo anexo e a comunicação para o caso.
- Resolva o caso.
- Obtenha e exiba uma lista de casos resolvidos para o dia atual.

.NET

AWS SDK for .NET

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

Execute um cenário interativo em um prompt de comando.

```
/// <summary>
/// Hello AWS Support example.
/// </summary>
public static class SupportCaseScenario
{
    /*
    Before running this .NET code example, set up your development environment,
 including your credentials.
    To use the AWS Support API, you must have one of the following AWS Support
 plans: Business, Enterprise On-Ramp, or Enterprise.

    This .NET example performs the following tasks:
    1.  Get and display services. Select a service from the list.
    2.  Select a category from the selected service.
```

```
   3.  Get and display severity levels and select a severity level from the
list.
   4.  Create a support case using the selected service, category, and severity
level.
   5.  Get and display a list of open support cases for the current day.
   6.  Create an attachment set with a sample text file to add to the case.
   7.  Add a communication with the attachment to the support case.
   8.  List the communications of the support case.
   9.  Describe the attachment set.
   10. Resolve the support case.
   11. Get a list of resolved cases for the current day.
  */

   private static SupportWrapper _supportWrapper = null!;

   static async Task Main(string[] args)
   {
       // Set up dependency injection for the AWS Support service.
       // Use your AWS profile name, or leave it blank to use the default
profile.
       using var host = Host.CreateDefaultBuilder(args)
           .ConfigureLogging(logging =>
               logging.AddFilter("System", LogLevel.Debug)
                   .AddFilter<DebugLoggerProvider>("Microsoft",
LogLevel.Information)
                   .AddFilter<ConsoleLoggerProvider>("Microsoft",
LogLevel.Trace))
           .ConfigureServices((_, services) =>
               services.AddAWSService<IAmazonAWSSupport>(new AWSOptions()
{ Profile = "default" })
                   .AddTransient<SupportWrapper>()
           )
           .Build();

       var logger = LoggerFactory.Create(builder =>
       {
           builder.AddConsole();
       }).CreateLogger(typeof(SupportCaseScenario));

       _supportWrapper = host.Services.GetRequiredService<SupportWrapper>();

       Console.WriteLine(new string('-', 80));
       Console.WriteLine("Welcome to the AWS Support case example scenario.");
       Console.WriteLine(new string('-', 80));
```

```
        try
        {
            var apiSupported = await _supportWrapper.VerifySubscription();
            if (!apiSupported)
            {
                logger.LogError("You must have a Business, Enterprise On-Ramp, or
Enterprise Support " +
                                "plan to use the AWS Support API. \n\tPlease
upgrade your subscription to run these examples.");
                return;
            }

            var service = await DisplayAndSelectServices();

            var category = DisplayAndSelectCategories(service);

            var severityLevel = await DisplayAndSelectSeverity();

            var caseId = await CreateSupportCase(service, category,
severityLevel);

            await DescribeTodayOpenCases();

            var attachmentSetId = await CreateAttachmentSet();

            await AddCommunicationToCase(attachmentSetId, caseId);

            var attachmentId = await ListCommunicationsForCase(caseId);

            await DescribeCaseAttachment(attachmentId);

            await ResolveCase(caseId);

            await DescribeTodayResolvedCases();

            Console.WriteLine(new string('-', 80));
            Console.WriteLine("AWS Support case example scenario complete.");
            Console.WriteLine(new string('-', 80));
        }
        catch (Exception ex)
        {
            logger.LogError(ex, "There was a problem executing the scenario.");
        }
```

```
    }

    /// <summary>
    /// List some available services from AWS Support, and select a service for
the example.
    /// </summary>
    /// <returns>The selected service.</returns>
    private static async Task<Service> DisplayAndSelectServices()
    {
        Console.WriteLine(new string('-', 80));
        var services = await _supportWrapper.DescribeServices();
        Console.WriteLine($"AWS Support client returned {services.Count}
services.");

        Console.WriteLine($"1. Displaying first 10 services:");
        for (int i = 0; i < 10 && i < services.Count; i++)
        {
            Console.WriteLine($"\t{i + 1}. {services[i].Name}");
        }

        var choiceNumber = 0;
        while (choiceNumber < 1 || choiceNumber > services.Count)
        {
            Console.WriteLine(
                "Select an example support service by entering a number from the
preceding list:");
            var choice = Console.ReadLine();
            Int32.TryParse(choice, out choiceNumber);
        }
        Console.WriteLine(new string('-', 80));

        return services[choiceNumber - 1];
    }

    /// <summary>
    /// List the available categories for a service and select a category for the
example.
    /// </summary>
    /// <param name="service">Service to use for displaying categories.</param>
    /// <returns>The selected category.</returns>
    private static Category DisplayAndSelectCategories(Service service)
    {
        Console.WriteLine(new string('-', 80));
```

```
        Console.WriteLine($"2. Available support categories for Service
\"{service.Name}\":");
        for (int i = 0; i < service.Categories.Count; i++)
        {
            Console.WriteLine($"\t{i + 1}. {service.Categories[i].Name}");
        }

        var choiceNumber = 0;
        while (choiceNumber < 1 || choiceNumber > service.Categories.Count)
        {
            Console.WriteLine(
                "Select an example support category by entering a number from the
preceding list:");
            var choice = Console.ReadLine();
            Int32.TryParse(choice, out choiceNumber);
        }

        Console.WriteLine(new string('-', 80));

        return service.Categories[choiceNumber - 1];
    }

    /// <summary>
    /// List available severity levels from AWS Support, and select a level for
the example.
    /// </summary>
    /// <returns>The selected severity level.</returns>
    private static async Task<SeverityLevel> DisplayAndSelectSeverity()
    {
        Console.WriteLine(new string('-', 80));
        var severityLevels = await _supportWrapper.DescribeSeverityLevels();

        Console.WriteLine($"3. Get and display available severity levels:");
        for (int i = 0; i < 10 && i < severityLevels.Count; i++)
        {
            Console.WriteLine($"\t{i + 1}. {severityLevels[i].Name}");
        }

        var choiceNumber = 0;
        while (choiceNumber < 1 || choiceNumber > severityLevels.Count)
        {
            Console.WriteLine(
                "Select an example severity level by entering a number from the
preceding list:");
```

```
            var choice = Console.ReadLine();
            Int32.TryParse(choice, out choiceNumber);
        }
        Console.WriteLine(new string('-', 80));

        return severityLevels[choiceNumber - 1];
    }

    /// <summary>
    /// Create an example support case.
    /// </summary>
    /// <param name="service">Service to use for the new case.</param>
    /// <param name="category">Category to use for the new case.</param>
    /// <param name="severity">Severity to use for the new case.</param>
    /// <returns>The caseId of the new support case.</returns>
    private static async Task<string> CreateSupportCase(Service service,
        Category category, SeverityLevel severity)
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"4. Create an example support case" +
                          $" with the following settings:" +
                          $" \n\tService: {service.Name}, Category:
{category.Name} " +
                          $"and Severity Level: {severity.Name}.");
        var caseId = await _supportWrapper.CreateCase(service.Code,
category.Code, severity.Code,
            "Example case for testing, ignore.", "This is my example support
case.");

        Console.WriteLine($"\tNew case created with ID {caseId}");

        Console.WriteLine(new string('-', 80));

        return caseId;
    }

    /// <summary>
    /// List open cases for the current day.
    /// </summary>
    /// <returns>Async task.</returns>
    private static async Task DescribeTodayOpenCases()
    {
        Console.WriteLine($"5. List the open support cases for the current
day.");
```

```
        // Describe the cases. If it is empty, try again and allow time for the
new case to appear.
        List<CaseDetails> currentOpenCases = null!;
        while (currentOpenCases == null || currentOpenCases.Count == 0)
        {
            Thread.Sleep(1000);
            currentOpenCases = await _supportWrapper.DescribeCases(
                new List<string>(),
                null,
                false,
                false,
                DateTime.UtcNow.Date,
                DateTime.UtcNow);
        }

        foreach (var openCase in currentOpenCases)
        {
            Console.WriteLine($"\tCase: {openCase.CaseId} created
{openCase.TimeCreated}");
        }

        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// Create an attachment set for a support case.
    /// </summary>
    /// <returns>The attachment set id.</returns>
    private static async Task<string> CreateAttachmentSet()
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"6. Create an attachment set for a support case.");
        var fileName = "example_attachment.txt";

        // Create the file if it does not already exist.
        if (!File.Exists(fileName))
        {
            await using StreamWriter sw = File.CreateText(fileName);
            await sw.WriteLineAsync(
                "This is a sample file for attachment to a support case.");
        }

        await using var ms = new MemoryStream(await
File.ReadAllBytesAsync(fileName));
```

```
        var attachmentSetId = await _supportWrapper.AddAttachmentToSet(
            ms,
            fileName);

        Console.WriteLine($"\tNew attachment set created with id: \n
\t{attachmentSetId.Substring(0, 65)}...");

        Console.WriteLine(new string('-', 80));

        return attachmentSetId;
    }

    /// <summary>
    /// Add an attachment set and communication to a case.
    /// </summary>
    /// <param name="attachmentSetId">Id of the attachment set.</param>
    /// <param name="caseId">Id of the case to receive the attachment set.</
param>
    /// <returns>Async task.</returns>
    private static async Task AddCommunicationToCase(string attachmentSetId,
 string caseId)
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"7. Add attachment set and communication to
 {caseId}.");

        await _supportWrapper.AddCommunicationToCase(
            caseId,
            "This is an example communication added to a support case.",
            attachmentSetId);

        Console.WriteLine($"\tNew attachment set and communication added to
 {caseId}");

        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// List the communications for a case.
    /// </summary>
    /// <param name="caseId">Id of the case to describe.</param>
    /// <returns>An attachment id.</returns>
    private static async Task<string> ListCommunicationsForCase(string caseId)
```

```
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"8. List communications for case {caseId}.");

        var communications = await
_supportWrapper.DescribeCommunications(caseId);
        var attachmentId = "";
        foreach (var communication in communications)
        {
            Console.WriteLine(
                $"\tCommunication created on: {communication.TimeCreated} has
{communication.AttachmentSet.Count} attachments.");
            if (communication.AttachmentSet.Any())
            {
                attachmentId = communication.AttachmentSet.First().AttachmentId;
            }
        }

        Console.WriteLine(new string('-', 80));
        return attachmentId;
    }

    /// <summary>
    /// Describe an attachment by id.
    /// </summary>
    /// <param name="attachmentId">Id of the attachment to describe.</param>
    /// <returns>Async task.</returns>
    private static async Task DescribeCaseAttachment(string attachmentId)
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"9. Describe the attachment set.");

        var attachment = await _supportWrapper.DescribeAttachment(attachmentId);
        var data = Encoding.ASCII.GetString(attachment.Data.ToArray());
        Console.WriteLine($"\tAttachment includes {attachment.FileName} with
data: \n\t{data}");

        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// Resolve the support case.
    /// </summary>
    /// <param name="caseId">Id of the case to resolve.</param>
```

```
    /// <returns>Async task.</returns>
    private static async Task ResolveCase(string caseId)
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"10. Resolve case {caseId}.");

        var status = await _supportWrapper.ResolveCase(caseId);
        Console.WriteLine($"\tCase {caseId} has final status {status}");

        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// List resolved cases for the current day.
    /// </summary>
    /// <returns>Async Task.</returns>
    private static async Task DescribeTodayResolvedCases()
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"11. List the resolved support cases for the current
 day.");
        var currentCases = await _supportWrapper.DescribeCases(
            new List<string>(),
            null,
            false,
            true,
            DateTime.UtcNow.Date,
            DateTime.UtcNow);

        foreach (var currentCase in currentCases)
        {
            if (currentCase.Status == "resolved")
            {
                Console.WriteLine(
                    $"\tCase: {currentCase.CaseId}: status
 {currentCase.Status}");
            }
        }

        Console.WriteLine(new string('-', 80));
    }
}
```

Métodos de embalagem usados pelo cenário para AWS Support ações.

```
/// <summary>
/// Wrapper methods to use AWS Support for working with support cases.
/// </summary>
public class SupportWrapper
{
    private readonly IAmazonAWSSupport _amazonSupport;
    public SupportWrapper(IAmazonAWSSupport amazonSupport)
    {
        _amazonSupport = amazonSupport;
    }


    /// <summary>
    /// Get the descriptions of AWS services.
    /// </summary>
    /// <param name="name">Optional language for services.
    /// Currently Chinese (“zh”), English ("en"), Japanese ("ja") and Korean
 (“ko”) are supported.</param>
    /// <returns>The list of AWS service descriptions.</returns>
    public async Task<List<Service>> DescribeServices(string language = "en")
    {
        var response = await _amazonSupport.DescribeServicesAsync(
            new DescribeServicesRequest()
            {
                Language = language
            });
        return response.Services;
    }



    /// <summary>
    /// Get the descriptions of support severity levels.
    /// </summary>
    /// <param name="name">Optional language for severity levels.
    /// Currently Chinese (“zh”), English ("en"), Japanese ("ja") and Korean
 (“ko”) are supported.</param>
    /// <returns>The list of support severity levels.</returns>
    public async Task<List<SeverityLevel>> DescribeSeverityLevels(string language
 = "en")
    {
```

```
        var response = await _amazonSupport.DescribeSeverityLevelsAsync(
            new DescribeSeverityLevelsRequest()
            {
                Language = language
            });
        return response.SeverityLevels;
    }



    /// <summary>
    /// Create a new support case.
    /// </summary>
    /// <param name="serviceCode">Service code for the new case.</param>
    /// <param name="categoryCode">Category for the new case.</param>
    /// <param name="severityCode">Severity code for the new case.</param>
    /// <param name="subject">Subject of the new case.</param>
    /// <param name="body">Body text of the new case.</param>
    /// <param name="language">Optional language support for your case.
    /// Currently Chinese (“zh”), English ("en"), Japanese ("ja") and Korean
(“ko”) are supported.</param>
    /// <param name="attachmentSetId">Optional Id for an attachment set for the
new case.</param>
    /// <param name="issueType">Optional issue type for the new case. Options are
"customer-service" or "technical".</param>
    /// <returns>The caseId of the new support case.</returns>
    public async Task<string> CreateCase(string serviceCode, string categoryCode,
string severityCode, string subject,
        string body, string language = "en", string? attachmentSetId = null,
string issueType = "customer-service")
    {
        var response = await _amazonSupport.CreateCaseAsync(
            new CreateCaseRequest()
            {
                ServiceCode = serviceCode,
                CategoryCode = categoryCode,
                SeverityCode = severityCode,
                Subject = subject,
                Language = language,
                AttachmentSetId = attachmentSetId,
                IssueType = issueType,
                CommunicationBody = body
            });
        return response.CaseId;
```

```
    }



    /// <summary>
    /// Add an attachment to a set, or create a new attachment set if one does
not exist.
    /// </summary>
    /// <param name="data">The data for the attachment.</param>
    /// <param name="fileName">The file name for the attachment.</param>
    /// <param name="attachmentSetId">Optional setId for the attachment. Creates
a new attachment set if empty.</param>
    /// <returns>The setId of the attachment.</returns>
    public async Task<string> AddAttachmentToSet(MemoryStream data, string
fileName, string? attachmentSetId = null)
    {
        var response = await _amazonSupport.AddAttachmentsToSetAsync(
            new AddAttachmentsToSetRequest
            {
                AttachmentSetId = attachmentSetId,
                Attachments = new List<Attachment>
                {
                    new Attachment
                    {
                        Data = data,
                        FileName = fileName
                    }
                }
            });
        return response.AttachmentSetId;
    }



    /// <summary>
    /// Get description of a specific attachment.
    /// </summary>
    /// <param name="attachmentId">Id of the attachment, usually fetched by
describing the communications of a case.</param>
    /// <returns>The attachment object.</returns>
    public async Task<Attachment> DescribeAttachment(string attachmentId)
    {
        var response = await _amazonSupport.DescribeAttachmentAsync(
            new DescribeAttachmentRequest()
```

```
            {
                AttachmentId = attachmentId
            });
        return response.Attachment;
    }



    /// <summary>
    /// Add communication to a case, including optional attachment set ID and CC
 email addresses.
    /// </summary>
    /// <param name="caseId">Id for the support case.</param>
    /// <param name="body">Body text of the communication.</param>
    /// <param name="attachmentSetId">Optional Id for an attachment set.</param>
    /// <param name="ccEmailAddresses">Optional list of CC email addresses.</
param>
    /// <returns>True if successful.</returns>
    public async Task<bool> AddCommunicationToCase(string caseId, string body,
        string? attachmentSetId = null, List<string>? ccEmailAddresses = null)
    {
        var response = await _amazonSupport.AddCommunicationToCaseAsync(
            new AddCommunicationToCaseRequest()
            {
                CaseId = caseId,
                CommunicationBody = body,
                AttachmentSetId = attachmentSetId,
                CcEmailAddresses = ccEmailAddresses
            });
        return response.Result;
    }



    /// <summary>
    /// Describe the communications for a case, optionally with a date filter.
    /// </summary>
    /// <param name="caseId">The ID of the support case.</param>
    /// <param name="afterTime">The optional start date for a filtered search.</
param>
    /// <param name="beforeTime">The optional end date for a filtered search.</
param>
    /// <returns>The list of communications for the case.</returns>
```

```
    public async Task<List<Communication>> DescribeCommunications(string caseId,
 DateTime? afterTime = null, DateTime? beforeTime = null)
    {
        var results = new List<Communication>();
        var paginateCommunications =
 _amazonSupport.Paginators.DescribeCommunications(
            new DescribeCommunicationsRequest()
            {
                CaseId = caseId,
                AfterTime = afterTime?.ToString("s"),
                BeforeTime = beforeTime?.ToString("s")
            });
        // Get the entire list using the paginator.
        await foreach (var communications in
 paginateCommunications.Communications)
        {
            results.Add(communications);
        }
        return results;
    }



    /// <summary>
    /// Get case details for a list of case ids, optionally with date filters.
    /// </summary>
    /// <param name="caseIds">The list of case IDs.</param>
    /// <param name="displayId">Optional display ID.</param>
    /// <param name="includeCommunication">True to include communication.
 Defaults to true.</param>
    /// <param name="includeResolvedCases">True to include resolved cases.
 Defaults to false.</param>
    /// <param name="afterTime">The optional start date for a filtered search.</
param>
    /// <param name="beforeTime">The optional end date for a filtered search.</
param>
    /// <param name="language">Optional language support for your case.
    /// Currently Chinese (“zh”), English ("en"), Japanese ("ja") and Korean
 (“ko”) are supported.</param>
    /// <returns>A list of CaseDetails.</returns>
    public async Task<List<CaseDetails>> DescribeCases(List<string> caseIds,
 string? displayId = null, bool includeCommunication = true,
        bool includeResolvedCases = false, DateTime? afterTime = null, DateTime?
 beforeTime = null,
```

```
        string language = "en")
    {
        var results = new List<CaseDetails>();
        var paginateCases = _amazonSupport.Paginators.DescribeCases(
            new DescribeCasesRequest()
            {
                CaseIdList = caseIds,
                DisplayId = displayId,
                IncludeCommunications = includeCommunication,
                IncludeResolvedCases = includeResolvedCases,
                AfterTime = afterTime?.ToString("s"),
                BeforeTime = beforeTime?.ToString("s"),
                Language = language
            });
        // Get the entire list using the paginator.
        await foreach (var cases in paginateCases.Cases)
        {
            results.Add(cases);
        }
        return results;
    }



    /// <summary>
    /// Resolve a support case by caseId.
    /// </summary>
    /// <param name="caseId">Id for the support case.</param>
    /// <returns>The final status of the case after resolving.</returns>
    public async Task<string> ResolveCase(string caseId)
    {
        var response = await _amazonSupport.ResolveCaseAsync(
            new ResolveCaseRequest()
            {
                CaseId = caseId
            });
        return response.FinalCaseStatus;
    }



    /// <summary>
    /// Verify the support level for AWS Support API access.
    /// </summary>
    /// <returns>True if the subscription level supports API access.</returns>
```

```
    public async Task<bool> VerifySubscription()
    {
        try
        {
            var response = await _amazonSupport.DescribeServicesAsync(
                new DescribeServicesRequest()
                {
                    Language = "en"
                });
            return response.HttpStatusCode == HttpStatusCode.OK;
        }
        catch (Amazon.AWSSupport.AmazonAWSSupportException ex)
        {
            if (ex.ErrorCode == "SubscriptionRequiredException")
            {
                return false;
            }
            else throw;
        }
    }
}
```

- Para obter detalhes da API, consulte os tópicos a seguir na Referência da API do AWS SDK for .NET .
  - AddAttachmentsToSet
  - AddCommunicationToCase
  - CreateCase
  - DescribeAttachment
  - DescribeCases
  - DescribeCommunications
  - DescribeServices
  - DescribeSeverityLevels
  - ResolveCase

Java

SDK para Java 2.x

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

Execute várias AWS Support operações.

```
import software.amazon.awssdk.core.SdkBytes;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.support.SupportClient;
import software.amazon.awssdk.services.support.model.AddAttachmentsToSetResponse;
import
 software.amazon.awssdk.services.support.model.AddCommunicationToCaseRequest;
import
 software.amazon.awssdk.services.support.model.AddCommunicationToCaseResponse;
import software.amazon.awssdk.services.support.model.Attachment;
import software.amazon.awssdk.services.support.model.AttachmentDetails;
import software.amazon.awssdk.services.support.model.CaseDetails;
import software.amazon.awssdk.services.support.model.Category;
import software.amazon.awssdk.services.support.model.Communication;
import software.amazon.awssdk.services.support.model.CreateCaseRequest;
import software.amazon.awssdk.services.support.model.CreateCaseResponse;
import software.amazon.awssdk.services.support.model.DescribeAttachmentRequest;
import software.amazon.awssdk.services.support.model.DescribeAttachmentResponse;
import software.amazon.awssdk.services.support.model.DescribeCasesRequest;
import software.amazon.awssdk.services.support.model.DescribeCasesResponse;
import
 software.amazon.awssdk.services.support.model.DescribeCommunicationsRequest;
import
 software.amazon.awssdk.services.support.model.DescribeCommunicationsResponse;
import software.amazon.awssdk.services.support.model.DescribeServicesRequest;
import software.amazon.awssdk.services.support.model.DescribeServicesResponse;
import
 software.amazon.awssdk.services.support.model.DescribeSeverityLevelsRequest;
import
 software.amazon.awssdk.services.support.model.DescribeSeverityLevelsResponse;
import software.amazon.awssdk.services.support.model.ResolveCaseRequest;
import software.amazon.awssdk.services.support.model.ResolveCaseResponse;
```

```
import software.amazon.awssdk.services.support.model.Service;
import software.amazon.awssdk.services.support.model.SeverityLevel;
import software.amazon.awssdk.services.support.model.SupportException;
import software.amazon.awssdk.services.support.model.AddAttachmentsToSetRequest;
import java.io.File;
import java.io.FileInputStream;
import java.io.FileNotFoundException;
import java.io.InputStream;
import java.time.Instant;
import java.time.temporal.ChronoUnit;
import java.util.ArrayList;
import java.util.List;

/**
 * Before running this Java (v2) code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 *
 * In addition, you must have the AWS Business Support Plan to use the AWS
 * Support Java API. For more information, see:
 *
 * https://aws.amazon.com/premiumsupport/plans/
 *
 * This Java example performs the following tasks:
 *
 * 1. Gets and displays available services.
 * 2. Gets and displays severity levels.
 * 3. Creates a support case by using the selected service, category, and
 * severity level.
 * 4. Gets a list of open cases for the current day.
 * 5. Creates an attachment set with a generated file.
 * 6. Adds a communication with the attachment to the support case.
 * 7. Lists the communications of the support case.
 * 8. Describes the attachment set included with the communication.
 * 9. Resolves the support case.
 * 10. Gets a list of resolved cases for the current day.
 */
public class SupportScenario {
```

```
   public static final String DASHES = new String(new char[80]).replace("\0",
"-");

   public static void main(String[] args) {
       final String usage = """

               Usage:
                   <fileAttachment>Where:
                   fileAttachment - The file can be a simple saved .txt file to
use as an email attachment.\s
               """;

       if (args.length != 1) {
           System.out.println(usage);
           System.exit(1);
       }

       String fileAttachment = args[0];
       Region region = Region.US_WEST_2;
       SupportClient supportClient = SupportClient.builder()
               .region(region)
               .build();

       System.out.println(DASHES);
       System.out.println("***** Welcome to the AWS Support case example
scenario.");
       System.out.println(DASHES);

       System.out.println(DASHES);
       System.out.println("1. Get and display available services.");
       List<String> sevCatList = displayServices(supportClient);
       System.out.println(DASHES);

       System.out.println(DASHES);
       System.out.println("2. Get and display Support severity levels.");
       String sevLevel = displaySevLevels(supportClient);
       System.out.println(DASHES);

       System.out.println(DASHES);
       System.out.println("3. Create a support case using the selected service,
category, and severity level.");
       String caseId = createSupportCase(supportClient, sevCatList, sevLevel);
       if (caseId.compareTo("") == 0) {
           System.out.println("A support case was not successfully created!");
```

```
            System.exit(1);
        } else
            System.out.println("Support case " + caseId + " was successfully
created!");
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("4. Get open support cases.");
        getOpenCase(supportClient);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("5. Create an attachment set with a generated file to
add to the case.");
        String attachmentSetId = addAttachment(supportClient, fileAttachment);
        System.out.println("The Attachment Set id value is" + attachmentSetId);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("6. Add communication with the attachment to the
support case.");
        addAttachSupportCase(supportClient, caseId, attachmentSetId);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("7. List the communications of the support case.");
        String attachId = listCommunications(supportClient, caseId);
        System.out.println("The Attachment id value is" + attachId);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("8. Describe the attachment set included with the
communication.");
        describeAttachment(supportClient, attachId);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("9. Resolve the support case.");
        resolveSupportCase(supportClient, caseId);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("10. Get a list of resolved cases for the current
day.");
```

```
        getResolvedCase(supportClient);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("***** This Scenario has successfully completed");
        System.out.println(DASHES);
    }

    public static void getResolvedCase(SupportClient supportClient) {
        try {
            // Specify the start and end time.
            Instant now = Instant.now();
            java.time.LocalDate.now();
            Instant yesterday = now.minus(1, ChronoUnit.DAYS);

            DescribeCasesRequest describeCasesRequest =
DescribeCasesRequest.builder()
                    .maxResults(30)
                    .afterTime(yesterday.toString())
                    .beforeTime(now.toString())
                    .includeResolvedCases(true)
                    .build();

            DescribeCasesResponse response =
supportClient.describeCases(describeCasesRequest);
            List<CaseDetails> cases = response.cases();
            for (CaseDetails sinCase : cases) {
                if (sinCase.status().compareTo("resolved") == 0)
                    System.out.println("The case status is " + sinCase.status());
            }

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }

    public static void resolveSupportCase(SupportClient supportClient, String
caseId) {
        try {
            ResolveCaseRequest caseRequest = ResolveCaseRequest.builder()
                    .caseId(caseId)
                    .build();
```

```
            ResolveCaseResponse response =
supportClient.resolveCase(caseRequest);
            System.out.println("The status of case " + caseId + " is " +
response.finalCaseStatus());

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }

    public static void describeAttachment(SupportClient supportClient, String
attachId) {
        try {
            DescribeAttachmentRequest attachmentRequest =
DescribeAttachmentRequest.builder()
                    .attachmentId(attachId)
                    .build();

            DescribeAttachmentResponse response =
supportClient.describeAttachment(attachmentRequest);
            System.out.println("The name of the file is " +
response.attachment().fileName());

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }

    public static String listCommunications(SupportClient supportClient, String
caseId) {
        try {
            String attachId = null;
            DescribeCommunicationsRequest communicationsRequest =
DescribeCommunicationsRequest.builder()
                    .caseId(caseId)
                    .maxResults(10)
                    .build();

            DescribeCommunicationsResponse response =
supportClient.describeCommunications(communicationsRequest);
            List<Communication> communications = response.communications();
            for (Communication comm : communications) {
```

```
                System.out.println("the body is: " + comm.body());

                // Get the attachment id value.
                List<AttachmentDetails> attachments = comm.attachmentSet();
                for (AttachmentDetails detail : attachments) {
                    attachId = detail.attachmentId();
                }
            }
            return attachId;

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return "";
    }

    public static void addAttachSupportCase(SupportClient supportClient, String
caseId, String attachmentSetId) {
        try {
            AddCommunicationToCaseRequest caseRequest =
AddCommunicationToCaseRequest.builder()
                    .caseId(caseId)
                    .attachmentSetId(attachmentSetId)
                    .communicationBody("Please refer to attachment for details.")
                    .build();

            AddCommunicationToCaseResponse response =
supportClient.addCommunicationToCase(caseRequest);
            if (response.result())
                System.out.println("You have successfully added a communication
to an AWS Support case");
            else
                System.out.println("There was an error adding the communication
to an AWS Support case");

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }

    public static String addAttachment(SupportClient supportClient, String
fileAttachment) {
```

```
        try {
            File myFile = new File(fileAttachment);
            InputStream sourceStream = new FileInputStream(myFile);
            SdkBytes sourceBytes = SdkBytes.fromInputStream(sourceStream);

            Attachment attachment = Attachment.builder()
                    .fileName(myFile.getName())
                    .data(sourceBytes)
                    .build();

            AddAttachmentsToSetRequest setRequest =
AddAttachmentsToSetRequest.builder()
                    .attachments(attachment)
                    .build();

            AddAttachmentsToSetResponse response =
supportClient.addAttachmentsToSet(setRequest);
            return response.attachmentSetId();

        } catch (SupportException | FileNotFoundException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return "";
    }

    public static void getOpenCase(SupportClient supportClient) {
        try {
            // Specify the start and end time.
            Instant now = Instant.now();
            java.time.LocalDate.now();
            Instant yesterday = now.minus(1, ChronoUnit.DAYS);

            DescribeCasesRequest describeCasesRequest =
DescribeCasesRequest.builder()
                    .maxResults(20)
                    .afterTime(yesterday.toString())
                    .beforeTime(now.toString())
                    .build();

            DescribeCasesResponse response =
supportClient.describeCases(describeCasesRequest);
            List<CaseDetails> cases = response.cases();
            for (CaseDetails sinCase : cases) {
```

```
                System.out.println("The case status is " + sinCase.status());
                System.out.println("The case Id is " + sinCase.caseId());
                System.out.println("The case subject is " + sinCase.subject());
            }

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }

    public static String createSupportCase(SupportClient supportClient,
List<String> sevCatList, String sevLevel) {
        try {
            String serviceCode = sevCatList.get(0);
            String caseCat = sevCatList.get(1);
            CreateCaseRequest caseRequest = CreateCaseRequest.builder()
                    .categoryCode(caseCat.toLowerCase())
                    .serviceCode(serviceCode.toLowerCase())
                    .severityCode(sevLevel.toLowerCase())
                    .communicationBody("Test issue with " +
serviceCode.toLowerCase())
                    .subject("Test case, please ignore")
                    .language("en")
                    .issueType("technical")
                    .build();

            CreateCaseResponse response = supportClient.createCase(caseRequest);
            return response.caseId();

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return "";
    }

    public static String displaySevLevels(SupportClient supportClient) {
        try {
            DescribeSeverityLevelsRequest severityLevelsRequest =
DescribeSeverityLevelsRequest.builder()
                    .language("en")
                    .build();
```

```
            DescribeSeverityLevelsResponse response =
supportClient.describeSeverityLevels(severityLevelsRequest);
            List<SeverityLevel> severityLevels = response.severityLevels();
            String levelName = null;
            for (SeverityLevel sevLevel : severityLevels) {
                System.out.println("The severity level name is: " +
sevLevel.name());
                if (sevLevel.name().compareTo("High") == 0)
                    levelName = sevLevel.name();
            }
            return levelName;

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return "";
    }

    // Return a List that contains a Service name and Category name.
    public static List<String> displayServices(SupportClient supportClient) {
        try {
            DescribeServicesRequest servicesRequest =
DescribeServicesRequest.builder()
                    .language("en")
                    .build();

            DescribeServicesResponse response =
supportClient.describeServices(servicesRequest);
            String serviceCode = null;
            String catName = null;
            List<String> sevCatList = new ArrayList<>();
            List<Service> services = response.services();

            System.out.println("Get the first 10 services");
            int index = 1;
            for (Service service : services) {
                if (index == 11)
                    break;

                System.out.println("The Service name is: " + service.name());
                if (service.name().compareTo("Account") == 0)
                    serviceCode = service.code();
```

```
                // Get the Categories for this service.
                List<Category> categories = service.categories();
                for (Category cat : categories) {
                    System.out.println("The category name is: " + cat.name());
                    if (cat.name().compareTo("Security") == 0)
                        catName = cat.name();
                }
                index++;
            }

            // Push the two values to the list.
            sevCatList.add(serviceCode);
            sevCatList.add(catName);
            return sevCatList;

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return null;
    }
}
```

- Para obter detalhes da API, consulte os tópicos a seguir na Referência da API do AWS SDK for Java 2.x .
  - AddAttachmentsToSet
  - AddCommunicationToCase
  - CreateCase
  - DescribeAttachment
  - DescribeCases
  - DescribeCommunications
  - DescribeServices
  - DescribeSeverityLevels
  - ResolveCase

JavaScript

SDK para JavaScript (v3)

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

Execute um cenário interativo no terminal.

```
import {
  AddAttachmentsToSetCommand,
  AddCommunicationToCaseCommand,
  CreateCaseCommand,
  DescribeAttachmentCommand,
  DescribeCasesCommand,
  DescribeCommunicationsCommand,
  DescribeServicesCommand,
  DescribeSeverityLevelsCommand,
  ResolveCaseCommand,
  SupportClient,
} from "@aws-sdk/client-support";
import inquirer from "inquirer";

// Retry an asynchronous function on failure.
const retry = async ({ intervalInMs = 500, maxRetries = 10 }, fn) => {
  try {
    return await fn();
  } catch (err) {
    console.log(`Function call failed. Retrying.`);
    console.error(err.message);
    if (maxRetries === 0) throw err;
    await new Promise((resolve) => setTimeout(resolve, intervalInMs));
    return retry({ intervalInMs, maxRetries: maxRetries - 1 }, fn);
  }
};

const wrapText = (text, char = "=") => {
  const rule = char.repeat(80);
  return `${rule}\n    ${text}\n${rule}\n`;
};
```

```
const client = new SupportClient({ region: "us-east-1" });

// Verify that the account has a Support plan.
export const verifyAccount = async () => {
  const command = new DescribeServicesCommand({});

  try {
    await client.send(command);
  } catch (err) {
    if (err.name === "SubscriptionRequiredException") {
      throw new Error(
        "You must be subscribed to the AWS Support plan to use this feature."
      );
    } else {
      throw err;
    }
  }
};

// Get the list of available services.
export const getService = async () => {
  const { services } = await client.send(new DescribeServicesCommand({}));
  const { selectedService } = await inquirer.prompt({
    name: "selectedService",
    type: "list",
    message:
      "Select a service. Your support case will be created for this service. The
 list of services is truncated for readability.",
    choices: services.slice(0, 10).map((s) => ({ name: s.name, value: s })),
  });
  return selectedService;
};

// Get the list of available support case categories for a service.
export const getCategory = async (service) => {
  const { selectedCategory } = await inquirer.prompt({
    name: "selectedCategory",
    type: "list",
    message: "Select a category.",
    choices: service.categories.map((c) => ({ name: c.name, value: c })),
  });
  return selectedCategory;
};
```

```
// Get the available severity levels for the account.
export const getSeverityLevel = async () => {
  const command = new DescribeSeverityLevelsCommand({});
  const { severityLevels } = await client.send(command);
  const { selectedSeverityLevel } = await inquirer.prompt({
    name: "selectedSeverityLevel",
    type: "list",
    message: "Select a severity level.",
    choices: severityLevels.map((s) => ({ name: s.name, value: s })),
  });
  return selectedSeverityLevel;
};

// Create a new support case and return the caseId.
export const createCase = async ({
  selectedService,
  selectedCategory,
  selectedSeverityLevel,
}) => {
  const command = new CreateCaseCommand({
    subject: "IGNORE: Test case",
    communicationBody: "This is a test. Please ignore.",
    serviceCode: selectedService.code,
    categoryCode: selectedCategory.code,
    severityCode: selectedSeverityLevel.code,
  });
  const { caseId } = await client.send(command);
  return caseId;
};

// Get a list of open support cases created today.
export const getTodaysOpenCases = async () => {
  const d = new Date();
  const startOfToday = new Date(d.getFullYear(), d.getMonth(), d.getDate());
  const command = new DescribeCasesCommand({
    includeCommunications: false,
    afterTime: startOfToday.toISOString(),
  });

  const { cases } = await client.send(command);

  if (cases.length === 0) {
    throw new Error(
```

```
      "Unexpected number of cases. Expected more than 0 open cases."
    );
  }
  return cases;
};

// Create an attachment set.
export const createAttachmentSet = async () => {
  const command = new AddAttachmentsToSetCommand({
    attachments: [
      {
        fileName: "example.txt",
        data: new TextEncoder().encode("some example text"),
      },
    ],
  });
  const { attachmentSetId } = await client.send(command);
  return attachmentSetId;
};

export const linkAttachmentSetToCase = async (attachmentSetId, caseId) => {
  const command = new AddCommunicationToCaseCommand({
    attachmentSetId,
    caseId,
    communicationBody: "Adding attachment set to case.",
  });
  await client.send(command);
};

// Get all communications for a support case.
export const getCommunications = async (caseId) => {
  const command = new DescribeCommunicationsCommand({
    caseId,
  });
  const { communications } = await client.send(command);
  return communications;
};

// Get an attachment set.
export const getFirstAttachment = (communications) => {
  const firstCommWithAttachment = communications.find(
    (c) => c.attachmentSet.length > 0
  );
  return firstCommWithAttachment?.attachmentSet[0].attachmentId;
```

```
};

// Get an attachment.
export const getAttachment = async (attachmentId) => {
  const command = new DescribeAttachmentCommand({
    attachmentId,
  });
  const { attachment } = await client.send(command);
  return attachment;
};

// Resolve the case matching the given case ID.
export const resolveCase = async (caseId) => {
  const { shouldResolve } = await inquirer.prompt({
    name: "shouldResolve",
    type: "confirm",
    message: `Do you want to resolve ${caseId}?`,
  });

  if (shouldResolve) {
    const command = new ResolveCaseCommand({
      caseId: caseId,
    });

    await client.send(command);
    return true;
  }
  return false;
};

// Find a specific case in the list of provided cases by case ID.
// If the case is not found, and the results are paginated, continue
// paging through the results.
export const findCase = async ({ caseId, cases, nextToken }) => {
  const foundCase = cases.find((c) => c.caseId === caseId);

  if (foundCase) {
    return foundCase;
  }

  if (nextToken) {
    const response = await client.send(
      new DescribeCasesCommand({
        nextToken,
```

```
        includeResolvedCases: true,
      })
    );
    return findCase({
      caseId,
      cases: response.cases,
      nextToken: response.nextToken,
    });
  }

  throw new Error(`${caseId} not found.`);
};

// Get all cases created today.
export const getTodaysResolvedCases = async (caseIdToWaitFor) => {
  const d = new Date("2023-01-18");
  const startOfToday = new Date(d.getFullYear(), d.getMonth(), d.getDate());
  const command = new DescribeCasesCommand({
    includeCommunications: false,
    afterTime: startOfToday.toISOString(),
    includeResolvedCases: true,
  });
  const { cases, nextToken } = await client.send(command);
  await findCase({ cases, caseId: caseIdToWaitFor, nextToken });
  return cases.filter((c) => c.status === "resolved");
};

const main = async () => {
  let caseId;
  try {
    console.log(wrapText("Welcome to the AWS Support basic usage scenario."));

    // Verify that the account is subscribed to support.
    await verifyAccount();

    // Provided a truncated list of services and prompt the user to select one.
    const selectedService = await getService();

    // Provided the categories for the selected service and prompt the user to
 select one.
    const selectedCategory = await getCategory(selectedService);

    // Provide the severity available severity levels for the account and prompt
 the user to select one.
```

```
    const selectedSeverityLevel = await getSeverityLevel();

    // Create a support case.
    console.log("\nCreating a support case.");
    caseId = await createCase({
      selectedService,
      selectedCategory,
      selectedSeverityLevel,
    });
    console.log(`Support case created: ${caseId}`);

    // Display a list of open support cases created today.
    const todaysOpenCases = await retry(
      { intervalInMs: 1000, maxRetries: 15 },
      getTodaysOpenCases
    );
    console.log(
      `\nOpen support cases created today: ${todaysOpenCases.length}`
    );
    console.log(todaysOpenCases.map((c) => `${c.caseId}`).join("\n"));

    // Create an attachment set.
    console.log("\nCreating an attachment set.");
    const attachmentSetId = await createAttachmentSet();
    console.log(`Attachment set created: ${attachmentSetId}`);

    // Add the attachment set to the support case.
    console.log(`\nAdding attachment set to ${caseId}`);
    await linkAttachmentSetToCase(attachmentSetId, caseId);
    console.log(`Attachment set added to ${caseId}`);

    // List the communications for a support case.
    console.log(`\nListing communications for ${caseId}`);
    const communications = await getCommunications(caseId);
    console.log(
      communications
        .map(
          (c) =>
            `Communication created on ${c.timeCreated}. Has
${c.attachmentSet.length} attachments.`
        )
        .join("\n")
    );
```

```
    // Describe the first attachment.
    console.log(`\nDescribing attachment ${attachmentSetId}`);
    const attachmentId = getFirstAttachment(communications);
    const attachment = await getAttachment(attachmentId);
    console.log(
      `Attachment is the file '${
        attachment.fileName
      }' with data: \n${new TextDecoder().decode(attachment.data)}`
    );

    // Confirm that the support case should be resolved.
    const isResolved = await resolveCase(caseId);
    if (isResolved) {
      // List the resolved cases and include the one previously created.
      // Resolved cases can take a while to appear.
      console.log(
        "\nWaiting for case status to be marked as resolved. This can take some
 time."
      );
      const resolvedCases = await retry(
        { intervalInMs: 20000, maxRetries: 15 },
        () => getTodaysResolvedCases(caseId)
      );
      console.log("Resolved cases:");
      console.log(resolvedCases.map((c) => c.caseId).join("\n"));
    }
  } catch (err) {
    console.error(err);
  }
};
```

- Para obter detalhes da API, consulte os tópicos a seguir na Referência da API do AWS SDK for JavaScript .
  - AddAttachmentsToSet
  - AddCommunicationToCase
  - CreateCase
  - DescribeAttachment
  - DescribeCases
  - DescribeCommunications

- DescribeServices
- DescribeSeverityLevels
- ResolveCase

Kotlin

SDK for Kotlin

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

```
/**
Before running this Kotlin code example, set up your development environment,
including your credentials.

For more information, see the following documentation topic:

https://docs.aws.amazon.com/sdk-for-kotlin/latest/developer-guide/setup.html
In addition, you must have the AWS Business Support Plan to use the AWS Support
 Java API. For more information, see:

https://aws.amazon.com/premiumsupport/plans/

This Kotlin example performs the following tasks:
1. Gets and displays available services.
2. Gets and displays severity levels.
3. Creates a support case by using the selected service, category, and severity
 level.
4. Gets a list of open cases for the current day.
5. Creates an attachment set with a generated file.
6. Adds a communication with the attachment to the support case.
7. Lists the communications of the support case.
8. Describes the attachment set included with the communication.
9. Resolves the support case.
10. Gets a list of resolved cases for the current day.
*/

suspend fun main(args: Array<String>) {
```

```
    val usage = """
    Usage:
        <fileAttachment>
    Where:
         fileAttachment - The file can be a simple saved .txt file to use as an
email attachment.
    """

    if (args.size != 1) {
        println(usage)
        exitProcess(0)
    }

    val fileAttachment = args[0]
    println("***** Welcome to the AWS Support case example scenario.")
    println("***** Step 1. Get and display available services.")
    val sevCatList = displayServices()

    println("***** Step 2. Get and display Support severity levels.")
    val sevLevel = displaySevLevels()

    println("***** Step 3. Create a support case using the selected service,
category, and severity level.")
    val caseIdVal = createSupportCase(sevCatList, sevLevel)
    if (caseIdVal != null) {
        println("Support case $caseIdVal was successfully created!")
    } else {
        println("A support case was not successfully created!")
        exitProcess(1)
    }

    println("***** Step 4. Get open support cases.")
    getOpenCase()

    println("***** Step 5. Create an attachment set with a generated file to add
to the case.")
    val attachmentSetId = addAttachment(fileAttachment)
    println("The Attachment Set id value is $attachmentSetId")

    println("***** Step 6. Add communication with the attachment to the support
case.")
    addAttachSupportCase(caseIdVal, attachmentSetId)

    println("***** Step 7. List the communications of the support case.")
```

```
    val attachId = listCommunications(caseIdVal)
    println("The Attachment id value is $attachId")

    println("***** Step 8. Describe the attachment set included with the
 communication.")
    describeAttachment(attachId)

    println("***** Step 9. Resolve the support case.")
    resolveSupportCase(caseIdVal)

    println("***** Step 10. Get a list of resolved cases for the current day.")
    getResolvedCase()
    println("***** This Scenario has successfully completed")
}

suspend fun getResolvedCase() {
    // Specify the start and end time.
    val now = Instant.now()
    LocalDate.now()
    val yesterday = now.minus(1, ChronoUnit.DAYS)
    val describeCasesRequest = DescribeCasesRequest {
        maxResults = 30
        afterTime = yesterday.toString()
        beforeTime = now.toString()
        includeResolvedCases = true
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeCases(describeCasesRequest)
        response.cases?.forEach { sinCase ->
            println("The case status is ${sinCase.status}")
            println("The case Id is ${sinCase.caseId}")
            println("The case subject is ${sinCase.subject}")
        }
    }
}

suspend fun resolveSupportCase(caseIdVal: String) {
    val caseRequest = ResolveCaseRequest {
        caseId = caseIdVal
    }
    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.resolveCase(caseRequest)
        println("The status of case $caseIdVal is ${response.finalCaseStatus}")
```

```
    }
}

suspend fun describeAttachment(attachId: String?) {
    val attachmentRequest = DescribeAttachmentRequest {
        attachmentId = attachId
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeAttachment(attachmentRequest)
        println("The name of the file is ${response.attachment?.fileName}")
    }
}

suspend fun listCommunications(caseIdVal: String?): String? {
    val communicationsRequest = DescribeCommunicationsRequest {
        caseId = caseIdVal
        maxResults = 10
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response =
 supportClient.describeCommunications(communicationsRequest)
        response.communications?.forEach { comm ->
            println("the body is: " + comm.body)
            comm.attachmentSet?.forEach { detail ->
                return detail.attachmentId
            }
        }
    }
    return ""
}

suspend fun addAttachSupportCase(caseIdVal: String?, attachmentSetIdVal: String?)
 {
    val caseRequest = AddCommunicationToCaseRequest {
        caseId = caseIdVal
        attachmentSetId = attachmentSetIdVal
        communicationBody = "Please refer to attachment for details."
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.addCommunicationToCase(caseRequest)
        if (response.result) {
```

```
            println("You have successfully added a communication to an AWS
 Support case")
        } else {
            println("There was an error adding the communication to an AWS
 Support case")
        }
    }
}

suspend fun addAttachment(fileAttachment: String): String? {
    val myFile = File(fileAttachment)
    val sourceBytes = (File(fileAttachment).readBytes())
    val attachmentVal = Attachment {
        fileName = myFile.name
        data = sourceBytes
    }

    val setRequest = AddAttachmentsToSetRequest {
        attachments = listOf(attachmentVal)
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.addAttachmentsToSet(setRequest)
        return response.attachmentSetId
    }
}

suspend fun getOpenCase() {
    // Specify the start and end time.
    val now = Instant.now()
    LocalDate.now()
    val yesterday = now.minus(1, ChronoUnit.DAYS)
    val describeCasesRequest = DescribeCasesRequest {
        maxResults = 20
        afterTime = yesterday.toString()
        beforeTime = now.toString()
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeCases(describeCasesRequest)
        response.cases?.forEach { sinCase ->
            println("The case status is ${sinCase.status}")
            println("The case Id is ${sinCase.caseId}")
            println("The case subject is ${sinCase.subject}")
```

```
        }
    }
}

suspend fun createSupportCase(sevCatListVal: List<String>, sevLevelVal: String):
 String? {
    val serCode = sevCatListVal[0]
    val caseCategory = sevCatListVal[1]
    val caseRequest = CreateCaseRequest {
        categoryCode = caseCategory.lowercase(Locale.getDefault())
        serviceCode = serCode.lowercase(Locale.getDefault())
        severityCode = sevLevelVal.lowercase(Locale.getDefault())
        communicationBody = "Test issue with
 ${serCode.lowercase(Locale.getDefault())}"
        subject = "Test case, please ignore"
        language = "en"
        issueType = "technical"
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.createCase(caseRequest)
        return response.caseId
    }
}

suspend fun displaySevLevels(): String {
    var levelName = ""
    val severityLevelsRequest = DescribeSeverityLevelsRequest {
        language = "en"
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response =
 supportClient.describeSeverityLevels(severityLevelsRequest)
        response.severityLevels?.forEach { sevLevel ->
            println("The severity level name is: ${sevLevel.name}")
            if (sevLevel.name == "High") {
                levelName = sevLevel.name!!
            }
        }
        return levelName
    }
}
```

```
// Return a List that contains a Service name and Category name.
suspend fun displayServices(): List<String> {
    var serviceCode = ""
    var catName = ""
    val sevCatList = mutableListOf<String>()
    val servicesRequest = DescribeServicesRequest {
        language = "en"
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeServices(servicesRequest)
        println("Get the first 10 services")
        var index = 1

        response.services?.forEach { service ->
            if (index == 11) {
                return@forEach
            }

            println("The Service name is ${service.name}")
            if (service.name == "Account") {
                serviceCode = service.code.toString()
            }

            // Get the categories for this service.
            service.categories?.forEach { cat ->
                println("The category name is ${cat.name}")
                if (cat.name == "Security") {
                    catName = cat.name!!
                }
            }
            index++
        }
    }

    // Push the two values to the list.
    serviceCode.let { sevCatList.add(it) }
    catName.let { sevCatList.add(it) }
    return sevCatList
}
```

- Para obter detalhes da API, consulte os tópicos a seguir na Referência da API do AWS SDK para Kotlin.
  - AddAttachmentsToSet
  - AddCommunicationToCase
  - CreateCase
  - DescribeAttachment
  - DescribeCases
  - DescribeCommunications
  - DescribeServices
  - DescribeSeverityLevels
  - ResolveCase

Python

SDK para Python (Boto3)

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

Execute um cenário interativo em um prompt de comando.

```
class SupportCasesScenario:
    """Runs an interactive scenario that shows how to get started using AWS
 Support."""

    def __init__(self, support_wrapper):
        """
        :param support_wrapper: An object that wraps AWS Support actions.
        """
        self.support_wrapper = support_wrapper

    def display_and_select_service(self):
        """
        Lists support services and prompts the user to select one.
```

```
        :return: The support service selected by the user.
        """
        print("-" * 88)
        services_list = self.support_wrapper.describe_services("en")
        print(f"AWS Support client returned {len(services_list)} services.")
        print("Displaying first 10 services:")

        service_choices = [svc["name"] for svc in services_list[:10]]
        selected_index = q.choose(
            "Select an example support service by entering a number from the
preceding list:",
            service_choices,
        )
        selected_service = services_list[selected_index]
        print("-" * 88)
        return selected_service

    def display_and_select_category(self, service):
        """
        Lists categories for a support service and prompts the user to select
one.

        :param service: The service of the categories.
        :return: The selected category.
        """
        print("-" * 88)
        print(
            f"Available support categories for Service {service['name']}
{len(service['categories'])}:"
        )
        categories_choices = [category["name"] for category in
service["categories"]]
        selected_index = q.choose(
            "Select an example support category by entering a number from the
preceding list:",
            categories_choices,
        )
        selected_category = service["categories"][selected_index]
        print("-" * 88)
        return selected_category

    def display_and_select_severity(self):
        """
        Lists available severity levels and prompts the user to select one.
```

```
        :return: The selected severity level.
        """
        print("-" * 88)
        severity_levels_list =
self.support_wrapper.describe_severity_levels("en")
        print(f"Available severity levels:")
        severity_choices = [level["name"] for level in severity_levels_list]
        selected_index = q.choose(
            "Select an example severity level by entering a number from the
preceding list:",
            severity_choices,
        )
        selected_severity = severity_levels_list[selected_index]
        print("-" * 88)
        return selected_severity

    def create_example_case(self, service, category, severity_level):
        """
        Creates an example support case with the user's selections.

        :param service: The service for the new case.
        :param category: The category for the new case.
        :param severity_level: The severity level for the new case.
        :return: The caseId of the new support case.
        """
        print("-" * 88)
        print(f"Creating new case for service {service['name']}.")
        case_id = self.support_wrapper.create_case(service, category,
severity_level)
        print(f"\tNew case created with ID {case_id}.")
        print("-" * 88)
        return case_id

    def list_open_cases(self):
        """
        List the open cases for the current day.
        """
        print("-" * 88)
        print("Let's list the open cases for the current day.")
        start_time = str(datetime.utcnow().date())
        end_time = str(datetime.utcnow().date() + timedelta(days=1))
        open_cases = self.support_wrapper.describe_cases(start_time, end_time,
False)
```

```
        for case in open_cases:
            print(f"\tCase: {case['caseId']}: status {case['status']}.")
        print("-" * 88)

    def create_attachment_set(self):
        """
        Create an attachment set with a sample file.

        :return: The attachment set ID of the new attachment set.
        """
        print("-" * 88)
        print("Creating attachment set with a sample file.")
        attachment_set_id = self.support_wrapper.add_attachment_to_set()
        print(f"\tNew attachment set created with ID {attachment_set_id}.")
        print("-" * 88)
        return attachment_set_id

    def add_communication(self, case_id, attachment_set_id):
        """
        Add a communication with an attachment set to the case.

        :param case_id: The ID of the case for the communication.
        :param attachment_set_id: The ID of the attachment set to
        add to the communication.
        """
        print("-" * 88)
        print(f"Adding a communication and attachment set to the case.")
        self.support_wrapper.add_communication_to_case(attachment_set_id,
case_id)
        print(
            f"Added a communication and attachment set {attachment_set_id} to the
case {case_id}."
        )
        print("-" * 88)

    def list_communications(self, case_id):
        """
        List the communications associated with a case.

        :param case_id: The ID of the case.
        :return: The attachment ID of an attachment.
        """
        print("-" * 88)
        print("Let's list the communications for our case.")
```

```
        attachment_id = ""
        communications =
self.support_wrapper.describe_all_case_communications(case_id)
        for communication in communications:
            print(
                f"\tCommunication created on {communication['timeCreated']} "
                f"has {len(communication['attachmentSet'])} attachments."
            )
            if len(communication["attachmentSet"]) > 0:
                attachment_id = communication["attachmentSet"][0]["attachmentId"]
        print("-" * 88)
        return attachment_id

    def describe_case_attachment(self, attachment_id):
        """
        Describe an attachment associated with a case.

        :param attachment_id: The ID of the attachment.
        """
        print("-" * 88)
        print("Let's list the communications for our case.")
        attached_file = self.support_wrapper.describe_attachment(attachment_id)
        print(f"\tAttachment includes file {attached_file}.")
        print("-" * 88)

    def resolve_case(self, case_id):
        """
        Shows how to resolve an AWS Support case by its ID.

        :param case_id: The ID of the case to resolve.
        """
        print("-" * 88)
        print(f"Resolving case with ID {case_id}.")
        case_status = self.support_wrapper.resolve_case(case_id)
        print(f"\tFinal case status is {case_status}.")
        print("-" * 88)

    def list_resolved_cases(self):
        """
        List the resolved cases for the current day.
        """
        print("-" * 88)
        print("Let's list the resolved cases for the current day.")
        start_time = str(datetime.utcnow().date())
```

```
        end_time = str(datetime.utcnow().date() + timedelta(days=1))
        resolved_cases = self.support_wrapper.describe_cases(start_time,
 end_time, True)
        for case in resolved_cases:
            print(f"\tCase: {case['caseId']}: status {case['status']}.")
        print("-" * 88)

    def run_scenario(self):
        logging.basicConfig(level=logging.INFO, format="%(levelname)s:
 %(message)s")

        print("-" * 88)
        print("Welcome to the AWS Support get started with support cases demo.")
        print("-" * 88)

        selected_service = self.display_and_select_service()
        selected_category = self.display_and_select_category(selected_service)
        selected_severity = self.display_and_select_severity()
        new_case_id = self.create_example_case(
            selected_service, selected_category, selected_severity
        )
        wait(10)
        self.list_open_cases()
        new_attachment_set_id = self.create_attachment_set()
        self.add_communication(new_case_id, new_attachment_set_id)
        new_attachment_id = self.list_communications(new_case_id)
        self.describe_case_attachment(new_attachment_id)
        self.resolve_case(new_case_id)
        wait(10)
        self.list_resolved_cases()

        print("\nThanks for watching!")
        print("-" * 88)


if __name__ == "__main__":
    try:
        scenario = SupportCasesScenario(SupportWrapper.from_client())
        scenario.run_scenario()
    except Exception:
        logging.exception("Something went wrong with the demo.")
```

Definir uma classe que envolva ações de suporte ao cliente.

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def describe_services(self, language):
        """
        Get the descriptions of AWS services available for support for a
 language.

        :param language: The language for support services.
        Currently, only "en" (English) and "ja" (Japanese) are supported.
        :return: The list of AWS service descriptions.
        """
        try:
            response = self.support_client.describe_services(language=language)
            services = response["services"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
 Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
 subscription to run these "
                    "examples."
                )
            else:
                logger.error(
```

```
                    "Couldn't get Support services for language %s. Here's why:
%s: %s",
                    language,
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return services


    def describe_severity_levels(self, language):
        """
        Get the descriptions of available severity levels for support cases for a
language.

        :param language: The language for support severity levels.
        Currently, only "en" (English) and "ja" (Japanese) are supported.
        :return: The list of severity levels.
        """
        try:
            response =
self.support_client.describe_severity_levels(language=language)
            severity_levels = response["severityLevels"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't get severity levels for language %s. Here's why:
%s: %s",
                    language,
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return severity_levels
```

```
    def create_case(self, service, category, severity):
        """
        Create a new support case.

        :param service: The service to use for the new case.
        :param category: The category to use for the new case.
        :param severity: The severity to use for the new case.
        :return: The caseId of the new case.
        """
        try:
            response = self.support_client.create_case(
                subject="Example case for testing, ignore.",
                serviceCode=service["code"],
                severityCode=severity["code"],
                categoryCode=category["code"],
                communicationBody="Example support case body.",
                language="en",
                issueType="customer-service",
            )
            case_id = response["caseId"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't create case. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return case_id


    def add_attachment_to_set(self):
        """
```

```
        Add an attachment to a set, or create a new attachment set if one does
not exist.

        :return: The attachment set ID.
        """
        try:
            response = self.support_client.add_attachments_to_set(
                attachments=[
                    {
                        "fileName": "attachment_file.txt",
                        "data": b"This is a sample file for attachment to a
support case.",
                    }
                ]
            )
            new_set_id = response["attachmentSetId"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't add attachment. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return new_set_id


    def add_communication_to_case(self, attachment_set_id, case_id):
        """
        Add a communication and an attachment set to a case.

        :param attachment_set_id: The ID of an existing attachment set.
        :param case_id: The ID of the case.
        """
        try:
```

```
            self.support_client.add_communication_to_case(
                caseId=case_id,
                communicationBody="This is an example communication added to a
support case.",
                attachmentSetId=attachment_set_id,
            )
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't add communication. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise


    def describe_all_case_communications(self, case_id):
        """
        Describe all the communications for a case using a paginator.

        :param case_id: The ID of the case.
        :return: The communications for the case.
        """
        try:
            communications = []
            paginator =
self.support_client.get_paginator("describe_communications")
            for page in paginator.paginate(caseId=case_id):
                communications += page["communications"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
```

```
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't describe communications. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return communications


    def describe_attachment(self, attachment_id):
        """
        Get information about an attachment by its attachmentID.

        :param attachment_id: The ID of the attachment.
        :return: The name of the attached file.
        """
        try:
            response = self.support_client.describe_attachment(
                attachmentId=attachment_id
            )
            attached_file = response["attachment"]["fileName"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't get attachment description. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return attached_file
```

```
    def resolve_case(self, case_id):
        """
        Resolve a support case by its caseId.

        :param case_id: The ID of the case to resolve.
        :return: The final status of the case.
        """
        try:
            response = self.support_client.resolve_case(caseId=case_id)
            final_status = response["finalCaseStatus"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't resolve case. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return final_status


    def describe_cases(self, after_time, before_time, resolved):
        """
        Describe support cases over a period of time, optionally filtering
        by status.

        :param after_time: The start time to include for cases.
        :param before_time: The end time to include for cases.
        :param resolved: True to include resolved cases in the results,
            otherwise results are open cases.
        :return: The final status of the case.
        """
        try:
            cases = []
```

```
            paginator = self.support_client.get_paginator("describe_cases")
            for page in paginator.paginate(
                afterTime=after_time,
                beforeTime=before_time,
                includeResolvedCases=resolved,
                language="en",
            ):
                cases += page["cases"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't describe cases. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            if resolved:
                cases = filter(lambda case: case["status"] == "resolved", cases)
            return cases
```

- Para obter detalhes da API, consulte os tópicos a seguir na Referência da API do AWS SDK para Python (Boto3).
  - AddAttachmentsToSet
  - AddCommunicationToCase
  - CreateCase
  - DescribeAttachment
  - DescribeCases
  - DescribeCommunications

- DescribeServices
- DescribeSeverityLevels
- ResolveCase

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsar o AWS Support com um SDK da AWS. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Monitorar e registrar em log para o AWS Support

O monitoramento é uma parte importante para manter a confiabilidade, a disponibilidade e a performance do AWS Support e das outras soluções da AWS. A AWS fornece as ferramentas de monitoramento a seguir para observar o AWS Support, informar quando algo está errado e realizar ações automaticamente quando apropriado:

- O Amazon EventBridge oferece uma transmissão quase em tempo real dos eventos do sistema que descrevem as alterações nos recursos da AWS. O EventBridge habilita a computação orientada a eventos automatizada, já que é possível escrever regras que monitoram determinados eventos e acionam ações automatizadas em outros serviços da AWS quando esses eventos ocorrem. Para obter mais informações, consulte o Guia do usuário do Amazon EventBridge.
- O AWS CloudTrail captura chamadas de API e eventos relacionados feitos por ou em nome de sua conta da AWS e entrega os arquivos de log a um bucket do Amazon S3 que você especificar. Você pode identificar quais usuários e contas chamaram a AWS, o endereço IP de origem do qual as chamadas foram feitas e quando elas ocorreram. Para obter mais informações, consulte o Guia do usuário da AWS CloudTrail.

Tópicos

- Monitorando AWS Support casos com a Amazon EventBridge
- Registrar em log chamadas de API do AWS Support com o AWS CloudTrail
- Como fazer registro em log no aplicativo AWS Support nas chamadas de API do Slack com o AWS CloudTrail

Monitorando AWS Support casos com a Amazon EventBridge

Você pode usar EventBridge a Amazon para detectar e reagir às mudanças em seus AWS Support casos. Em seguida, com base nas regras que você cria, EventBridge invoca uma ou mais ações de destino quando um evento corresponde aos valores que você especifica em uma regra.

Dependendo do evento, envie notificações, capture informações, tome medidas corretivas, inicie eventos ou realize outras ações. Por exemplo, você poderá ser notificado sempre que as seguintes ações ocorrerem na conta:

- Criar um caso de suporte

- Adicionar uma correspondência de caso a um caso de suporte existente
- Resolver um caso de suporte
- Reabrir um caso de suporte

> **Note**
>
> O AWS Support entrega eventos em uma base de melhor esforço. Não é garantido que os eventos sejam sempre entregues ao EventBridge.

Criar uma regra do EventBridge para casos do AWS Support

Você pode criar uma EventBridge regra para ser notificado sobre eventos de AWS Support casos. A regra monitorará as atualizações de casos de suporte em sua conta, incluindo ações que você, seus usuários do IAM ou agentes de suporte executam. Antes de criar uma regra para eventos de caso de AWS Support, faça o seguinte:

- Familiarize-se com eventos, regras e metas em EventBridge. Para obter mais informações, consulte O que é a Amazon EventBridge? no Guia do EventBridge usuário da Amazon.
- Crie os destinos para usar em sua regra de evento. Por exemplo, é possível criar um tópico do Amazon Simple Notification Service (Amazon SNS) para que sempre que um caso de suporte for atualizado, você receba uma mensagem de texto ou e-mail. Para obter mais informações, consulte EventBridgealvos.

> **Note**
>
> O AWS Support é um serviço global. Para receber atualizações dos seus casos de suporte, você pode usar uma das seguintes regiões: Leste dos EUA (Norte da Virgínia), Oeste dos EUA (Oregon) ou Europa (Irlanda).

Para criar uma EventBridge regra para eventos de AWS Support caso

1. Abra o EventBridge console da Amazon em https://console.aws.amazon.com/events/.
2. Caso ainda não tenha feito isso, use o Region selector (Seletor de regiões) no canto superior direito da página e escolha US East (N. Virginia) (Leste dos EUA (Norte da Virgínia)).

3. No painel de navegação, escolha Regras.
4. Escolha Criar regra.
5. Na página Definir detalhe de regra, insira um nome e uma descrição para sua regra.
6. Mantenha os valores padrão do Barramento de eventos e Tipo de regra e, depois, escolha Próximo.
7. Na página Criar padrão de evento, em Origem do evento, escolha AWSeventos ou eventos de EventBridge parceiros.
8. Em Event pattern (Padrão de evento), mantenha o valor padrão para Serviços da AWS.
9. Em AWS service (Serviço da AWS), escolha Support (Suporte).
10. Para Event type (Tipo de evento), escolha Support Case Update (Atualização do caso de suporte).
11. Escolha Próximo.
12. Na seção Select targets (Selecionar destinos), escolha o tipo de destino criado para essa regra e, em seguida, configure quaisquer opções adicionais necessárias para esse tipo. Por exemplo, se você escolher o Amazon SNS, verifique se o tópico do SNS está configurado corretamente para que você seja notificado por e-mail ou SMS.
13. Escolha Próximo.
14. (Opcional) Na página Configurar tags, adicione tags e escolha Próximo.
15. Na página Review and create (Revisar e criar), analise a configuração da regra e verifique se ela atende aos requisitos de monitoramento de eventos.
16. Escolha Criar regra. Sua regra agora monitorará eventos de casos de AWS Support e, em seguida, enviará o evento para o destino que você especificou.

Observações

- Ao receber um evento, você pode usar o parâmetro `origin` para determinar se você ou um agente de AWS Support adicionou uma correspondência de caso a um caso de suporte. O valor de `origin` pode ser `CUSTOMER` ou `AWS`.

  No momento, apenas eventos para a ação `AddCommunicationToCase` terão esse valor.
- Para obter mais informações sobre a criação de padrões de eventos, consulte Padrões de eventos no Guia EventBridge do usuário da Amazon.

- Você também pode criar outra regra para a chamada de AWS API por meio do tipo de CloudTrail evento. Esta regra monitorará logs do AWS CloudTrail para chamadas de API do AWS Support na sua conta.

Eventos de exemplo do AWS Support

Os eventos a seguir são criados quando ações de suporte ocorrem em sua conta.

Example : criar caso de suporte

O evento a seguir é criado quando um caso de suporte é criado.


```
{
    "version": "0",
    "id": "3433df007-9285-55a3-f6d1-536944be45d7",
    "detail-type": "Support Case Update",
    "source": "aws.support",
    "account": "111122223333",
    "time": "2022-02-21T15:51:19Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "case-id": "case-111122223333-muen-2022-7118885805350839",
        "display-id": "1234563851",
        "communication-id": "",
        "event-name": "CreateCase",
        "origin": ""
    }
}
```


Example : atualizar caso de suporte

O evento a seguir é criado quando o AWS Support responde a um caso de suporte.


```
{
    "version": "0",
    "id": "f90cb8cb-32be-1c91-c0ba-d50b4ca5e51b",
    "detail-type": "Support Case Update",
    "source": "aws.support",
    "account": "111122223333",
```

```
    "time": "2022-02-21T15:51:31Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "case-id": "case-111122223333-muen-2022-7118885805350839",
        "display-id": "1234563851",
        "communication-id": "ekko:us-east-1:12345678-268a-424b-be08-54613cab84d2",
        "event-name": "AddCommunicationToCase",
        "origin": "AWS"
    }
}
```

Example : resolver caso de suporte

O evento a seguir é criado quando um caso de suporte é resolvido.

```
{
    "version": "0",
    "id": "1aa4458d-556f-732e-ddc1-4a5b2fbd14a5",
    "detail-type": "Support Case Update",
    "source": "aws.support",
    "account": "111122223333",
    "time": "2022-02-21T15:51:31Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "case-id": "case-111122223333-muen-2022-7118885805350839",
        "display-id": "1234563851",
        "communication-id": "",
        "event-name": "ResolveCase",
        "origin": ""
    }
}
```

Example : reabrir caso de suporte

O evento a seguir é criado quando um caso de suporte é reaberto.

```
{
    "version": "0",
    "id": "3bb9d8fe-6089-ad27-9508-804209b233ad",
    "detail-type": "Support Case Update",
    "source": "aws.support",
```

```
    "account": "111122223333",
    "time": "2022-02-21T15:47:19Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "case-id": "case-111122223333-muen-2021-27f40618fe0303ea",
        "display-id": "1234563851",
        "communication-id": "",
        "event-name": "ReopenCase",
        "origin": ""
    }
}
```

Consulte também

Para obter mais informações sobre como usar EventBridge comAWS Support, consulte os seguintes recursos:

- Como automatizar a AWS Support API com a Amazon EventBridge
- AWS Supportnotificador de atividade de caso em GitHub

Registrar em log chamadas de API do AWS Support com o AWS CloudTrail

O AWS Support é integrado ao AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, uma função ou um serviço da AWS no AWS Support. O CloudTrail captura as chamadas de API do AWS Support como eventos. As chamadas capturadas incluem as chamadas do console do AWS Support e as chamadas de código para as operações da API do AWS Support.

Se você criar uma trilha, poderá habilitar a entrega contínua de eventos do CloudTrail para um bucket do Amazon Simple Storage Service (Amazon S3), incluindo eventos para o AWS Support. Se você não configurar uma trilha, ainda poderá visualizar os eventos mais recentes no console do CloudTrail em Event history (Histórico de eventos).

Usando as informações coletadas pelo CloudTrail, é possível determinar a solicitação feita para o AWS Support, o endereço IP no qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita, além de detalhes adicionais.

Para saber mais sobre o CloudTrail, incluindo como configurá-lo e ativá-lo, consulte o Guia do usuário do AWS CloudTrail.

Informações do AWS Support no CloudTrail

O CloudTrail é habilitado em sua conta da AWS quando ela é criada. Quando a atividade do evento compatível ocorrer no AWS Support, ela será registrada em um evento do CloudTrail juntamente com outros eventos de serviços da AWS no Event history (Histórico de eventos). Você pode visualizar, pesquisar e baixar eventos recentes em sua conta da AWS. Para obter mais informações, consulte Visualizar eventos com o histórico de eventos do CloudTrail.

Para obter um registro contínuo de eventos na conta da AWS, incluindo eventos do AWS Support, crie uma trilha. Uma trilha permite que o CloudTrail entregue arquivos de log a um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, ela é aplicada a todas as regiões da AWS. A trilha registra em log eventos de todas as regiões na partição da AWS e entrega os arquivos de log para o bucket do Amazon S3 especificado por você. Além disso, é possível configurar outros serviços da AWS para analisar mais ainda mais e agir com base nos dados de eventos coletados nos logs do CloudTrail. Para obter mais informações, consulte:

- Visão geral da criação de uma trilha
- Serviços e integrações compatíveis com o CloudTrail
- Configurar notificações do Amazon SNS para o CloudTrail
- Receber arquivos de log do CloudTrail de várias regiões e Receber arquivos de log do CloudTrail de várias contas

Todas as operações de API do AWS Support são registradas pelo CloudTrail e são documentadas na Referência de API do AWS Support.

Por exemplo, as chamadas para as operações `CreateCase`, `DescribeCases` e `ResolveCase` geram entradas nos arquivos de log do CloudTrail.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com credenciais de usuário raiz ou do AWS Identity and Access Management (IAM).
- Se a solicitação foi feita com credenciais de segurança temporárias de uma função ou de um usuário federado.

- Se a solicitação foi feita por outro serviço da AWS.

Para obter mais informações, consulte Elemento userIdentity do CloudTrail.

Também é possível agregar arquivos de log do AWS Support de várias regiões da AWS e contas da AWS em um único bucket do Amazon S3.

Informações do AWS Trusted Advisor no registro do CloudTrail

O Trusted Advisor é um serviço no AWS Support que permite que você verifique sua conta da AWS para obter maneiras de economizar custos, melhorar a segurança e otimizar sua conta.

Todas as operações de API do Trusted Advisor são registradas pelo CloudTrail e são documentadas na Referência de API do AWS Support.

Por exemplo, as chamadas para as operações `DescribeTrustedAdvisorCheckRefreshStatuses`, `DescribeTrustedAdvisorCheckResult` e `RefreshTrustedAdvisorCheck` geram entradas nos arquivos de log do CloudTrail.

> **Note**
>
> O CloudTrail também registra ações do console do Trusted Advisor. Consulte Registro de ações do console do AWS Trusted Advisor com AWS CloudTrail.

Noções básicas sobre entradas de arquivos de log do AWS Support

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log a um bucket do Amazon S3 especificado. Os arquivos de log do CloudTrail contêm uma ou mais entradas de log. Um evento representa uma solicitação única de qualquer fonte. Ele inclui informações sobre a operação solicitada, a data e a hora da operação, os parâmetros de solicitação e assim por diante. Os arquivos de log do CloudTrail não são um rastreamento de pilha ordenada de chamadas de API pública. Dessa forma, eles não são exibidos em uma ordem específica.

Example : Entrada de log para CreateCase

O exemplo a seguir mostra uma entrada de log do CloudTrail para a operação CreateCase.

```
{
```

```
   "Records": [
      {
         "eventVersion": "1.04",
         "userIdentity": {
            "type": "IAMUser",
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
            "arn": "arn:aws:iam::111122223333:user/janedoe",
            "accountId": "111122223333",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "userName": "janedoe",
            "sessionContext": {
               "attributes": {
                  "mfaAuthenticated": "false",
                  "creationDate": "2016-04-13T17:51:37Z"
               }
            },
            "invokedBy": "signin.amazonaws.com"
         },
         "eventTime": "2016-04-13T18:05:53Z",
         "eventSource": "support.amazonaws.com",
         "eventName": "CreateCase",
         "awsRegion": "us-east-1",
         "sourceIPAddress": "198.51.100.15",
         "userAgent": "signin.amazonaws.com",
         "requestParameters": {
            "severityCode": "low",
            "categoryCode": "other",
            "language": "en",
            "serviceCode": "support-api",
            "issueType": "technical"
         },
         "responseElements": {
            "caseId": "case-111122223333-muen-2016-c3f2077e504940f2"
         },
         "requestID": "58c257ef-01a2-11e6-be2a-01c031063738",
         "eventID": "5aa34bfc-ad5b-4fb1-8a55-2277c86e746a",
         "eventType": "AwsApiCall",
         "recipientAccountId": "111122223333"
      }
   ],
   ...
}
```

Example : Entrada de log para RefreshTrustedAdvisorCheck

O exemplo a seguir mostra uma entrada de log do CloudTrail para a operação RefreshTrustedAdvisorCheck.


```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/Admin",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Admin"
    },
    "eventTime": "2020-10-21T16:34:13Z",
    "eventSource": "support.amazonaws.com",
    "eventName": "RefreshTrustedAdvisorCheck",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "72.21.198.67",
    "userAgent": "signin.amazonaws.com",
    "requestParameters": {
        "checkId": "Pfx0RwqBli"
    },
    "responseElements": null,
    "requestID": "4c4d5fc8-c403-4f82-9544-41f820e0fa01",
    "eventID": "2f4630ac-5c27-4f0d-b93f-63742d6fc85e",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```


Como fazer registro em log no aplicativo AWS Support nas chamadas de API do Slack com o AWS CloudTrail

O aplicativo AWS Support no Slack está integrado com o AWS CloudTrail. O CloudTrail fornece um registro de ações executadas por um usuário, um perfil ou um AWS service (Serviço da AWS) no aplicativo AWS Support. Para criar esse registro, o CloudTrail captura todas as chamadas de API públicas para o aplicativo AWS Support como eventos. As chamadas capturadas incluem as chamadas do console do aplicativo AWS Support e as chamadas de código para as operações da API pública do aplicativo AWS Support. Se você criar uma trilha, poderá habilitar a entrega contínua

de eventos do CloudTrail para um bucket do Amazon S3. Isso inclui eventos para o aplicativo AWS Support. Se você não configurar uma trilha, ainda poderá visualizar os eventos mais recentes no console do CloudTrail em Event history (Histórico de eventos). Você pode usar as informações que o CloudTrail coleta para determinar se a solicitação foi feita para o aplicativo AWS Support. Você também pode determinar o endereço IP do qual a chamada foi feita, quem fez a solicitação, quando ela foi feita e detalhes adicionais.

Para saber mais sobre o CloudTrail, consulte o Guia do usuário do AWS CloudTrail.

Informações do aplicativo AWS Support no CloudTrail

O CloudTrail é ativado em sua Conta da AWS quando ela é criada. Quando ocorre uma atividade de API pública no aplicativo AWS Support, essa atividade é registrada em um evento do CloudTrail junto com outros eventos de serviços da AWS no Event history (Histórico de eventos). Você pode visualizar, pesquisar e baixar eventos recentes em sua Conta da AWS. Para obter mais informações, consulte Viewing events with CloudTrail Event history (Como visualizar eventos com o histórico de eventos do CloudTrail).

Para obter um registro de eventos em andamento na sua Conta da AWS, incluindo eventos do aplicativo AWS Support, crie uma trilha. Por padrão, quando você cria uma trilha no console, ela é aplicada a todas as Regiões da AWS. A trilha registra em log eventos de todas as regiões na partição da AWS e entrega os arquivos de log para o bucket do Amazon S3 especificado por você. Além disso, você pode configurar outros Serviços da AWS para analisar mais ainda os dados de eventos coletados nos logs do CloudTrail e agir de acordo com esses dados. Para obter mais informações, consulte as informações a seguir.

- Visão geral da criação de uma trilha
- Serviços e integrações compatíveis com o CloudTrail
- Configurar notificações do Amazon SNS para o CloudTrail
- Receber arquivos de log do CloudTrail de várias regiões e Receber arquivos de log do CloudTrail de várias contas

O CloudTrail registra todas as ações do aplicativo AWS Support. Essas ações estão também documentadas em AWS Support App in Slack API Reference. Por exemplo, as chamadas para as ações `CreateSlackChannelConfiguration`, `GetAccountAlias` e `UpdateSlackChannelConfiguration` geram entradas nos arquivos de log do CloudTrail.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com credenciais de usuário raiz ou do AWS Identity and Access Management (IAM).
- Se a solicitação foi feita com credenciais de segurança temporárias de uma função ou de um usuário federado.
- Se a solicitação foi feita por outro AWS service (Serviço da AWS).

Para obter mais informações, consulte Elemento userIdentity do CloudTrail.

Noções básicas sobre entradas de arquivos de log do aplicativo AWS Support

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log a um bucket do Amazon S3 especificado. Os arquivos de log do CloudTrail contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer fonte e inclui informações sobre a ação solicitada, a data e a hora da ação, os parâmetros de solicitação e assim por diante. Os arquivos de log do CloudTrail não são um rastreamento de pilha ordenada das chamadas de API pública. Isso significa que os logs não aparecem em nenhuma ordem específica.

Example : exemplo de log para **`CreateSlackChannelConfiguration`**

O exemplo a seguir mostra uma entrada de log do CloudTrail para a operação CreateSlackChannelConfiguration.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE:JaneDoe",
        "arn": "arn:aws:sts::111122223333:assumed-role/Administrator/JaneDoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Administrator",
```

```
                "accountId": "111122223333",
                "userName": "Administrator"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-02-26T01:37:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-02-26T01:48:20Z",
    "eventSource": "supportapp.amazonaws.com",
    "eventName": "CreateSlackChannelConfiguration",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "205.251.233.183",
    "userAgent": "aws-cli/1.3.23 Python/2.7.6 Linux/2.6.18-164.el5",
    "requestParameters": {
        "notifyOnCreateOrReopenCase": true,
        "teamId": "T012ABCDEFG",
        "notifyOnAddCorrespondenceToCase": true,
        "notifyOnCaseSeverity": "all",
        "channelName": "troubleshooting-channel",
        "notifyOnResolveCase": true,
        "channelId": "C01234A5BCD",
        "channelRoleArn": "arn:aws:iam::111122223333:role/AWSSupportAppRole"
    },
    "responseElements": null,
    "requestID": "d06df6ca-c233-4ffb-bbff-63470c5dc255",
    "eventID": "0898ce29-a396-444a-899d-b068f390c361",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Example : exemplo de log para **`ListSlackChannelConfigurations`**

O exemplo a seguir mostra uma entrada de log do CloudTrail para a operação ListSlackChannelConfigurations.

```
{
    "eventVersion": "1.08",
```

```
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE:AWSSupportAppRole",
        "arn": "arn:aws:sts::111122223333:assumed-role/AWSSupportAppRole",
        "accountId": "111122223333",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/AWSSupportAppRole",
                "accountId": "111122223333",
                "userName": "AWSSupportAppRole"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-03-01T20:06:32Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-03-01T20:06:46Z",
    "eventSource": "supportapp.amazonaws.com",
    "eventName": "ListSlackChannelConfigurations",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "72.21.217.131",
    "userAgent": "aws-cli/1.3.23 Python/2.7.6 Linux/2.6.18-164.el5",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "20f81d63-31c5-4351-bd02-9eda7f76e7b8",
    "eventID": "70acb7fe-3f84-47cd-8c28-cc148ad06d21",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


Example : exemplo de log para **`GetAccountAlias`**

O exemplo a seguir mostra uma entrada de log do CloudTrail para a operação GetAccountAlias.


```
{
    "eventVersion": "1.08",
```

```
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE:devdsk",
        "arn": "arn:aws:sts::111122223333:assumed-role/AWSSupportAppRole/devdsk",
        "accountId": "111122223333",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/AWSSupportAppRole",
                "accountId": "111122223333",
                "userName": "AWSSupportAppRole"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-03-01T20:31:27Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-03-01T20:31:47Z",
    "eventSource": "supportapp.amazonaws.com",
    "eventName": "GetAccountAlias",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "72.21.217.142",
    "userAgent": "aws-cli/1.3.23 Python/2.7.6 Linux/2.6.18-164.el5",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "a225966c-0906-408b-b8dd-f246665e6758",
    "eventID": "79ebba8d-3285-4023-831a-64af7de8d4ad",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Como monitorar e registrar nos planos do AWS Support

O monitoramento é uma parte importante para manter a confiabilidade, a disponibilidade e a performance dos planos de suporte e de outras soluções da AWS. A AWS fornece as ferramentas de monitoramento a seguir para observar os planos de suporte, informar quando algo está errado e realizar ações automaticamente quando apropriado:

- O AWS CloudTrail captura chamadas de API e eventos relacionados feitos por ou em nome de sua conta da AWS e entrega os arquivos de log a um bucket do Amazon S3 que você especificar. Você pode identificar quais usuários e contas chamaram a AWS, o endereço IP de origem do qual as chamadas foram feitas e quando elas ocorreram. Para obter mais informações, consulte o Guia do usuário da AWS CloudTrail.

Tópicos

- Como registrar as chamadas de API dos planos do AWS Support com o AWS CloudTrail

Como registrar as chamadas de API dos planos do AWS Support com o AWS CloudTrail

Os planos do AWS Support são integrados ao AWS CloudTrail, um produto que fornece um registro de ações tomadas por um usuário, um perfil ou um AWS service (Serviço da AWS). O CloudTrail captura as chamadas de API dos planos do AWS Support como eventos. As chamadas capturadas incluem chamadas do console dos planos do AWS Support e chamadas de código para as operações de API dos planos do AWS Support.

Se você criar uma trilha, poderá habilitar a entrega contínua de eventos do CloudTrail para um bucket do Amazon Simple Storage Service (Amazon S3), incluindo eventos para os planos do AWS Support. Se você não configurar uma trilha, ainda poderá visualizar os eventos mais recentes no console do CloudTrail em Event history (Histórico de eventos).

Com as informações coletadas pelo CloudTrail, determine a solicitação feita para os planos do AWS Support, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e os detalhes adicionais.

Para saber mais sobre o CloudTrail, incluindo como configurá-lo e ativá-lo, consulte o Guia do usuário do AWS CloudTrail.

Informações dos planos do AWS Support no CloudTrail

O CloudTrail é habilitado em sua Conta da AWS quando ela é criada. Quando a atividade do evento compatível ocorrer nos planos do AWS Support, ela será registrada em um evento do CloudTrail juntamente com outros eventos do AWS service (Serviço da AWS) no Event history (Histórico de eventos). Você pode visualizar, pesquisar e baixar eventos recentes em sua conta da . Para obter mais informações, consulte Visualizar eventos com o histórico de eventos do CloudTrail.

Para obter um registro contínuo de eventos em sua conta, incluindo eventos para os planos do AWS Support, crie uma trilha. Uma trilha permite que o CloudTrail entregue arquivos de log a um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, ela é aplicada a todas as Regiões da AWS. A trilha registra em log eventos de todas as regiões na partição da AWS e entrega os arquivos de log para o bucket do Amazon S3 especificado por você. Além disso, você pode configurar outros Serviços da AWS para analisar mais ainda mais e agir com base nos dados de eventos coletados nos logs do CloudTrail. Para obter mais informações, consulte as informações a seguir.

- Visão geral da criação de uma trilha
- Serviços e integrações compatíveis com o CloudTrail
- Configurar notificações do Amazon SNS para o CloudTrail
- Receber arquivos de log do CloudTrail de várias regiões e Receber arquivos de log do CloudTrail de várias contas

Todas as operações de API dos planos do AWS Support são registradas pelo CloudTrail. Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com credenciais de usuário raiz ou do AWS Identity and Access Management (IAM).
- Se a solicitação foi feita com credenciais de segurança temporárias de uma função ou de um usuário federado.
- Se a solicitação foi feita por outro AWS service (Serviço da AWS).

Para obter mais informações, consulte Elemento userIdentity do CloudTrail.

Você também pode agregar arquivos de log do AWS Support de várias Regiões da AWS e contas em um único bucket do Amazon S3.

Noções básicas sobre as entradas de arquivos de log dos planos do AWS Support

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log a um bucket do Amazon S3 especificado. Os arquivos de log do CloudTrail contêm uma ou mais entradas de log. Um evento representa uma solicitação única de qualquer fonte. Ele inclui informações sobre a operação solicitada, a data e a hora da operação, os parâmetros de solicitação e assim por diante. Os arquivos de log do CloudTrail não são um rastreamento de pilha ordenada de chamadas de API pública. Dessa forma, eles não são exibidos em uma ordem específica.

Example : entrada de log para **`GetSupportPlan`**

O exemplo a seguir mostra uma entrada de log do CloudTrail para a operação `GetSupportPlan`.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:sts::111122223333:user/janedoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-06-29T16:30:04Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-06-29T16:39:11Z",
    "eventSource": "supportplans.amazonaws.com",
    "eventName": "GetSupportPlan",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.183",
```

```
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101
 Firefox/91.0",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "7665c39a-d6bf-4d0d-8010-2f59740b8ecb",
    "eventID": "b711bc30-16a5-4579-8f0d-9ada8fe6d1ce",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Example : entrada de log para **`GetSupportPlanUpdateStatus`**

O exemplo a seguir mostra uma entrada de log do CloudTrail para a operação `GetSupportPlanUpdateStatus`.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:sts::111122223333:user/janedoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-06-29T16:30:04Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-06-29T16:39:02Z",
    "eventSource": "supportplans.amazonaws.com",
```

```
    "eventName": "GetSupportPlanUpdateStatus",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.183",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101
 Firefox/91.0",
    "requestParameters": {
        "supportPlanUpdateArn":
 "arn:aws:supportplans::111122223333:supportplanupdate/7f03b7a233a0e87ebc79e56d4d2bcaf19e976c37
    },
    "responseElements": null,
    "requestID": "75e5c767-8703-4ed3-b01e-4dda28020322",
    "eventID": "28d1c0e3-ccb6-4fd1-8793-65be010114cc",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Example : entrada de log para **`StartSupportPlanUpdate`**

O exemplo a seguir mostra uma entrada de log do CloudTrail para a operação `StartSupportPlanUpdate`.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:sts::111122223333:user/janedoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-06-29T16:30:04Z",
```

```
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-06-29T16:38:55Z",
    "eventSource": "supportplans.amazonaws.com",
    "eventName": "StartSupportPlanUpdate",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.183",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101
 Firefox/91.0",
    "requestParameters": {
        "clientToken": "98add111-dcc9-464d-8722-438d697fe242",
        "update": {
            "supportLevel": "BASIC"
        }
    },
    "responseElements": {
        "Access-Control-Expose-Headers": "x-amzn-RequestId,x-amzn-ErrorType,x-amzn-
ErrorMessage,Date",
        "supportPlanUpdateArn":
 "arn:aws:supportplans::111122223333:supportplanupdate/7f03b7a233a0e87ebc79e56d4d2bcaf19e976c37
    },
    "requestID": "e5ff9382-5fb8-4764-9993-0f33fb0b1e17",
    "eventID": "5dba89f8-2e5b-42b9-9b8f-395580c52962",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Example : entrada de log para **`CreateSupportPlanSchedule`**

O exemplo a seguir mostra uma entrada de log do CloudTrail para a operação `CreateSupportPlanSchedule`.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:sts::111122223333:user/janedoe",
```

```
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-05-09T16:30:04Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-05-09T16:30:04Z",
    "eventSource": "supportplans.amazonaws.com",
    "eventName": "CreateSupportPlanSchedule",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.183",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101
 Firefox/91.0",
    "requestParameters": {
        "clientToken": "b998de5e-ad1c-4448-90db-2bf86d6d9e9a",
        "scheduleCreationDetails": {
            "startLevel": "BUSINESS",
            "startOffer": "TrialPlan7FB93B",
            "startTimestamp": "2023-06-03T17:23:56.109Z",
            "endLevel": "BUSINESS",
            "endOffer": "StandardPlan2074BB",
            "endTimestamp": "2023-09-03T17:23:55.109Z"
        }
    },
    "responseElements": {
        "Access-Control-Expose-Headers": "x-amzn-RequestId,x-amzn-ErrorType,x-amzn-
ErrorMessage,Date",
        "supportPlanUpdateArn":
 "arn:aws:supportplans::111122223333:supportplanschedule/
b9a9a4336a3974950a6e670f7dab79b77a4b104db548a0d57050ce4544721d4b"
    },
    "requestID": "150450b8-e61a-4b15-93a8-c3b557a1ca48",
    "eventID": "a2a1ba44-610d-4dc8-bf16-29f1635b57a9",
```

```
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Registrar alterações no seu plano AWS Support

> **Important**
>
> A partir de 3 de agosto de 2022, as operações a seguir foram descontinuadas e não aparecerão nos seus novos logs do CloudTrail. Para ver uma lista das operações suportadas, consulte Noções básicas sobre as entradas de arquivos de log dos planos do AWS Support.

- `DescribeSupportLevelSummary` - Esta ação aparece no seu log quando você abre a caixa de diálogo Planos do Support.
- `UpdateProbationAutoCancellation` - Depois de se inscrever no suporte ao desenvolvedor ou comercial e, em seguida, tentar cancelar dentro de 30 dias, seu plano será cancelado automaticamente no fim desse período. Esta ação aparece no seu log quando você escolheOpt-out of automatic cancellation (Cancelar cancelamento automático) no banner que aparece na guia Planos do Support. Você retomará seu plano de suporte ao desenvolvedor ou comercial.
- `UpdateSupportLevel`: esta ação aparece em seu log quando você altera o seu plano de suporte.

> **Note**
>
> O campo `eventSource` tem o namespace `support-subscription.amazonaws.com` para essas ações.

Example : Entrada de log para DescribeUpportLevelSummary

O exemplo a seguir mostra uma entrada de log do CloudTrail para a ação `DescribeSupportLevelSummary`.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "Root",
    "principalId": "111122223333",
    "arn": "arn:aws:iam::111122223333:root",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {},
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-01-07T22:08:05Z"
      }
    }
  },
  "eventTime": "2021-01-07T22:08:07Z",
  "eventSource": "support-subscription.amazonaws.com",
  "eventName": "DescribeSupportLevelSummary",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "100.127.8.67",
  "userAgent": "AWS-SupportPlansConsole, aws-internal/3",
  "requestParameters": {
    "lang": "en"
  },
  "responseElements": null,
  "requestID": "b423b84d-829b-4090-a239-2b639b123abc",
  "eventID": "e1eeda0e-d77c-487b-a7e5-4014f7123abc",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "111122223333"
}
```


Example : Entrada de log para UpdateProbationAutoCancelation

O exemplo a seguir mostra uma entrada de log do CloudTrail para a ação `UpdateProbationAutoCancellation`.


```
{
  "eventVersion": "1.08",
```

```
  "userIdentity": {
    "type": "Root",
    "principalId": "111122223333",
    "arn": "arn:aws:iam::111122223333:root",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE"
  },
  "eventTime": "2021-01-07T23:28:43Z",
  "eventSource": "support-subscription.amazonaws.com",
  "eventName": "UpdateProbationAutoCancellation",
  "awsRegion": "us-east-1", "sourceIPAddress": "100.127.8.67",
  "userAgent": "AWS-SupportPlansConsole, aws-internal/3",
  "requestParameters": {
    "lang": "en"
  },
  "responseElements": null,
  "requestID": "5492206a-e200-4c33-9fcf-4162d4123abc",
  "eventID": "f4a58c09-0bb0-4ba2-a8d3-df6909123abc",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "111122223333"
}
```


Example : Entrada de log para UpdateSupportLevel

O exemplo a seguir mostra uma entrada de log do CloudTrail para a ação `UpdateSupportLevel` para alterar para o Support ao Desenvolvedor.


```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "Root",
    "principalId": "111122223333",
    "arn": "arn:aws:iam::111122223333:root",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {},
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
```

```
        "creationDate": "2021-01-07T22:08:05Z"
      }
    }
  },
  "eventTime": "2021-01-07T22:08:43Z",
  "eventSource": "support-subscription.amazonaws.com",
  "eventName": "UpdateSupportLevel",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "100.127.8.247",
  "userAgent": "AWS-SupportPlansConsole, aws-internal/3",
  "requestParameters": {
    "supportLevel": "new_developer"
  },
  "responseElements": {
    "aispl": false,
    "supportLevel": "new_developer"
  },
  "requestID": "5df3da3a-61cd-4a3c-8f41-e5276b123abc",
  "eventID": "c69fb149-c206-47ce-8766-8df6ec123abc",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "111122223333"
}
```

Monitorar e registrar em log para o AWS Trusted Advisor

O monitoramento é uma parte importante para manter a confiabilidade, a disponibilidade e a performance do Trusted Advisor e das outras soluções da AWS. A AWS fornece as ferramentas de monitoramento a seguir para observar o Trusted Advisor, informar quando algo está errado e realizar ações automaticamente quando apropriado:

- O Amazon EventBridge oferece uma transmissão quase em tempo real dos eventos do sistema que descrevem as alterações nos recursos da AWS. O EventBridge habilita a computação orientada a eventos automatizada, já que é possível escrever regras que monitoram determinados eventos e acionam ações automatizadas em outros serviços da AWS quando esses eventos ocorrem.

  Por exemplo, o Trusted Advisor fornece a verificação Amazon S3 Bucket Permissions (Permissões de bucket do Amazon S3). Essa verificação identifica se você possui buckets que tenham permissões de acesso livre ou concedam acesso a qualquer usuário autenticado da AWS. Se uma permissão de bucket for alterada, o status será alterado para a verificação Trusted Advisor. O EventBridge detecta esse evento e envia uma notificação para que você possa agir. Para obter mais informações, consulte o Guia do usuário do Amazon EventBridge.
- As verificações do AWS Trusted Advisor identificam formas de reduzir os custos, aumentar a performance e melhorar a segurança da sua conta da AWS. Você pode usar o EventBridge para monitorar o status das verificações do Trusted Advisor. É possível usar o Amazon CloudWatch para criar alarmes em métricas do Trusted Advisor. Esses alarmes notificam quando o status muda para uma verificação do Trusted Advisor, como um recurso atualizado ou uma cota de serviço atingida.
- O AWS CloudTrail captura chamadas de API e eventos relacionados feitos por ou em nome de sua conta da AWS e entrega os arquivos de log a um bucket do Amazon S3 que você especificar. Você pode identificar quais usuários e contas chamaram a AWS, o endereço IP de origem do qual as chamadas foram feitas e quando elas ocorreram. Para obter mais informações, consulte o Guia do usuário da AWS CloudTrail.

Tópicos

- Monitorando resultados de AWS Trusted Advisor cheques com a Amazon EventBridge
- Criar alarmes do Amazon CloudWatch para monitorar métricas do AWS Trusted Advisor
- Registro de ações do console do AWS Trusted Advisor com AWS CloudTrail

Monitorando resultados de AWS Trusted Advisor cheques com a Amazon EventBridge

Você pode usar EventBridge para detectar quando você verifica o status de Trusted Advisor alteração. Em seguida, com base nas regras que você cria, EventBridge invoca uma ou mais ações de destino quando o status muda para um valor especificado em uma regra.

Dependendo do tipo de alteração de status, convém enviar notificações, capturar informações de status, tomar medidas corretivas, iniciar eventos ou realizar outras ações. Por exemplo, você pode especificar os seguintes tipos de destino se uma verificação alterar o status de nenhum problema detectado (verde) para a ação recomendada (vermelho).

- Use uma função do AWS Lambda para enviar uma notificação para um canal Slack.
- Envie dados sobre a verificação para um stream do Amazon Kinesis para oferecer suporte ao monitoramento abrangente do status em tempo real.
- Envie um tópico do Amazon Simple Notification Service para o seu e-mail.
- Seja notificado com uma ação de CloudWatch alarme da Amazon.

Para obter mais informações sobre como usar EventBridge as funções Lambda para automatizar respostasTrusted Advisor, consulte Trusted Advisor ferramentas em. GitHub

> **Observações**
>
> - O Trusted Advisor entrega eventos em uma base de melhor esforço. Não é garantido que os eventos sejam sempre entregues ao EventBridge.
> - É necessário ter um plano Business, Enterprise On-Ramp ou Enterprise do AWS Support para criar uma regra para verificações do Trusted Advisor. Para obter mais informações, consulte Mudando AWS Support os planos.
> - Como Trusted Advisor é um serviço global, todos os eventos são emitidos EventBridge na região Leste dos EUA (Norte da Virgínia).

Siga este procedimento para criar uma EventBridge regra paraTrusted Advisor. Antes de criar regras de eventos, faça o seguinte:

- Familiarize-se com eventos, regras e metas em EventBridge. Para obter mais informações, consulte O que é a Amazon EventBridge? no Guia do EventBridge usuário da Amazon.
- Crie o destino que você usará na regra de evento.

Para criar uma EventBridge regra para Trusted Advisor

1. Abra o EventBridge console da Amazon em https://console.aws.amazon.com/events/.
2. Para alterar a região, use o Region selector (Seletor de regiões) no canto superior direito da página e escolha US East (N. Virginia) (Leste dos EUA (Norte da Virgínia)).
3. No painel de navegação, escolha Regras.
4. Escolha Criar regra.
5. Na página Definir detalhe de regra, insira um nome e uma descrição para sua regra.
6. Mantenha os valores padrão do Barramento de eventos e Tipo de regra e, depois, escolha Próximo.
7. Na página Criar padrão de evento, em Origem do evento, escolha AWSeventos ou eventos de EventBridge parceiros.
8. Em Event pattern (Padrão de evento), mantenha o valor padrão para Serviços da AWS.
9. Para AWS service (Serviço da AWS), escolha Trusted Advisor.
10. Para Event type (Tipo de evento), escolha Check Item Refresh Status (Verificar status de atualização do item).
11. Escolha uma das seguintes opções para verificar status:
    - Escolha Any status (Qualquer status) para criar uma regra que monitora qualquer alteração de status.
    - Selecione Specific status(es) (Status específicos) e escolha os valores que você deseja que sua regra monitore.
        - ERROR: o Trusted Advisor recomenda uma ação para a verificação.
        - INFO: o Trusted Advisor não é capaz de determinar o status da verificação.
        - OK: o Trusted Advisor não detecta problemas na verificação.
        - WARN: o Trusted Advisor detecta um possível problema na verificação e recomenda investigação.
12. Escolha uma das seguintes opções para as verificações:
    - Escolha Any check (Qualquer verificação).

- Escolha Specific check(s) (Verificações específicas) e escolha um ou mais nomes de verificação na lista.

13. Escolha uma das seguintes opções para recursos da AWS:

    - Escolha Any resource ID (Qualquer ID do recurso) para criar uma regra que monitora todos os recursos.
    - Escolha Specific resource ID(s) by ARN (IDs de recursos específicos por ARN) e insira os nomes dos recursos da Amazon (ARNs) desejados.

14. Escolha Próximo.
15. Na seção Select target(s) (Selecionar destino(s)), escolha o tipo de destino criado para esta regra e, em seguida, configure quaisquer opções adicionais necessárias para esse tipo. Por exemplo, você pode enviar o evento para uma fila do Amazon SQS ou a um tópico do Amazon SNS.
16. Escolha Próximo.
17. (Opcional) Na página Configurar tags, adicione tags e escolha Próximo.
18. Na página Analisar e criar, analise a configuração da regra garantindo que ela atenda aos requisitos de monitoramento de eventos.
19. Escolha Criar regra. Sua regra agora monitorará para verificações do Trusted Advisor e, em seguida, enviará o evento para o destino que você especificou.

Criar alarmes do Amazon CloudWatch para monitorar métricas do AWS Trusted Advisor

Quando o AWS Trusted Advisor atualiza suas verificações, o Trusted Advisor publica métricas sobre seus resultados de verificação no CloudWatch. É possível visualizar essas métricas no CloudWatch. Também é possível criar alarmes para detectar alterações de status de recursos e nas verificações do Trusted Advisor e o uso de cotas de serviço (anteriormente chamadas de limites). Por exemplo, é possível criar um alarme para monitorar as alterações de status das verificações na categoria Service Limits (Limites de serviço). Em seguida, o alarme vai notificar você quando você atingir ou exceder uma cota de serviço para a sua conta da AWS.

Siga este procedimento para criar um alarme do CloudWatch para uma métrica do Trusted Advisor específica.

Tópicos

- Pré-requisitos
- Métricas do CloudWatch para Trusted Advisor
- Métricas e dimensões do Trusted Advisor

Pré-requisitos

Antes de criar alarmes do CloudWatch para o Trusted Advisor, analise as seguintes informações:

- Entenda como o CloudWatch usa métricas e alarmes. Para obter mais informações, consulte Como o CloudWatch funciona no Manual do usuário do Amazon CloudWatch.
- Use o console do Trusted Advisor ou a API do AWS Support para atualizar suas verificações e obter os resultados de verificação mais recentes. Para obter mais informações, consulte Atualizar resultados da verificação.

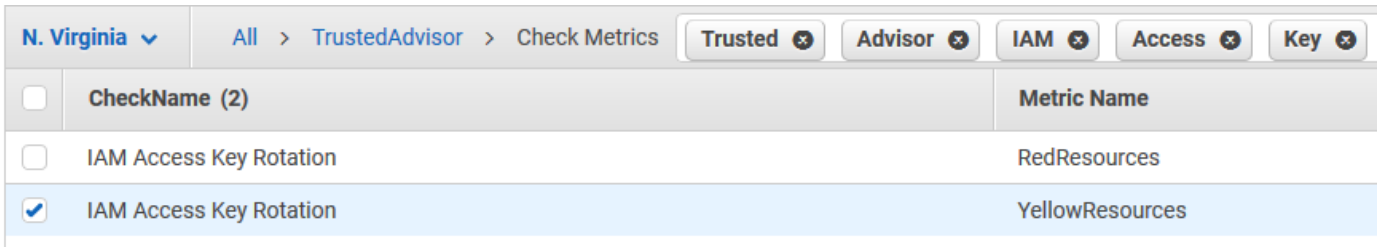
Para criar um alarme do CloudWatch para métricas do Trusted Advisor

1. Abra o console do CloudWatch em https://console.aws.amazon.com/cloudwatch/.
2. Use o Region selector (Seletor de regiões) e escolha a região da AWS Leste dos EUA (Norte da Virgínia).
3. No painel de navegação, selecione Alarmes.
4. Selecione Criar alarme.
5. Escolha Selecionar métrica.
6. Em Metrics (Métricas), insira um ou mais valores de dimensão para filtrar a lista de métricas. Por exemplo, é possível inserir o nome da métrica ServiceLimitUsage ou a dimensão, como o nome do verificação do Trusted Advisor.

   > **Tip**
   >
   > - É possível pesquisar o **`Trusted Advisor`** para listar todas as métricas do serviço.
   > - Para obter uma lista dos nomes das métricas e dimensões, consulte Métricas e dimensões do Trusted Advisor.

7. Na tabela de resultados, marque a caixa de seleção da métrica.

No exemplo a seguir, o nome da verificação é IAM Access Key Rotation (Mudança da chave de acesso do IAM) e o nome da métrica é YellowResources.

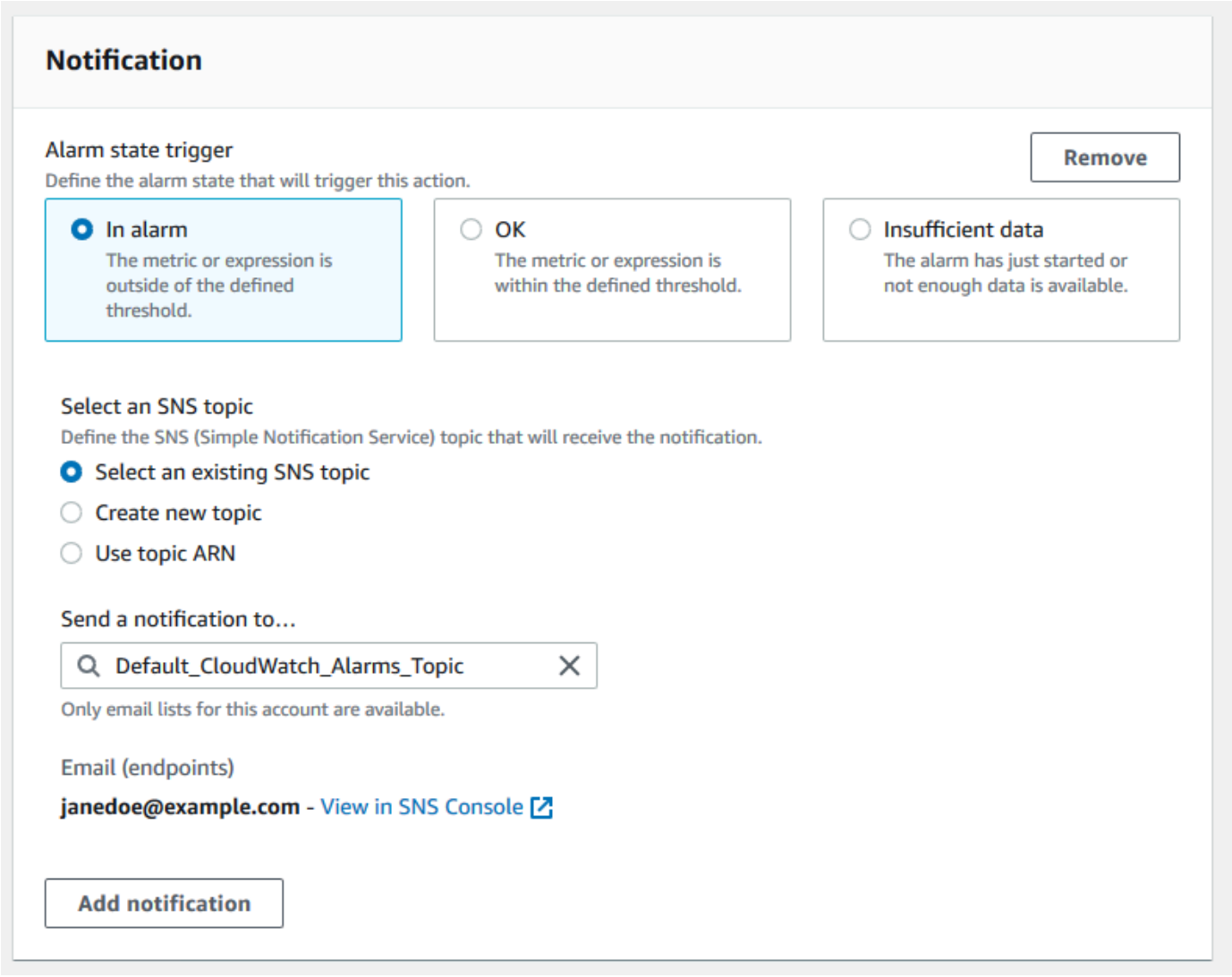


8. Escolha Selecionar métrica.
9. Em Specify metric and conditions (Especificar métrica e condições), verifique se Metric name (Nome da métrica) e CheckName que você escolheu aparecem na página.
10. Em Period (Período), é possível especificar o período em que deseja que o alarme inicie quando o status da verificação mudar, como 5 minutos.
11. Em Conditions (Condições), escolha Static (Estático) e, em seguida, especifique a condição de alarme para quando o alarme deve iniciar.

    Por exemplo, se você escolher o Greater/Equal >=threshold (Maior/Igual >=limiar) e inserir **1** como o valor limite, isso significa que o alarme começará quando o Trusted Advisor detectar pelo menos uma chave de acesso do IAM que não foi alternada nos últimos 90 dias.

    > **Observações**
    >
    > - Para as métricas GreenChecks, RedChecks, YellowChecks, RedResources e YellowResources,você pode especificar um limite que seja qualquer número inteiro maior ou igual a zero.
    > - O Trusted Advisor não envia métricas para GreenResources, que são recursos para os quais o Trusted Advisor não detectou nenhum problema.

12. Escolha Next (Próximo).
13. Na página Configure actions (Configurar ações), em Alarm state trigger (Acionamento do estado do alarme), escolha In alarm (Em alarme).
14. Em Select an SNS topic (Selecione um tópico do SNS), escolha um tópico existente do Amazon Simple Notification Service (Amazon SNS) ou crie um.



15. Escolha Next (Próximo).
16. Em Name e Description (Nome e Descrição), insira um nome e uma descrição para o seu alarme.
17. Escolha Next (Próximo).
18. Na página Preview and create (Visualizar e criar), analise os detalhes do alarme e escolha Create alarm (Criar alarme).

    Quando o status IAM Access Key Rotation (Alternância da chave de acesso do IAM) mudar para vermelho por 5 minutos, o alarme enviará uma notificação para o tópico do SNS.

Example : Notificação por e-mail para um alarme do CloudWatch

A mensagem de e-mail a seguir mostra que um alarme detectou uma alteração na verificação IAM Access Key Rotation (Alternância da chave de acesso do IAM).

```
You are receiving this email because your Amazon CloudWatch Alarm
 "IAMAcessKeyRotationCheckAlarm" in the US East (N. Virginia) region has entered the
 ALARM state,
because "Threshold Crossed: 1 out of the last 1 datapoints [9.0 (26/03/21 22:44:00)]
 was greater than or equal to the threshold (1.0) (minimum 1 datapoint for OK -> ALARM
 transition)." at "Friday 26 March, 2021 22:49:42 UTC".

View this alarm in the AWS Management Console:
https://us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-
east-1#s=Alarms&alarm=IAMAcessKeyRotationCheckAlarm

Alarm Details:
- Name:                       IAMAcessKeyRotationCheckAlarm
- Description:                This alarm starts when one or more AWS access keys in my
 AWS account have not been rotated in the last 90 days.
- State Change:               INSUFFICIENT_DATA -> ALARM
- Reason for State Change:    Threshold Crossed: 1 out of the last 1 datapoints [9.0
 (26/03/21 22:44:00)] was greater than or equal to the threshold (1.0) (minimum 1
 datapoint for OK -> ALARM transition).
- Timestamp:                  Friday 26 March, 2021 22:49:42 UTC
- AWS Account:                123456789012
- Alarm Arn:                  arn:aws:cloudwatch:us-
east-1:123456789012:alarm:IAMAcessKeyRotationCheckAlarm

Threshold:
- The alarm is in the ALARM state when the metric is GreaterThanOrEqualToThreshold 1.0
 for 300 seconds.

Monitored Metric:
- MetricNamespace:                    AWS/TrustedAdvisor
- MetricName:                         RedResources
- Dimensions:                         [CheckName = IAM Access Key Rotation]
- Period:                             300 seconds
- Statistic:                          Average
- Unit:                               not specified
- TreatMissingData:                   missing


State Change Actions:
```

```
- OK:
- ALARM: [arn:aws:sns:us-east-1:123456789012:Default_CloudWatch_Alarms_Topic]
- INSUFFICIENT_DATA:
```

Métricas do CloudWatch para Trusted Advisor

É possível usar o console do CloudWatch ou oAWS Command Line Interface (AWS CLI) para encontrar as métricas disponíveis para Trusted Advisor.

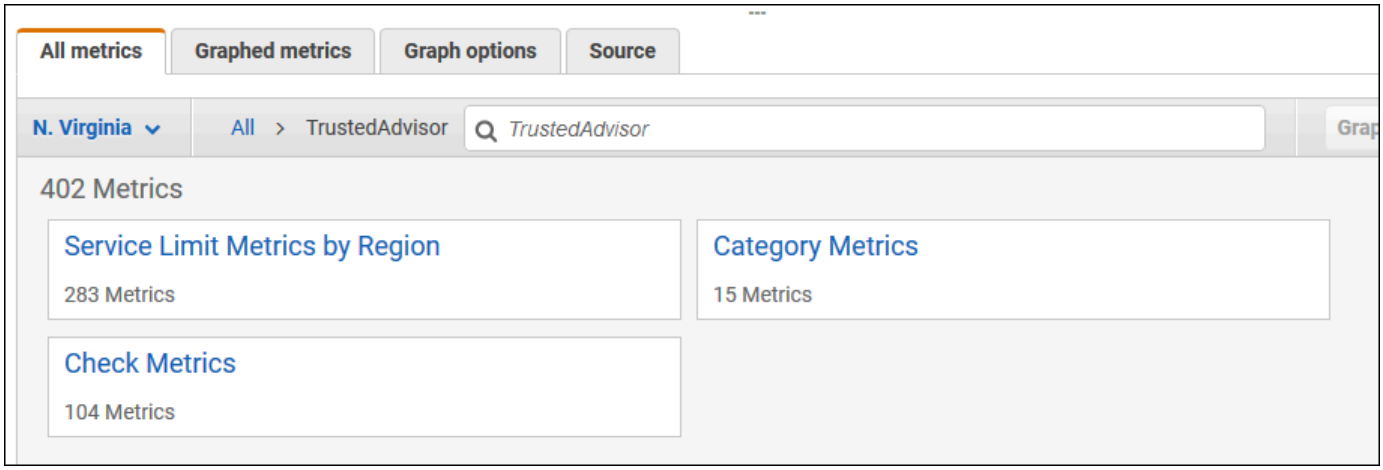
Para obter uma lista de namespaces, métricas e dimensões de todos os serviços que publicam métricas, consulte Serviços do AWS que publicam métricas do CloudWatch no Manual do usuário do Amazon CloudWatch.

Para visualizar métricas do Trusted Advisor (console)

É possível fazer login no console do CloudWatch e visualizar as métricas disponíveis para o Trusted Advisor.

Para visualizar métricas do Trusted Advisor disponíveis (console)

1. Abra o console do CloudWatch em https://console.aws.amazon.com/cloudwatch/.
2. Use o Region selector (Seletor de regiões) e escolha a região da AWS Leste dos EUA (Norte da Virgínia).
3. No painel de navegação, escolha Metrics (Métricas).
4. Insira um namespace de métrica, como **`TrustedAdvisor`**.
5. Escolha uma dimensão de métrica, como Check Metrics (Métricas de verificação).



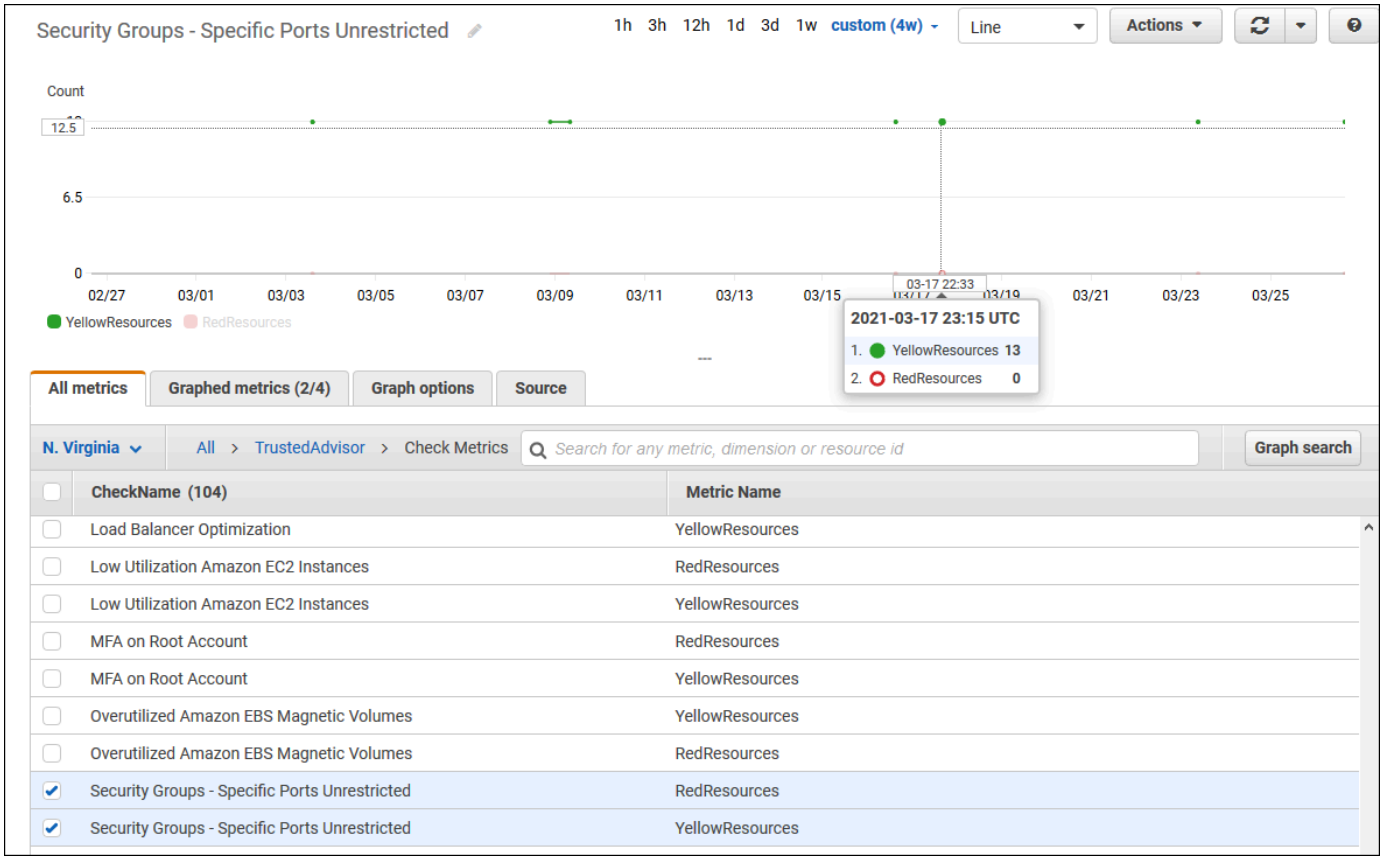
6. A guia All metrics (Todas as métricas) exibe todas as métricas dessa dimensão no namespace. Você pode fazer o seguinte:

a. Para classificar a tabela, escolha o cabeçalho da coluna.

b. Para criar um gráfico de uma métrica, marque a caixa de seleção ao lado da métrica. Para selecionar todas as métricas, marque a caixa de seleção na linha de cabeçalho da tabela.

c. Para filtrar por métrica, escolha o nome da métrica e Add to search (Adicionar à pesquisa).

O exemplo a seguir mostra os resultados da verificação Security Groups - Specific Ports Unrestricted (Grupos de segurança – portas específicas sem restrição). A verificação identificou 13 recursos que são amarelos. O Trusted Advisorrecomenda que você investigue verificações que são amarelas.



7. (Opcional) Para adicionar esse gráfico a um painel do CloudWatch, escolha Actions (Ações) e Add to dashboard (Adicionar ao painel).

Para obter mais informações sobre como criar um gráfico para visualizar suas métricas, consulte Criar gráficos de uma métrica no Manual do usuário do Amazon CloudWatch.

Visualizar métricas do Trusted Advisor (CLI)

É possível usar o comando da AWS CLI list-metrics para visualizar métricas disponíveis para o Trusted Advisor.

Example : Lista todas as métricas para Trusted Advisor

O exemplo a seguir especifica o namespace `AWS/TrustedAdvisor` para visualizar todas as métricas para o Trusted Advisor.

```
aws cloudwatch list-metrics --namespace AWS/TrustedAdvisor
```

A saída deverá ser semelhante a:

```
{
    "Metrics": [
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "ServiceName",
                    "Value": "EBS"
                },
                {
                    "Name": "ServiceLimit",
                    "Value": "Magnetic (standard) volume storage (TiB)"
                },
                {
                    "Name": "Region",
                    "Value": "ap-northeast-2"
                }
            ],
            "MetricName": "ServiceLimitUsage"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "CheckName",
                    "Value": "Overutilized Amazon EBS Magnetic Volumes"
                }
            ],
            "MetricName": "YellowResources"
```

```
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "ServiceName",
                    "Value": "EBS"
                },
                {
                    "Name": "ServiceLimit",
                    "Value": "Provisioned IOPS"
                },
                {
                    "Name": "Region",
                    "Value": "eu-west-1"
                }
            ],
            "MetricName": "ServiceLimitUsage"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "ServiceName",
                    "Value": "EBS"
                },
                {
                    "Name": "ServiceLimit",
                    "Value": "Provisioned IOPS"
                },
                {
                    "Name": "Region",
                    "Value": "ap-south-1"
                }
            ],
            "MetricName": "ServiceLimitUsage"
        },
    ...
  ]
}
```

Example : Listar todas as métricas para uma dimensão

O exemplo a seguir especifica o namespace `AWS/TrustedAdvisor` e a dimensão `Region` para visualizar os resultados somente para a região AWS especificada.

```
aws cloudwatch list-metrics --namespace AWS/TrustedAdvisor --dimensions
 Name=Region,Value=us-east-1
```

A saída deverá ser semelhante a:

```
{
    "Metrics": [
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "ServiceName",
                    "Value": "SES"
                },
                {
                    "Name": "ServiceLimit",
                    "Value": "Daily sending quota"
                },
                {
                    "Name": "Region",
                    "Value": "us-east-1"
                }
            ],
            "MetricName": "ServiceLimitUsage"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "ServiceName",
                    "Value": "AutoScaling"
                },
                {
                    "Name": "ServiceLimit",
                    "Value": "Launch configurations"
                },
                {
                    "Name": "Region",
```

```
                    "Value": "us-east-1"
                }
            ],
            "MetricName": "ServiceLimitUsage"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "ServiceName",
                    "Value": "CloudFormation"
                },
                {
                    "Name": "ServiceLimit",
                    "Value": "Stacks"
                },
                {
                    "Name": "Region",
                    "Value": "us-east-1"
                }
            ],
            "MetricName": "ServiceLimitUsage"
        },
    ...
  ]
}
```

Example : Listar métricas para um nome de métrica específico

O exemplo a seguir especifica o namespace `AWS/TrustedAdvisor` e o nome da métrica `RedResources` para visualizar os resultados somente para a métrica especificada.

```
aws cloudwatch list-metrics --namespace AWS/TrustedAdvisor --metric-name RedResources
```

A saída deverá ser semelhante a:

```
{
    "Metrics": [
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "CheckName",
```

```
                    "Value": "Amazon RDS Security Group Access Risk"
                }
            ],
            "MetricName": "RedResources"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "CheckName",
                    "Value": "Exposed Access Keys"
                }
            ],
            "MetricName": "RedResources"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "CheckName",
                    "Value": "Large Number of Rules in an EC2 Security Group"
                }
            ],
            "MetricName": "RedResources"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "CheckName",
                    "Value": "Auto Scaling Group Health Check"
                }
            ],
            "MetricName": "RedResources"
        },
    ...
  ]
}
```

Métricas e dimensões do Trusted Advisor

Consulte as seguintes métricas e dimensões do Trusted Advisor que podem usar para seus alarmes e gráficos do CloudWatch.

Métricas de nível de verificação do Trusted Advisor

É possível usar as métricas a seguir para verificações do Trusted Advisor.

Métrica	Descrição
`RedResources`	O número de recursos que estão em um estado vermelho (ação recomendada).
`YellowResources`	O número de recursos que estão em um estado amarelo (investig ação recomendada).

Métricas de nível de categoria do Trusted Advisor

É possível usar as seguintes métricas para categorias do Trusted Advisor.

Métrica	Descrição
`GreenChecks`	O número de verificações do Trusted Advisor que estão em um estado verde (nenhum problema detectado).
`RedChecks`	O número de verificações do Trusted Advisor que estão em um estado vermelho (ação recomendada).
`YellowChecks`	O número de verificações do Trusted Advisor que estão em um estado amarelo (investigação recomendada).

Métricas de nível de cota de serviço do Trusted Advisor

É possível usar as seguintes métricas para as cotas de AWS service (Serviço da AWS)

Métrica	Descrição
`ServiceLimitUsage`	A porcentagem de uso de recursos em relação a uma cota de serviço (anteriormente chamada de limites).

Dimensões para métricas de nível de verificação

É possível usar as dimensões a seguir para as verificações do Trusted Advisor.

Dimensão	Descrição
`CheckName`	O nome de uma verificação do Trusted Advisor. É possível encontrar todos os nomes de verificações na seção Console do Trusted Advisor ou em Referência de verificação do AWS Trusted Advisor.

Dimensões para métricas de nível de categoria

É possível usar a dimensão a seguir para as categorias de verificação do Trusted Advisor.

Dimensão	Descrição
`Category`	O nome da categoria de verificação da Trusted Advisor. É possível encontrar todas as categorias de verificação no console do Trusted Advisor ou na página Visualizar categorias de verificação.

Dimensões para métricas de cota de serviço

É possível usar as seguintes dimensões para as métricas de cota de serviço do Trusted Advisor.

Dimensão	Descrição
`Region`	A Região da AWS para uma cota de serviço.
`ServiceName`	O nome da AWS service (Serviço da AWS).
`ServiceLimit`	O nome do cota de serviço.

Dimensão	Descrição
	Para obter mais informações sobre cotas de serviço, consulte AWS service (Serviço da AWS) quotas, na Referência geral da AWS.

Registro de ações do console do AWS Trusted Advisor com AWS CloudTrail

Trusted Advisoré integrado comAWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, função ou AWS serviço emTrusted Advisor. CloudTrail captura ações para eventos Trusted Advisor como. As chamadas capturadas incluem as chamadas do console do Trusted Advisor. Se você criar uma trilha, poderá habilitar a entrega contínua de CloudTrail eventos para um bucket do Amazon Simple Storage Service (Amazon S3), incluindo eventos para. Trusted Advisor Se você não configurar uma trilha, ainda poderá ver os eventos mais recentes no CloudTrail console no Histórico de eventos. Usando as informações coletadas por CloudTrail, você pode determinar a solicitação que foi feitaTrusted Advisor, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e detalhes adicionais.

Para saber mais CloudTrail, inclusive como configurá-lo e ativá-lo, consulte o Guia AWS CloudTrail do usuário.

Trusted Advisorinformações em CloudTrail

CloudTrail é ativado em sua AWS conta quando você cria a conta. Quando uma atividade de evento suportada ocorre no Trusted Advisor console, essa atividade é registrada em um CloudTrail evento junto com outros eventos AWS de serviço no histórico de eventos. Você pode visualizar, pesquisar e baixar eventos recentes em sua conta AWS. Para obter mais informações, consulte Visualização de eventos com histórico de CloudTrail eventos.

Para um registro contínuo de eventos em sua AWS conta, inclusive eventos para Trusted Advisor, crie uma trilha. Uma trilha permite CloudTrail entregar arquivos de log para um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, ela é aplicada a todas as Regiões da AWS. A trilha registra em log eventos de todas as Regiões na partição da AWS e entrega os arquivos de log para o bucket do Amazon S3 especificado por você. Além disso, você pode configurar outros AWS serviços para analisar e agir com base nos dados de eventos coletados nos CloudTrail registros. Para ver mais informações, consulte:

- Visão geral da criação de uma trilha
- CloudTrail Serviços e integrações compatíveis
- Configurando notificações do Amazon SNS para CloudTrail
- Recebendo arquivos de CloudTrail log de várias regiões e recebendo arquivos de CloudTrail log de várias contas

Trusted Advisorsuporta o registro de um subconjunto das ações do Trusted Advisor console como eventos em arquivos de CloudTrail log. CloudTrail registra as seguintes ações:

- `CreateEngagement`
- `CreateEngagementAttachment`
- `CreateEngagementCommunication`
- `CreateExcelReport`
- `DescribeAccount`
- `DescribeAccountAccess`
- `DescribeCheckItems`
- `DescribeCheckRefreshStatuses`
- `DescribeCheckSummaries`
- `DescribeChecks`
- `DescribeNotificationPreferences`
- `DescribeOrganization`
- `DescribeOrganizationAccounts`
- `DescribeReports`
- `DescribeServiceMetadata`
- `ExcludeCheckItems`
- `GenerateReport`
- `GetEngagement`
- `GetEngagementAttachment`
- `GetEngagementType`
- `GetExcelReport`
- `GetOrganizationRecommendation`

- GetRecommendation
- IncludeCheckItems
- ListAccountsForParent
- ListChecks
- ListEngagementCommunications
- ListEngagementTypes
- ListEngagements
- ListOrganizationRecommendationAccounts
- ListOrganizationRecommendationResources
- ListOrganizationRecommendations
- ListOrganizationalUnitsForParent
- ListRecommendationResources
- ListRecommendations
- ListRoots
- RefreshCheck
- SetAccountAccess
- SetOrganizationAccess
- UpdateEngagement
- UpdateEngagementStatus
- UpdateNotificationPreferences
- UpdateOrganizationRecommendationLifecycle
- UpdateRecommendationLifecycle

Para obter uma lista completa de ações do console do Trusted Advisor, consulte Trusted Advisor ações.

> **Note**
>
> CloudTrail também registra as operações Trusted Advisor da API na Referência AWS Support da API. Para obter mais informações, consulte Registrar em log chamadas de API do AWS Support com o AWS CloudTrail.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com credenciais de usuário raiz ou usuário do IAM AWS Identity and Access Management
- 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 serviço da AWS.

Para obter mais informações, consulte o elemento CloudTrail UserIdentity.

Exemplo: entradas do arquivo de log do Trusted Advisor

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log para um bucket do Amazon S3 que você especificar. CloudTrail os arquivos de log contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer fonte e inclui informações sobre a ação solicitada, a data e a hora da ação, os parâmetros da solicitação e assim por diante. CloudTrail os arquivos de log não são um rastreamento de pilha ordenado das chamadas públicas de API, portanto, eles não aparecem em nenhuma ordem específica.

Example : Entrada de registro para RefreshCheck

O exemplo a seguir mostra uma entrada de CloudTrail registro que demonstra a `RefreshCheck` ação da verificação de versão (ID) do Amazon S3 Bucket. R365s2Qddf


```
{
        "eventVersion":"1.04",
        "userIdentity":{
        "type":"IAMUser",
        "principalId":"AIDACKCEVSQ6C2EXAMPLE",
        "arn":"arn:aws:iam::123456789012:user/janedoe",
        "accountId":"123456789012",
        "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
        "userName":"janedoe",
        "sessionContext":{
        "attributes":{
        "mfaAuthenticated":"false",
        "creationDate":"2020-10-21T22:06:18Z"
        }
        }
```

```
        },
        "eventTime":"2020-10-21T22:06:33Z",
        "eventSource":"trustedadvisor.amazonaws.com",
        "eventName":"RefreshCheck",
        "awsRegion":"us-east-1",
        "sourceIPAddress":"100.127.34.136",
        "userAgent":"signin.amazonaws.com",
        "requestParameters":{
        "checkId":"R365s2Qddf"
        },
        "responseElements":{
        "status":{
        "checkId":"R365s2Qddf",
        "status":"enqueued",
        "millisUntilNextRefreshable":3599993
        }
        },
        "requestID":"d23ec729-8995-494c-8054-dedeaEXAMPLE",
        "eventID":"a49d5202-560f-4a4e-b38a-02f1cEXAMPLE",
        "eventType":"AwsApiCall",
        "recipientAccountId":"123456789012"
        }
```

Example : Entrada de registro para UpdateNotificationPreferences

O exemplo a seguir mostra uma entrada de CloudTrail registro que demonstra a `UpdateNotificationPreferences` ação.

```
{
        "eventVersion":"1.04",
        "userIdentity":{
        "type":"IAMUser",
        "principalId":"AIDACKCEVSQ6C2EXAMPLE",
        "arn":"arn:aws:iam::123456789012:user/janedoe",
        "accountId":"123456789012",
        "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
        "userName":"janedoe",
        "sessionContext":{
        "attributes":{
        "mfaAuthenticated":"false",
        "creationDate":"2020-10-21T22:06:18Z"
        }
```

```
        }
        },
        "eventTime":"2020-10-21T22:09:49Z",
        "eventSource":"trustedadvisor.amazonaws.com",
        "eventName":"UpdateNotificationPreferences",
        "awsRegion":"us-east-1",
        "sourceIPAddress":"100.127.34.167",
        "userAgent":"signin.amazonaws.com",
        "requestParameters":{
        "contacts":[
        {
        "id":"billing",
        "type":"email",
        "active":false
        },
        {
        "id":"operational",
        "type":"email",
        "active":false
        },
        {
        "id":"security",
        "type":"email",
        "active":false
        }
        ],
        "language":"en"
        },
        "responseElements":null,
        "requestID":"695295f3-c81c-486e-9404-fa148EXAMPLE",
        "eventID":"5f923d8c-d210-4037-bd32-997c6EXAMPLE",
        "eventType":"AwsApiCall",
        "recipientAccountId":"123456789012"
        }
```

Example : Entrada de registro para GenerateReport

O exemplo a seguir mostra uma entrada de CloudTrail registro que demonstra a `GenerateReport` ação. Esta ação cria um relatório para a sua organização da AWS.

```
{
        "eventVersion":"1.04",
```

```
        "userIdentity":{
        "type":"IAMUser",
        "principalId":"AIDACKCEVSQ6C2EXAMPLE",
        "arn":"arn:aws:iam::123456789012:user/janedoe",
        "accountId":"123456789012",
        "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
        "userName":"janedoe",
        "sessionContext":{
        "attributes":{
        "mfaAuthenticated":"false",
        "creationDate":"2020-11-03T13:03:10Z"
        }
        }
        },
        "eventTime":"2020-11-03T13:04:29Z",
        "eventSource":"trustedadvisor.amazonaws.com",
        "eventName":"GenerateReport",
        "awsRegion":"us-east-1",
        "sourceIPAddress":"100.127.36.171",
        "userAgent":"signin.amazonaws.com",
        "requestParameters":{
        "refresh":false,
        "includeSuppressedResources":false,
        "language":"en",
        "format":"JSON",
        "name":"organizational-view-report",
        "preference":{
        "accounts":[

        ],
        "organizationalUnitIds":[
        "r-j134"
        ],
        "preferenceName":"organizational-view-report",
        "format":"json",
        "language":"en"
        }
        },
        "responseElements":{
        "status":"ENQUEUED"
        },
        "requestID":"bb866dc1-60af-47fd-a660-21498EXAMPLE",
        "eventID":"2606c89d-c107-47bd-a7c6-ec92fEXAMPLE",
        "eventType":"AwsApiCall",
```

```
        "recipientAccountId":"123456789012"
        }
```

Recursos de solução de problemas

Para obter respostas para perguntas de solução de problemas comuns, consulte a Central de conhecimento do AWS Support.

Para Windows, o Amazon EC2 oferece o EC2Rescue, que os clientes podem usar para examinar suas instâncias do Windows para ajudar a identificar problemas comuns, coletar arquivos de log e ajudar a AWS Support solucionar seus problemas. Você também pode usar o EC2Rescue para analisar volumes de inicialização de instâncias não funcionais. Para obter mais informações, consulte Como posso usar o EC2Rescue para solucionar problemas e corrigir problemas comuns em minha instância do Windows EC2?

Solução de problemas de erros específicos do serviço

A maioria AWS service (Serviço da AWS) da documentação contém tópicos de solução de problemas que podem ajudar você a começar antes de entrar em contato AWS Support. A tabela a seguir fornece links para os tópicos de solução de problemas, organizados por serviço.

> **Note**
>
> A tabela a seguir fornece uma lista dos serviços mais comuns. Para pesquisar outros tópicos de solução de problemas, use a caixa de texto de pesquisa na página de destino da Documentação da AWS.

Serviço	Link
Amazon Web Services	Solução de problemas de erros do AWS Signature versão 4
Amazon API Gateway	Solução de problemas com APIs HTTP
Amazon AppStream	Solucionar problemas da Amazon AppStream
Amazon Athena	Solução de problemas no Athena
Amazon Aurora MySQL	Solução de problemas do Amazon Aurora
Amazon Aurora PostgreSQL	Solução de problemas do Amazon Aurora

Serviço	Link
Amazon EC2 Auto Scaling	Solução de problemas de Auto Scaling
AWS Certificate Manager (ACM)	Solução de problemas
AWS CloudFormation	Resolução de problemas AWS CloudFormation
Amazon CloudFront	Solução de problemas | Solução de problemas em distribuições do RTMP
AWS CloudHSM	Solução de problemas
Amazon CloudSearch	Solução de problemas da Amazon CloudSearch
AWS CodeDeploy	Resolução de problemas AWS CodeDeploy
Amazon CloudWatch	Resolução de problemas
AWS Database Migration Service	Solução de problemas de tarefas de migração no AWS Database Migration Service
AWS Data Pipeline	Solução de problemas
AWS Direct Connect	Resolução de problemas AWS Direct Connect
AWS Directory Service	Solução de problemas AWS Directory Service administrativos
Amazon DynamoDB	Solução de problemas | Solução de problemas no estabelecimento de conexão SSL/TLS
AWS Elastic Beanstalk	Solução de problemas

Serviço	Link
Amazon Elastic Compute Cloud (Amazon EC2)	Solução de problemas em instâncias | Solução de problemas em instâncias do Windows | Solução de problemas em VM Import/Export | Solução de problemas de erros de solicitação de API | Solução de problemas no gerenciamento de pacotes do AWS | Solução de problemas no AWS Systems Manager para Microsoft SCVMM | Diagnóstico da AWS para Microsoft Windows Server
Amazon Elastic Container Service (Amazon ECS)	Solução de problemas do Amazon ECS
Amazon Elastic Kubernetes Service (Amazon EKS)	Solução de problemas do Amazon EKS
Elastic Load Balancing	Solução de problemas em seus Application Load Balancers | Solução de problemas em seu Classic Load Balancer
Amazon ElastiCache para Memcached	Solução de problemas de aplicativos
Amazon ElastiCache para Redis	Solução de problemas de aplicativos
Amazon EMR	Solução de problemas em um cluster
AWS Flow Framework	Dicas de depuração e solução de problemas
AWS Glue	Solução de problemas AWS Glue
AWS Glue DataBrew	Solução de problemas de identidade e acesso do AWS Glue DataBrew
AWS GovCloud (US)	Solução de problemas
AWS Identity and Access Management (IAM)	Solução de problemas do IAM

Serviço	Link
Amazon Keyspaces (para Apache Cassandra)	Solução de problemas do Amazon Keyspaces (para Apache Cassandra)
Amazon Kinesis Data Streams	Solução de problemas de produtores do Amazon Kinesis Data Streams | Solução de problemas de consumidores do Amazon Kinesis Data Streams
Amazon Managed Service for Apache Flink	Solução de problemas de performance | Solução de problemas do Amazon Managed Service for Apache Flink para aplicações SQL
Amazon Data Firehose	Solução de problemas do Amazon Data Firehose
AWS Lambda	AWS Lambda Funções de solução de problemas e monitoramento com CloudWatch
OpenSearch Serviço Amazon	Solução de problemas do Amazon OpenSearch Service
AWS OpsWorks	Guia de depuração e solução de problemas
Amazon Personalize	Solução de problemas
Amazon QLDB	Solução de problemas do Amazon QLDB
Amazon QuickSight	Solução de problemas da Amazon QuickSight | Solução de problemas de erros de linha ignorada
AWS Resource Access Manager (AWS RAM)	Solução de problemas com o AWS RAM
Amazon Redshift	Solução de problemas de consultas | Solução de problemas de carregamento de dados | Solução de problemas de conexão no Amazon Redshift | Solução de problemas de registro de log de auditoria do Amazon Redshift | Solução de problemas de consultas no Amazon Redshift Spectrum

Serviço	Link
Amazon Relational Database Service (Amazon RDS)	Solução de problemas | Solução de problemas de aplicações no Amazon RDS | Solução de problemas de banco de dados para o Amazon RDS Custom
Amazon Route 53	Solução de problemas do Amazon Route 53
Amazon SageMaker	Solucionar erros | Solução de problemas do Amazon Studio SageMaker
Amazon Silk	Solução de problemas
Amazon Simple Email Service (Amazon SES)	Solução de problemas do Amazon SES
Amazon Simple Storage Service (Amazon S3)	Solução de problemas
Amazon Simple Workflow Service (Amazon SWF)	AWS estrutura de fluxo para Java: dicas de solução de problemas e depuração | estrutura de AWS fluxo para Ruby: solução de problemas e depuração de fluxos de trabalho
AWS Storage Gateway	Solução de problemas em seu gateway
AWS Systems Manager	Solução de problemas do SSM Agent
Amazon Virtual Private Cloud (Amazon VPC)	Solução de problemas
AWS Virtual Private Network (AWS VPN)	Solução de problemas do dispositivo de gateway do cliente
AWS WAF	Testando e ajustando suas AWS WAF proteções
Amazon WorkMail	Solução de problemas do aplicativo WorkMail web da Amazon
Amazon WorkSpaces	Solução de WorkSpaces problemas da Amazon | Solução de problemas de WorkSpaces clientes da Amazon

Histórico do documento

A tabela a seguir descreve as mudanças importantes na documentação desde a última versão do AWS Support serviço.

- AWS Support Versão da API: 15-04-2013
- AWS Support Versão da API do aplicativo: 2021-08-20

A tabela a seguir descreve atualizações importantes na AWS Trusted Advisor documentação AWS Support e, a partir de 10 de maio de 2021. Agora é possível assinar um feed RSS para receber notificações sobre atualizações.

Alteração	Descrição	Data
Documentação atualizada de tolerância a falhas e verificação de segurança	Foi adicionada 1 nova verificação de tolerância a falhas. 1 tolerância a falhas e 1 verificação de segurança atualizadas. Para obter mais informações, consulte Registro de alterações para AWS Trusted Advisor verificações.	29 de março de 2024
Documentação atualizada para `AWSSupportServiceRolePolicy`	Adição de novas permissões para fornecer serviços de faturamento, administrativo e de suporte para a função vinculada ao serviço. Para obter mais informações, consulte Políticas gerenciadas pela AWS : AWSSupportServiceRolePolicy.	22 de março de 2024
Documentação atualizada do AWS Support plano	Atualizações nos recursos dos AWS Support planos. Para obter mais informaçõ	11 de março de 2024

	es, consulte AWS Support os planos.	
Documentação atualizada para Trusted Advisor	Foi adicionada 1 verificação de tolerância a falhas. Para obter mais informações, consulte Registro de alterações para AWS Trusted Advisor verificações.	29 de fevereiro de 2024
Documentação atualizada para Trusted Advisor	Foi adicionada 1 verificação de tolerância a falhas. Para obter mais informações, consulte Registro de alterações para AWS Trusted Advisor verificações.	31 de janeiro de 2024
Documentação atualizada para `AWSTrustedAdvisorServiceRolePolicy`	Foram adicionadas novas ações do IAM `cloudtrail:GetTrail` `cloudtrail:ListTrails` `cloudtrail:GetEventSelectors` ,,`outposts:GetOutpost` , `outposts:ListAssets` e `outposts:ListOutposts` para integrar novas verificações. Para obter mais informações, consulte Políticas gerenciadas pela AWS : AWSTrustedAdvisorServiceRolePolicy.	18 de janeiro de 2024

Documentação atualizada para `AWSSupportServiceRolePolicy`	Adição de novas permissões para fornecer serviços de faturamento, administrativo e de suporte para a função vinculada ao serviço. Para obter mais informações, consulte Políticas gerenciadas pela AWS : AWSSupportServiceRolePolicy.	17 de janeiro de 2024
Documentação atualizada para Trusted Advisor	1 verificação de tolerância a falhas atualizada para alterar o título e a descrição. Para obter mais informações, consulte Registro de alterações para AWS Trusted Advisor verificações.	8 de janeiro de 2024
Documentação atualizada para Trusted Advisor	1 verificação de segurança atualizada para refletir a mudança no período de suspensão de uso. Para obter mais informações, consulte Registro de alterações para AWS Trusted Advisor verificações.	21 de dezembro de 2023
Documentação atualizada para Trusted Advisor	Foram adicionadas 2 verificações de segurança e 2 verificações de desempenho. Para obter mais informações, consulte Registro de alterações para AWS Trusted Advisor verificações.	20 de dezembro de 2023

Documentação atualizada para Trusted Advisor	Foi adicionada 1 verificação de segurança. Para obter mais informações, consulte Registro de alterações para AWS Trusted Advisor verificações.	15 de dezembro de 2023
Documentação atualizada do Trusted Advisor Engage	Documentação atualizada do Trusted Advisor Engage com alterações na opção de notificação por e-mail.	14 de dezembro de 2023
Documentação atualizada do Trusted Advisor Engage	Documentação atualizada do Trusted Advisor Engage com alterações nos compromissos agendados.	11 de dezembro de 2023
Documentação atualizada para Trusted Advisor	Foram adicionadas 2 novas verificações de tolerância a falhas e 1 verificação de otimização de custos. Para obter mais informações, consulte Registro de alterações para AWS Trusted Advisor verificações.	7 de dezembro de 2023
Documentação atualizada para `AWSSupportServiceRolePolicy`	Adição de novas permissões para fornecer serviços de faturamento, administrativo e de suporte para a função vinculada ao serviço. Para obter mais informações, consulte Políticas gerenciadas pela AWS : AWSSupportServiceRolePolicy.	6 de dezembro de 2023

Políticas AWS gerenciadas atualizadas para Trusted Advisor	As políticas foram `AWSTrustedAdvisorPriorityReadOnlyAccess` AWS atualizadas `AWSTrustedAdvisorPriorityFullAccess` e gerenciadas para incluir IDs de declaração. Para obter mais informações, consulte AWS Políticas gerenciadas para o AWS Trusted Advisor.	6 de dezembro de 2023
Documentação atualizada para Trusted Advisor	Foram adicionadas 3 novas verificações de tolerância a falhas. Para obter mais informações, consulte Registro de alterações para AWS Trusted Advisor verificações.	17 de novembro de 2023
Documentação atualizada para Trusted Advisor	Foram adicionadas 37 novas verificações para o Amazon RDS. Para obter mais informações, consulte Registro de alterações para AWS Trusted Advisor verificações.	15 de novembro de 2023

Documentação atualizada para `AWSTrustedAdvisorServiceRolePolicy`	Foram adicionadas novas ações `ec2:DescribeRegions` do IAM `ecs:DescribeTaskDefinition` e `ecs:ListTaskDefinitions` para integrar novas verificações. `s3:GetLifecycleConfiguration` Para obter mais informações, consulte Políticas gerenciadas pela AWS : AWSTrustedAdvisorServiceRolePolicy.	9 de novembro de 2023
Documentação atualizada para `AWSSupportServiceRolePolicy`	Adição de novas permissões para fornecer serviços de faturamento, administrativo e de suporte para a função vinculada ao serviço. Para obter mais informações, consulte Políticas gerenciadas pela AWS : AWSSupportServiceRolePolicy.	27 de outubro de 2023
Documentação atualizada para Trusted Advisor	Foram adicionadas 64 novas verificações integradas de AWS Config. Para obter mais informações, consulte Registro de alterações para AWS Trusted Advisor verificações.	26 de outubro de 2023

Documentação atualizada para Trusted Advisor	Foram adicionadas seis novas verificações de tolerância a falhas Trusted Advisor. Para obter mais informaçõ es, consulte o Registro de alterações para AWS Trusted Advisor verificações.	12 de outubro de 2023
Documentação atualizada para `AWSTrustedAdvisorS erviceRolePolicy`	Foram adicionadas novas ações `route53re solver:ListResolve rEndpoints` , `route53re solver:ListResolve rEndpointIpAddress es` , `ec2:Descr ibeSubnets` , `kafka:Lis tClustersV2` e `kafka:ListNodes` do IAM para integrar as novas verificações de resiliência. Para obter mais informações, consulte Políticas gerenciad as pela AWS : AWSTruste dAdvisorServiceRolePolicy.	14 de setembro de 2023
Documentação atualizada para `AWSSupportServiceR olePolicy`	Adição de novas permissõe s para fornecer serviços de faturamento, administrativo e de suporte para a função vinculada ao serviço. Para obter mais informações, consulte Políticas gerenciad as pela AWS : AWSSuppor tServiceRolePolicy.	28 de agosto de 2023

Documentação atualizada para Trusted Advisor	Foi adicionada uma nova verificação de limites de serviço para o Lambda. Para obter mais informaçõ es, consulte o Registro de alterações para AWS Trusted Advisor verificações.	17 de agosto de 2023
Documentação atualizada para Trusted Advisor	Foi adicionada uma nova verificação de tolerância a falhas para o Lambda. Para obter mais informaçõ es, consulte o Registro de alterações para AWS Trusted Advisor verificações.	3 de agosto de 2023
Documentação atualizada do Trusted Advisor Engage	Documentação atualizada do Trusted Advisor Engage com alterações nos formulários para criar e editar interaçõe s. Página adicionada com exemplos de políticas de controle de serviço para AWS Trusted Advisor.	27 de julho de 2023
Documentação atualizada para `AWSSupportServiceR olePolicy`	Adição de novas permissõe s para fornecer serviços de faturamento, administrativo e de suporte para a função vinculada ao serviço. Para obter mais informações, consulte Políticas gerenciad as pela AWS : AWSSuppor tServiceRolePolicy.	26 de junho de 2023

Documentação atualizada para Trusted Advisor	Foram adicionadas duas novas verificações de tolerância a falhas para o Amazon MQ. Foi adicionada uma nova verificação de tolerância a falhas e uma nova verificação de performance para o Amazon Elastic File System. Para obter mais informações, consulte o Registro de alterações para AWS Trusted Advisor verificações.	1.º de junho de 2023
Documentação atualizada para Trusted Advisor	Foram adicionadas duas novas verificações de tolerância a falhas para o NAT Gateway. Para obter mais informações, consulte o Registro de alterações para AWS Trusted Advisor verificações.	16 de maio de 2023
Documentação atualizada para AWS Support planos	Foi adicionada uma nova permissão e CloudTrail documentação para a criação de cronogramas de planos de suporte. Para obter mais informações, consulte Gerenciar o acesso aos AWS Support planos, políticas AWS gerenciadas para AWS Support planos e chamadas da API de AWS Support planos de registro com AWS CloudTrail.	8 de maio de 2023

Documentação atualizada para `AWSSupportServiceRolePolicy`	Adição de novas permissões para fornecer serviços de faturamento, administrativo e de suporte para a função vinculada ao serviço. Para obter mais informações, consulte Políticas gerenciadas pela AWS : AWSSupportServiceRolePolicy.	2 de maio de 2023
Documentação atualizada para Trusted Advisor Engage e Trusted Advisor Priority	Pré-requisitos esclarecidos para Trusted Advisor Engage e Priority. Trusted Advisor Foi adicionado um exemplo de política do IAM com a capacidade de usar o Trusted Advisor Engage e permitir acesso confiável ao Trusted Advisor.	28 de abril de 2023
Documentação atualizada para Trusted Advisor	Foram adicionadas duas novas verificações de tolerância a falhas para AWS Resilience Hub o Incident Manager. Para obter mais informações, consulte o Registro de alterações para AWS Trusted Advisor verificações.	27 de abril de 2023

Documentação adicionada para Trusted Advisor Engage	Você pode usar o AWS Trusted Advisor Engage para aproveitar ao máximo seus AWS Support planos, facilitando a visualização, a solicitação e o rastreamento de todos os seus compromissos proativos e a comunicação com sua Conta da AWS equipe sobre os compromissos contínuos. Para obter mais informações, consulte Get started with AWS Trusted Advisor Engage.	6 de abril de 2023
Documentação atualizada para Trusted Advisor	Foram adicionadas duas novas verificações de tolerância a falhas para o Amazon ECS. Para obter mais informações, consulte o Registro de alterações para AWS Trusted Advisor verificações.	30 de março de 2023
Documentação atualizada para `AWSSupportServiceRolePolicy`	Adição de novas permissões para fornecer serviços de faturamento, administrativo e de suporte para a função vinculada ao serviço. Para obter mais informações, consulte Políticas gerenciadas pela AWS : AWSSupportServiceRolePolicy.	16 de março de 2023

Documentação adicionada para Trusted Advisor Priority	Atualizou o console Trusted Advisor Priority: • Os botões Confirmar e Ignorar substituíram os botões Aceitar e Rejeitar. • Você não precisa inserir seu cargo ou nome para reconhecer, resolver, rejeitar ou reabrir as recomenda ções. Para obter mais informaçõ es, consulte Introdução ao Trusted Advisor Priority.	16 de fevereiro de 2023
Exemplos de código atualizad os para AWS Support	Foram adicionados exemplos de código.NET, Java e Kotlin que mostram como usar AWS Support com um kit de desenvolvimento de AWS software (SDK). Para obter mais informações, consulte Exemplos de código para AWS Support usar AWS SDKs.	16 de janeiro de 2023
Documentação atualizada para `AWSSupportServiceR olePolicy`	Adição de novas permissõe s para fornecer serviços de faturamento, administrativo e de suporte para a função vinculada ao serviço. Para obter mais informações, consulte Políticas gerenciad as pela AWS : AWSSuppor tServiceRolePolicy.	10 de janeiro de 2023

Documentação atualizada para o AWS Support aplicativo	É possível pesquisar casos de suporte no Slack usando as opções de filtro ou pesquisando por ID do caso. Para obter mais informações, consulte Como procurar casos de suporte no Slack.	29 de dezembro de 2022
Documentação atualizada para o AWS Support aplicativo	Você também pode usar o Terraform para criar seus recursos para o AWS Support aplicativo. Para obter mais informações, consulte Criar recursos de AWS Support aplicativos usando o Terraform.	22 de dezembro de 2022
Documentação atualizada para Trusted Advisor	Foram adicionadas três novas verificações de tolerância a falhas para Amazon MemoryDB ElastiCache, Amazon e. AWS CloudHSM Para obter mais informações, consulte o Registro de alterações para AWS Trusted Advisor verificações.	15 de dezembro de 2022

Documentação atualizada do AWS Support aplicativo no Slack	Já é possível solicitar suporte por chat ao vivo para as seguintes opções: • Casos de suporte para conta e faturamento. • Suporte em japonês para casos de suporte técnico. • Para obter mais informaçõ es, consulte Como criar casos de suporte em um canal do Slack.	14 de dezembro de 2022
Documentação atualizada para AWS Support	Foi adicionada documentação sobre novos endpoints para a AWS Support API. Para obter mais informações, consulte Sobre a API do AWS Support.	14 de dezembro de 2022
Documentação adicionada para AWS CloudFormation modelos a serem usados no AWS Support aplicativo no Slack	Você pode usar CloudForm ation modelos para criar espaços de trabalho e canais de configuração do Slack para Contas da AWS entrar. AWS Organizations Para obter mais informações, consulte Criação de recursos de AWS Support aplicativos com AWS CloudFormation.	5 de dezembro de 2022

Documentação atualizada para Trusted Advisor	Foram adicionadas duas novas verificações de tolerância a falhas para AWS Resilience Hub. Para obter mais informações, consulte o Registro de alterações para AWS Trusted Advisor verificações.	17 de novembro de 2022
Documentação adicionada para suas AWS Security Hub descobertas em Trusted Advisor	Suas descobertas dos controles do Security Hub são removidas do Trusted Advisor Faster. Para obter mais informações, consulte o Registro de alterações para AWS Trusted Advisor verificações.	17 de novembro de 2022
Documentação atualizada para AWS Trusted Advisor	Documentação adicionada para Trusted Advisor Recomendações. Para obter mais informações, consulte o Registro de alterações para AWS Trusted Advisor verificações.	16 de novembro de 2022
Documentação atualizada do AWS Support aplicativo no Slack	Foi adicionada a documentação para o suporte ao idioma japonês. Para obter mais informações, consulte Como criar casos de suporte em um canal do Slack.	11 de novembro de 2022

Documentação atualizada para AWS Support planos	Foram adicionadas informações de solução de problemas para permitir o acesso aos planos do Support em uma organização. Para obter mais informações, consulte Solução de problemas.	9 de novembro de 2022
Documentação atualizada do AWS Support aplicativo no Slack	Documentação adicionada para permissões `supportapp`. Para obter mais informações, consulte Permissões necessárias para que o AWS Support aplicativo se conecte ao Slack.	1º de novembro de 2022
Documentação atualizada do AWS Support aplicativo no Slack	Você pode usar a operação `RegisterSlackWorkspaceForOrganization` da API para registrar um espaço de trabalho do Slack para seu Conta da AWS. Para chamar essa API, sua conta deve fazer parte de uma organização no AWS Organizations. Para obter mais informações, consulte Referência da API do AWS Support no Slack.	19 de outubro de 2022

Documentação atualizada para `AWSSupportServiceRolePolicy`	Adição de novas permissões para fornecer serviços de faturamento, administrativo e de suporte para a função vinculada ao serviço. Para obter mais informações, consulte Políticas gerenciadas pela AWS : AWSSupportServiceRolePolicy.	4 de outubro de 2022
Updated documentation for Support Plans (Documentação atualizada dos planos de suporte)	Agora você pode usar AWS Identity and Access Management (IAM) para gerenciar permissões para alterar o plano de suporte do seu Conta da AWS. Para obter mais informações, consulte os tópicos a seguir. • Gerenciando o acesso aos AWS Support planos • AWS políticas gerenciadas para AWS Support planos • Mudando AWS Support os planos • Chamadas da API Logging AWS Support Plans com AWS CloudTrail	29 de setembro de 2022

Documentação atualizada do AWS Support aplicativo no Slack	Foi adicionada documentação sobre como configurar um canal público ou privado para usar com o AWS Support aplicativo. Para obter mais informações, consulte Configuring a Slack channel (Como configurar um canal do Slack).	22 de setembro de 2022
Documentação atualizada para AWS Support	Foi adicionada uma nova seção sobre segurança para seus casos de suporte. Para obter mais informações, consulte Segurança para seus AWS Support casos.	9 de setembro de 2022
Documentação atualizada para Trusted Advisor	Inclusão de uma nova verificação de segurança para o Amazon EC2. Para obter mais informações, consulte o Registro de alterações para AWS Trusted Advisor verificações.	1º de setembro de 2022

Documentação atualizada do AWS Support aplicativo no Slack	Consulte os seguintes tópicos: Você pode usar o AWS Support aplicativo para gerenciar seus casos de suporte, solicitar aumentos de cota de serviço e conversar com agentes de suporte diretamente nos seus canais do Slack. Para obter mais informações, consulte a documentação do AWS Support App no Slack. Você pode anexar políticas AWS gerenciadas às suas funções do IAM para usar o AWS Support aplicativo. Para obter mais informaçõ es, consulte políticas AWS gerenciadas para AWS Support aplicativos no Slack. Nova referência de API para o AWS Support aplicativo. Consulte a Referência da API do AWS Support App.	24 de agosto de 2022
Documentação atualizada para `AWSSupportServiceR olePolicy`	Adição de novas permissõe s para fornecer serviços de faturamento, administrativo e de suporte para a função vinculada ao serviço. Para obter mais informações, consulte Políticas gerenciad as pela AWS : AWSSuppor tServiceRolePolicy.	17 de agosto de 2022

Documentação adicionada para Trusted Advisor Priority	Trusted Advisor O Priority adiciona suporte aos seguintes recursos: • Administradores delegados • Notificações diárias e semanais por e-mail para resumos de recomendações • Reabrir recomendações resolvidas ou rejeitadas • AWS políticas gerenciadas Para obter mais informaçõ es, consulte Introdução ao Trusted Advisor Priority.	17 de agosto de 2022
Documentação atualizada para Trusted Advisor	A página Preferências no Trusted Advisor console foi atualizada. Para obter mais informações, consulte Introdução ao AWS Trusted Advisor.	15 de julho de 2022

Documentação atualizada para Trusted Advisor	Atualizações das verificações para incluir as seguintes informações: • Alert Criteria (Critérios de alerta) • Recommended Action (Ação recomendada) • Recursos adicionais • Report columns (Colunas do relatório) Para obter mais informações, consulte Referência da verificação do AWS Trusted Advisor.	7 de julho de 2022
Documentação atualizada para AWS Support	Adição de documentação que explica como gerenciar casos de suporte. • Updating an existing support case (Atualizar um caso de suporte existente) • Solução de problemas	28 de junho de 2022
Documentação atualizada para `AWSSupportServiceRolePolicy`	Atualização de permissões para fornecer serviços de faturamento, administrativo e de suporte para a função vinculada ao serviço. Para obter mais informações, consulte Políticas gerenciadas pela AWS : AWSSupportServiceRolePolicy.	23 de junho de 2022

Documentação atualizada para Trusted Advisor	Trusted Advisor suporta controles adicionais do padrão de segurança AWS Foundational Security Best Practices, provenientes de. AWS Security Hub Para obter mais informações, consulte o Registro de alterações para AWS Trusted Advisor verificações.	23 de junho de 2022
Documentação atualizada para Trusted Advisor	Adição de informações sobre como solicitar aumentos de cotas de serviço. Para obter mais informações, consulte Service limits (Limites de serviço).	21 de junho de 2022
Documentação atualizada para AWS Support	A experiência de criação de casos foi atualizada no console do Support Center. Para obter mais informações, consulte Criar casos de suporte e gerenciamento de casos.	18 de maio de 2022
Documentação atualizada para Trusted Advisor	Adição de quatro verificações para o Amazon EBS e o AWS Lambda. Para obter mais informações, consulte Aceitar AWS Compute Optimizer para adicionar Trusted Advisor cheques.	4 de maio de 2022

Documentação atualizada para `AWSSupportServiceRolePolicy`	Adição de novas permissões para fornecer serviços de faturamento, administrativo e de suporte para a função vinculada ao serviço. Para obter mais informações, consulte Políticas gerenciadas pela AWS : AWSSupportServiceRolePolicy.	27 de abril de 2022
Atualização da documentação para a verificação de chaves de acesso expostas	Agora essa verificação é atualizada automaticamente para você. Para obter mais informações, consulte Registro de alterações para AWS Trusted Advisor verificações.	25 de abril de 2022
Documentação atualizada para Trusted Advisor	As AWS Direct Connect verificações na categoria de tolerância a falhas são atualizadas. Para obter mais informações, consulte Registro de alterações para AWS Trusted Advisor verificações.	29 de março de 2022
Documentação atualizada para `AWSSupportServiceRolePolicy`	Adição de novas permissões para fornecer serviços de faturamento, administrativo e de suporte para a função vinculada ao serviço. Para obter mais informações, consulte Políticas gerenciadas pela AWS : AWSSupportServiceRolePolicy.	14 de março de 2022

Documentação adicionada para Trusted Advisor Priority	Você pode usar o Trusted Advisor Priority para ver uma lista de recomendações priorizadas do seu gerente técnico de contas (TAM). Para obter mais informaçõ es, consulte Introdução ao Trusted Advisor Priority.	28 de fevereiro de 2022
Documentação atualizada para usar a Amazon EventBrid ge para Trusted Advisor	Você pode criar uma EventBridge regra para monitorar as alterações em seus Trusted Advisor cheques. Para obter mais informaçõ es, consulte Monitorando os resultados da AWS Trusted Advisor verificação com EventBridge.	21 de fevereiro de 2022
Nova documentação para usar EventBridge a Amazon para monitorar AWS Support casos	Você pode criar uma EventBridge regra para monitorar e receber notificaç ões sobre seus casos de suporte. Para obter mais informações, consulte Monitoramento de AWS Support casos com EventBrid ge.	21 de fevereiro de 2022

Documentação atualizada para `AWSSupportServiceRolePolicy`	Adição de novas permissões para fornecer serviços de faturamento, administrativo e de suporte para a função vinculada ao serviço. Para obter mais informações, consulte Políticas gerenciadas pela AWS : AWSSupportServiceRolePolicy.	17 de fevereiro de 2022
Documentação adicionada para integração com AWS Security Hub	No Trusted Advisor console, agora você pode ver as descobertas dos controles do Security Hub que fazem parte do padrão de segurança AWS Foundational Security Best Practices. Para obter mais informações, consulte Visualizando AWS Security Hub controles no AWS Trusted Advisor console.	18 de janeiro de 2022

Documentação atualizada para Trusted Advisor	Foram adicionadas três novas verificações para instâncias do Amazon EC2 que estão executando o Microsoft SQL Server. • Consolidação de instâncias do Amazon EC2 para Microsoft SQL Server • Instâncias do Amazon EC2 superprovisionadas para Microsoft SQL Server • Fim do suporte para instâncias do Amazon EC2 com o Microsoft SQL Server Para obter mais informações, consulte Referência da verificação do AWS Trusted Advisor.	20 de dezembro de 2021

Documentação atualizada para Trusted Advisor	Trusted Advisor adicionou quatro novas verificações para AWS Well-Architected • Problemas de alto risco do AWS Well-Architected para otimização de custos • Problemas de alto risco do AWS Well-Architected em relação à performance • Problemas de alto risco do AWS Well-Architected em relação à segurança • Problemas de alto risco do AWS Well-Architected em relação à confiabilidade Para obter mais informaçõ es, consulte Referência da verificação do AWS Trusted Advisor.	20 de dezembro de 2021
Documentação atualizada	Se você tiver um plano Enterprise On-Ramp Support, terá acesso a todas as Trusted Advisor verificações e à AWS Support API.	24 de novembro de 2021
Documentação atualizada para Trusted Advisor	Trusted Advisor adicionou duas novas verificações para o Amazon Comprehend. Para obter mais informaçõ es, consulte Referência da verificação do AWS Trusted Advisor.	29 de setembro de 2021

Documentação atualizada para Trusted Advisor	O nome da verificação para Amazon OpenSearch Service Reserved Instance Optimization foi atualizado. Para obter mais informações, consulte Registro de alterações para AWS Trusted Advisor verificações.	8 de setembro de 2021
Documentação atualizada para Trusted Advisor verificações	Foi adicionado um tópico de referência para todas as Trusted Advisor verificações. Para obter mais informações, consulte Referência de verificação do AWS Trusted Advisor.	1º de setembro de 2021
Documentação atualizada para políticas Trusted Advisor gerenciadas	Documentação atualizada das políticas Trusted Advisor gerenciadas. Para obter mais informações, consulte políticas AWS gerenciadas para AWS SupportAWS Trusted Advisor e.	10 de agosto de 2021
Documentação atualizada para Trusted Advisor	Documentação atualizada para o Trusted Advisor console. Para obter mais informações, consulte Começar com AWS Trusted Advisor.	16 de julho de 2021

Documentação atualizada para criar AWS Support casos	Adicionada documentação sobre como abrir um caso de suporte relacionado para casos que estão permanentemente fechados. Para obter mais informações, consulte Reabrir um caso encerrado e Criar um caso relacionado.	8 de junho de 2021
Documentação atualizada para Trusted Advisor	Trusted Advisor adicionou duas novas verificações para o armazenamento de volume do Amazon Elastic Block Store (Amazon EBS). Para obter mais informações, consulte Registro de alterações para AWS Trusted Advisor verificações.	8 de junho de 2021
Documentação atualizada	Os tópicos a seguir foram atualizados: • Procedimentos atualizados e conteúdo adicionado ao tópico Criação de CloudWatch alarmes da Amazon para monitorar AWS Trusted Advisor métricas • Foram adicionadas as cotas de serviço para a seção AWS Support API	12 de maio de 2021

Atualizações anteriores

Alteração	Descrição	Data
Documentação atualizada para Trusted Advisor	Adicionada documentação para filtrar, atualizar e baixar os resultados da verificação. Para obter mais informações, consulte as seções a seguir: • Filtrar as verificações • Atualizar resultados da verificação • Baixar dos resultados	16 de março de 2021
Documentação atualizada sobre políticas AWS gerenciadas	Foram adicionadas informações sobre a política `AWSSupportServiceRolePolicy` AWS gerenciada. Para obter mais informaçõ es, consulte Usar perfis vinculados ao serviço do AWS Support.	16 de março de 2021
Verificações adicionadas para AWS Lambda	Foram adicionadas quatro AWS Trusted Advisor verificações para Lambda no. Registro de alterações para AWS Trusted Advisor	8 de março de 2021
Verificações de limite de serviço atualizad as para o Amazon Elastic Block Store	Cinco AWS Trusted Advisor verificações atualizadas do Amazon EBS noRegistro de alterações para AWS Trusted Advisor.	5 de março de 2021
Documentação atualizada para CloudTrail registro	CloudTrail suporta o registro de ações do console quando você altera seu AWS Support plano. Para obter mais informações, consulte Registrar alterações no seu plano AWS Support.	9 de fevereiro de 2021
Documentação atualizada para Trusted Advisor	Atualização do tópico do Conceitos básicos das recomendações do Trusted Advisor.	29 de janeiro de 2021

Alteração	Descrição	Data
Documentação atualizada para Trusted Advisor relatórios	Foi adicionada uma Solução de problemas seção para usar Trusted Advisor relatórios com outros AWS serviços.	4 de dezembro de 2020
AWS Trusted Advisor Suporte adicionado para AWS CloudTrail registro	CloudTrail suporta o registro de um subconjunto de ações do Trusted Advisor console. Para obter mais informações, consulte Registro de ações do console do AWS Trusted Advisor com AWS CloudTrail.	23 de novembro de 2020
Adicionado um tópico de log de alterações	Veja as alterações nas AWS Trusted Advisor verificações e categorias noRegistro de alterações para AWS Trusted Advisor.	18 de novembro de 2020
Suporte adicionado a unidades organizacionais	Agora você pode criar relatórios para Trusted Advisor verificações de unidades organizacionais (OUs). Para obter mais informações, consulte Criar relatórios da visualização organizacional.	17 de novembro de 2020
Atualizou o registro com o AWS CloudTrail tópico	Foi adicionada uma entrada de registro de exemplo para uma operação de Trusted Advisor API. Consulte Informações do AWS Trusted Advisor no registro do CloudTrail.	22 de outubro de 2020
AWS Support Cotas adicionadas	Adicionadas informações sobre as cotas e restrições do AWS Support. Consulte AWS Support endpoints and quotas na Referência geral da AWS.	4 de agosto de 2020
Visão organizacional para AWS Trusted Advisor	Agora você pode criar relatórios de Trusted Advisor cheques para contas que fazem parte do AWS Organizations. Consulte Visualização organizacional para AWS Trusted Advisor.	17 de julho de 2020

Alteração	Descrição	Data
Segurança e AWS Support	Atualização de informações sobre considera ções de segurança ao usar o AWS Support e o Trusted Advisor. Consulte Segurança em AWS Support	5 de maio de 2020
Segurança e AWS Support	Adição de informações sobre considerações de segurança no uso do AWS Support.	10 de janeiro de 2020
Usando Trusted Advisor como um serviço da web	Foram adicionadas instruções atualizadas para atualizar Trusted Advisor os dados após obter a lista de Trusted Advisor verificações.	1 de novembro de 2018
Uso de funções vinculadas a serviço	Adição de uma nova seção.	11 de julho de 2018
Conceitos básicos: solução de problemas	Adição de links de solução de problemas para o Route 53 e o AWS Certificate Manager.	1 de setembro de 2017
Exemplo de gerenciamento de casos: criação de um caso	Adição de uma nota sobre a caixa CC para os usuários que têm o plano de suporte Básico.	1° de agosto de 2017
Monitorando os resultados da Trusted Advisor verificação com CloudWatch eventos	Adição de uma nova seção.	18 de novembro de 2016
Gerenciamento de casos	Atualização dos nomes dos níveis de gravidade dos casos.	27 de outubro de 2016
Registrando AWS Support chamadas com AWS CloudTrail	Adição de uma nova seção.	21 de abril de 2016

Alteração	Descrição	Data
Conceitos básicos: solução de problemas	Adição de mais links de solução de problemas.	19 de maio de 2015
Conceitos básicos: solução de problemas	Adição de mais links de solução de problemas.	18 de novembro de 2014
Conceitos básicos: gerenciamento de casos	Atualizado para refletir o Service Catalog no AWS Management Console.	30 de outubro de 2014
Programando a vida útil de um AWS Support caso	Adição de informações sobre novos elementos de API para adicionar anexos a casos e para omissão de comunicações de casos ao recuperar o histórico do caso.	16 de julho de 2014
Acessando AWS Support	Remoção de contatos de suporte designados como um método de acesso.	28 de maio de 2014
Conceitos básicos	Adição da seção Conceitos básicos.	13 de dezembro de 2013
Publicação inicial	Novo AWS Support serviço lançado.	30 de abril de 2013

AWS Glossário

Para obter a terminologia mais recente da AWS, consulte o glossário da AWS na Referência do Glossário da AWS.

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.