



Guia do usuário

AWS Support



Versão da API 2025-06-11

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

AWS Support: Guia do usuário

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

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

Table of Contents

Comece com AWS Support	1
Criar casos de suporte e gerenciamento de casos	1
Criar um caso de suporte	2
Descrever o problema	5
Escolhendo um nível de severidade inicial	5
Entendendo os tempos de AWS Support resposta	7
Alterando o nível de gravidade de um caso de suporte	8
Exemplo: criar um caso de suporte para conta e faturamento	11
Solução de problemas	17
Criar um aumento de cota de serviço	18
Atualizar, resolver e reabrir casos	19
Atualizar um caso de suporte existente	20
Resolver um caso de suporte	21
Reabrir um caso resolvido	23
Abrir um caso relacionado	24
Histórico de caso	26
Trabalhando com AWS SDKs	26
Sobre a AWS Support API	28
Gerenciamento de casos de suporte	28
AWS Trusted Advisor	29
Endpoints	29
Support em AWS SDKs	30
AWS Support Planos	31
Características dos AWS Support planos	31
Mudando AWS Support os planos	33
Informações relacionadas	34
AWS Trusted Advisor	35
Conceitos básicos das recomendações do Trusted Advisor	36
Faça login no Trusted Advisor console	36
Visualizar categorias de verificação	38
Visualizar verificações específicas	40
Filtrar as verificações	41
Atualizar resultados da verificação	42
Baixar dos resultados	43

Visualização organizacional	44
Preferências	44
Comece a usar a Trusted Advisor API	46
Usando Trusted Advisor como um serviço da web	47
Obtenha a lista de Trusted Advisor cheques disponíveis	47
Atualize a lista de verificações disponíveis Trusted Advisor	48
Trusted Advisor Faça uma pesquisa e verifique se há mudanças de status	48
Solicitar um resultado de Trusted Advisor verificação	51
Mostrar detalhes de um Trusted Advisor cheque	52
Visão organizacional para AWS Trusted Advisor	52
Pré-requisitos	53
Habilitar a visualização organizacional	53
Verificações de atualização Trusted Advisor	54
Criar relatórios da visualização organizacional	55
Visualize o resumo do relatório.	59
Baixar um relatório da visualização organizacional	60
Desabilitar a visualização organizacional	65
Utilização de políticas do IAM para permitir acesso à visualização organizacional	67
Usando outros AWS serviços para visualizar Trusted Advisor relatórios	70
Exibir Trusted Advisor cheques fornecidos por AWS Config	80
Solução de problemas	81
Visualize seus controles do Security Hub em Trusted Advisor	82
Pré-requisitos	83
Para visualizar os resultados do Security Hub	84
Atualizar os resultados do Security Hub	86
Desativar o Security Hub de Trusted Advisor	87
Solução de problemas	87
Opte por receber Trusted Advisor cheques AWS Compute Optimizer	91
Informações relacionadas	92
Comece com o AWS Trusted Advisor Priority	92
Pré-requisitos	93
Ativar Trusted Advisor prioridade	94
Visualizar recomendações priorizadas	94
Reconhecer uma recomendação	97
Ignorar uma recomendação	100
Resolver uma recomendação	102

Reabrir uma recomendação	104
Baixar os detalhes da recomendação	105
Registrar administradores delegados	106
Cancelar o registro dos administradores delegados	107
Gerenciar notificações Trusted Advisor prioritárias	107
Desativar Trusted Advisor prioridade	108
Comece a usar o AWS Trusted Advisor Engage (versão prévia)	109
Pré-requisitos	109
Visualize o painel de interações	110
Visualize o catálogo de tipos de interação	111
Solicitar uma interação	112
Editar uma interação	114
Enviar anexos e notas	115
Alterar o status da interação	116
Diferencie entre as interações recomendadas e solicitadas	117
Pesquisar interações	117
Trusted Advisor verifique a referência	118
Otimização de custo	119
Performance	189
Segurança	243
Tolerância a falhas	294
Limites do serviço	419
Excelência operacional	439
Registro de alterações para AWS Trusted Advisor	486
Verificações novas e atualizadas	486
Nova verificação - uso AWS STS global de endpoints em Regiões da AWS	486
Novas verificações do Cust Optimization Hub	487
CloudFront verificações específicas revisadas	488
Verificações revisadas	489
Verificações obsoletas AWS Security Hub	490
Nova verificação: Amazon RDS Continuous Backup não habilitado	490
Nova verificação: Registro AWS CloudTrail de eventos de gerenciamento	491
Atualização da verificação de recursos do grupo Auto Scaling	491
Atualização da verificação de acesso externo do IAM Access Analyzer	491
Adicionado 1 novo cheque	492
3 verificações atualizadas	492

Foram adicionadas 4 verificações	492
3 verificações atualizadas	492
Foram adicionados 9 novos cheques	493
Atualizou 1 verificação de segurança e adicionou 1 verificação de segurança	493
6 verificações de segurança atualizadas	494
1 verificações de tolerância a falhas atualizadas	494
9 cheques atualizados	494
Foram removidas 5 verificações e adicionadas 1 cheque	495
Verificações de tolerância a falhas removidas	495
Nova verificação de tolerância a falhas	495
Tolerância a falhas e verificações de segurança atualizadas	496
Nova verificação de tolerância a falhas	496
Verificação atualizada de tolerância a falhas	496
Verificação de segurança atualizada	496
Novas verificações de segurança e desempenho	496
Nova verificação de segurança	497
Novas verificações de tolerância a falhas e otimização de custos	497
Novas verificações de tolerância a falhas	497
Novas verificações para o Amazon RDS	498
Nova AWS Trusted Advisor API	498
Trusted Advisor verifique a remoção	498
Integração de AWS Config cheques em Trusted Advisor	499
Novas verificações de tolerância a falhas	499
Verificação de novos limites de serviço	499
Nova verificação de tolerância a falhas	500
Novas verificações de tolerância a falhas e performance	500
Novas verificações de tolerância a falhas	500
Novas verificações de tolerância a falhas	500
Expansão regional das verificações de tolerância a falhas do Amazon ECS	501
Novas verificações de tolerância a falhas	501
Novas verificações de tolerância a falhas	497
Atualizações na Trusted Advisor integração com AWS Security Hub	502
Novas verificações de tolerância a falhas para o AWS Resilience Hub	497
Atualização para o Trusted Advisor console	503
Novos cheques para a Amazon EC2	503
Verificações do Security Hub adicionadas ao Trusted Advisor	503

Cheques adicionados de AWS Compute Optimizer	504
Atualizações para a verificação de chaves de acesso expostas	504
Verificações atualizadas para AWS Direct Connect	505
AWS Security Hub controles adicionados ao AWS Trusted Advisor console	506
Novas verificações para Amazon EC2 e AWS Well-Architected	506
Nome do cheque atualizado para o Amazon OpenSearch Service	507
Verificações adicionadas para o armazenamento de volumes do Amazon Elastic Block Store	507
Verificações adicionadas para AWS Lambda	508
Trusted Advisor verifique a remoção	508
Verificações atualizadas para o Amazon Elastic Block Store	509
Trusted Advisor verifique a remoção	510
Trusted Advisor verifique a remoção	511
AWS Support Aplicativo no Slack	512
Pré-requisitos	513
Gerenciar o acesso ao widget do AWS Support aplicativo	514
Gerenciar o acesso ao AWS Support aplicativo	515
Autorizar um espaço de trabalho do Slack	522
Autorizar várias contas	524
Configurar um canal do Slack	525
Atualizar a configuração do seu canal do Slack	530
Criar casos de suporte no Slack	531
Responder a casos de suporte no Slack	537
Participe de uma sessão de bate-papo ao vivo com AWS Support	539
Procurar casos de suporte no Slack	545
Usar os resultados da pesquisa	547
Resolver casos de suporte no Slack	549
Reabrir casos de suporte no Slack	549
Solicitar aumentos de cota de serviço	550
Excluir uma configuração de canal do Slack do AWS Support aplicativo	553
Excluir uma configuração do espaço de trabalho do Slack do aplicativo AWS Support	553
AWS Support Comandos do aplicativo no Slack	555
Comandos do canal do Slack	555
Comandos do canal de chat ao vivo	555
Visualizar correspondências do aplicativo AWS Support no AWS Support Center Console	556
Crie AWS CloudFormation recursos para o AWS Support aplicativo no Slack	557

AWS Support Aplicativo e AWS CloudFormation modelos	557
Criar recursos de configuração do Slack para a organização	557
Saiba mais sobre CloudFormation	563
Crie recursos de AWS Support aplicativos usando o Terraform	563
Segurança	565
Proteção de dados	566
Segurança para casos de suporte	567
Gerenciamento de identidade e acesso	568
Público	568
Autenticação com identidades	569
Gerenciar o acesso usando políticas	572
Como AWS Support funciona com o IAM	575
Exemplos de políticas baseadas em identidade	577
Uso de perfis vinculados ao serviço	580
AWS políticas gerenciadas	587
Gerencie o acesso ao AWS Support Centro	656
Gerencie o acesso aos AWS Support planos	663
Gerencie o acesso ao AWS Trusted Advisor	668
Políticas de controle de serviço de exemplo para o AWS Trusted Advisor	681
Solução de problemas	683
Resposta a incidentes	686
Registro e monitoramento em AWS Support e AWS Trusted Advisor	686
Validação de conformidade	687
Resiliência	688
Segurança da infraestrutura	688
Análise de configuração e vulnerabilidade	689
Exemplos de código	690
Conceitos básicos	698
Olá Suporte	699
Conheça os conceitos básicos	706
Ações	764
Monitoramento e registro para Suporte	836
Monitorando Suporte casos com EventBridge	836
Criação de uma EventBridge regra para AWS Support casos	837
Exemplos de AWS Support eventos	839
Consulte também	841

Registrando chamadas de AWS Support API com AWS CloudTrail	841
AWS Support informações em CloudTrail	842
AWS Trusted Advisor informações no CloudTrail registro	843
Entendendo as entradas do arquivo de AWS Support log	843
Registrando chamadas da API do AWS Support aplicativo com CloudTrail	845
AWS Support Informações do aplicativo em CloudTrail	846
Entendendo as entradas do arquivo de log do AWS Support aplicativo	847
Como monitorar e registrar planos de suporte	851
Chamadas da API Logging AWS Support Plans com AWS CloudTrail	851
AWS Support Informações sobre planos em CloudTrail	852
Entendendo as entradas do arquivo de log de AWS Support planos	853
Registrando ações do console para alterações em seu Suporte plano	859
Monitoramento e registro para Trusted Advisor	863
Monitorando Trusted Advisor os resultados da verificação com EventBridge	864
Criação CloudWatch de alarmes para monitorar métricas Trusted Advisor	866
Pré-requisitos	867
CloudWatch métricas para Trusted Advisor	871
Trusted Advisor métricas e dimensões	877
Registrando ações AWS Trusted Advisor do console com AWS CloudTrail	879
Trusted Advisor informações em CloudTrail	879
Exemplo: entradas do arquivo de Trusted Advisor log	882
Recursos de solução de problemas	886
Solução de problemas de erros específicos do serviço	886
Histórico do documento	891
Atualizações anteriores	928
AWS Glossário	932
.....	cmxxxiii

Começando com AWS Support

Suporte oferece uma variedade de planos que fornecem acesso a ferramentas e conhecimentos que apoiam o sucesso e a integridade operacional de suas AWS soluções. Todos os planos de suporte oferecem acesso 24 horas por dia, 7 dias por semana, ao atendimento ao cliente, à AWS documentação, aos documentos técnicos e aos fóruns de suporte. Para obter suporte técnico e mais recursos para planejar, implantar e melhorar seu AWS ambiente, você pode escolher um plano de suporte para seu caso de AWS uso.

Observações

- Para criar um caso de suporte no AWS Management Console, consulte [Criar um caso de suporte](#).
- Para obter mais informações sobre os diferentes AWS Support planos, consulte [Comparar AWS Support planos](#) [Mudando AWS Support os planos](#) e.
- Os planos de suporte oferecem tempos de resposta diferentes para seus casos de suporte. Consulte [Escolha do nível inicial de gravidade do caso de suporte](#) e [Entendendo os tempos de AWS Support resposta](#).

Tópicos

- [Criar casos de suporte e gerenciamento de casos](#)
- [Criar um aumento de cota de serviço](#)
- [Atualizar, resolver e reabrir um caso](#)
- [Usando AWS Support com um AWS SDK](#)

Criar casos de suporte e gerenciamento de casos

No AWS Management Console, você pode criar três tipos de casos de clientes em Suporte:

- 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 é cliente de uma empresa AWS Partner que faz parte do e usa o Resold Support AWS Partner Network, entre em contato AWS Partner diretamente com você para qualquer problema relacionado ao faturamento. AWS Support não posso ajudar com problemas não técnicos do Resold Support, como cobrança e gerenciamento de contas. Para obter mais informações, consulte os tópicos a seguir.
 - [Como AWS os parceiros podem determinar AWS Support os planos 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

- Você pode entrar no Support Center como usuário 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 do ponto de interrogação



e depois 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 Próxima etapa: solucione ou entre em contato conosco.
10. Na página Entre em contato 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.

Escolha do nível inicial de gravidade do caso de suporte

Talvez você queira criar um caso de suporte com a maior severidade permitida pelo seu plano de suporte. No entanto, é uma prática recomendada escolher a severidade mais alta somente para casos que não podem ser contornados ou que afetam diretamente os aplicativos de produção. Para obter informações sobre como criar seus serviços para que a perda de um único recurso não afete seus aplicativos, consulte o artigo [técnico AWS Criando aplicativos tolerantes a falhas](#).

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

Observações

- Se você tiver um plano Enterprise Support ou Enterprise On-Ramp, poderá reatribuir o nível de gravidade do caso de suporte para refletir as mudanças na urgência e no impacto nos negócios. Por exemplo, você pode alterar seu caso de suporte de Sistema danificado para Sistema de produção danificado. Quando você altera a gravidade do caso, AWS Support recebe uma notificação e encaminha o caso de acordo com o novo nível de gravidade. Para obter mais informações, consulte [Alterando o nível de gravidade do seu caso de suporte](#).

- Se você não tiver suporte corporativo ou um plano Enterprise On-Ramp, não poderá alterar o nível de gravidade de um caso de suporte depois de criá-lo. Se sua situação mudar, fale com o Suporte agente para seu caso de suporte.
- Para obter mais informações sobre o nível de severidade, consulte a [Referência de API do AWS Support](#).

Gravidade	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

Gravidade	Código de nível de severidade e	Tempo da primeira resposta	Descrição e plano de suporte
-----------	---------------------------------	----------------------------	------------------------------

esse tempo é de 30 minutos para o plano de suporte Enterprise On-Ramp.

Entendendo os tempos de AWS Support resposta

AWS Support faz todos os esforços razoáveis para responder à sua solicitação inicial dentro do prazo indicado. Para obter informações sobre o escopo do suporte para cada Suporte plano, consulte [AWS Support recursos](#).

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.

Alterando o nível de gravidade do seu caso de suporte

Se você tiver um plano Enterprise Support ou Enterprise On-Ramp, poderá reatribuir o nível de gravidade do caso de suporte para refletir as mudanças na urgência e no impacto nos negócios. Por exemplo, você pode alterar seu caso de suporte de Sistema danificado para Sistema de produção danificado. Quando você altera a gravidade do caso, AWS Support recebe uma notificação e atende ao caso de acordo com o novo nível de gravidade.

Note

Conta ou cobrança em japonês (JP), solicitação de aumento de cota de serviço (SQIR) e conta ou casos de cobrança em turco (TR) criados nesses idiomas têm uma severidade padrão e não podem ser alterados.

Para alterar a gravidade de um caso de suporte, conclua as seguintes etapas:

1. Faça login no [AWS Support Center Console](#).

Tip

No AWS Management Console, você também pode escolher o ícone do ponto de interrogação



e depois escolher Support Center.

2. Selecione o caso para o qual você deseja alterar o nível de gravidade.
3. Em Detalhes do caso, escolha o ícone de lápis ao lado do campo Gravidade, conforme mostrado no exemplo a seguir.

Case details	
Subject [Redacted]	Status Unassigned
Case ID [Redacted]	Severity General guidance 
Created 2025-04-24T08:49:10.815Z	Category -
Case type Technical	Language Portuguese

4. Em Severidade, escolha o novo nível de severidade entre as seguintes opções:

- Orientações gerais
- Sistema prejudicado
- Sistema de produção prejudicado
- Sistema de produção desativado

- Sistema crítico para os negócios inativo
5. Em Motivo da alteração da gravidade do caso, escolha entre as opções disponíveis o motivo pelo qual você está alterando a gravidade do caso.
 6. (Opcional) Em Conte-nos mais, insira informações adicionais sobre essa alteração.
 7. Execute um destes procedimentos:
 - Se você estiver diminuindo a gravidade do caso de suporte ou se estiver elevando-a da orientação geral para Sistema comprometido ou Sistema de produção comprometido, escolha Atualizar.
 - Se você estiver aumentando a gravidade do sistema de produção inativo ou do sistema essencial para os negócios, use uma das opções na seção Métodos de contato para interagir e AWS Support, em seguida, escolha Atualizar. O exemplo a seguir mostra as opções disponíveis na seção Métodos de contato.

Change case severity ×

Severity

Production system down ▼

Reason for case severity change

- ▼

Tell us more - optional

Tell us more about the reason for the escalation

Contact methods [Info](#)

For high severity issues we recommend using our live contact mechanisms

Web ☐
We'll respond by email and Support Center.

Chat(Recommended) ☒
Chat online with a representative.

Phone(Recommended) ☐
We'll call you back at your number.

[Cancel](#) [Update](#)

 Note

- Se você atualizar a gravidade do seu caso de suporte para Sistema de produção inativo ou Sistema crítico de negócios inativo, deverá esperar 60 minutos antes de poder alterar a gravidade novamente.
- Se o seu caso de suporte estiver atualmente configurado como sistema crítico para negócios inativo, você será solicitado a iniciar um contato ao vivo com, em AWS Support vez de atribuir uma severidade maior.
- Se você está aumentando o nível de gravidade do seu caso de suporte depois de já aumentá-lo pelo menos uma vez, você pode se deparar com um período de espera. Por exemplo, se você alterar a gravidade de Sistema comprometido para Sistema de produção comprometido às 6h, seu caso de suporte ficará abaixo do tempo de primeira resposta de 4 horas para o nível de gravidade comprometido do sistema de produção. Nesse cenário, você pode atualizar o nível de gravidade novamente às 10h, após a janela de 4 horas. Para obter uma lista dos tempos de primeira resposta para cada nível de severidade, consulte a tabela em [Entendendo os tempos de AWS Support resposta](#).

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.



Hello!

We're here to help.

Account: 123456789012 • Support plan: Basic • [Change](#) 

How can we help?

Choose the related issue for your case.

1

☒ Account and billing

[Looking for Service limit increase?](#)

☐ Technical

2

Service

Billing ▼

3

Category

Other Billing Questions ▼

4

Severity [Info](#)

General question ▼

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 de 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 [Escolha do nível inicial de gravidade do caso de suporte](#).

 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.

Additional information

Describe your issue

✔ Case draft saved

1

Subject

I have an issue with my bill

Maximum 250 characters (222 remaining)

Description

Don't share any sensitive information in case correspondences, such as credentials, credit cards, signed URLs, or personally identifiable information.

[Learn more](#) 

2

I found a charge on my bill for unused resources.

Maximum 5000 characters (4951 remaining)

3

 **Attach files**

Up to 3 attachments, each less than 5MB



Description Guidance

Provide a detailed description of your issue. If you have a question about a charge, provide the date, amount, or any other details about the charge.

Cancel

Previous

Next step: Solve now or contact us

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

2. **Description (Descrição)** — Descreva seu caso de suporte. Essas são as informações mais importantes que você fornece para Suporte. 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.

How can we help?
[Account and billing](#), [Billing](#),
[Dispute a Charge](#), [General ...](#)

Additional information
[I have an issue in my account](#)

Solve now or contact us

Solve now | **Contact us**

Preferred contact language

English

Q |

English ✓

中文

한국어

日本語

☐ Phone
We'll call you back at your number.

☐ Chat
Chat online with a representative.

Cancel Previous Submit

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.

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

Pois AWS GovCloud (US), o ponto final é `*.connect-fips.us-east-1.amazonaws.com`.

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

Se você ainda não conseguir se conectar à janela de bate-papo, entre em contato AWS Support usando as opções de contato por e-mail ou telefone.

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 do ponto de interrogação



e, em seguida, 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 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

- Você deve fazer login na pessoa Conta da AWS que enviou o caso de suporte. Se você fizer login como usuário AWS Identity and Access Management (IAM), deverá ter as permissões necessárias para visualizar os casos de suporte. Para obter mais informações, consulte [Gerencie o acesso ao AWS Support Centro](#).
- Se você não responder ao caso em alguns dias, 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 [Escolha do nível inicial de gravidade do caso de suporte](#).

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 do ponto de interrogação



e, em seguida, 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 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 do ponto de interrogação



e, em seguida, 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 seu caso AWS Support foi resolvido para você, você pode usar o link de feedback para fornecer mais informações sobre sua experiência com 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.

Please let us know if we helped resolve your issue:

If YES, click here:

<https://console.aws.amazon.com/support/feedback?eventId=1234567890&language=en&questionnaireId=Support-HMD-Yes> 

If NO, click here:

<https://console.aws.amazon.com/support/feedback?eventId=1234567890&language=en&questionnaireId=Support-HMD-No> 

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 do ponto de interrogação



e, em seguida, 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 do ponto de interrogação



e, em seguida, 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).

This case can't be reopened ✕

This case has been permanently closed after 14 days of inactivity. If you're experiencing the same issue or a similar one, you can create a related case. If you're experiencing a different issue, create a new case.

Cancel Create new case Create related case

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.

Case ID 234567891 [Info](#) Resolve case

Case details

Subject Same issue is happening for my Amazon EC2 instances	Status Unassigned
Case ID 234567891	Severity General question
Created 2021-04-21T20:30:23.945Z	Category General Info and Getting Started
Case type Account	Additional contacts johndoe@example.com
Opened by janedoe@example.com	

Related cases

Subject	Case ID
Problem with EC2 instances	1234567890

Correspondence Reply

Jane Doe Wed Apr 21 2021 13:30:23 GMT-0700 (Pacific Daylight Time)	I keep getting an error for my EC2 instances. What do you recommend that I do to fix it?
--	--

Histórico de caso

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

Usando AWS Support com um AWS SDK

AWS kits de desenvolvimento de software (SDKs) estão disponíveis para muitas linguagens de programação populares. Cada SDK fornece uma API, exemplos de código e documentação que permitem que os desenvolvedores criem facilmente aplicações em seu idioma de preferência.

Documentação do SDK	Exemplos de código
AWS SDK para C++	AWS SDK para C++ exemplos de código
AWS CLI	AWS CLI exemplos de código
AWS SDK para Go	AWS SDK para Go exemplos de código
AWS SDK para Java	AWS SDK para Java exemplos de código
AWS SDK para JavaScript	AWS SDK para JavaScript exemplos de código
AWS SDK para Kotlin	AWS SDK para Kotlin exemplos de código
AWS SDK para .NET	AWS SDK para .NET exemplos de código
AWS SDK para PHP	AWS SDK para PHP exemplos de código
Ferramentas da AWS para PowerShell	Ferramentas para exemplos PowerShell de código
AWS SDK para Python (Boto3)	AWS SDK para Python (Boto3) exemplos de código
AWS SDK para Ruby	AWS SDK para Ruby exemplos de código
AWS SDK para Rust	AWS SDK para Rust exemplos de código
SDK da AWS para SAP ABAP	SDK da AWS para SAP ABAP exemplos de código
AWS SDK for Swift	AWS SDK for Swift exemplos de código

Exemplo de disponibilidade

Não consegue encontrar o que precisa? Solicite um exemplo de código usando o link
Fornecer feedback na parte inferior desta página.

Sobre a AWS Support API

A AWS Support API fornece acesso a alguns dos recursos do [AWS Support Center](#).

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

Você deve ter um plano Business, Enterprise On-Ramp ou Enterprise Support para usar a AWS Support API. Para obter mais informações, consulte [Suporte](#).

Para obter mais informações sobre as operações e os tipos de dados fornecidos pela Suporte, consulte a [Referência da AWS Support API](#).

Tópicos

- [Gerenciamento de casos de suporte](#)
- [AWS Trusted Advisor](#)
- [Endpoints](#)
- [Support em AWS SDKs](#)

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 [Registrando chamadas de AWS Support API com AWS CloudTrail](#).

Para exemplos de código que demonstram como gerenciar todo o ciclo de vida de um caso de suporte, consulte [Exemplos de código para Suporte usar AWS SDKs..](#)

AWS Trusted Advisor

Você pode usar as Trusted Advisor operações para realizar as seguintes tarefas:

- Obtenha os nomes e identificadores dos Trusted Advisor cheques
- Solicite que uma Trusted Advisor verificação seja executada AWS em sua conta e recursos
- Obtenha resumos e informações detalhadas sobre os resultados da sua Trusted Advisor verificação
- Atualize seus cheques Trusted Advisor
- Obtenha o status de cada Trusted Advisor cheque

A AWS Support API oferece suporte CloudTrail ao registro de Trusted Advisor operações. Para obter mais informações, consulte [AWS Trusted Advisor informações no CloudTrail registro](#).

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

Por exemplo, código Java que demonstra como usar as Trusted Advisor operações, consulte [Usando Trusted Advisor como um serviço da web](#).

Endpoints

Suporte 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.

Você pode usar os seguintes endpoints para a Suporte API:

- 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 [CreateCase](#) operação 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 [ResolveCase](#) operação para resolvê-lo.
- Para chamar as AWS Trusted Advisor operações na AWS Support API, você deve usar o endpoint do Leste dos EUA (Norte da Virgínia). Atualmente, os endpoints do Oeste dos EUA (Oregon) e da Europa (Irlanda) não oferecem suporte às operações. Trusted Advisor

Para obter mais informações sobre AWS endpoints, consulte [AWS Support endpoints e cotas](#) no. Referência geral da Amazon Web Services

Support em AWS SDKs

O AWS Command Line Interface (AWS CLI) e os kits AWS de desenvolvimento de software (SDKs) incluem suporte para a Suporte API.

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

Suporte oferece cinco planos de suporte:

- Básico
- 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:

- One-on-one respostas a 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 Suporte, 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 de software de terceiros — Ajuda com os sistemas operacionais e a configuração da instância 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.
- Análises empresariais de gerenciamento.

Para obter mais informações sobre os recursos e preços de cada plano de suporte, consulte [AWS Support 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.

 Note

[Se você trabalha com um AWS parceiro e quer saber mais sobre o Suporte liderado por parceiros, consulte AWS Partner-Led Support](#)

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 [AWS Support FAQs](#).

- 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 [Suporte](#) 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 [AWS Support FAQs](#). 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 as [verificações selecionadas](#) nas categorias Segurança e Tolerância a falhas. As atualizações automáticas de verificação não estão disponíveis nos planos Basic e Developer Support. Você deve atualizar manualmente as verificações do Trusted Advisor na categoria Segurança. Para atualizar manualmente uma verificação, faça o seguinte:

1. Faça login no Trusted Advisor console em <https://console.aws.amazon.com/trustedadvisor/casa>.
2. Selecione o botão Atualizar no cheque que você deseja atualizar.

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 obter 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, consulte [Gerencie o acesso ao AWS Trusted Advisor](#).

Para obter mais informações, consulte [Trusted Advisor](#).

Tópicos

- [Conceitos básicos das recomendações do Trusted Advisor](#)
- [Comece a usar a Trusted Advisor API](#)
- [Usando Trusted Advisor como um serviço da web](#)
- [Visão organizacional para AWS Trusted Advisor](#)
- [Exibir AWS Trusted Advisor cheques fornecidos por AWS Config](#)
- [Visualizando AWS Security Hub controles em AWS Trusted Advisor](#)

- [Opte por receber Trusted Advisor cheques AWS Compute Optimizer](#)
- [Comece com o AWS Trusted Advisor Priority](#)
- [Comece a usar o AWS Trusted Advisor Engage \(versão prévia\)](#)
- [AWS Trusted Advisor verifique a referência](#)
- [Registro de alterações para AWS Trusted Advisor](#)

Conceitos básicos das recomendações do Trusted Advisor

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

Você também pode usar a AWS Trusted Advisor API para realizar operações em suas Trusted Advisor verificações. Para obter mais informações, consulte a [Referência de APIs do AWS Trusted Advisor](#)

Tópicos

- [Faça login no Trusted Advisor console](#)
- [Visualizar categorias de verificação](#)
- [Visualizar verificações específicas](#)
- [Filtrar as verificações](#)
- [Atualizar resultados da verificação](#)
- [Baixar dos resultados](#)
- [Visualização organizacional](#)
- [Preferências](#)

Faça login no Trusted Advisor console

Você pode ver as verificações e o status de cada verificação no Trusted Advisor console.

 Note

Você deve ter permissões AWS Identity and Access Management (IAM) para acessar o Trusted Advisor console. Para obter mais informações, consulte [Gerencie o acesso ao AWS Trusted Advisor](#).

Para entrar no Trusted Advisor console

1. Faça login no Trusted Advisor console em <https://console.aws.amazon.com/trustedadvisor/casa>.
2. Na página Recomendações do Trusted Advisor , visualize o resumo de cada categoria de verificação:
 - Ação recomendada (vermelho) — 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 Advisor detecta 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, podem ser EC2 instâncias da Amazon que você não quer que o cheque 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 : Trusted Advisor Recomendações

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

Trusted Advisor > Recommendations

Trusted Advisor Recommendations

Use this page to get an overview of the check results in your AWS account. Choose a check name or category to view the recommended actions or potential issues that Trusted Advisor has identified. Each check provides more information about how to address any issues. You can also download a summary of all check results. [Learn more](#)

Checks summary

 42
Action recommended
[Info](#)

Security	30
Performance	1
Fault tolerance	9
Cost optimization	1
Service limits	1

 127
Investigation recommended
[Info](#)

Fault tolerance	29
Performance	9
Operational Excellence	12
Cost optimization	14
Security	63

 28
Checks with excluded items
[Info](#)

Security	11
Cost optimization	11
Service limits	1
Performance	2
Fault tolerance	3

Potential monthly savings

\$7,082.26

Trusted Advisor has identified 18 cost optimization checks that can save you money. For example, you might have unused resources in your AWS account that can be deleted. Choose a cost optimization check to view the recommendations.

[View all cost optimization checks](#)

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 sua AWS solução mais segura.
- Tolerância a falhas — recomendações que ajudam a aumentar a resiliência da sua AWS solução. 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 ajudá-lo a operar seu AWS ambiente de forma eficaz e em grande escala.

Para visualizar categorias de verificação

1. Faça login no Trusted Advisor console em <https://console.aws.amazon.com/trustedadvisor/casa>.
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) — Trusted Advisor recomenda uma ação para a verificação.
 - Investigação recomendada (amarelo): Trusted Advisor detecta um possível problema para a verificação.
 - Nenhum problema detectado (verde) — Trusted Advisor não detecta um problema na 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 10 cheques (verdes) que não apresentam problemas.

Cost optimization

 Refresh all checks  Download all checks

Choose a check name to see recommendations for ways to help save money for your AWS account. Trusted Advisor might recommend that you delete unused and idle resources, or use reserved capacity.

Overview

Potential monthly savings
\$7,082.26

 1
Action recommended
[Info](#)

 14
Investigation recommended
[Info](#)

 10
No problems detected
[Info](#)

 11
Checks with excluded items
[Info](#)

Cost optimization checks

Filter by tag key [Learn more about using tags](#)

Tag Key Tag Value

Reset Apply filter

Search by keyword [Info](#)

Filter checks

Source All sources

View All checks

 Amazon Comprehend Underutilized Endpoints

Checks the throughput configuration of your endpoints.

Last updated: 2 hours ago  

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 Trusted Advisor console em <https://console.aws.amazon.com/trustedadvisor/casa>.
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

A seguinte verificação de EC2 instâncias Amazon de baixa utilização lista as instâncias afetadas na conta. Essa verificação identifica 38 EC2 instâncias da Amazon que têm baixo uso e recomenda que você interrompa ou encerre os recursos.

▼

 Low Utilization Amazon EC2 Instances

Last updated: 14 hours ago  

Checks the Amazon Elastic Compute Cloud (Amazon EC2) instances that were running at any time during the last 14 days and alerts you if the daily CPU utilization was 10% or less and network I/O was 5 MB or less on 4 or more days. Running instances generate hourly usage charges. Although some scenarios can result in low utilization by design, you can often lower your costs by managing the number and size of your instances.

Estimated monthly savings are calculated by using the current usage rate for On-Demand Instances and the estimated number of days the instance might be underutilized. Actual savings will vary if you are using Reserved Instances or Spot Instances, or if the instance is not running for a full day. To get daily utilization data, download the report for this check.

Alert Criteria

Yellow: An instance had 10% or less daily average CPU utilization and 5 MB or less network I/O on at least 4 of the previous 14 days.

Recommended Action

Consider stopping or terminating instances that have low utilization, or scale the number of instances by using Auto Scaling. For more information, see [Stop and Start Your Instance](#), [Terminate Your Instance](#), and [What is Auto Scaling?](#)

Additional Resources

[Monitoring Amazon EC2](#)
[Instance Metadata and User Data](#)
[Amazon CloudWatch Developer Guide](#)
[Auto Scaling Developer Guide](#)

Low Utilization Amazon EC2 Instances (38)

Exclude & Refresh

Included items ▼

38 of 39 Amazon EC2 instances have low average daily utilization. Monthly savings of up to \$713.23 might be available by minimizing underutilized instances. 1 items have been excluded.

< 1 2 > 

Region/AZ ▼	Instance ID ▼	Instance Name ▼	Instance Type ▼	Estimated Monthly Savings ▼	CPU Utilization 14-Day Average ▼
ca-central-1b	i-0f818268643c7ae32		t2.micro	\$9.22	0.1%
ca-central-1a	i-06c233a11aa626588		t2.micro	\$9.22	0.1%

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 cheques que avaliam itens em sua conta, como AWS recursos, você pode usar filtros de tag para mostrar somente itens que tenham a tag especificada.

Para filtrar as verificações

1. Faça login no Trusted Advisor console em <https://console.aws.amazon.com/trustedadvisor/casa>.
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 seus AWS recursos, como EC2 instâncias ou AWS CloudTrail trilhas da Amazon, você pode filtrar seus resultados para que as verificações mostrem somente itens que tenham 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 Trusted Advisor, consulte os seguintes tópicos:

- [AWS Support habilita recursos de marcação para 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 você tiver um plano Developer ou Basic Support, poderá entrar no Trusted Advisor console para atualizar as verificações. Se você tiver um plano Business, Enterprise On-Ramp ou Enterprise Support, atualize Trusted Advisor automaticamente os cheques em sua conta semanalmente.

Para atualizar cheques Trusted Advisor

1. Navegue até o AWS Trusted Advisor console em <https://console.aws.amazon.com/trustedadvisor>.

2. Na página Trusted Advisor Recomendações ou em uma categoria de cheques, 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 operação de API [RefreshTrustedAdvisorCheck](#).

Observações

- Trusted Advisor atualiza automaticamente alguns cheques várias vezes ao dia, como o AWS Well-Architected problemas de alto risco para verificação de confiabilidade. 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 AWS Security Hub ativou sua conta, não poderá usar o Trusted Advisor console para atualizar os controles do Security Hub. Para obter mais informações, consulte [Atualizar os resultados do Security Hub](#).

Baixar dos resultados

Você pode baixar os resultados da verificação para ter uma visão geral Trusted Advisor da sua conta. É possível baixar os resultados de todas as verificações ou de uma verificação específica.

Para baixar, verifique os resultados em Trusted Advisor Recomendações

1. Navegue até o AWS Trusted Advisor console 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

Você pode configurar o recurso de visualização organizacional para criar um relatório para todas as contas dos membros em sua AWS organização. Para obter mais informações, consulte [Visão organizacional para AWS Trusted Advisor](#).

Preferências

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 AWS Organizations. Isso é necessário para o recurso [Visão organizacional para AWS Trusted Advisor](#), o [Trusted Advisor Priority](#) e o [Trusted Advisor Engage](#).

Configurar as preferências de notificação

Especifique quem pode receber as mensagens de Trusted Advisor e-mail semanais com os resultados da verificação e o idioma. Você recebe uma notificação por e-mail sobre o resumo da verificação de Trusted Advisor Recomendações uma vez por semana.

As notificações por e-mail para Trusted Advisor Recomendações não incluem resultados para Trusted Advisor Prioridade. Para obter mais informações, consulte [Gerenciar notificações Trusted Advisor prioritárias](#).

Para configurar preferências de notificação

1. Faça login no Trusted Advisor console em <https://console.aws.amazon.com/trustedadvisor/casa>.
2. No painel de navegação, em Preferences (Preferências), escolha Notifications (Notificações).

3. Em Recommendations (Recomendações), selecione a quem notificar os resultados da verificação. Você pode adicionar e remover contatos da página [Configurações da conta](#) no Gerenciamento de Faturamento e Custos da AWS console.
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 sua conta com AWS Organizations, poderá criar relatórios para todas as contas de membros em sua organização. Para obter mais informações, consulte [Visão organizacional para AWS Trusted Advisor](#).

Desativar Trusted Advisor

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

Para desativar Trusted Advisor

1. Faça login no Trusted Advisor console em <https://console.aws.amazon.com/trustedadvisor/casa>.
2. No painel de navegação, em Preferências, escolha Gerenciar o Trusted Advisor.
3. Em Trusted Advisor, desative Enabled (Habilitado). Essa ação desativa todos Trusted Advisor os cheques em sua conta.
4. Em seguida, você pode excluir manualmente a da sua conta. Para obter mais informações, consulte [Excluir um perfil vinculado ao serviço para o Trusted Advisor](#).

Informações relacionadas

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

- [Como faço para começar a usar Trusted Advisor?](#)
- [AWS Trusted Advisor verifique a referência](#)

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 [ListRecommendationResources](#) da API para ver recomendações e contas e recursos correspondentes.
- Use a operação da [UpdateRecommendationLifecycle](#) API para atualizar o ciclo de vida de uma recomendação gerenciada pela Trusted Advisor Priority.
- Use a operação [BatchUpdateRecommendationResourceExclusion](#) da API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.
- As chamadas [ListOrganizationRecommendationsGetOrganizationRecommendation](#), [ListOrganizationRecommendationResources](#), [ListOrganizationRecommendationAccounts](#), e de [UpdateOrganizationRecommendationLifecycle](#) API 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](#).

Usando Trusted Advisor como um serviço da web

O AWS Support serviço permite que você escreva aplicativos que interajam com [AWS Trusted Advisor](#). Este tópico mostra como obter uma lista de Trusted Advisor verificações, 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

- [Obtenha a lista de Trusted Advisor cheques disponíveis](#)
- [Atualize a lista de verificações disponíveis Trusted Advisor](#)
- [Trusted Advisor Faça uma pesquisa e verifique se há mudanças de status](#)
- [Solicitar um resultado de Trusted Advisor verificação](#)
- [Mostrar detalhes de um Trusted Advisor cheque](#)

Obtenha a lista de Trusted Advisor cheques disponíveis

O trecho de código Java a seguir cria uma instância de um Suporte cliente que você pode usar para chamar todas as operações de Trusted Advisor API. Em seguida, o código obtém a lista de Trusted Advisor verificações e seus CheckId valores correspondentes chamando a operação da [DescribeTrustedAdvisorChecks](#)API. 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());  
}  
}
```

Atualize a lista de verificações disponíveis Trusted Advisor

O trecho de código Java a seguir cria uma instância de um Suporte cliente que você pode usar para atualizar Trusted Advisor dados.

```
// 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());  
}
```

Trusted Advisor Faça uma pesquisa e verifique se há mudanças de status

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 Trusted Advisor serviço:

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 Trusted Advisor verificação

Depois de selecionar a verificação dos resultados detalhados que você deseja, você envia uma solicitação usando a operação da [DescribeTrustedAdvisorCheckResult](#) API.

Tip

Os nomes e descrições dos Trusted Advisor cheques 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 [DescribeTrustedAdvisorChecks](#) API 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 Trusted Advisor verificação não gera dados de resultados atualizados.

Mostrar detalhes de um Trusted Advisor cheque

O seguinte trecho de código Java itera sobre a `DescribeTrustedAdvisorCheckResultResult` instância retornada na seção anterior para obter uma lista dos recursos sinalizados pela verificação.

Trusted Advisor

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

Visão organizacional para AWS Trusted Advisor

A visualização organizacional permite que você visualize os Trusted Advisor cheques de todas as contas do seu [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, você pode usar os relatórios para identificar quais contas em sua organização estão usando AWS Identity and Access Management (IAM) com a verificação de uso do IAM ou se você recomendou ações 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](#)
- [Verificações de atualização 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](#)
- [Usando outros AWS serviços para visualizar Trusted Advisor relatórios](#)

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. Você pode encontrar seu plano de suporte no AWS Support Centro 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:

- 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 .
- O `AWSServiceRoleForTrustedAdvisorReporting` service-linked-role é criado para você na conta de gerenciamento da sua organização. Essa função inclui as permissões Trusted Advisor necessárias para ligar para 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](#).

Você ativa a visualização organizacional no Trusted Advisor console.

Para habilitar a visualização organizacional

1. Faça login como administrador na conta de gerenciamento da organização e abra o AWS Trusted Advisor console 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 AWS Organizations, ative Ativado.

 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 AWS Support plano determina quais Trusted Advisor cheques estão disponíveis para uma conta.

Verificações de atualização Trusted Advisor

Antes de criar um relatório para sua organização, recomendamos que você atualize os status dos seus Trusted Advisor cheques. 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 Business, Enterprise On-Ramp ou Enterprise Support, atualize Trusted Advisor automaticamente os cheques em sua conta semanalmente.

 Note

Se você tiver contas em sua organização que tenham um plano de suporte básico ou de desenvolvedor, um usuário dessas contas deverá entrar no Trusted Advisor console para atualizar as verificações. Não é possível atualizar verificações para todas as contas a partir da conta de gerenciamento da organização.

Para atualizar cheques Trusted Advisor

1. Navegue até o AWS Trusted Advisor console 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 AWS Trusted Advisor console em <https://console.aws.amazon.com/trustedadvisor>.
2. No painel de navegação, selecione Organizational View (Visualização organizacional).
3. Escolha Criar relatório.
4. Por padrão, o relatório inclui todas as AWS regiões, 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 Região, especifique as AWS Regiões ou escolha 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 Organização, selecione as unidades organizacionais (OUs) a serem incluídas em seu relatório. Para obter mais informações sobre OUs, consulte [Gerenciamento de unidades organizacionais](#) no Guia AWS Organizations do usuário.
6. Escolha Criar relatório.

Example : Criar opções de filtro de relatório

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

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

Report filters

Choose the filter options for your report.

Report name

Trusted-Advisor-report

The report name can be up to 100 characters and can't start with a hyphen. Valid characters: A-Z, a-z, 0-9, and - (hyphen)

Format

JSON

Region

Choose Region

us-east-1 ✕

us-east-2 ✕

us-west-1 ✕

Check category

Choose category

Security ✕

Performance ✕

Checks

Choose check names

Resource status

Choose status

All ✕

No exemplo a seguir, o relatório inclui a OU da equipe de suporte e uma AWS conta que fazem parte da organização.

AWS organization

You can select the organizational units (OUs) and individual AWS accounts to include in your report.

Organizational structure

▼   **Root**
r-xa9c

▶ ☐  **instance-management**
ou-xa9c-example1

▼ ☒  **support-team**
ou-xa9c-example2

☒  **Jane Doe**
111122223333 | janedoe@example.com

☒  **Mateo Jackson**
444455556666 | mateojackson@example.com

▶ ☐  **security-team**
ou-xa9c-example3

☒  **Ana Carolina Silva**
777788889999 | anacarolinasilva@example.com

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.

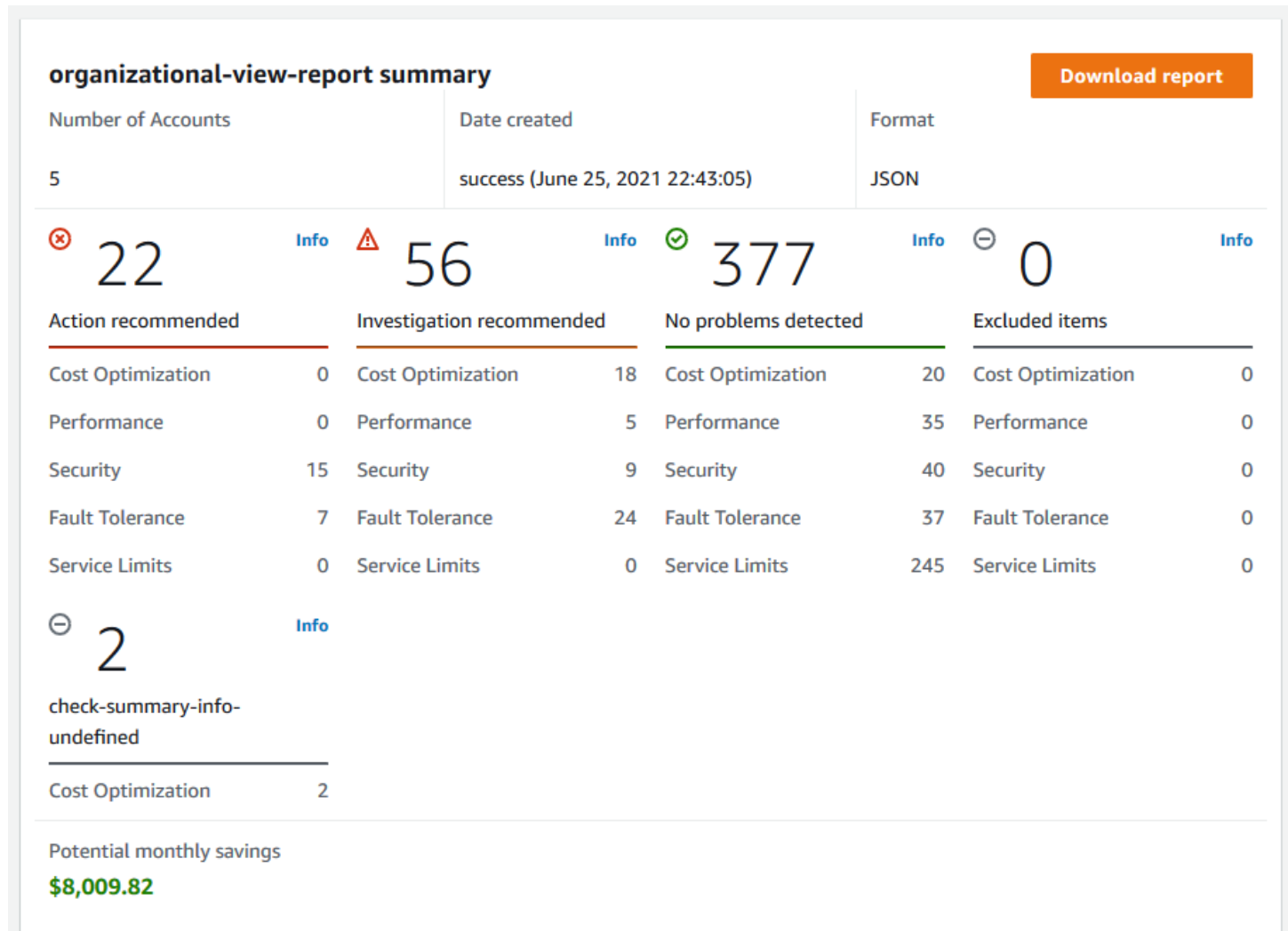
Visualize o resumo do relatório.

Depois que o relatório estiver pronto, você poderá ver o resumo do relatório no Trusted Advisor console. 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 AWS Trusted Advisor console 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 seu relatório estiver pronto, baixe-o do Trusted Advisor console. 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 AWS Trusted Advisor console 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.

Organizational View

With AWS organizations, you can create reports for check results across all AWS accounts within an organization. This provides you a centralized view for all AWS Trusted Advisor checks. You can also view and download reports on this page. Use this report to identify issues and take action for accounts in your organization. [Learn more](#).

Reports (50)

Create report

Download report

	Report name	Date generated	Status	Format
☐	all-regions-check-report	June 15, 2021 18:43:42	Success	JSON
☐	json-us-east-1-region-only	June 14, 2021 20:54:29	Success	JSON
☐	security-checks-only-all-accounts	June 10, 2021 03:33:59	Success	JSON

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.

Trusted Advisor usa o seguinte código de cores para os resultados da verificação:

- Green— Trusted Advisor não detecta um problema na verificação.
- Yellow— Trusted Advisor detecta um possível problema na verificação.
- Red— Trusted Advisor detecta um erro e recomenda uma ação para a verificação.
- Blue— não é Trusted Advisor possível determinar o status do cheque.

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 as propriedades IDs e da política de senha do IAM (Yw2K9puPzl) e rotação de chaves do IAM (DqdJqYeRm5) cheques.

```

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

AccountId	CheckId	ResourceId	TimeStamp	CheckName	Category
1.11122E+11	Qch7DwouX1	LnW14f1M40NMjmMLvY5v	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	vioZmlba45kf2JWle_W0j5	1.58983E+12	Amazon S3 Bucket Permissions	Security
4.44456E+11	Pfx0RwqBli	wAvASS3YOWy6WWxIBHf	1.58983E+12	Amazon S3 Bucket Permissions	Security
1.23457E+11	Pfx0RwqBli	Llc4zRaUSilGRSlmqMa5V	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-5JC	1.58983E+12	IAM Password Policy	Security
7.77789E+11	H7lgTzjTYb	1xHQ5ovV8bS0H1Z-t7Kbit	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 em sua organização, a verificação de expiração do lease de instância EC2 reservada da Amazon não aparecerá em seu relatório.
- A conta não atualizou os resultados da verificação. Isso pode acontecer quando usuários com um plano de suporte básico ou de desenvolvedor entram no Trusted Advisor console 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 [Verificações de atualização 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, você pode usar uma interface SQL com um AWS serviço como o Amazon Athena para executar consultas em seus relatórios. Você também pode usar QuickSight a Amazon para criar painéis e visualizar seus dados. Para obter mais informações, consulte [Usando outros AWS serviços para visualizar Trusted Advisor relatórios](#).

Desabilitar a visualização organizacional

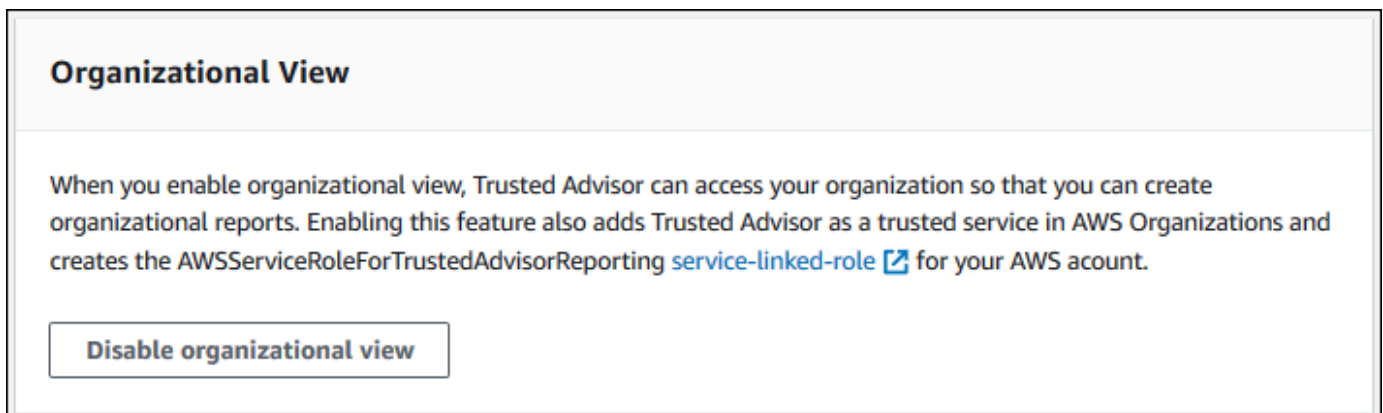
Siga este procedimento para desabilitar o modo de visualização organizacional. Você deve fazer login na conta de gerenciamento da organização ou assumir uma função com as permissões necessárias para desabilitar esse recurso. Não é possível desabilitar esse recurso usando outra conta da organização.

Depois que você desabilitar esse recurso, acontecerá o seguinte:

- Trusted Advisor é removido como um serviço confiável em 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 desativar a exibição organizacional para Trusted Advisor

1. Faça login na conta de gerenciamento da organização e abra o AWS Trusted Advisor console 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 desativar a visualização organizacional, Trusted Advisor não agrega mais cheques de outras AWS contas em sua organização. No entanto, a função `AWSServiceRoleForTrustedAdvisorReporting` vinculada ao serviço permanece na conta de gerenciamento da organização até que você a exclua por meio do console do IAM, da API do IAM ou AWS Command Line Interface (AWS CLI). Para obter mais informações, consulte [Excluir um perfil vinculado ao serviço](#) no Guia do usuário do IAM.

 Note

Você pode usar outros AWS serviços para consultar e visualizar seus dados para relatórios de visualização organizacional. Para obter mais informações, consulte os seguintes recursos:

- [Exibir recomendações do AWS Trusted Advisor em escala com AWS Organizations](#) no Blog de gerenciamento e governança da AWS
- [Usando outros AWS serviços para visualizar Trusted Advisor relatórios](#)

Utilização de políticas do IAM para permitir acesso à visualização organizacional

Você pode usar as seguintes políticas AWS Identity and Access Management (IAM) para permitir que usuários ou funções em sua conta tenham acesso à visualização organizacional em 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 para 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 ativou AWS CloudTrail em sua conta, as seguintes funções podem aparecer em suas entradas de registro:

- `AWSServiceRoleForTrustedAdvisorReporting`— A função vinculada ao serviço Trusted Advisor usada para acessar contas em sua organização.
- `AWSServiceRoleForTrustedAdvisor`— A função vinculada ao serviço Trusted Advisor usada para acessar serviços em sua organização.

Para obter mais informações sobre funções vinculadas ao serviço, consulte [Usar perfis vinculados ao serviço do Trusted Advisor](#).

Usando outros AWS serviços para visualizar Trusted Advisor relatórios

Siga este tutorial para carregar e visualizar seus dados usando outros AWS serviços. Neste tópico, você cria um bucket do Amazon Simple Storage Service (Amazon S3) para armazenar seu relatório e AWS CloudFormation um modelo para criar recursos em sua conta. Em seguida, você pode usar o Amazon Athena para analisar ou executar consultas para seu relatório ou 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 como usuário AWS Identity and Access Management (IAM) com permissões de administrador.
- Use a AWS região Leste dos EUA (Norte da Virgínia) para configurar rapidamente seus AWS serviços e recursos.
- Crie uma QuickSight conta. Para obter mais informações, consulte [Introdução à análise de dados QuickSight no](#) Guia do QuickSight usuário da Amazon.

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 *bucket-name* página, escolha Criar pasta, digite o nome **folder1** e escolha 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. Esse modelo informa 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 IAM AWS Lambda, AWS Glue e.

Para criar seus recursos com AWS CloudFormation

1. Baixe o [trusted-advisor-reports-templatearquivo.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 AWS CloudFormation console 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 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 Eu reconheço que isso 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.

Trusted-Advisor-reports				Delete	Update	Stack actions ▼
Stack info	Events	Resources	Outputs	Parameters	Template	Change sets
Resources (12)						
Search resources						
Logical ID ▲	Physical ID ▼	Type ▼	Status ▼			
AWSPutS3TANotification	2020/05/27/[\$LATEST]5bfd3cb8b29a4b85bc0f8d861EXAMPLE1	Custom::AWSPutS3TANotification	✔ CREATE_COMPLETE			
AWSS3TAEvtLambdaPermission	Trusted-Advisor-reports-AWSS3TAEvtLambdaPermission-10KT2EXAMPLE1	AWS::Lambda::Permission	✔ CREATE_COMPLETE			
AWSS3TALambdaExecutor	Trusted-Advisor-reports-AWSS3TALambdaExecutor-1BJCOEXAMPLE1 ↗	AWS::IAM::Role	✔ CREATE_COMPLETE			
AWSS3TANotification	Trusted-Advisor-reports-AWSS3TANotification-15J3KEXAMPLE1 ↗	AWS::Lambda::Function	✔ CREATE_COMPLETE			
AWStartTACrawler	2020/05/27/[\$LATEST]66726149d3d64a1f9242cdccEXAMPLE1	Custom::AWStartTACrawler	✔ CREATE_COMPLETE			
AWSTACrawler	AWSTACrawler	AWS::Glue::Crawler	✔ CREATE_COMPLETE			

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.

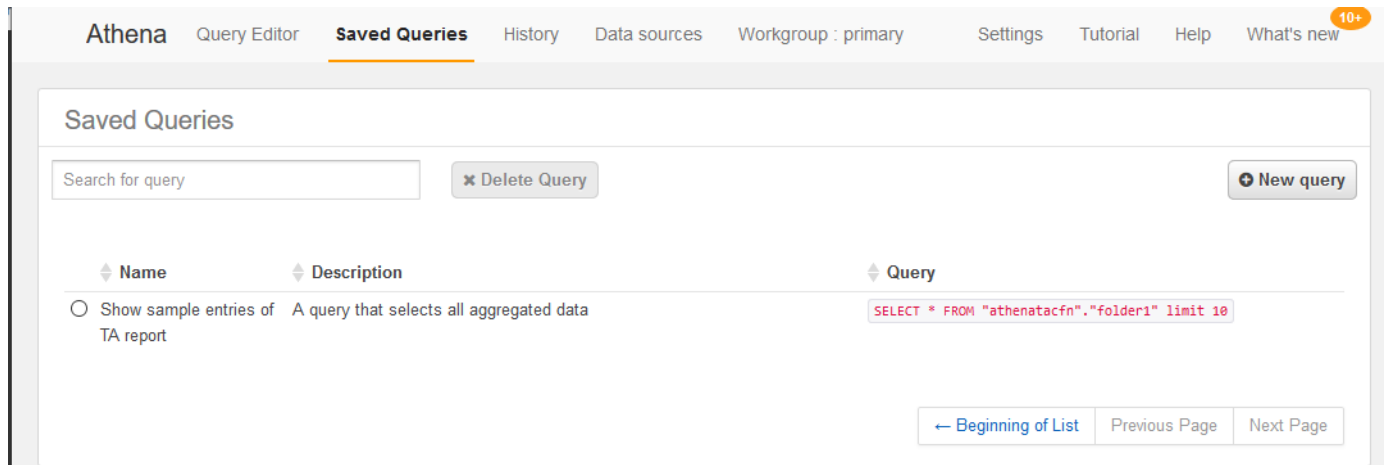
Observações

- 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**.

- 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
```

- Selecione Executar consulta. Os resultados da consulta são exibidos.

Example : Consulta do Athena

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

New query 1

✔ Show sample ent... ✕ +

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

2

Run query

Save as

Create ▾

(Run time: 0.83 seconds, Data scanned: 94.75 KB)

Format query

Clear

Use Ctrl + Enter to run query, Ctrl + Space to autocomplete

Results

	volume type ▾	checkname ▾	accountid ▾	category ▾	issuppressed ▾	snapshot
1	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	snap-0d4
2	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	snap-06b
3	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	
4	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	
5	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	snap-0ef4
6	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	snap-0a5
7	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	snap-078
8	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	
9	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	snap-0ff6!
10	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	

Para obter mais informações, consulte [Executar consultas SQL usando o Amazon Athena](#) no Manual do usuário do Amazon Athena.

Crie um painel em QuickSight

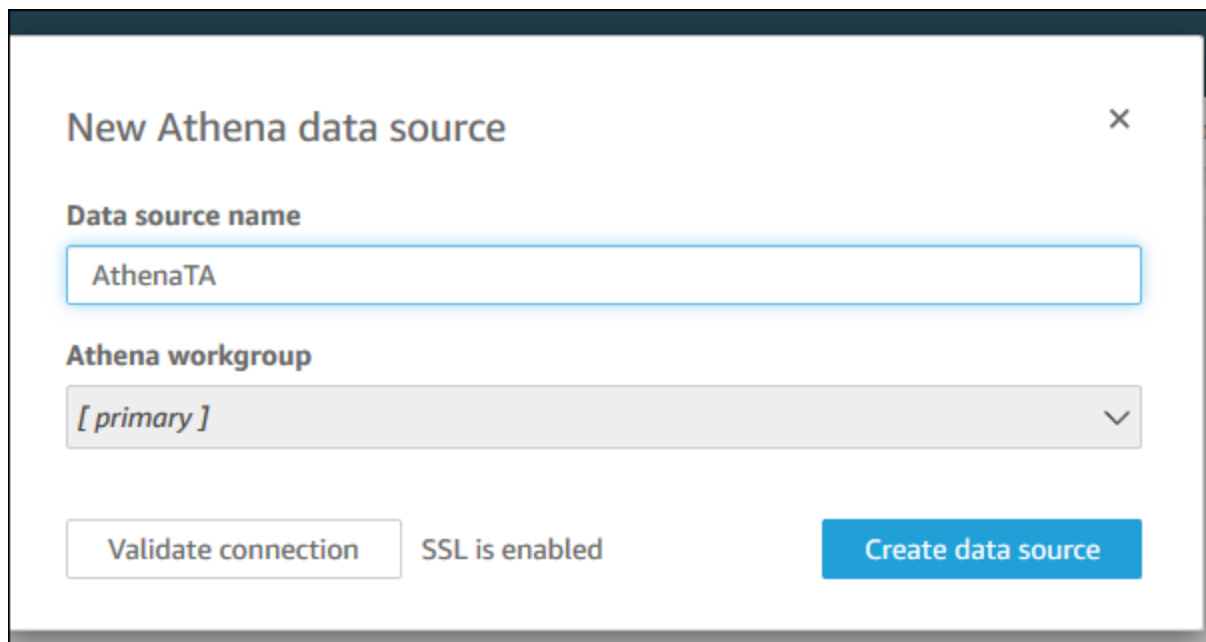
Você também pode configurar QuickSight para poder visualizar seus dados em um painel e visualizar as informações do relatório.

Note

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

Para criar um painel no QuickSight

1. Navegue até o QuickSight console 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).



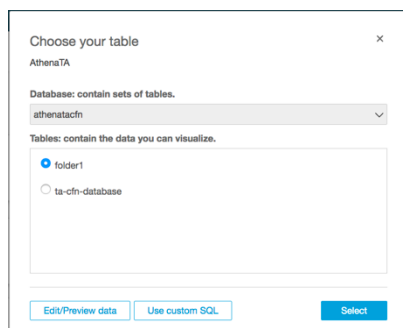
New Athena data source [X]

Data source name
AthenaTA

Athena workgroup
[primary]

Validate connection SSL is enabled Create data source

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



Choose your table [X]

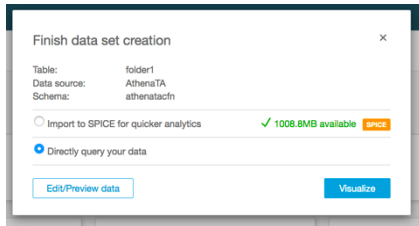
AthenaTA

Database: contain sets of tables.
athenatacfn

Tables: contain the data you can visualize.
☒ folder1
☐ ta-cfn-database

Edit/Preview data Use custom SQL Select

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 QuickSight. Para obter mais informações, consulte [Como trabalhar com painéis](#) no Guia do QuickSight usuário da Amazon.

Example : QuickSight painel

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

- Conta afetada IDs
- Resumo por AWS regiões
- 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 ele QuickSight possa usar o Athena. Para obter mais informações, consulte [Não consigo me conectar ao Amazon Athena no Guia QuickSight](#) do usuário da Amazon.

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 as Trusted Advisor verificações em sua 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 [Verificações de atualização 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

Você pode usar o AWS Glue console para visualizar o esquema e identificar rapidamente se há colunas duplicadas em seu relatório.

Para localizar colunas duplicadas

1. Abra o AWS Glue console 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 Tabelas.
4. Escolha o nome da pasta, como *folder1*, e em Esquema, visualize os valores para 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 o fez, atualize seus Trusted Advisor cheques para as contas em sua organização. Consulte [Verificações de atualização Trusted Advisor](#).
2. Crie e baixe outro relatório JSON no Trusted Advisor console. 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 AWS Trusted Advisor cheques fornecidos por AWS Config

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

O AWS Config console orienta você na configuração e ativação das regras gerenciadas. Você também pode usar a AWS Command Line Interface (AWS CLI) ou a AWS Config API para transmitir o código JSON que define sua 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 AWS Config, consulte o [Guia do AWS Config desenvolvedor](#).

AWS Config as regras gerenciadas possibilitam um conjunto de Trusted Advisor verificações em todas as categorias. Quando você ativa determinadas regras gerenciadas, as Trusted Advisor

verificações correspondentes são ativadas automaticamente. Para ver quais Trusted Advisor verificações são baseadas em regras AWS Config gerenciadas específicas, consulte [AWS Trusted Advisor verifique a referência](#).

Os AWS Config cheques avançados estão disponíveis para clientes com os planos [AWS Business Support](#), [AWS Enterprise On-Ramp](#) e Enterprise [AWS Support](#). Se você ativar AWS Config e tiver um desses planos do AWS Support, verá automaticamente as recomendações baseadas nas regras AWS Config gerenciadas implantadas correspondentes.

Note

Os resultados dessas verificações são atualizados automaticamente com base nas atualizações acionadas por alterações nas regras gerenciadas. 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 ativar a gravação e gerenciar as regras para AWS Config, mas não vejo as Trusted Advisor verificações correspondentes.](#)
- [Eu implantei a mesma regra AWS Config gerenciada duas vezes, o que vou ver? Trusted Advisor](#)
- [Desativei a gravação AWS Config em uma AWS região. O que eu vou ver em Trusted Advisor?](#)

Acabei de ativar a gravação e gerenciar as regras para AWS Config, mas não vejo as Trusted Advisor verificações correspondentes.

Depois que a AWS Config regra gera os resultados da avaliação, você vê os resultados quase Trusted Advisor 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 AWS Config gerenciada duas vezes, o que vou ver? Trusted Advisor

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

Desativei a gravação AWS Config em uma AWS região. O que eu vou ver em Trusted Advisor?

Se você desativou o registro de recursos AWS Config em uma AWS região, Trusted Advisor não receberá mais dados das regras e verificações gerenciadas correspondentes nessa região. Os resultados das regras gerenciadas existentes permanecem AWS Config ininterruptos Trusted Advisor até AWS Config expirarem, com base na política de retenção de gravadores. Se você excluir uma regra gerenciada, os dados de Trusted Advisor verificação geralmente serão excluídos quase em tempo real.

Visualizando AWS Security Hub controles em AWS Trusted Advisor

Depois de habilitar AWS Security Hub para o seu Conta da AWS, você pode ver seus controles de segurança e suas descobertas no Trusted Advisor console. Você pode usar os controles do Security Hub para identificar vulnerabilidades de segurança em sua conta da mesma forma que você pode usar Trusted Advisor cheques. 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 recomendações de segurança no Security Hub Trusted Advisor e no Security Hub em um local conveniente.

Observações

- Em Trusted Advisor, você pode visualizar 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 .

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

- Trusted Advisor controles integrados do Security Hub até 26 de setembro de 2024. Os controles lançados após 26 de setembro de 2024 ainda não estão integrados ao Trusted Advisor. Você pode encontrar controles lançados após essa data no [log do Security Hub](#).

Tópicos

- [Pré-requisitos](#)
- [Para visualizar os resultados do Security Hub](#)
- [Atualizar os resultados do Security Hub](#)
- [Desativar o Security Hub de 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 AWS Support planos](#).
- Você deve habilitar a gravação de recursos AWS Config para as Regiões da AWS que você deseja para seus 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. Não é necessário entrar em contato com contas de membros individuais Suporte para ativar 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 ver suas descobertas do Security Hub em 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. Atualmente, você não pode usar o Trusted Advisor console 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 [Visão 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 .

▼

⊗

IAM root user access key should not exist

Last updated: an hour ago

↺

↻

Checks if the root user access key is available.

Source

[AWS Security Hub](#)
 Security Hub control ID: IAM.4

Alert Criteria

Red: Critical or High. Security Hub control failed.

Recommended Action

Follow the [Security Hub documentation](#) to fix the issue.

IAM root user access key should not exist (1)

Exclude & Refresh

Included items ▼

1 of 1 resources failed this Security Hub control.

<

1

>

⚙️

☐	Status ▼	Region ▼	Resource ▼	Last Updated Time ▼
☐	⊗	us-east-1	AWS:::Account:123456789012	2021-12-12T19:56:26.305Z

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. Em seguida, pode levar até 24 horas para que esses dados apareçam no Trusted Advisor console. Se você habilitou recentemente o padrão de segurança AWS Foundational Security Best Practices v1.0.0, verifique o Trusted Advisor console novamente mais tarde.

Note

- A programação de atualização para cada controle do Security Hub é periódica ou é acionada por alteração. Atualmente, você não pode usar o Trusted Advisor console ou a AWS Support API para atualizar seus 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. Atualmente, você não pode usar o Trusted Advisor console 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).

Desativar o Security Hub de Trusted Advisor

Siga este procedimento se não quiser que as informações do Security Hub apareçam no console do Trusted Advisor. Esse procedimento só desativa 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 [AWS Support](#) solicite a desativação da integração do Security Hub com Trusted Advisor o.

Depois de AWS Support desativar esse recurso, o Security Hub não envia mais dados para o Trusted Advisor. Seus 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 membro de uma organização, entre em contato Suporte 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 as descobertas do Security Hub no Trusted Advisor console](#)

- [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 ativar ou desativar esse recurso para uma conta de membro que pertence a uma AWS organização](#)
- [Vejo várias Regiões da AWS para o mesmo recurso afetado em uma verificação do Security Hub](#)
- [Desativei o Security Hub ou AWS Config em uma região](#)
- [Meu controle está arquivado no Security Hub, mas ainda vejo as descobertas em Trusted Advisor](#)
- [Continuo não conseguindo visualizar os resultados do Security Hub](#)

Não vejo as descobertas do Security Hub no Trusted Advisor console

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 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 Trusted Advisor dentro de 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. Em seguida, pode levar até 24 horas para que esses dados apareçam no Trusted Advisor console. Confira o console do Trusted Advisor novamente mais tarde.

Observações

- Somente suas descobertas sobre controles no padrão de segurança AWS Foundational Security Best Practices aparecerão em, Trusted Advisor exceto os controles que têm a categoria: Recuperação > 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 seus dados Trusted Advisor automaticamente para. 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 desativar todos os controles do padrão de segurança AWS Foundational Security Best Practices, suas descobertas serão arquivadas nos próximos cinco dias. Esse período de cinco dias para arquivamento é aproximado e é apenas um melhor esforço, não sendo garantido. Quando suas descobertas são arquivadas, elas são removidas de 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 Trusted Advisor console, você pode escolher o nome do controle do Security Hub e, em seguida, escolher a opção 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. Você não pode suprimir os recursos do Security Hub

do Trusted Advisor console. 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 ativar ou desativar esse recurso para uma conta de membro que pertence a uma AWS organização

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](#).

Vejo várias Regiões da AWS para o mesmo recurso afetado em 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 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 AWS Config em uma região

Se você interromper a gravação de recursos com AWS Config ou desativar o Security Hub em um Região da AWS, Trusted Advisor não receberá mais dados de nenhum controle nessa região. Trusted Advisor remove suas descobertas do Security Hub em 7 a 9 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 [Desativar o Security Hub de Trusted Advisor](#).

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

Quando o RecordState status muda ARCHIVED para uma descoberta, Trusted Advisor exclui a descoberta desse controle do Security Hub da sua conta. Talvez você ainda veja a descoberta Trusted Advisor por até 7 a 9 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](#).

Opte por receber Trusted Advisor cheques 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 vê as mesmas recomendações em suas verificações. Trusted Advisor

Você pode ativar sua Conta da AWS única conta ou todas as contas de membros que fazem parte de uma organização em 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. Em seguida, pode levar até 48 horas para visualizar seus resultados nas Trusted Advisor seguintes verificações:

[Otimização de custo](#)

- Volumes superprovisionados do Amazon EBS
- AWS Lambda funções superprovisionadas para o tamanho da memória

[Desempenho](#)

- Volumes subprovisionados do Amazon EBS

- AWS Lambda funções subprovisionadas para o tamanho da 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.
- Trusted Advisor já tem as verificações de volumes subutilizados do Amazon EBS e volumes magnéticos do Amazon EBS sobreutilizados.

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
- [Solicite modificações em seus volumes do Amazon EBS](#) no Guia do EC2 usuário da Amazon

Comece com o AWS Trusted Advisor Priority

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

Por exemplo, sua equipe de conta pode identificar se o usuário raiz AWS da sua conta não tem autenticação multifatorial (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 Trusted Advisor

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

Trusted Advisor As recomendações prioritárias vêm dessas duas fontes:

- Serviços da AWS — Serviços como Trusted Advisor, AWS Security Hub, e AWS Well-Architected criam recomendações automaticamente. A equipe da sua conta compartilha essas recomendações com você para que elas apareçam em Trusted Advisor Prioridade.
- Sua equipe de contas: a sua equipe de contas pode criar recomendações manuais.

Trusted Advisor A prioridade 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. Você pode usar o Trusted Advisor Priority para encontrar recomendações para todas as contas dos membros em sua organização.

Tópicos

- [Pré-requisitos](#)
- [Ativar Trusted Advisor prioridade](#)
- [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 notificações Trusted Advisor prioritárias](#)
- [Desativar Trusted Advisor prioridade](#)

Pré-requisitos

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

- Você deve ter um plano de suporte Enterprise da .

- 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 recursos em sua organização](#) no Manual do usuário do AWS Organizations .
- Sua organização deve ter habilitado o acesso confiável Trusted Advisor a. Para habilitar o acesso confiável, faça login como conta de gerenciamento. Abra a página [Sua organização](#) no Trusted Advisor console.
- Você deve estar conectado à sua AWS conta para ver as recomendações Trusted Advisor prioritárias 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](#).
- Você deve ter permissões 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](#) [AWS políticas gerenciadas para AWS Trusted Advisor](#) e.

Ativar Trusted Advisor prioridade

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 Trusted Advisor Prioridade no console indicar que você precisa de acesso confiável com AWS Organizations, escolha Habilitar acesso confiável com AWS Organizations. Para obter mais informações, consulte a seção [Pré-requisitos](#).

Visualizar recomendações priorizadas

Depois que sua equipe de contas ativar a Trusted Advisor Prioridade para você, você poderá ver as recomendações mais recentes para sua AWS conta.

Para visualizar recomendações priorizadas

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

Se você estiver usando uma conta AWS Organizations de gerenciamento ou de administrador delegado, vá 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 de Serviços da AWS sua Conta da AWS equipe 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 recomendações priorizadas em todas as contas da sua organização AWS

Tanto a conta de gerenciamento quanto os administradores delegados Trusted Advisor prioritários 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 Trusted Advisor console em <https://console.aws.amazon.com/trustedadvisor/casa>.
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 de Serviços da AWS sua Conta da AWS equipe 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 Trusted Advisor prioritárias

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.

The screenshot displays the 'Trusted Advisor Priority' page. At the top, there's a navigation bar with 'Trusted Advisor' and 'Priority'. Below it, the title 'Trusted Advisor Priority' is followed by an 'Info' icon. A subtitle states: 'You can use this page to find critical recommendations, trends, and activities for your organization.' There are two tabs: 'My organization' (selected) and 'My account'. A dropdown menu 'Select an account from your organization' shows 'All accounts'. The main content area is divided into two sections: 'Action needed' and 'Overview'. The 'Action needed' section shows 'Pending response' with a count of 15 and 'In progress' with a count of 27. The 'Overview' section shows 'Dismissed in the last 90 days' (5), 'Resolved in the last 90 days' (22), 'No update in 30+ days' (10), and 'Average time to resolve' (46 days). Below this, there's a section for 'Active prioritized recommendations (42)' with a search bar and a table of recommendations. The table has columns: Recommendations, Status, Source, Category, and Age (days). Two recommendations are listed: 'Low Utilization Amazon EC2 Instances test test' (Status: Pending response, Source: AWS Trusted Advisor, Category: Cost optimization, Age: 33 day(s)) and 'RDS DB instances should have deletion protection enabled' (Status: Pending response, Source: AWS Security Hub, Category: Security, Age: 20 day(s)).

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 Trusted Advisor console em <https://console.aws.amazon.com/trustedadvisor/casa>.
2. Se você estiver usando uma conta AWS Organizations de gerenciamento ou de administrador delegado, vá 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 com uma resposta pendente aparecem na guia Ativo na página Trusted Advisor Prioridade.

8. Siga as ações recomendadas para resolver a recomendação. Para obter mais informações, consulte [Resolver uma recomendação](#).

Example : Recomendação manual da Trusted Advisor Priority

A imagem a seguir mostra a recomendação de EC2 instâncias de baixa utilização que está pendente de resposta.

The screenshot displays the AWS Trusted Advisor console interface. At the top, there's a navigation bar with 'Trusted Advisor > Priority > Low Utilization Amazon EC2 Instances - Production accounts'. Below this, there are tabs for 'My organization' and 'My account', with 'My account' selected. The main heading is 'Low Utilization Amazon EC2 Instances - Production accounts'. To the right of this heading are three buttons: 'Copy recommendation link', 'Download', and 'Acknowledge' (highlighted in orange), followed by a 'Dismiss' button. Below the heading, there are two tabs: 'Details' and 'Affected resources', with 'Details' selected. The 'Overview' section shows a table with the following data:

Source	Category	Age	Status
AWS Trusted Advisor	Cost optimization	33 days(s) Shared on: Jun 20, 2023	Pending response

The 'Shared by' field shows 'person@amazon.com'. The 'Details' section contains a 'Description' of the recommendation, an 'Estimated monthly savings' calculation, 'Alert Criteria' (Yellow: An instance had 10% or less daily average CPU utilization and 5 MB or less network I/O on at least 4 of the previous 14 days), and a 'Recommended Action' to consider stopping or terminating instances. At the bottom, there are 'Additional Resources' links: 'Monitoring Amazon EC2', 'Instance Metadata and User Data', 'Amazon CloudWatch Developer Guide', and 'Auto Scaling Developer Guide'.

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

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 Trusted Advisor console em <https://console.aws.amazon.com/trustedadvisor/casa>.
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 da Trusted Advisor Priority

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

Trusted Advisor > Priority > Low Utilization Amazon EC2 Instances - Production accounts

My organization My account

Low Utilization Amazon EC2 Instances - Production accounts

Copy recommendation link Download Acknowledge Dismiss

Details Affected accounts Affected resources

Overview

Source AWS Trusted Advisor	Category Cost optimization	Age 0 day(s) Shared on: Jul 10, 2023	Status ⚠ Pending response
Shared by person@amazon.com			

Status Summary

This is a summary of the status of this recommendation across all your accounts

- 1 account Pending response
- 1 account In progress

Details

Description
Checks the Amazon Elastic Compute Cloud (Amazon EC2) instances that were running at any time during the last 14 days and alerts you if the daily CPU utilization was 10% or less and network I/O was 5 MB or less on 4 or more days. Running instances generate hourly usage charges. Although some scenarios can result in low utilization by design, you can often lower your costs by managing the number and size of your instances.

Estimated monthly savings are calculated by using the current usage rate for On-Demand Instances and the estimated number of days the instance might be underutilized. Actual savings will vary if you are using Reserved Instances or Spot Instances, or if the instance is not running for a full day. To get daily utilization data, download the report for this check.

Alert Criteria
Yellow: An instance had 10% or less daily average CPU utilization and 5 MB or less network I/O on at least 4 of the previous 14 days.

Recommended Action
Consider stopping or terminating instances that have low utilization, or scale the number of instances by using Auto Scaling. For more information, see [Stop and Start Your Instance](#), [Terminate Your Instance](#), and [What is Auto Scaling?](#)

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 um teste Conta da AWS que planeja excluir, não precisa seguir as ações recomendadas.

Ignorar uma recomendação

1. Faça login no Trusted Advisor console em <https://console.aws.amazon.com/trustedadvisor/casa>.
2. Se você estiver usando uma conta AWS Organizations de gerenciamento ou de administrador delegado, vá 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 Descartado e aparece na guia Fechado na página Trusted Advisor Prioridade.

Para descartar uma recomendação para todas as contas da sua organização AWS

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

1. Faça login no Trusted Advisor console em <https://console.aws.amazon.com/trustedadvisor/casa>.
2. Na página Trusted Advisor Prioridade, 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 Trusted Advisor Prioridade.

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.

Trusted Advisor A Priority também notifica sua equipe de conta de que você rejeitou a recomendação.

Example : Ignorar uma recomendação da Priority Trusted Advisor

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

Dismiss recommendation ✕

 Please note: This action will apply to all accounts affected by this recommendation

Choose a reason for why you're dismissing this recommendation

The affected AWS account was temporarily created for an event ▼

Note - *optional*

These are test accounts that we will delete soon

Cancel Dismiss

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 Trusted Advisor console em <https://console.aws.amazon.com/trustedadvisor/casa>.
2. Na página Trusted Advisor Prioridade, verifique se você está na guia Minha organização.
3. No Trusted Advisor Priority, selecione a recomendação e escolha Resolve (Resolver).

- Na caixa de diálogo Resolver recomendação, escolha Resolver. As recomendações resolvidas aparecem na guia Fechado na página Trusted Advisor Prioridade. Trusted Advisor O Priority notifica sua equipe de conta de que você resolveu a recomendação.

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

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

Note

As contas de membros não têm acesso às recomendações agregadas.

- Faça login no Trusted Advisor console em <https://console.aws.amazon.com/trustedadvisor/casa>.
- Se você estiver usando uma conta AWS Organizations de gerenciamento ou de administrador delegado, vá para a guia Minha conta.
- Na guia Ativo, selecione o nome da recomendação.
- Se a recomendação não se aplica à sua conta, escolha Resolver.
- Na caixa de diálogo Resolver recomendação, escolha Resolver. As recomendações resolvidas aparecem na guia Fechado na página Trusted Advisor Prioridade. Trusted Advisor O Priority notifica sua equipe de conta de que você resolveu a recomendação.

Example : Recomendação manual da Trusted Advisor Priority

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

The screenshot displays the AWS Trusted Advisor console interface. At the top, the breadcrumb navigation shows 'Trusted Advisor > Priority > Low Utilization Amazon EC2 Instances - Production accounts'. Below this, there are tabs for 'My organization' (selected) and 'My account'. The main heading is 'Low Utilization Amazon EC2 Instances - Production accounts', with buttons for 'Copy recommendation link' and 'Download'. Below the heading are three tabs: 'Details' (selected), 'Affected accounts', and 'Affected resources'. The 'Details' tab contains an 'Overview' section with a table and a 'Status Summary' section.

Source	Category	Age	Status
AWS Trusted Advisor	Cost optimization	0 day(s) Shared on: Jul 10, 2023	Resolved

Shared by: person@amazon.com
Resolved on: Jul 10, 2023

Status Summary
This is a summary of the status of this recommendation across all your accounts
2 accounts Resolved

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 Trusted Advisor console em <https://console.aws.amazon.com/trustedadvisor/casa>.
2. Se você estiver usando uma conta AWS Organizations de gerenciamento ou de administrador delegado, vá para a guia Minha conta.
3. Na página Trusted Advisor Priority, 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 AWS

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

Note

As contas de membros não têm acesso às recomendações agregadas.

1. Faça login no Trusted Advisor console em <https://console.aws.amazon.com/trustedadvisor/casa>.
2. Na página Trusted Advisor Prioridade, 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).

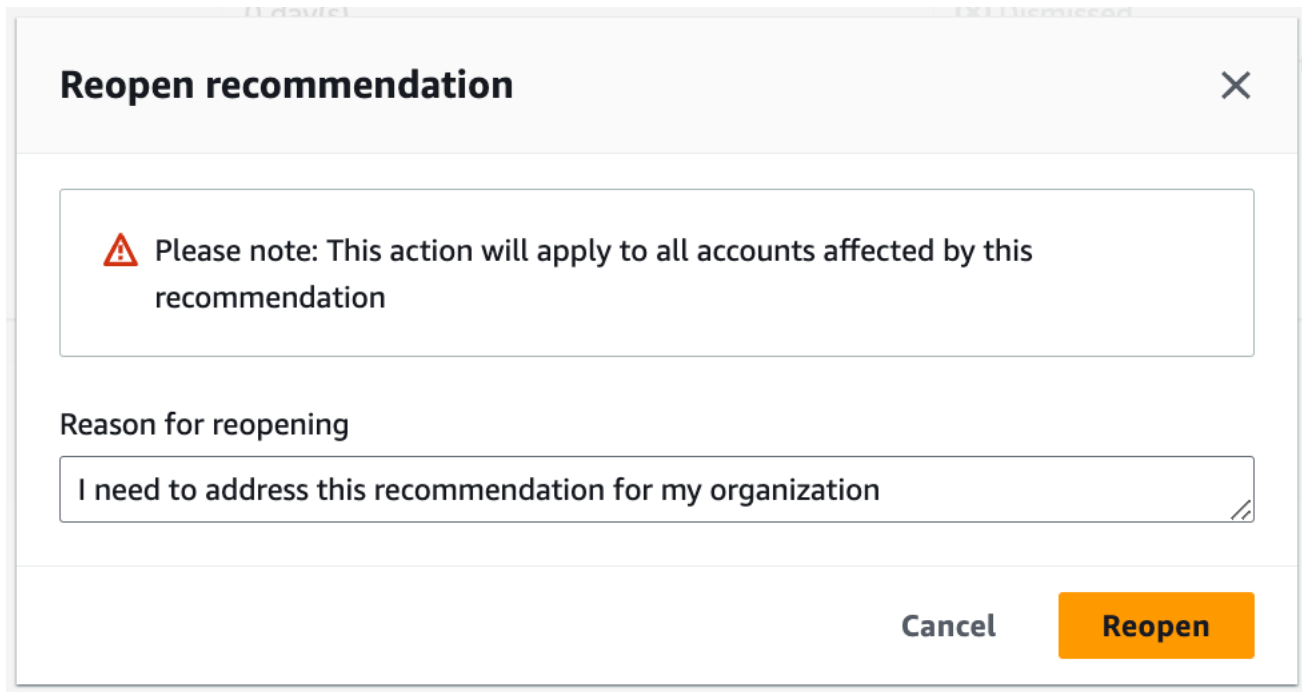
 Tip

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 : reabra uma recomendação do Priority Trusted Advisor

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



Reopen recommendation ✕

 Please note: This action will apply to all accounts affected by this recommendation

Reason for reopening

I need to address this recommendation for my organization

Cancel Reopen

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 Trusted Advisor console em <https://console.aws.amazon.com/trustedadvisor/casa>.
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 delegado podem revisar, reconhecer, resolver, ignorar e reabrir recomendações em Prioridade. Trusted Advisor

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

1. Faça login no Trusted Advisor console em <https://console.aws.amazon.com/trustedadvisor/casa> como 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. As contas que não são mais administradores delegados não receberão notificações por e-mail da Trusted Advisor Priority.

Para cancelar o registro de um administrador delegado da

1. Faça login no Trusted Advisor console em <https://console.aws.amazon.com/trustedadvisor/casa> como 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 notificações Trusted Advisor prioritárias

Trusted Advisor O Priority entrega 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 que você recebe atualizações do Trusted Advisor Priority.

Se você registrou contas de membros como administradores delegados, eles também podem configurar suas contas para receber notificações Trusted Advisor prioritárias por e-mail.

Trusted Advisor As notificações prioritárias por e-mail não incluem resultados de cheques para contas individuais e são separadas da notificação semanal para Trusted Advisor Recomendações. Para obter mais informações, consulte [Configurar as preferências de notificação](#).

Note

Somente a conta de gerenciamento ou o administrador delegado podem configurar notificações Trusted Advisor prioritárias por e-mail.

Para gerenciar suas notificações Trusted Advisor prioritárias

1. Entre no Trusted Advisor console em <https://console.aws.amazon.com/trustedadvisor/casa> como uma conta gerencial 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. Você pode adicionar e remover contatos da página [Configurações da conta](#) no Gerenciamento de Faturamento e Custos da AWS console.
5. Em Language (Idioma), escolha o idioma da notificação por e-mail.
6. Escolha Save your preferences (Salvar suas preferências).

Note

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

Desativar Trusted Advisor prioridade

Entre em contato com sua equipe de contas e peça que esse recurso seja desabilitado. Depois que esse recurso for desativado, as recomendações priorizadas não aparecerão mais no Trusted Advisor console.

Se você desativar a Trusted Advisor Prioridade e ativá-la novamente mais tarde, ainda poderá ver as recomendações que sua equipe de conta enviou antes de você desativar a Trusted Advisor Prioridade.

Comece a usar o AWS Trusted Advisor Engage (versão prévia)

Note

AWS Trusted Advisor O Engage está em versão prévia e está sujeito a alterações. Você pode ver a versão prévia dos termos de serviço aqui <https://aws.amazon.com/service-terms/>.

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.

Por exemplo, você pode solicitar uma “Análise de negócios gerenciais” para sua Conta da AWS equipe acessando a página Engage no AWS Trusted Advisor console. 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 recursos em sua organização](#) no Manual do usuário do AWS Organizations .

- Sua organização deve ter habilitado o acesso confiável Trusted Advisor a. Você pode ativar o acesso confiável fazendo login como conta de gerenciamento e acessando a página [Sua organização](#) no Trusted Advisor console.
- Você deve ter permissões 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 dentro de uma AWS organização pode criar uma solicitação de engajamento. Se uma conta proprietária do Engajamento for transferida para uma AWS organização diferente, o Engajamento só poderá ser acessado pela 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 Trusted Advisor console para ver um painel onde você pode gerenciar os engajamentos com sua Conta da AWS equipe.

Para gerenciar suas interações:

1. Faça login no Trusted Advisor console em <https://console.aws.amazon.com/trustedadvisor/casa>.
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

Trusted Advisor

Pursuit

Priority

Recommendations

Cost optimization

Performance

Security

Fault tolerance

Service limits

Operational excellence

Engage

Data trends

Organizational view

▼ Preferences

Manage Trusted Advisor

Notifications

Your organization

Integrations

Trusted Advisor > Engage

Trusted Advisor Engage (Preview)

You can use this page to view, request, manage, and track engagements.

Active Closed

Active Engagements (2)

The following are all your requested and recommended Engagements.

Search

2 matches

Desired Completion Date > 2024-12-08

Clear filters

Request ID	Request title	Engagement Type	Account ID	Status	Effective Date	Desired Completion Date	Age (days)	Outcome labels
172609090906772	Cost Opt	Cost Optimization	303615524644	In Progress	Sep 11, 2024 Recommended	Dec 16, 2024	0	
172609066800544	Countdown for Product Launch XYZ	Countdown	303615524644	Pending Response	Sep 11, 2024 Requested	Jan 20, 2025	0	

All available Engagements (16)

Find initiative

AWS Executive Engagement

AWS Executive Engagement is a personalized engagement for customers to meet with AWS executives and discuss their business needs and objectives. Customers can share feedback, ask questions, and receive insights on industry trends and best practices to support their business growth and innovation initiatives.

AWS GameDays

AWS GameDays are interactive team-based learning exercises designed to give players a chance to test AWS skills in a real-world, gamified and risk-free environment. It's a Simulation of live application hosted on AWS to test skills by maintaining and fixing a production state. It provides complete hands-on opportunity to learn about AWS best practices, services, and architectural patterns. During an event, players are given a starting architecture that they evolve in response to internal & external events on pre-packaged AWS accounts. There are multiple portfolios of GameDays to select from, which specializes on different AWS domains & services.

Architecture Reviews

Evaluation of architecture and designs that can scale over time leveraging the AWS Well-Architected framework.

Cost Optimization

Cost Optimization engagements ensure the effective utilization of AWS resources, with actionable recommendations to realize immediate savings and achieve ongoing cost efficiency based on customer priorities.

Cost Optimization Workshop

The Cost Optimization Workshop is an engagement which improves cost effective utilization of AWS resources. Customers are provided actionable recommendations to realize immediate savings and achieve ongoing cost efficiency. Workshop activities enable the customer to achieve rapid results based on their cost optimization priorities.

Countdown

Architecture and scaling guidance and operational support during the preparation and execution of planned events such as shopping holidays, product launches, or migrations.

Visualize o catálogo de tipos de interação

Você pode ver o catálogo de tipos de engajamento para encontrar os tipos mais recentes de engajamento que você pode solicitar para sua Conta da AWS equipe.

Visualizar o catálogo de tipos de interação:

1.

Faça login no Trusted Advisor console em <https://console.aws.amazon.com/trustedadvisor/casa>.
2.

Na página Trusted Advisor Engage, você pode encontrar o catálogo de tipos de interação.

Example : catálogo de tipos de interação

All available Engagements (16)

[AWS Executive Engagement](#)
AWS Executive Engagement is a personalized engagement for customers to meet with AWS executives and discuss their business needs and objectives. Customers can share feedback, ask questions, and receive insights on industry trends and best practices to support their business growth and innovation initiatives.

[AWS GameDays](#)
AWS GameDays are interactive team-based learning exercises designed to give players a chance to test AWS skills in a real-world, gamified and risk-free environment. It's a Simulation of live application hosted on AWS to test skills by maintaining and fixing a production state. It provides complete hands-on opportunity to learn about AWS best practices, services, and architectural patterns. During an event, players are given a starting architecture that they evolve in response to internal & external events on pre-packaged AWS accounts. There are multiple portfolios of GameDays to select from, which specializes on different AWS domains & services.

[Architecture Reviews](#)
Evaluation of architecture and designs that can scale over time leveraging the AWS Well-Architected framework.

[Cost Optimization](#)
Cost Optimization engagements ensure the effective utilization of AWS resources, with actionable recommendations to realize immediate savings and achieve ongoing cost efficiency based on customer priorities.

[Cost Optimization Workshop](#)
The Cost Optimization Workshop is an engagement which improves cost effective utilization of AWS resources. Customers are provided actionable recommendations to realize immediate savings and achieve ongoing cost efficiency. Workshop activities enable the customer to achieve rapid results based on their cost optimization priorities.

[Countdown](#)
Architecture and scaling guidance and operational support during the preparation and execution of planned events such as shopping holidays, product launches, or migrations.

Solicitar uma interação

Você pode solicitar engajamentos para sua Conta da AWS equipe de acordo com os tipos de engajamento incluídos em seu AWS Support Plan.

Para solicitar uma interação:

1. Faça login no Trusted Advisor console em <https://console.aws.amazon.com/trustedadvisor/casa>.
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 engajamento é visível em sua conta, na conta de gerenciamento e em todas as contas de administrador delegado da sua AWS organização.
 - Organização: essa solicitação de engajamento é visível para todas as contas da sua AWS organização.

- 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 AWS será usado quando um escalonamento for necessário para esse compromisso.
- Correspondência: uma nota e um anexo de arquivo opcional para você fornecer detalhes sobre essa interação.

4. Escolha Enviar solicitação.

Example : solicitar interação

Trusted Advisor

Priority

Recommendations

Cost optimization

Performance

Security

Fault tolerance

Service limits

Operational excellence

Engage

data-trends

Organizational view

▼ Preferences

Manage Trusted Advisor

Notifications

Your organization

Trusted Advisor > Engage > Request engagement

Request Engagement

You can request any available Engagement that will help you to meet your business needs.

Request Details

Title

test engagement

Select Engagement

Cost Optimization

Description

Cost Optimization engagements ensure the effective utilization of AWS resources, with actionable recommendations to realize immediate savings and achieve ongoing cost efficiency based on customer priorities.

Desired Completion Date

2023/12/28

Request Visibility

Request Visibility

☒ My account
This engagement request is visible only to your account

☐ My account and Admin accounts
This engagement request is visible to your account, your AWS Organization's management account, and Trusted Advisor Delegated Admin accounts

☐ Organization
This engagement request is visible to all accounts in my organization

Contacts

Engagement Requester Email

test_engagement@amazon.com

Email notification - optional

☐ Send an email with this engagement's updates to Engagement Requester Email

Point of escalation

☒ Same as customer point of contact

☐ Use a different email

Correspondence

Enter a note for your assigned TAM and optionally attach a file. Don't share any sensitive information in correspondences, such as passwords, credit card data, signed URLs, or personally identifiable information.

Upload an artifact

File size must not exceed 5 MB

Enter a note

Enter your note here

Editar uma interação

Você pode editar os detalhes da sua solicitação de interação.

Para editar uma interação:

1. Faça login no Trusted Advisor console em <https://console.aws.amazon.com/trustedadvisor/casa>.
2. Na página Trusted Advisor Engage, selecione uma interação existente.
3. Selecione 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 engajamento é visível em sua conta, na conta de gerenciamento e em todas as contas de administrador delegado da sua AWS organização.
 - Organização: essa solicitação de engajamento é visível para todas as contas da sua AWS organização.
 - 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 AWS será usado quando um escalonamento for necessário para esse compromisso.
5. Escolha Salvar.

Example : editar interação

The screenshot shows the AWS Trusted Advisor console interface. On the left is a sidebar with navigation options: Priority, Recommendations (Cost optimization, Performance, Security, Fault tolerance, Service limits, Operational excellence), Engage (data-trends, Organizational view), and Preferences (Manage Trusted Advisor, Notifications, Your organization). The main content area is titled 'Edit request' and contains three sections: 'Engagement details', 'Request Visibility', and 'Contacts'. The 'Engagement details' section includes fields for Title (test engagement), Engagement (Well Architected Review), Description (Well Architected Framework Reviews (WAFR) provide a mechanism for evaluating workloads, identifying high-risk issues, and recording improvements.), and Desired Completion Date (2024/01/31). The 'Request Visibility' section has three radio button options: 'My account' (selected), 'My account and Admin accounts', and 'Organization'. The 'Contacts' section includes a field for Engagement Requester Email (test_engagement@amazon.com), a checkbox for 'Email notification - optional' (checked), and a section for 'Point of escalation' with two radio button options: 'Same as customer point of contact' (selected) and 'Use a different email'. At the bottom right are 'Save' and 'Cancel' buttons.

Trusted Advisor > Engage > 170240852401061

Edit request

Engagement details

Title
test engagement

Engagement
Well Architected Review

Description
Well Architected Framework Reviews (WAFR) provide a mechanism for evaluating workloads, identifying high-risk issues, and recording improvements.

Desired Completion Date
2024/01/31

Request Visibility

Request Visibility

☒ My account
This engagement request is visible only to your account

☐ My account and Admin accounts
This engagement request is visible to your account, your AWS Organization's management account, and Trusted Advisor Delegated Admin accounts

☐ Organization
This engagement request is visible to all accounts in my organization

Contacts

Engagement Requester Email
test_engagement@amazon.com

Email notification - optional
☒ Send an email with this engagement's updates to Engagement Requester Email

Point of escalation
☒ Same as customer point of contact
☐ Use a different email

Save Cancel

Enviar anexos e notas

Você pode se comunicar com sua Conta da AWS equipe em compromissos individuais enviando notas e anexos de arquivo para apoiar sua solicitação de engajamento. Você pode incluir um único anexo e uma nota por comunicação, só pode anexar arquivos a um compromisso com o mesmo Conta da AWS que solicitou o compromisso 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 Trusted Advisor console em <https://console.aws.amazon.com/trustedadvisor/casa>.
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 nenhuma informação confidencial em correspondências, como senhas, dados de cartão de crédito, informações assinadas URLs ou de identificação pessoal.
5. Escolha Salvar.

Example : adicionar nota e anexar arquivo a uma interação

Trusted Advisor ×

Trusted Advisor > Engage > 12284269831

Cost Optimization Complete

Request Details

Request ID	Type	Status
12284269831	Cost Optimization	In Progress
Date	Age	
Mar 19, 2023	8 days	
Recommended		

▼ Correspondence

Enter a note for your assigned TAM and optionally attach a file. Don't share any sensitive information in correspondences, such as passwords, credit card data, signed URLs, or personally identifiable information.

Upload an artifact

Choose file

File size must not exceed 5 MB

hr-app-emporium-highlevel-architecture.pptx
File size: 3.7 MB
Last date modified: 27-03-2023 12:53:55

Enter a note

this is a high level architecture for hr-app-emporium service.

Save

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 Trusted Advisor console em <https://console.aws.amazon.com/trustedadvisor/casa>.
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

Trusted Advisor

Pursuit

Beta

Priority

Recommendations

Cost optimization

Performance

Security

Fault tolerance

Service limits

Operational excellence

Engage

Data trends

Organizational view

▼ Preferences

Manage Trusted Advisor

Notifications

Your organization

Integrations

Successfully updated Engagement request.

Trusted Advisor > Engage > 172609066800544

Countdown for Product Launch XYZ

Reopen

Request Details

Request ID

172609066800544

Creation Date

Sep 11, 2024

Requested

Complete By

Jan 20, 2025

Type

Countdown

Effective Date

Sep 11, 2024

Request Visibility

My account

Status

Cancelled

Age

6 minutes

Contacts

Single point of contact

avtholl@amazon.com

Point of escalation

avtholl@amazon.com

Audit trail

View only uploaded artifacts

Customer Note

By: aws-kumo-emporium+es-management-test-allowlisted@amazon.com • 9/11/2024, 3:37:49 PM

Note

Enter a note for your assigned TAM and optionally attach a file. Don't share any sensitive information in correspondences, such as passwords, credit card data, signed URLs, or personally identifiable information.

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 Trusted Advisor console em <https://console.aws.amazon.com/trustedadvisor/casa>.
2. Na página Trusted Advisor Engajamento, veja a coluna Data de vigência para distinguir entre compromissos recomendados e solicitados:
 - Recomendado: solicitação de engajamento criada por suas Conta da AWS equipes.
 - Solicitada: solicitação de interação criada pelo usuário.

Pesquisar interações

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

Para pesquisar interações:

1. Faça login no Trusted Advisor console em <https://console.aws.amazon.com/trustedadvisor/casa>.
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

The screenshot shows the AWS Trusted Advisor Engage console. On the left, there is a navigation menu with options like Pursuit, Priority, Recommendations, and Engage. The main area displays 'Active Engagements (2)' with a search bar and a 'Clear filters' button. A dropdown menu is open, showing properties like Engagement Type, Request title, Status, Age (days), Desired Completion Date, and Effective Date. The table below shows two engagements: 'Cost Optimization' and 'Countdown', both with account ID 303615524644. The first is 'In Progress' and the second is 'Pending Response'.

Engagement Type	Account ID	Status	Effective Date	Desired Completion Date	Age (day)
Cost Optimization	303615524644	In Progress	Sep 11, 2024 Recommended	Dec 16, 2024	0
Countdown	303615524644	Pending Response	Sep 11, 2024 Requested	Jan 20, 2025	0

AWS Trusted Advisor verifique a referência

Você pode ver todos os nomes e descrições dos Trusted Advisor cheques IDs 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 mais informações, consulte os tópicos a seguir.

- [Comece a usar a Trusted Advisor API](#)
- [AWS Trusted Advisor API Reference](#)

 Note

Se você tiver um plano de Suporte Básico e Suporte ao Desenvolvedor, poderá usar o Trusted Advisor console para acessar todas as verificações na [Limites do serviço](#) categoria e as seguintes verificações nas categorias Segurança e Tolerância a Falhas:

- [Snapshots públicos do Amazon EBS](#)
- [Snapshots públicos do Amazon RDS](#)
- [Permissões do bucket do Amazon S3](#)
- [MFA na conta raiz](#)
- [Grupos de segurança - Portas específicas irrestritas](#)
- [AWS STS uso global de endpoints em Regiões da AWS](#)

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 não faz parte do AWS Organizations](#)
- [Recomendações de otimização de custos do Amazon Aurora para armazenamento em cluster de banco de dados](#)
- [Endpoints do Amazon Comprehend subutilizados](#)
- [Recomendações de compra de capacidade reservada do Amazon DynamoDB](#)
- [Recomendações de otimização de custos do Amazon EBS para volumes](#)
- [Volumes superprovisionados do Amazon EBS](#)

- [Recomendações de otimização de EC2 custos da Amazon para grupos do Amazon EC2 Auto Scaling](#)
- [Recomendações EC2 de otimização de custos da Amazon para instâncias](#)
- [Consolidação de EC2 instâncias da Amazon para Microsoft SQL Server](#)
- [EC2 Instâncias da Amazon provisionadas em excesso para o Microsoft SQL Server](#)
- [EC2 Instâncias da Amazon paradas](#)
- [Expiração do leasing da Amazon EC2 Reserved Instance](#)
- [Otimização de instâncias EC2 reservadas da Amazon](#)
- [Repositório Amazon ECR sem política de ciclo de vida configurada](#)
- [Otimização de nós ElastiCache reservados da Amazon](#)
- [Recomendações de compra de nós ElastiCache reservados da Amazon](#)
- [AWS Fargate recomendações de otimização de custos para o Amazon ECS](#)
- [Recomendações de compra de nós reservados do Amazon MemoryDB](#)
- [Otimização da instância reservada do Amazon OpenSearch Service](#)
- [Recomendações de compra de instâncias reservadas do Amazon OpenSearch Service](#)
- [Recomendações de otimização de custos do Amazon RDS para instâncias de banco de dados](#)
- [Recomendações de otimização de custos do Amazon RDS para armazenamento de instâncias de banco de dados](#)
- [Instâncias de banco de dados inativas do Amazon RDS](#)
- [Recomendações de compra de instâncias reservadas do Amazon RDS](#)
- [Otimização de nós reservados do Amazon Redshift](#)
- [Recomendações de compra de nós reservados do Amazon Redshift](#)
- [Otimização de instâncias reservadas 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](#)
- [AWS Lambda recomendações de otimização de custos para funções](#)
- [AWS Lambda funções com tempos limite excessivos](#)
- [AWS Lambda funções com altas taxas de erro](#)
- [Funções superprovisionadas do AWS Lambda para tamanho de memória](#)

- [AWS Recomendações de compra da Savings Plans para computação](#)
- [AWS Recomendações de compra de Savings Plans para Amazon SageMaker AI](#)
- [Problemas de alto risco do AWS Well-Architected para otimização de custos](#)
- [Balanceadores de carga obsoletos](#)
- [Inativo AWS Network Firewall](#)
- [Endpoints de interface VPC inativos](#)
- [Endpoints inativos do Load Balancer do Gateway](#)
- [Gateways NAT inativos](#)
- [Instâncias Amazon EC2 de baixa utilização](#)
- [Savings Plan](#)
- [Endereços de IP elástico não associados](#)
- [Volumes subutilizados do Amazon EBS](#)
- [Clusters subutilizados do Amazon Redshift](#)

Conta da AWS não faz parte do AWS Organizations

Descrição

Verifica se um Conta da AWS faz parte AWS Organizations da conta de gerenciamento apropriada.

AWS Organizations é um serviço de gerenciamento de contas para consolidar várias AWS contas em uma organização gerenciada centralmente. 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 `MasterAccountId` parâmetro das AWS Config regras.

Para obter mais informações, consulte [O que é 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

ID da verificação

c18d2gz127

Origem

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

CrITÉRIOS de alerta

Amarelo: Essa AWS conta não faz parte da AWS Organizations.

Ação recomendada

Adicione essa AWS conta como parte do AWS Organizations.

Para obter mais informações, consulte o [Tutorial: criar e configurar uma organização](#).

Colunas do relatório

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

Recomendações de otimização de custos do Amazon Aurora para armazenamento em cluster de banco de dados

Descrição

Verifica as configurações de armazenamento e os padrões de uso do cluster de banco de dados Amazon Aurora para fornecer recomendações para possíveis reduções de custos.

Para cada recurso, Trusted Advisor mostra somente a principal ação recomendada de Hub de Otimização de Custos da AWS.

Para usar essa verificação, você deve optar pelo [Cost Optimization Hub AWS Compute Optimizer](#).

 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

ID da verificação

c1z7kmr17n

Origem

Hub de Otimização de Custos da AWS

Critérios de alerta

Amarelo: um armazenamento em cluster de banco de dados Aurora tem uma ação de redução de custos identificada pelo Cost Optimization Hub.

Ação recomendada

Considere a implementação da recomendação. A recomendação é um dos tipos de recomendação listados em [Entendendo as estratégias de otimização de custos](#) no Guia AWS Cost Management do usuário. Para obter mais informações sobre a implementação dessas recomendações, consulte o Manual de [otimização de custos de serviços](#) do AWS Cloud Financial Management (CFM).

Use as recomendações detalhadas AWS Compute Optimizer para entender o impacto potencial dessas mudanças no custo e no desempenho.

Recursos adicionais

- Entendendo as recomendações de armazenamento em cluster de banco de dados do Aurora.
- AWS Compute Optimizer Recomendações de armazenamento em cluster de banco de dados Aurora

- [Configurações do Amazon Aurora](#)

Colunas do relatório

- Status
- Região
- ID do recurso
- Recommended Action (Ação recomendada)
- Resumo do recurso atual
- Resumo dos recursos recomendados
- Custo mensal estimado
- Economia mensal estimada
- Carimbo de data/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

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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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.

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

Recomendações de compra de capacidade reservada do Amazon DynamoDB

Descrição

Verifica seus padrões de uso do Amazon DynamoDB e fornece recomendações para possíveis reduções de custos por meio da compra de capacidade reservada.

Essa verificação gera recomendações no [escopo do pagador para a conta do pagador e no escopo vinculado para uma conta vinculada](#).

Trusted Advisor mostra somente a ação mais recomendada de Hub de Otimização de Custos da AWS.

 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

ID da verificação

c1z7kmr15n

Origem

Hub de Otimização de Custos da AWS

Critérios de alerta

Amarelo: A conta tem uma ação de redução de custos identificada pelo Cost Optimization Hub for DynamoDB.

Ação recomendada

Considere [a implementação da recomendação](#). Para obter mais informações sobre a implementação dessas recomendações, consulte o Manual de [otimização de custos de serviços](#) do AWS Cloud Financial Management (CFM).

Recursos adicionais

- [Capacidade reservada do DynamoDB](#)
- [Acessando recomendações de reserva](#)
- [Capacidade reservada do Amazon DynamoDB](#)

Colunas do relatório

- Status
- Região
- Resumo dos recursos recomendados
- Custo mensal estimado
- Economia mensal estimada
- Carimbo de data/hora da última atualização

Recomendações de otimização de custos do Amazon EBS para volumes

Descrição

Verifica as configurações de volume e os padrões de uso do Amazon EBS para fornecer recomendações para possíveis economias de custos.

Para cada recurso, Trusted Advisor mostra somente a principal ação recomendada de Hub de Otimização de Custos da AWS.

Para usar essa verificação, você deve optar pelo [Cost Optimization Hub AWS Compute Optimizer](#).

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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

ID da verificação

c1z7kmr02n

Origem

Hub de Otimização de Custos da AWS

Crêterios de alerta

Amarelo: o volume do EBS tem uma ação de redução de custos identificada pelo Cost Optimization Hub.

Ação recomendada

Considere a implementação da recomendação. A recomendação é um dos tipos de recomendação listados em [Entendendo as estratégias de otimização de custos](#) no Guia AWS Cost Management do usuário. Para obter mais informações sobre a implementação dessas

recomendações, consulte o Manual de [otimização de custos de serviços](#) do AWS Cloud Financial Management (CFM).

Use as recomendações detalhadas AWS Compute Optimizer para entender o impacto potencial dessas mudanças no custo e no desempenho.

Recursos adicionais

- [Visualizando recomendações de volume do Amazon EBS](#)
- [Métricas de volume do EBS](#)
- [Tipos de volume do Amazon EBS](#)
- [Solicitar modificações de volume do Amazon EBS](#)

Colunas do relatório

- Status
- Região
- ID do recurso
- Recommended Action (Ação recomendada)
- Resumo do recurso atual
- Resumo dos recursos recomendados
- Custo mensal estimado
- Economia mensal estimada
- Carimbo de data/hora da última atualização

Volumes superprovisionados do Amazon EBS

Descrição

Note

Esta é uma verificação de legado. Recomendamos usar a nova verificação (ID de verificação: [c1z7kmr02n](#)) que oferece recomendações personalizadas adicionais.

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 varia 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

ID da verificação

C0r6dfpM03

Critérios de alerta

Amarelo: um volume do EBS que foi superprovisionado durante o período de análise. 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 superprovisionados do EBS segue as melhores práticas. AWS O algoritmo é atualizado quando um novo padrão é identificado.

Ação recomendada

Considere reduzir o tamanho de volumes que têm baixa utilização.

Para obter mais informações, consulte [Opte por receber Trusted Advisor cheques 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

Recomendações de otimização de EC2 custos da Amazon para grupos do Amazon EC2 Auto Scaling

Descrição

Verifica as configurações de grupo e os padrões de uso do Amazon EC2 Auto Scaling para fornecer recomendações para possíveis reduções de custos.

Para cada recurso, Trusted Advisor mostra somente a principal ação recomendada de Hub de Otimização de Custos da AWS.

Para usar essa verificação, você deve optar pelo [Cost Optimization Hub AWS Compute Optimizer](#).

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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

ID da verificação

c1z7kmr01n

Origem

Hub de Otimização de Custos da AWS

Crítérios de alerta

Amarelo: o grupo Amazon EC2 Auto Scaling tem uma ação de redução de custos identificada pelo Cost Optimization Hub.

Ação recomendada

Considere a implementação da recomendação. A recomendação é um dos tipos de recomendação listados em [Entendendo as estratégias de otimização de custos](#) no Guia AWS Cost Management do usuário. Para obter mais informações sobre a implementação dessas recomendações, consulte o Manual de [otimização de custos de serviços](#) do AWS Cloud Financial Management (CFM).

Use as recomendações detalhadas AWS Compute Optimizer para entender o impacto potencial dessas mudanças no custo e no desempenho.

Recursos adicionais

- [Visualizando recomendações de volume do Amazon EC2 Auto Scaling](#)
- [Grupos do Amazon EC2 Auto Scaling](#)
- [O que é o Amazon EC2 Auto Scaling](#)

Colunas do relatório

- Status
- Região
- ID do recurso
- Recommended Action (Ação recomendada)
- Resumo do recurso atual

- Resumo dos recursos recomendados
- Custo mensal estimado
- Economia mensal estimada
- Carimbo de data/hora da última atualização

Recomendações EC2 de otimização de custos da Amazon para instâncias

Descrição

Verifica as configurações e os padrões de uso da sua EC2 instância Amazon para fornecer recomendações para possíveis economias de custos.

Para cada recurso, Trusted Advisor mostra somente a principal ação recomendada de Hub de Otimização de Custos da AWS.

Para usar essa verificação, você deve optar pelo [Cost Optimization Hub AWS Compute Optimizer](#).

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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

ID da verificação

c1z7kmr00n

Origem

Hub de Otimização de Custos da AWS

Critérios de alerta

Amarelo: a EC2 instância tem uma ação de redução de custos identificada pelo Cost Optimization Hub.

Ação recomendada

Considere a implementação da recomendação. A recomendação é um dos tipos de recomendação listados em [Entendendo as estratégias de otimização de custos](#) no Guia AWS Cost Management do usuário. Para obter mais informações sobre a implementação dessas recomendações, consulte o Manual de [otimização de custos de serviços](#) do AWS Cloud Financial Management (CFM).

Use as recomendações detalhadas AWS Compute Optimizer para entender o impacto potencial dessas mudanças no custo e no desempenho.

Recursos adicionais

- [Visualizando recomendações de EC2 instâncias](#)
- [EC2 métricas de instância](#)
- [Alterações no tipo de EC2 instância da Amazon](#)

Colunas do relatório

- Status
- Região
- ID do recurso
- Recommended Action (Ação recomendada)
- Resumo do recurso atual
- Resumo dos recursos recomendados
- Custo mensal estimado
- Economia mensal estimada
- Carimbo de data/hora da última atualização

Consolidação de EC2 instâncias da Amazon 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 v. CPUs. 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

ID da verificação

Qsdfp3A4L2

Critérios de alerta

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

Recommended Action (Ação recomendada)

Considere consolidar cargas de trabalho menores do SQL Server em instâncias com pelo menos quatro v. CPUs

Recursos adicionais

- [Microsoft SQL Server na AWS](#)
- [Licenciamento da Microsoft em 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

EC2 Instâncias da Amazon provisionadas em excesso para o 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 a edição SQL Server Standard pode usar até 48 CPUs v. Uma instância com o SQL Server Web pode usar até 32 CPUs v. Essa verificação alerta você se uma instância exceder esse limite de vCPU.

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.

A economia mensal estimada é calculada usando a mesma família de instâncias com o número máximo de v CPUs que uma instância do SQL Server pode usar e os preços 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

ID da verificação

Qsdfp3A4L1

Critérios de alerta

- Vermelho: uma instância com a edição SQL Server Standard tem mais de 48 CPUs v.
- Vermelho: uma instância com o SQL Server Web Edition tem mais de 32 CPUs v.

Ação recomendada

Para a edição SQL Server Standard, considere mudar para uma instância na mesma família de instâncias com 48 CPUs v. Para a edição Web do SQL Server, considere mudar para uma

instância na mesma família de instâncias com 32 CPUs v. Se a memória for intensiva, considere mudar para instâncias R5 com memória otimizada. Para obter mais informações, consulte [Melhores práticas para implantar o Microsoft SQL Server na Amazon EC2](#).

Recursos adicionais

- [Microsoft SQL Server na AWS](#)
- Você pode usar o [Launch Wizard](#) para simplificar sua 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

EC2 Instâncias da Amazon paradas

Descrição

Verifica se há EC2 instâncias da Amazon que foram 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 estou sendo cobrado pela Amazon EC2 quando 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

ID da verificação

c18d2gz150

Origem

AWS Config Managed Rule: ec2-stopped-instance

CrITÉRIOS de alerta

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

Ação recomendada

Analise as EC2 instâncias da Amazon que foram interrompidas por 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

- [Preços EC2 sob demanda da Amazon](#)

Colunas do relatório

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

Expiração do leasing da Amazon EC2 Reserved Instance

Descrição

Verifica as Instâncias EC2 Reservadas da Amazon que estão programadas para expirar nos próximos 30 dias ou expiraram nos 30 dias anteriores.

As instâncias reservadas não são renovadas automaticamente. Você pode continuar usando uma EC2 instância da Amazon coberta pela reserva sem interrupção, mas serão cobradas tarifas 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.

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 EC2 reservadas da Amazon

Descrição

Uma parte importante do uso AWS envolve balancear sua compra de Instância Reservada (RI) com o uso da Instância Sob Demanda. Essa verificação fornece recomendações que RIs ajudarão a reduzir os custos decorrentes do 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 adiantamento parcial RIs pode ajudar a reduzir custos.

Ação recomendada

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

Recursos adicionais

- Informações sobre RIs e como eles podem economizar seu dinheiro podem ser encontradas [aqui](#).
- Para obter mais informações sobre essa recomendação, consulte [Perguntas sobre verificação da otimização de instâncias reservadas](#) no Trusted Advisor FAQs.

Colunas do relatório

- Região
- Tipo de instância
- Plataforma

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

Repositório 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.

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
- AWS Config Regra
- Parâmetros de entrada
- Hora da última atualização

Otimização de nós ElastiCache reservados da Amazon

Descrição

Note

Esta é uma verificação de legado. Recomendamos usar a nova verificação (ID de verificação: [c1z7kmr13n](#)) que oferece recomendações personalizadas adicionais.

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. Esta 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.

Ação recomendada

[Para obter recomendações mais detalhadas, opções de personalização \(por exemplo, período de retrospectiva, opção de pagamento etc.\) e para comprar nós ElastiCache reservados, consulte Cost Explorer.](#)

Recursos adicionais

- Para obter informações sobre nós ElastiCache reservados e como eles podem economizar seu dinheiro, consulte [Amazon ElastiCache Reserved Nodes](#).
- Para obter mais informações sobre essa recomendação, consulte [Perguntas sobre verificação da otimização de instâncias reservadas](#) no Trusted Advisor FAQs.
- 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)

Recomendações de compra de nós ElastiCache reservados da Amazon

Descrição

Verifica seus padrões ElastiCache de uso da Amazon para fornecer recomendações sobre possíveis economias de custos por meio da compra de nós reservados.

Essa verificação gera recomendações no [escopo do pagador para a conta do pagador e no escopo vinculado para uma conta vinculada](#).

Trusted Advisor mostra somente a ação mais recomendada de Hub de Otimização de Custos da AWS.

Para usar essa verificação, você deve optar pelo [Cust Optimization Hub](#).

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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

ID da verificação

c1z7kmr13n

Origem

Hub de Otimização de Custos da AWS

Critérios de alerta

Amarelo: A conta tem uma ação de redução de custos identificada pelo Cost Optimization Hub for Amazon ElastiCache.

Ação recomendada

Considere [implementar a recomendação](#) Para obter mais informações sobre a implementação dessas recomendações, consulte o Manual de [otimização de custos de serviços](#) do AWS Cloud Financial Management (CFM).

Recursos adicionais

- [Nódulos reservados](#)
- [Acessando recomendações de reserva](#)
- [Nodes ElastiCache reservados da Amazon](#)

Colunas do relatório

- Status
- Região
- Resumo dos recursos recomendados
- Custo mensal estimado
- Economia mensal estimada
- Carimbo de data/hora da última atualização

AWS Fargate recomendações de otimização de custos para o Amazon ECS

Descrição

Verifica suas AWS Fargate configurações e padrões de uso do Amazon ECS para fornecer recomendações sobre possíveis reduções de custos.

Para cada recurso, Trusted Advisor mostra somente a principal ação recomendada de Hub de Otimização de Custos da AWS.

Para usar essa verificação, você deve optar pelo [Cost Optimization Hub AWS Compute Optimizer](#).

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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

ID da verificação

c1z7kmr06n

Origem

Hub de Otimização de Custos da AWS

CrITÉrios de alerta

Amarelo: os serviços do Amazon ECS ativados AWS Fargate têm uma ação de redução de custos identificada pelo Cost Optimization Hub.

Ação recomendada

Considere a implementação da recomendação. A recomendação é um dos tipos de recomendação listados em [Entendendo as estratégias de otimização de custos](#) no Guia AWS Cost Management do usuário. Para obter mais informações sobre a implementação dessas recomendações, consulte o Manual de [otimização de custos de serviços](#) do AWS Cloud Financial Management (CFM).

Use as recomendações detalhadas AWS Compute Optimizer para entender o impacto potencial dessas mudanças no custo e no desempenho.

Recursos adicionais

- [Visualizando os serviços do Amazon ECS nas recomendações do Fargate](#)
- [Métricas para serviços do Amazon ECS no Fargate](#)
- [AWS Fargate para Amazon ECS](#)
- [Atualização de um serviço do Amazon ECS usando o console](#)

Colunas do relatório

- Status
- Região
- ID do recurso
- Recommended Action (Ação recomendada)
- Resumo do recurso atual
- Resumo dos recursos recomendados
- Custo mensal estimado

- Economia mensal estimada
- Carimbo de data/hora da última atualização

Recomendações de compra de nós reservados do Amazon MemoryDB

Descrição

Verifica seus padrões de uso do Amazon MemoryDB para fornecer recomendações sobre possíveis economias de custo por meio da compra de nós reservados.

Essa verificação gera recomendações no [escopo do pagador para a conta do pagador e no escopo vinculado para uma conta vinculada](#).

Para cada recurso, Trusted Advisor mostra somente a principal ação recomendada de Hub de Otimização de Custos da AWS.

Para usar essa verificação, você deve optar pelo [Cust Optimization Hub](#).

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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

ID da verificação

c1z7kmr16n

Origem

Hub de Otimização de Custos da AWS

Critérios de alerta

Amarelo: A conta tem uma ação de redução de custos identificada pelo Cost Optimization Hub for MemoryDB.

Ação recomendada

Considere [a implementação da recomendação](#). Para obter mais informações sobre a implementação dessas recomendações, consulte o Manual de [otimização de custos de serviços](#) do AWS Cloud Financial Management (CFM).

Recursos adicionais

- [nós reservados do MemoryDB](#)
- [Acessando recomendações de reserva](#)
- [Trabalhando com nós reservados](#)

Colunas do relatório

- Status
- Região
- Resumo dos recursos recomendados
- Custo mensal estimado
- Economia mensal estimada
- Carimbo de data/hora da última atualização

Otimização da instância reservada do Amazon OpenSearch Service

Descrição

Note

Esta é uma verificação de legado. Recomendamos usar a nova verificação (ID de verificação: [c1z7kmr14n](#)) que oferece recomendações personalizadas adicionais.

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.

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 [Perguntas sobre verificação da otimização de instâncias reservadas](#) no Trusted Advisor FAQs.
- 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)

Recomendações de compra de instâncias reservadas do Amazon OpenSearch Service

Descrição

Verifica seus padrões OpenSearch de uso do Amazon Service para fornecer recomendações sobre possíveis economias de custo por meio de compras de Instâncias Reservadas (RI).

Essa verificação gera recomendações no [escopo do pagador para a conta do pagador e no escopo vinculado para uma conta vinculada](#).

Trusted Advisor mostra somente a ação mais recomendada de Hub de Otimização de Custos da AWS.

Para usar essa verificação, você deve optar pelo [Cust Optimization Hub](#).

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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

ID da verificação

c1z7kmr14n

Origem

Hub de Otimização de Custos da AWS

Critérios de alerta

Amarelo: A conta tem uma ação de redução de custos identificada pelo Cost Optimization Hub for Amazon OpenSearch Service.

Ação recomendada

Considere [a implementação da recomendação](#). Para obter mais informações sobre a implementação dessas recomendações, consulte o Manual de [otimização de custos de serviços](#) do AWS Cloud Financial Management (CFM).

Recursos adicionais

- [Instâncias reservadas no Amazon OpenSearch Service](#)
- [Acessando recomendações de reserva](#)
- [Compra de instâncias reservadas \(AWS CLI\)](#)

Colunas do relatório

- Status
- Região
- Resumo dos recursos recomendados
- Custo mensal estimado
- Economia mensal estimada
- Carimbo de data/hora da última atualização

Recomendações de otimização de custos do Amazon RDS para instâncias de banco de dados

Descrição

Verifica as configurações e os padrões de uso da instância de banco de dados do Amazon RDS para fornecer recomendações para possíveis economias de custos.

Para cada recurso, Trusted Advisor mostra somente a principal ação recomendada de Hub de Otimização de Custos da AWS.

Para usar essa verificação, você deve optar pelo [Cost Optimization Hub AWS Compute Optimizer](#).

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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

ID da verificação

c1z7kmr03n

Origem

Hub de Otimização de Custos da AWS

CrITÉRIOS de alerta

Amarelo: a instância de banco de dados do RDS tem uma ação de redução de custos identificada pelo Cost Optimization Hub.

Ação recomendada

Considere a implementação da recomendação. A recomendação é um dos tipos de recomendação listados em [Entendendo as estratégias de otimização de custos](#) no Guia AWS Cost Management do usuário. Para obter mais informações sobre a implementação dessas recomendações, consulte o Manual de [otimização de custos de serviços](#) do AWS Cloud Financial Management (CFM).

Use as recomendações detalhadas AWS Compute Optimizer para entender o impacto potencial dessas mudanças no custo e no desempenho.

Recursos adicionais

- [Visualizando recomendações do banco de dados do RDS](#)
- [Métricas do banco de dados RDS](#)
- [classes de instância de banco de dados](#)
- [Modificando uma instância de banco de dados Amazon RDS](#)

Colunas do relatório

- Status
- Região
- ID do recurso
- Recommended Action (Ação recomendada)
- Resumo do recurso atual

- Resumo dos recursos recomendados
- Custo mensal estimado
- Economia mensal estimada
- Carimbo de data/hora da última atualização

Recomendações de otimização de custos do Amazon RDS para armazenamento de instâncias de banco de dados

Descrição

Verifica as configurações de armazenamento e os padrões de uso da instância de banco de dados do Amazon RDS para fornecer recomendações para possíveis reduções de custos.

Para cada recurso, Trusted Advisor mostra somente a principal ação recomendada de Hub de Otimização de Custos da AWS.

Para usar essa verificação, você deve optar pelo [Cost Optimization Hub AWS Compute Optimizer](#).

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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

ID da verificação

c1z7kmr04n

Origem

Hub de Otimização de Custos da AWS

Critérios de alerta

Amarelo: O armazenamento de banco de dados do RDS tem uma ação de redução de custos identificada pelo Cost Optimization Hub.

Ação recomendada

Considere a implementação da recomendação. A recomendação é um dos tipos de recomendação listados em [Entendendo as estratégias de otimização de custos](#) no Guia AWS Cost Management do usuário. Para obter mais informações sobre a implementação dessas recomendações, consulte o Manual de [otimização de custos de serviços](#) do AWS Cloud Financial Management (CFM).

Use as recomendações detalhadas AWS Compute Optimizer para entender o impacto potencial dessas mudanças no custo e no desempenho.

Recursos adicionais

- [Visualizando recomendações do banco de dados do RDS](#)
- [Armazenamento de instâncias de banco de dados do Amazon RDS](#)

Colunas do relatório

- Status
- Região
- ID do recurso
- Recommended Action (Ação recomendada)
- Resumo do recurso atual
- Resumo dos recursos recomendados
- Custo mensal estimado
- Economia mensal estimada
- Carimbo de data/hora da última atualização

Instâncias de banco de dados inativas do Amazon RDS

Descrição

Note

Esta é uma verificação de legado. Recomendamos usar a nova verificação (ID de verificação: [c1z7kmr03n](#)) que oferece recomendações personalizadas adicionais.

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

Ti39ha1fu8

Critérios de alerta

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

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)

Recomendações de compra de instâncias reservadas do Amazon RDS

Descrição

Verifica seus padrões de uso do Amazon RDS para fornecer recomendações sobre possíveis economias de custo por meio de compras de Instâncias Reservadas (RI).

Essa verificação gera recomendações no [escopo do pagador para a conta do pagador e no escopo vinculado para uma conta vinculada](#).

Trusted Advisor mostra somente a ação mais recomendada de Hub de Otimização de Custos da AWS.

Para usar essa verificação, você deve optar pelo [Cust Optimization Hub](#).

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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

ID da verificação

c1z7kmr11n

Origem

Hub de Otimização de Custos da AWS

Critérios de alerta

Amarelo: o volume do EBS tem uma ação de redução de custos identificada pelo Cost Optimization Hub.

Ação recomendada

Considere [a implementação da recomendação](#). Para obter mais informações sobre a implementação dessas recomendações, consulte o Manual de [otimização de custos de serviços](#) do AWS Cloud Financial Management (CFM).

Recursos adicionais

- [Instância de banco de dados reservada para Amazon RDS](#)
- [Acessando recomendações de reserva](#)
- [Comprar instâncias de banco de dados reservadas para o Amazon RDS](#)

Colunas do relatório

- Status
- Região
- Resumo dos recursos recomendados
- Custo mensal estimado
- Economia mensal estimada
- Carimbo de data/hora da última atualização

Otimização de nós reservados do Amazon Redshift

Descrição

Note

Esta é uma verificação de legado. Recomendamos usar a nova verificação (ID de verificação: [c1z7kmr12n](#)) que oferece recomendações personalizadas adicionais.

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 [Perguntas sobre verificação da otimização de instâncias reservadas](#) no Trusted Advisor FAQs.
- 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)

Recomendações de compra de nós reservados do Amazon Redshift

Descrição

Verifica seus padrões de uso do Amazon Redshift para fornecer recomendações sobre possíveis economias de custo por meio da compra de nós reservados.

Essa verificação gera recomendações no [escopo do pagador para a conta do pagador e no escopo vinculado para uma conta vinculada](#).

Trusted Advisor mostra somente a ação mais recomendada de Hub de Otimização de Custos da AWS.

Para usar essa verificação, você deve optar pelo [Cust Optimization Hub](#).

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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

ID da verificação

c1z7kmr12n

Origem

Hub de Otimização de Custos da AWS

Critérios de alerta

Amarelo: A conta tem uma ação de redução de custos identificada pelo Cost Optimization Hub for Amazon Redshift.

Ação recomendada

Considere [a implementação da recomendação](#). Para obter mais informações sobre a implementação dessas recomendações, consulte o Manual de [otimização de custos de serviços](#) do AWS Cloud Financial Management (CFM).

Recursos adicionais

- [Nódulos reservados](#)
- [Acessando recomendações de reserva](#)
- [Adquirindo um nó reservado](#)

Colunas do relatório

- Status
- Região
- Resumo dos recursos recomendados
- Custo mensal estimado
- Economia mensal estimada
- Carimbo de data/hora da última atualização

Otimização de instâncias reservadas do Amazon Relational Database Service (RDS)

Descrição

Note

Esta é uma verificação de legado. Recomendamos usar a nova verificação (ID de verificação: [c1z7kmr11n](#)) que oferece recomendações personalizadas adicionais.

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 [Perguntas sobre verificação da otimização de instâncias reservadas](#) no Trusted Advisor FAQs.
- 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 que o Amazon Route 53 encaminhe consultas para a rede Região da AWS com a menor latência de rede, você deve criar conjuntos de registros de recursos de latência para um nome de domínio específico (como exemplo.com) em diferentes regiões. 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.

As zonas hospedadas criadas por AWS serviços não aparecerão nos resultados da sua 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 um Região da AWS, considere criar recursos em mais de um Região da AWS e definir conjuntos de registros de recursos de latência para cada um; consulte Roteamento baseado em [latência](#).

Se você não quiser usar vários Regiões da AWS, use 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 AWS Config regras.

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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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
- AWS Config Regra
- 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. Poderá levar algumas horas para que as alterações sejam exibidas. Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a BatchUpdateRecommendationResourceExclusion API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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.

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](#)

[Descobrimo 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 bucketNames que deseja verificar usando os parâmetros bucketNames nas 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

ID da verificação

c18d2gz171

Origem

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

Crítérios de alerta

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

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
- AWS Config Regra
- Parâmetros de entrada
- Hora da última atualização

AWS Lambda recomendações de otimização de custos para funções

Descrição

Verifica suas AWS Lambda configurações e padrões de uso para fornecer recomendações para possíveis economias de custos.

Para cada recurso, Trusted Advisor mostra somente a principal ação recomendada de Hub de Otimização de Custos da AWS.

Para usar essa verificação, você deve optar pelo [Cost Optimization Hub AWS Compute Optimizer](#).

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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

ID da verificação

c1z7kmr05n

Origem

Hub de Otimização de Custos da AWS

Critérios de alerta

Amarelo: a função Lambda tem uma ação de redução de custos identificada pelo Cost Optimization Hub.

Ação recomendada

Considere a implementação da recomendação. A recomendação é um dos tipos de recomendação listados em [Entendendo as estratégias de otimização de custos](#) no Guia AWS Cost Management do usuário. Para obter mais informações sobre a implementação dessas recomendações, consulte o Manual de [otimização de custos de serviços](#) do AWS Cloud Financial Management (CFM).

Use as recomendações detalhadas AWS Compute Optimizer para entender o impacto potencial dessas mudanças no custo e no desempenho.

Recursos adicionais

- [Visualizando as recomendações da função Lambda](#)
- [Métricas de função do Lambda](#)
- [Configurando funções AWS Lambda](#)

Colunas do relatório

- Status
- Região
- ID do recurso
- Recommended Action (Ação recomendada)
- Resumo do recurso atual
- Resumo dos recursos recomendados
- Custo mensal estimado
- Economia mensal estimada
- Carimbo de data/hora da última atualização

AWS Lambda funções com tempos limite excessivos

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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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.

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 limite dos clientes 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](#)
- [Usando AWS Lambda com AWS X-Ray](#)
- [Acessando CloudWatch os registros da Amazon para AWS Lambda](#)
- [Exemplo de aplicativo de processador de erros para 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

AWS Lambda funções 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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.

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).

Você também pode escolher entre um ecossistema de ferramentas de monitoramento e observabilidade fornecidas por AWS Lambda parceiros. 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)
- [Exemplo de aplicativo de processador de erros para 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 do dia atual
- Taxa de erros do dia atual
- *Média de invocações diárias
- Hora da última atualização

Funções superprovisionadas do AWS Lambda para tamanho de memória

Descrição

Note

Esta é uma verificação de legado. Recomendamos usar a nova verificação (ID de verificação: [c1z7kmr05n](#)) que oferece recomendações personalizadas adicionais.

Verifica as AWS Lambda funções que foram invocadas pelo menos uma vez durante o período de retrospectiva. 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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.

Ação recomendada

Considere reduzir o tamanho da memória das funções do Lambda.

Para obter mais informações, consulte [Opte por receber Trusted Advisor cheques 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

AWS Recomendações de compra da Savings Plans para computação

Descrição

Verifica seus padrões de uso de AWS computação na Amazon EC2 AWS Lambda e fornece recomendações de compra do Savings Plan. AWS Fargate Com essas recomendações, você

pode se comprometer com um valor de uso consistente, medido em dólares por hora, em troca de tarifas com desconto.

Essa verificação gera recomendações no [escopo do pagador para a conta do pagador e no escopo vinculado para uma conta vinculada](#).

Trusted Advisor mostra somente a ação mais recomendada de Hub de Otimização de Custos da AWS.

Para usar essa verificação, você deve optar pelo [Cust Optimization Hub](#).

 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

ID da verificação

c1z7kmr09n

Origem

Hub de Otimização de Custos da AWS

Critérios de alerta

Amarelo: A conta tem uma ação de redução de custos identificada pelo Cost Optimization Hub para recursos computacionais.

Ação recomendada

Considere [a implementação da recomendação](#). Para obter mais informações sobre a implementação dessas recomendações, consulte o Manual de [otimização de custos de serviços](#) do AWS Cloud Financial Management (CFM).

Recursos adicionais

- [O que são Savings Plans?](#)
- [Tipos de Savings Plans](#)

- [Comprando Savings Plans](#)

Colunas do relatório

- Status
- Região
- Resumo dos recursos recomendados
- Custo mensal estimado
- Economia mensal estimada
- Carimbo de data/hora da última atualização

AWS Recomendações de compra de Savings Plans para Amazon SageMaker AI

Descrição

Verifica seu uso do Amazon SageMaker AI e fornece recomendações de compra do Savings Plan. Com essas recomendações, você pode se comprometer com um valor de uso consistente, medido em dólares por hora, em troca de tarifas com desconto.

Essa verificação gera recomendações no [escopo do pagador para a conta do pagador e no escopo vinculado para uma conta vinculada](#).

Trusted Advisor mostra somente a ação mais recomendada de Hub de Otimização de Custos da AWS.

Para usar essa verificação, você deve optar pelo [Cust Optimization Hub](#).

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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

ID da verificação

c1z7kmr08n

Origem

Hub de Otimização de Custos da AWS

Critérios de alerta

Amarelo: A conta tem uma ação de redução de custos identificada pelo Cost Optimization Hub for Amazon SageMaker AI.

Ação recomendada

Considere [a implementação da recomendação](#). Para obter mais informações sobre a implementação dessas recomendações, consulte o Manual de [otimização de custos de serviços](#) do AWS Cloud Financial Management (CFM).

Recursos adicionais

- [O que são Savings Plans?](#)
- [Tipos de Savings Plans](#)
- [Comprando Savings Plans](#)

Colunas do relatório

- Status
- Região
- Resumo dos recursos recomendados
- Custo mensal estimado
- Economia mensal estimada
- Carimbo de data/hora da última atualização

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

Descrição

Verifica problemas de alto risco (HRIs) em suas cargas de trabalho no pilar de 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

ID da verificação

Wxdfp4B1L1

Critérios de alerta

- Vermelho: Pelo menos um problema ativo de alto risco foi identificado no pilar de otimização de custos da AWS Well-Architected.
- Verde: Nenhum problema ativo de alto risco foi detectado no pilar de otimização de custos 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 identificados HRIs para otimização de custos

- Número de HRIs 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 [Registrar suas EC2 instâncias da Amazon com seu Load Balancer](#) ou [Excluir seu Load Balancer](#).

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

Inativo AWS Network Firewall

Descrição

Verifica seus AWS Network Firewall endpoints e alerta você quando o Firewall de Rede parece estar inativo.

Um Network Firewall é considerado inativo se todos os seus endpoints não tiverem dados processados nos últimos 30 dias. Os endpoints do Network Firewall incorrem em cobranças por hora. Essa verificação alerta você sobre o Firewall de Rede sem dados processados nos últimos 30 dias. É uma prática recomendada remover firewalls de rede não utilizados ou atualizar sua arquitetura.

ID da verificação

c2v1fg0bfw

Critérios de alerta

- Amarelo: O Network Firewall processou 0 bytes nos últimos 30 dias.
- Verde: o Network Firewall processou mais de 0 bytes nos últimos 30 dias.

Recommended Action (Ação recomendada)

Se o Firewall de Rede não foi usado nos últimos 30 dias, considere excluí-lo.

Se um Transit Gateway for usado para comunicação entre VPCs, considere implantar seus firewalls de rede em uma arquitetura centralizada de inspeção de rede. Isso pode reduzir as cobranças horárias em firewalls de rede inativos.

Recursos adicionais

[Definição de preço do AWS Network Firewall](#)

[Modelos de implantação de inspeção com AWS Network Firewall](#)

Colunas do relatório

- Status
- Região
- Braço de Firewall de Rede
- Id da VPC
- Sub-redes
- TotalBytesProcessed
- Hora da última atualização

Endpoints de interface VPC inativos

Descrição

Verifica os endpoints da interface VPC e alerta você quando os endpoints parecem estar inativos. Um endpoint de interface VPC é considerado inativo se não tiver dados processados nos últimos 30 dias. Os endpoints da interface VPC têm cobranças por hora e custos de processamento de dados. Essa verificação alerta você sobre endpoints da interface VPC com 0 dados processados nos últimos 30 dias. É uma prática recomendada remover os endpoints não utilizados da interface VPC ou atualizar sua arquitetura.

ID da verificação

c2v1fg0jp6

Critérios de alerta

- Amarelo: o endpoint da interface VPC processou 0 bytes nos últimos 30 dias.
- Verde: o endpoint da interface VPC processou mais de 0 bytes nos últimos 30 dias

Recommended Action (Ação recomendada)

Se o endpoint da interface VPC não tiver sido usado nos últimos 30 dias, considere excluir o endpoint da interface VPC.

Se o Transit Gateway for usado para comunicação entre VPC, considere implantar seus endpoints de interface VPC em uma arquitetura centralizada para reduzir as cobranças por hora em endpoints de interface VPC inativos.

Recursos adicionais

- [AWS PrivateLink Preços](#)
- [Acesso centralizado aos endpoints privados da VPC](#)

Colunas do relatório

- Status
- Região
- ID do VPC Endpoint
- Id da VPC
- IDs de sub-rede
- Nome do serviço
- TotalBytesProcessed
- Hora da última atualização

Endpoints inativos do Load Balancer do Gateway

Descrição

Verifica seus endpoints do Gateway Load Balancer e avisa quando eles parecem estar inativos. Um endpoint do Gateway Load Balancer é considerado subutilizado se não tiver dados processados nos últimos 30 dias. Os endpoints do Gateway Load Balancer têm cobranças por hora e cobranças de processamento de dados. Essa verificação alerta você sobre endpoints do Gateway Load Balancer com 0 dados processados nos últimos 30 dias. Recomendamos que você remova os endpoints não utilizados do Gateway Load Balancer ou atualize sua arquitetura.

ID da verificação

c2v1fg0k35

Critérios de alerta

- Amarelo: o endpoint do Gateway Load Balancer processou 0 bytes nos últimos 30 dias
- Verde: o endpoint do Gateway Load Balancer processou mais de 0 bytes nos últimos 30 dias

Recommended Action (Ação recomendada)

Se o endpoint do Gateway Load Balancer não tiver sido usado nos últimos 30 dias, considere excluir o endpoint VPC.

Se o Transit Gateway for usado para comunicação entre VPCs, considere implantar seus endpoints do Gateway Load Balancer em uma arquitetura centralizada de inspeção de rede para reduzir as cobranças por hora nos endpoints inativos do Gateway Load Balancer.

Recursos adicionais

[Definição de preço do AWS PrivateLink](#)

[Arquitetura de inspeção centralizada com AWS Gateway Load Balancer e AWS Transit Gateway](#)

Colunas do relatório

- Status
- Região
- ID do VPC Endpoint
- Id da VPC
- ID da sub-rede
- Nome do serviço
- TotalBytesProcessed
- Hora da última atualização

Gateways NAT inativos

Descrição

Verifica se há gateways inativos em seus gateways NAT. Um gateway NAT é considerado inativo se nenhum dado (0 bytes) tiver sido processado nos últimos 30 dias. Os gateways NAT têm cobranças por hora e cobranças de processamento de dados.

ID da verificação

c2v1fg022t

Critérios de alerta

- Amarelo: o NAT Gateway processou 0 bytes nos últimos 30 dias
- Verde: o NAT Gateway processou mais de 0 bytes nos últimos 30 dias

Recommended Action (Ação recomendada)

Considere excluir qualquer gateway NAT que não tenha sido usado nos últimos 30 dias e que não seja necessário para acesso externo à rede fora da VPC.

Se um Transit Gateway for usado para comunicação entre VPCs, considere implantar um NAT Gateway centralizado para saída para a arquitetura da Internet. Isso pode reduzir o custo por hora de gateways NAT inativos.

Recursos adicionais

[Preços do NAT Gateway](#)

[Saída centralizada para a Internet](#)

Colunas do relatório

- Status
- Região
- ID do gateway NAT
- ID da sub-rede
- Id da VPC
- TotalBytesFromDest
- TotalBytesFromSrc
- TotalBytes
- Hora da última atualização

Instâncias Amazon EC2 de baixa utilização

Descrição

Note

Esta é uma verificação de legado. Recomendamos usar a nova verificação (ID de verificação: [c1z7kmr00n](#)) que oferece recomendações personalizadas adicionais.

Verifica as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) que estavam em execução a qualquer momento nos 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

- [Monitorando a 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

Note

Esta é uma verificação de legado. Recomendamos usar a nova verificação (ID de verificação: [c1z7kmr09n](#)) que oferece recomendações personalizadas adicionais.

Verifica seu uso da 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.

Eles são provenientes do AWS Cost Explorer, que pode obter informações mais detalhadas sobre recomendações. 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 endereços IP elásticos (EIPs) que não estão associados a uma instância do Amazon Elastic Compute Cloud (Amazon EC2) em execução.

EIPs são endereços IP estáticos projetados para computação dinâmica em nuvem. Ao contrário dos endereços IP estáticos tradicionais, EIPs mascaram a falha de uma instância ou zona de disponibilidade remapeando um endereço IP público para outra instância em sua 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 da 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

Note

Esta é uma verificação de legado. Recomendamos usar a nova verificação (ID de verificação: [c1z7kmr02n](#)) que oferece recomendações personalizadas adicionais.

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 você optou por criar sua conta AWS Compute Optimizer, recomendamos que, em vez disso, use a verificação de volumes sobreprovisionados do Amazon EBS. Para obter mais informações, consulte [Opte por receber Trusted Advisor cheques 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 Amazon EC2 Auto Scaling Group não está associado a um modelo de lançamento](#)
- [Otimização da taxa EC2 de transferência da Amazon para o EBS](#)
- [EC2 O tipo de virtualização 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](#)
- [AWS Lambda Funções 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 Amazon EC2 de alta utilização da CPU](#)

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 workload de leitura para o endpoint somente 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
- Aumento da 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 AWS Config regras.

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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

ID da verificação

c18d2gz136

Origem

AWS Config Regra 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
- AWS Config Regra
- Parâmetros de entrada
- Hora da última atualização

Otimização do Amazon EBS não habilitada

Descrição

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

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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

ID da verificação

c18d2gz142

Origem

AWS Config Regra gerenciada: ebs-optimized-instance

Crêterios de alerta

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

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
- AWS Config Regra
- Parâmetros de entrada
- Hora da última atualização

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

Descrição

Verifica os volumes de IOPS provisionadas (SSD) que estão conectados a uma instância otimizável do Amazon Elastic Compute Cloud (Amazon) do Amazon EBS que não é otimizada para EBS. EC2

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 EC2 instância da Amazon 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

ID da verificação

C016dfpM04

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 subprovisionados do EBS segue as melhores práticas. 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 [Opte por receber Trusted Advisor cheques 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 Amazon EC2 Auto Scaling Group não está associado a um modelo de lançamento

Descrição

Verifica se um grupo do Amazon EC2 Auto Scaling foi criado a partir de um modelo de EC2 lançamento da Amazon.

Use um modelo de lançamento para criar seus grupos do Amazon EC2 Auto Scaling para garantir o acesso aos recursos e melhorias mais recentes do grupo 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

ID da verificação

c18d2gz102

Origem

AWS Config Regra gerenciada: autoscaling-launch-template

Critérios de alerta

Amarelo: O grupo Amazon EC2 Auto Scaling não está associado a um modelo de lançamento válido.

Recommended Action (Ação recomendada)

Use um modelo de EC2 lançamento da Amazon 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
- AWS Config Regra

- Parâmetros de entrada
- Hora da última atualização

Otimização da taxa EC2 de transferência da Amazon para o EBS

Descrição

Verifica os volumes do Amazon EBS cujo desempenho pode ser afetado pela capacidade máxima de taxa de transferência da EC2 instância da Amazon à qual eles estão conectados.

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

ID da verificação

Bh2xRR2FGH

CrITÉrios de alerta

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

Recommended Action (Ação recomendada)

Compare a taxa de transferência máxima dos seus volumes do Amazon EBS (consulte [Tipos de volume do Amazon EBS](#)) com a taxa de transferência máxima da EC2 instância da Amazon à qual eles estão conectados. 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

EC2 O tipo de virtualização é paravirtual

Descrição

Verifica se o tipo de virtualização de uma EC2 instância da Amazon é paravirtual.

É uma prática recomendada usar instâncias de máquina virtual do hardware (HVM) em vez de instâncias paravirtuais, quando possível. Isso se deve aos aprimoramentos na virtualização de HVM e à disponibilidade de drivers fotovoltaicos para HVM AMIs, que fecharam a lacuna de desempenho que existia historicamente entre convidados fotovoltaicos e HVM. É importante observar que os tipos de instância da geração atual não são compatíveis com PV AMIs. 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 [Linux AMI virtualization types](#).

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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

ID da verificação

c18d2gz148

Origem

AWS Config Regra gerenciada: ec2- paravirtual-instance-check

Critérios de alerta

Amarelo: o tipo de virtualização das EC2 instâncias da Amazon é paravirtual.

Recommended Action (Ação recomendada)

Use a virtualização HVM para suas EC2 instâncias da Amazon 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
- AWS Config Regra
- 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

ID da verificação

c18d2gz176

Origem

AWS Config Regra 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
- AWS Config Regra
- Parâmetros de entrada

- Hora da última atualização

Otimização do modo throughput do Amazon EFS

Descrição

Verifica se o sistema de arquivos do Amazon EFS está atualmente configurado para usar o modo Bursting Throughput. A taxa de transferência do Amazon EFS Bursting usa “créditos” para desempenho acima da taxa de transferência básica (50 KiB/s por GiB). Depois que os créditos se esgotam, o desempenho é reduzido para a taxa de transferência básica, o que pode causar lentidão, falhas nos aplicativos e tempos limite para seus usuários. Para saber mais sobre o modo de intermitência, consulte o modo [Throughput no Guia](#) do usuário do Amazon EFS

ID da verificação

c1dfprch02

Critérios de alerta

- Amarelo: o sistema de arquivos está usando o modo Bursting Throughput.

Recommended Action (Ação recomendada)

Se seus créditos de taxa de transferência do Bursting estiverem baixos ou esgotados, considere mudar para o modo de taxa de transferência provisionada ou elástica para fornecer aos usuários e aplicativos a taxa de transferência desejada. Com a taxa de transferência provisionada, você pode definir a taxa de transferência necessária para sua carga de trabalho e pagar pela quantidade de taxa de transferência habilitada para o sistema de arquivos. Se não tiver certeza de seus requisitos de taxa de transferência, você pode usar o modo de taxa de transferência elástica, em que sua taxa de transferência se expande de forma elástica com sua carga de trabalho e você paga apenas pelo que usa, medido pelo total de dados transferidos. Você pode atualizar a configuração do sistema de arquivos para alternar entre os modos de taxa de transferência a qualquer momento. Para saber mais sobre preços de taxa de transferência, consulte os preços do [Amazon EFS](#). Você também pode estimar seus custos usando [AWS Calculadora de Preços](#).

Recursos adicionais

- [Taxa de transferência estrondosa](#)
- [Definição de preço do Amazon EFS](#)
- [AWS Calculadora de Preços](#)

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 as instâncias de banco de dados. Desativar o autovacuum aumenta o inchaço da tabela e do índice e afeta a performance.

Recomendamos que você ative o autovacuum nos 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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

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 nos 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
- Valores recomendados
- Hora da última atualização

Os clusters de banco de dados do Amazon RDS suportam somente volumes de até 64 TiB

Descrição

Clusters de banco de dados são compatíveis com 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

 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

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 dos clusters de banco de dados para oferecer compatibilidade com 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
- Valores recomendados
- Hora da última atualização

Instâncias de banco de dados Amazon RDS nos clusters com classes de instância heterogêneas

Descrição

Recomendamos usar a mesma classe e tamanho da instância de banco de dados para todas as instâncias no 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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

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 no 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
- Valores recomendados
- Nome do motor
- Hora da última atualização

Instâncias de banco de dados Amazon RDS nos clusters com tamanhos de instância heterogêneos

Descrição

Recomendamos usar a mesma classe e tamanho da instância de banco de dados para todas as instâncias no 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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

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 no 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
- Valores recomendados
- 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 a performance e causar erros.

Recomendamos definir os parâmetros de memória personalizados da instância de banco de dados como os valores padrão no 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

 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

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 os valores padrão.

Recursos adicionais

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
- Valores recomendados
- Hora da última atualização

O parâmetro `enable_index_onlyscan` do Amazon RDS está desativado

Descrição

O planejador ou o otimizador de consultas não pode usar o plano de analisar somente o índice quando ele 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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

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
- Valores recomendados
- Hora da última atualização

O parâmetro `enable_indexscan` do Amazon RDS está desativado

Descrição

O planejador ou o otimizador de consultas não pode usar o plano de analisar o índice quando ele 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

 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

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
- Valores recomendados
- Hora da última atualização

O parâmetro `general_logging` do Amazon RDS está ativado

Descrição

O registro em log geral é ativado para a instância de banco de dados. Essa configuração é útil para solucionar problemas no banco de dados. No entanto, ativar o registro em log geral aumenta a quantidade de operações de E/S e o espaço de armazenamento alocado, o que pode causar contenção e degradação da performance.

Confira os requisitos para uso do registro em log geral. 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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

c1qf5bt037

Critérios de alerta

Amarelo: grupos de parâmetros do banco de dados têm `general_logging` ativado.

Recommended Action (Ação recomendada)

Confira os requisitos para uso do registro em log geral. 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
- Valores recomendados
- 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 do MySQL adie algumas gravações necessárias para manter índices secundários. Esse recurso foi útil em ambientes com discos lentos. A alteração na configuração do buffer melhorou um pouco a performance 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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

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 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
- Valores recomendados
- 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

 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

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
- Valores recomendados
- 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 causa 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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

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 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
- Valores recomendados
- 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

Out-of-memory mortes foram detectadas: 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
- Out-of-memory mortes (contagem)
- Trocas excessivas (contagem)
- Último período de detecção
- Hora da última atualização

O volume magnético do Amazon RDS está em uso

Descrição

As 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 provisionadas.

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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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

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 provisionadas.

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
- Valores recomendados
- 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 a 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

 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

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
- Valores recomendados
- Hora da última atualização

O parâmetro de cache de consulta do Amazon RDS está ativado

Descrição

Quando as alterações exigirem que o cache de consultas seja limpo, a 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 definir 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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

c1qf5bt022

Crítérios 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 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
- Valores recomendados
- 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 executar a 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

 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

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

- Valores recomendados
- 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 aceitos. Recomendamos atualizar 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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

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:

- [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
- Valores recomendados
- Hora da última atualização

Recursos do Amazon RDS usando a edição final do mecanismo de suporte sob licença incluída

Descrição

Recomendamos atualizar a versão principal para a versão mais recente do mecanismo aceita pelo Amazon RDS para continuar com o suporte de licença atual. A versão do mecanismo do 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

 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

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 atualizar o 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
- Valores recomendados
- 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 recurso alias encaminha as consultas de DNS para um AWS recurso (por exemplo, um balanceador de carga do Elastic Load Balancing ou um bucket do Amazon S3) ou para outro conjunto de registros de recursos do Route 53. Quando você usa conjuntos de registros de recursos de alias, o Route 53 encaminha suas consultas de DNS para AWS recursos gratuitamente.

As zonas hospedadas criadas por AWS serviços não aparecerão nos resultados da sua 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).

Você também precisa alterar o tipo de registro de CNAME para A ou AAAA, dependendo do AWS recurso. 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

[Roteamento de consultas para recursos 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 AWS Lambda funções que foram invocadas pelo menos uma vez durante o período de retrospectiva. 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

ID da verificação

C0r6dfpM06

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 Lambda subprovisionadas quanto ao tamanho da memória segue as melhores práticas. 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 [Opte por receber Trusted Advisor cheques 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

AWS Lambda Funções sem limite de simultaneidade configurado

Descrição

Verifica se AWS Lambda as funções estão configuradas com limite de execução simultânea 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 reservada usando os `ConcurrencyLimitHigh` e `ConcurrencyLimitLow` 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

ID da verificação

c18d2gz181

Origem

AWS Config Regra 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
- AWS Config Regra
- Parâmetros de entrada
- Hora da última atualização

Problemas de alto risco do AWS Well-Architected em relação à performance

Descrição

Verifica se há problemas de alto risco (HRIs) em suas cargas de trabalho no pilar de desempenho. 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

ID da verificação

Wxdfp4B1L2

Critérios de alerta

- Vermelho: Pelo menos um problema ativo de alto risco foi identificado no pilar de desempenho do AWS Well-Architected.
- Verde: nenhum problema ativo de alto risco foi detectado no pilar de desempenho 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 identificados HRIs para desempenho
- Número de HRIs resolvidos para desempenho
- Número de perguntas respondidas para performance
- Número total de perguntas no pilar de performance
- Hora da última atualização

CloudFront Nomes de domínio alternativos

Descrição

Note

Essa verificação se aplica às CloudFront distribuições clássicas da Amazon.

Verifica se o DNS está configurado corretamente nas CloudFront distribuições clássicas da Amazon que usam nomes de domínio alternativos ()CNAMEs.

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 de DNS para rotear consultas de DNS para a CloudFront distribuição; consulte [Usando 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

Note

Essa verificação se aplica às CloudFront distribuições clássicas da Amazon.

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 Amazon EC2 de alta utilização da CPU

Descrição

Verifica as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) que estavam em execução a qualquer momento nos 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

ZRxQ1Psb6c

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

- [Monitorando a 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

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 [Visualizando AWS Security Hub controles em 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

- [Grupo de segurança do Application Load Balancer](#)
- [Período de retenção do Amazon CloudWatch Log Group](#)
- [Fim do suporte às EC2 instâncias da Amazon com Microsoft SQL Server](#)
- [Fim do suporte às EC2 instâncias da Amazon com Microsoft Windows Server](#)
- [Fim do suporte padrão para EC2 instâncias da Amazon 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](#)
- [Protocolo criptografado de grupos-alvo do Application Load Balancer](#)

- [AWS Backup Cofre sem política baseada em recursos para evitar a exclusão de pontos de recuperação](#)
- [AWS CloudTrail Registro](#)
- [AWS CloudTrail Registro de eventos de gerenciamento](#)
- [AWS Lambda Funções usando tempos de execução obsoletos](#)
- [Problemas de alto risco do AWS Well-Architected em relação à segurança](#)
- [CloudFront Certificados SSL personalizados no IAM Certificate Store](#)
- [CloudFront Certificado SSL no servidor de origem](#)
- [Segurança do ELB Listener](#)
- [Grupos de segurança do Classic Load Balancer](#)
- [Exposed Access Keys](#)
- [Alternância da chave de acesso do IAM](#)
- [Acesso externo ao IAM Access Analyzer](#)
- [Política de senha do IAM](#)
- [Provedor de identidade IAM SAML 2.0](#)
- [MFA na conta raiz](#)
- [Chave de acesso do usuário raiz](#)
- [Grupos de segurança - Portas específicas irrestritas](#)
- [Grupos de Segurança - Acesso Irrestrito](#)

Grupo de segurança do Application Load Balancer

Descrição

Verifica os grupos de segurança vinculados ao Application Load Balancer e seus alvos na Amazon EC2 . Os grupos de segurança do Application Load Balancer só devem permitir portas de entrada configuradas em um ouvinte. Os grupos de segurança de um alvo não devem aceitar conexões diretas da Internet na mesma porta em que o alvo recebe tráfego do balanceador de carga.

Se um grupo de segurança permitir acesso a portas que não estão configuradas para o balanceador de carga ou permite acesso direto aos alvos, o risco de perda de dados ou ataques maliciosos aumenta.

Essa verificação exclui os seguintes grupos:

- Grupos de destino que não estão associados a endereços IP ou EC2 instâncias.
- Regras do grupo de segurança para IPv6 tráfego.

 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

ID da verificação

8604e947f2

Critérios de alerta

- Vermelho: o Target tem um IP público e um grupo de segurança que permite conexões de entrada na porta de tráfego de qualquer lugar (0.0.0.0/0).
- Vermelho: O Application Load Balancer tem a autenticação ativada e o destino permite conexões de entrada na porta de tráfego de qualquer lugar (0.0.0.0/0).
- Amarelo: o grupo de segurança do Target permite conexões de entrada na porta de tráfego de qualquer lugar (0.0.0.0/0).
- Amarelo: o grupo de segurança Application Load Balancer permite conexões de entrada em portas que não têm um ouvinte correspondente.
- Verde: o grupo de segurança do Application Load Balancer só permite conexões de entrada em portas que correspondam a um ouvinte.

Recommended Action (Ação recomendada)

Para melhorar a segurança, certifique-se de que seus grupos de segurança permitam apenas os fluxos de tráfego necessários:

- Os grupos de segurança do Application Load Balancer devem permitir conexões de entrada somente para as mesmas portas configuradas em seus ouvintes.
- Use grupos de segurança exclusivos para balanceadores de carga e destinos.

- Os grupos de segurança de destino devem permitir conexões na porta de tráfego somente dos balanceadores de carga aos quais estão associados.

Recursos adicionais

- [Controle o tráfego para seus recursos da AWS usando grupos de segurança](#)
- [Grupos de segurança para o Application Load Balancer](#)

Colunas do relatório

- Status
- Região
- Grupo de destino
- Nome do ALB
- ID DE LABORATÓRIO
- ID do SG de destino
- Autenticação ativada
- Hora da última atualização

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 `MinRetentionTime` parâmetros `LogGroupName` 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

ID da verificação

c18d2gz186

Origem

AWS Config Managed Rule: cw-loggroup-retention-period-check

Crítérios 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 às EC2 instâncias da Amazon com Microsoft SQL Server

Descrição

Verifica as versões do SQL Server para 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

ID da verificação

Qsdfp3A4L3

Critérios de alerta

- Vermelho: uma EC2 instância tem uma versão do SQL Server que chegou ao fim do suporte.
- Amarelo: uma EC2 instância tem uma versão do SQL Server que chegará ao fim do 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 na 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 na Amazon EC2, considere o Programa de End-of-Support Migração (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 às EC2 instâncias da Amazon com Microsoft Windows Server

Descrição

Essa verificação alerta se suas versões do Microsoft SQL estão próximas ou chegaram ao fim do suporte. Cada versão do Windows Server oferece 10 anos de suporte, incluindo 5 anos de suporte principal e 5 anos de suporte estendido. Após o fim do suporte, a versão do Windows Server não receberá atualizações de segurança regulares. A execução de aplicativos com versões incompatíveis do Windows Server pode trazer riscos de segurança ou conformidade.

Note

Essa verificação gera resultados com base na AMI usada para iniciar a EC2 instância. É possível que o sistema operacional da instância atual seja diferente da AMI de lançamento. Por exemplo, se você executou uma instância de uma AMI do Windows

Server 2016 e depois atualizou para o Windows Server 2019, a AMI de inicialização não muda.

 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

ID da verificação

Qsdfp3A4L4

CrITÉRIOS de alerta

- Vermelho: uma EC2 instância tem uma versão do Windows Server que chegou ao fim do suporte (Windows Server 2003, 2003 R2, 2008 e 2008 R2).
- Amarelo: uma EC2 instância 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:

- Atualize a versão do Windows Server
- Parada forçada e início após a atualização
- Se estiver usando o EC2 Config, migre para o Launch EC2

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 EC2 instâncias da Amazon 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.

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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

ID da verificação

c1dfprch15

Critérios de alerta

Vermelho: uma EC2 instância da Amazon 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 EC2 instância da Amazon 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 EC2 instâncias da Amazon estão em conformidade.

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 [Suporte](#).

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 Linux não incluem uma versão do stunnel que suporte recursos TLS por padrão. Se você estiver usando uma distribuição Linux incompatível (consulte [Distribuições suportadas](#) no Guia do usuário do Amazon Elastic File System), é uma prática recomendada atualizá-la 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. Para compartilhar um instantâneo somente com usuários ou contas específicos, marque o instantâneo 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, use 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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

Amarelo: 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
- Valores recomendados
- 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 da Amazon Elastic Compute Cloud (Amazon EC2) ou de um endereço IP específico.

Note

[Essa verificação avalia somente grupos de segurança vinculados às instâncias do Amazon RDS executadas externamente em uma Amazon VPC.](#)

ID da verificação

nNauJisYIT

Critérios de alerta

- Amarelo: uma regra de grupo de segurança de banco de dados faz referência a um grupo de EC2 segurança da Amazon que concede acesso global em uma dessas portas: 20, 21, 22, 1433, 1434, 3306, 3389, 4333, 5432, 5500.
- Vermelho: uma regra de grupo de segurança de banco de dados concede acesso global (o sufixo da regra CIDR é /0).
- Verde: um grupo de segurança de banco de dados não inclui regras permissivas.

Recommended Action (Ação recomendada)

EC2-Classic foi aposentado em 15 de agosto de 2022. É recomendável mover suas instâncias do Amazon RDS para uma VPC e usar grupos de segurança da EC2 Amazon. Para obter mais informações sobre como mover sua instância de banco de dados para uma VPC, consulte [Como mover uma instância de banco de dados que não esteja em uma VPC para uma VPC](#).

Se você não conseguir migrar suas instâncias do Amazon RDS para uma VPC, revise 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 DBSecurity GroupIngress API [Authorize](#) 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

 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:

- [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 do [Amazon S3](#) com registros CNAME. URLs

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 registro MX, verifica se há um registro TXT associado que contém um valor SPF válido. O valor do registro TXT deve começar com "v=spf1". Os tipos de registro SPF foram descontinuados pela Internet Engineering Task Force (IETF). Com o Route 53, é uma prática recomendada usar um registro TXT em vez de um registro SPF. Trusted Advisor relata essa verificação como verde quando um registro MX tem pelo menos um registro TXT associado com um valor SPF válido.

ID da verificação

c9D319e7sG

Critérios de alerta

- Verde: um conjunto de registros de recurso MX tem um registro de recurso TXT que contém um valor SPF válido.
- Amarelo: um conjunto de registros de recurso MX tem um registro de recurso TXT ou SPF que contém um valor SPF válido.
- Vermelho: um conjunto de registros de recurso MX não tem um registro de recurso TXT ou SPF que contenha um valor 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

- [Tipo de registro MX](#)
- [Tipo de registro SPF](#)
- [Orientação do re:POST](#)
- [RFC 7208](#)

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

Pfx0RwqB1i

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.
- Verde: Todos os Amazon S3 são compatíveis com base na política de ACL e/ou bucket.

Recommended Action (Ação recomendada)

Se um bucket permitir acesso aberto, determine se o acesso aberto é realmente necessário. Por exemplo, para hospedar um site estático, você pode usar CloudFront a Amazon para servir o conteúdo hospedado no Amazon S3. Consulte [Restringir o acesso a uma origem do Amazon S3](#) no CloudFront Amazon Developer Guide. Quando possível, 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)

[Definindo configurações de bloqueio de acesso público para seus buckets 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 de VPC têm a resolução DNS ativada tanto para o aceitante quanto para o solicitante. VPCs

A resolução de DNS para uma conexão de emparelhamento de VPC permite a resolução de nomes de host DNS públicos para endereços IPv4 privados quando consultados em sua VPC. Isso permite o uso de nomes DNS para comunicação entre recursos em VPCs peering. 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 a VPC IDs usando os parâmetros 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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 tanto para o aceitante quanto para o solicitante em VPCs uma conexão de emparelhamento de 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

Protocolo criptografado de grupos-alvo do Application Load Balancer

Descrição

Verifica se os grupos-alvo do Application Load Balancer (ALB) estão usando o protocolo HTTPS para criptografar a comunicação em trânsito para tipos de instância ou IP de destino de back-end. As solicitações HTTPS entre o ALB e os destinos de back-end ajudam a manter a confidencialidade dos dados em trânsito.

ID da verificação

c2v1fg0p1w

Critérios de alerta

- Amarelo: grupo-alvo do Application Load Balancer usando HTTP.
- Verde: grupo-alvo do Application Load Balancer usando HTTPS.

Recommended Action (Ação recomendada)

Configure os tipos de destino de instância ou IP de back-end para oferecer suporte ao acesso HTTPS e altere o grupo de destino para usar o protocolo HTTPS para criptografar a comunicação entre ALB e os tipos de instância ou IP de destino de back-end.

Recursos adicionais

[Imponha a criptografia em trânsito](#)

[Tipos de destino do Application Load Balancer](#)

[Configuração de roteamento do Application Load Balancer](#)

[Proteção de dados no Elastic Load Balancing](#)

Colunas do relatório

- Status
- Região
- Braço ALB
- Nome do ALB
- ID de VPC do ALB
- Grupo-alvo Arn
- Nome do grupo-alvo
- Protocolo do grupo de destino
- 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 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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 CloudTrail Registro de eventos de gerenciamento

Descrição

Verifica seu uso de AWS CloudTrail. CloudTrail fornece maior visibilidade da atividade em sua Conta da AWS. Isso é feito registrando informações sobre as 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 da AWS (o padrão ao criar uma nova trilha), a trilha aparecerá várias vezes no Trusted Advisor relatório.

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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

ID da verificação

c25hn9x03v

Critérios de alerta

- Vermelho: Nenhuma trilha foi criada para uma Região da AWS, ou o registro não está habilitado para nenhuma trilha.

- Amarelo: CloudTrail está ativado, mas todas as trilhas relatam erros de entrega do registro.
- Verde: CloudTrail está ativado e nenhum erro de entrega de log é relatado.

Recommended Action (Ação recomendada)

Para criar uma trilha e começar a registrar no console, abra o [AWS CloudTrail console](#).

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 anexada 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)
- [Criando uma trilha para uma organização](#)

Colunas do relatório

- Status
- Região
- Registro ativado
- Erro de entrega relatado
- Hora da última atualização

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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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 se há problemas de alto risco (HRIs) em suas cargas de trabalho no pilar de 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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 identificados HRIs para segurança
- Número de HRIs 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

Note

Essa verificação se aplica às CloudFront distribuições clássicas da Amazon.

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. Os certificados criptografados usando o algoritmo de hash SHA-1 estão sendo descontinuados pela maioria dos 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)

Recomendamos usar AWS Certificate Manager para provisionar, gerenciar e implantar seus certificados de servidor. Com o ACM, você pode solicitar um novo certificado ou implantar um ACM existente ou um certificado externo nos recursos. AWS Os certificados fornecidos pelo ACM são gratuitos e podem ser renovados automaticamente. Para obter mais informações sobre o ACM, consulte o [AWS Certificate Manager Guia do usuário do](#) . Para verificar se o Regiões da AWS ACM oferece suporte, consulte [AWS Certificate Manager endpoints](#) e cotas no. Referência geral da AWS

Renove certificados expirados ou que estão prestes a expirar. Para obter mais informações sobre a renovação de um certificado, consulte [Gerenciamento de certificados de servidor](#) no IAM.

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)

[Importar certificados](#)

[AWS Certificate Manager Guia do usuário](#)

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 a 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

Crítérios 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 clássicos com ouvintes que não usam as configurações de segurança recomendadas para comunicação criptografada. AWS recomenda que você use um protocolo seguro (HTTPS ou SSL), políticas up-to-date de segurança e cifras e protocolos seguros. Quando você usa um protocolo seguro para uma conexão front-end (cliente para balanceador de carga), as solicitações são criptografadas entre seus clientes e o balanceador de carga. Isso cria um ambiente mais seguro. O Elastic Load Balancing fornece políticas de segurança predefinidas com cifras e protocolos que aderem às práticas recomendadas de segurança da AWS. Novas versões de políticas predefinidas são lançadas à medida que novas configurações se tornam disponíveis.

ID da verificação

a2sEc6ILx

Critérios de alerta

- Vermelho: um balanceador de carga não tem ouvintes configurados com um protocolo seguro (HTTPS).
- Amarelo: um ouvinte HTTPS do balanceador de carga é configurado com uma política de segurança que contém uma cifra fraca.

- Amarelo: um ouvinte HTTPS do balanceador de carga não está configurado com a Política de Segurança recomendada.
- Verde: um balanceador de carga tem pelo menos um ouvinte HTTPS E todos os ouvintes HTTPS estão configurados com a política recomendada.

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 Classic Load Balancer

Descrição

Verifica se há balanceadores de carga configurados com um grupo de segurança que permite acesso a portas que não estão configuradas para o balanceador de carga.

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.
- Verde: as regras de entrada de um grupo de segurança da Amazon VPC associado a um balanceador de carga não permitem acesso a portas que não estão definidas na configuração do ouvinte do 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](#)
- [Migre seu Classic Load Balancer](#)
- [Configure Your Classic Load Balancer](#) (Configurar o Classic Load Balancer)

Colunas do relatório

- Status
- Região
- Nome do balanceador de carga
- Grupo de segurança IDs
- Motivo

Exposed Access Keys

Descrição

Verifica os repositórios de código populares em busca de chaves de acesso que foram expostas ao público e do uso irregular do Amazon Elastic Compute Cloud EC2 (Amazon) 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 ou EC2 instâncias comprometidas. Em última análise, você é responsável pela segurança e proteção de suas chaves de acesso e AWS recursos.

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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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

12Fnkp18Y5

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 EC2 uso irregular da Amazon 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 EC2 instâncias da Amazon, solicitações de instâncias 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

Acesso externo ao IAM Access Analyzer

Descrição

Verifica se o acesso externo do IAM Access Analyzer no nível da conta está presente.

Os analisadores de acesso externo do IAM Access Analyzer ajudam a identificar recursos em suas contas que são compartilhados com uma entidade externa. O analisador então cria um painel centralizado com as descobertas. Depois que o novo analisador for ativado no console do IAM, as equipes de segurança poderão priorizar quais contas revisar com base em permissões excessivas. Um analisador de acesso externo cria descobertas de acesso público e entre contas para recursos e é fornecido sem custo adicional.

ID da verificação

07602fcad6

Critérios de alerta

- Vermelho: o acesso externo do analisador não está ativado no nível da conta.
- Verde: o acesso externo do analisador é ativado no nível da conta.

Recommended Action (Ação recomendada)

A criação de um analisador de acesso externo por conta ajuda as equipes de segurança a priorizar quais contas revisar com base em permissões excessivas. Para obter mais informações, consulte [Introdução às AWS Identity and Access Management Access Analyzer descobertas](#).

Além disso, é uma prática recomendada utilizar o analisador de acesso não utilizado, um recurso pago que simplifica a inspeção do acesso não utilizado para orientá-lo a obter o menor privilégio.

Para obter mais informações, consulte [Identificação do acesso não utilizado concedido aos usuários e funções do IAM](#).

Recursos adicionais

- [Como usar o AWS Identity and Access Management Access Analyzer](#)
- [Atualizações do IAM Access Analyzer: encontre acessos não utilizados, verifique as políticas antes da implantação](#)

Colunas do relatório

- Status
- Região
- Analisador de acesso externo de conta Arn
- Analisador de acesso externo da organização Arns
- Hora da última atualização

Política de senha 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

Yw2K9puPz1

Critérios de alerta

- Verde: uma política de senha é ativada com o requisito de conteúdo recomendado ativado.
- Amarelo: uma política de senha está habilitada, mas pelo menos um requisito de conteúdo não está habilitado.

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).

Para acessar o AWS Management Console, os usuários do IAM precisam de senhas. Como prática recomendada, AWS é altamente recomendável que, em vez de criar usuários do IAM, você use a federação. A federação permite que os usuários usem suas credenciais corporativas existentes para fazer login no AWS Management Console. Use o IAM Identity Center para criar ou federar o usuário e, em seguida, assumir uma função do IAM em uma conta.

Para saber mais sobre provedores de identidade e federação, consulte [Provedores de identidade e federação](#) no Guia do usuário do IAM. Para saber mais sobre o IAM Identity Center, consulte o [Guia do usuário do IAM Identity Center](#).

Recursos adicionais

[Gerenciamento de senhas](#)

Colunas do relatório

- Política de senha
- Letras maiúsculas
- Letras minúsculas
- Número
- Não alfanuméricos

Provedor de identidade IAM SAML 2.0

Descrição

Verifica se o Conta da AWS está configurado para acesso por meio de um provedor de identidade (IdP) compatível com SAML 2.0. Certifique-se de seguir as melhores práticas ao centralizar identidades e configurar usuários em um [provedor de identidade externo](#) ou. [AWS IAM Identity Center](#)

ID da verificação

c2v1fg0p86

Critérios de alerta

- Amarelo: essa conta não está configurada para acesso por meio de um provedor de identidade (IdP) compatível com SAML 2.0.
- Verde: Essa conta está configurada para acesso por meio de um provedor de identidade (IdP) compatível com SAML 2.0.

Recommended Action (Ação recomendada)

Ative o IAM Identity Center para Conta da AWS o. Para obter mais informações, consulte [Habilitando o IAM Identity Center](#). Depois de ativar o IAM Identity Center, você pode realizar tarefas comuns, como criar um conjunto de permissões e atribuir acesso aos grupos do Identity Center. Para obter mais informações, consulte [Tarefas comuns](#).

É uma prática recomendada gerenciar usuários humanos no IAM Identity Center. Mas você pode ativar o acesso de usuários federados com o IAM para usuários humanos em curto prazo para implantações de pequena escala. Para obter mais informações, consulte [Federação SAML 2.0](#).

Recursos adicionais

[O que é o Centro de identidade do IAM?](#)

[O que eu sou?](#)

Colunas do relatório

- Status
- Conta da AWS Identificação
- Hora da última atualização

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

 Note

Para sua conta AWS Organizations de gerenciamento, a AWS exige autenticação multifator (MFA) para o usuário raiz ao acessar o AWS Management Console.

Para suas contas de AWS Organizations membros, a AWS recomenda o uso da MFA. Além de aplicar o MFA, se você usar AWS Organizations para gerenciar várias contas, poderá aplicar um SCP para restringir o acesso ao usuário raiz da conta membro. Para obter mais informações, consulte [Práticas recomendadas para contas de membros](#) no Guia AWS Organizations do usuário.

ID da verificação

7DAFEemoDos

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).

Você pode ativar o MFA em sua conta a qualquer momento acessando a página de Credenciais de Segurança. Para fazer isso, escolha o menu suspenso da conta no AWS Management Console. A AWS oferece suporte a várias formas padrão do setor de MFA, como FIDO2 autenticadores virtuais. Isso dá a flexibilidade de escolher um dispositivo de MFA que atenda às suas necessidades. É uma prática recomendada registrar mais de um dispositivo de MFA para fins de resiliência no caso de um de seus dispositivos de MFA ser perdido ou parar de funcionar.

Recursos adicionais

Consulte [as etapas gerais para ativar dispositivos de MFA e Habilitar um dispositivo de MFA virtual para Conta da AWS seu usuário raiz \(console\) no Guia do usuário do IAM](#) para obter informações adicionais.

Chave de acesso do usuário raiz

Descrição

Verifica se a chave de acesso do usuário root está presente. É altamente recomendável que você não crie pares de chaves de acesso para seu usuário root. Como [apenas algumas tarefas exigem o usuário raiz](#) e você normalmente executa essas tarefas com pouca frequência, é uma prática recomendada fazer login no AWS Management Console para realizar as tarefas do usuário raiz. Antes de criar chaves de acesso, analise as [alternativas às chaves de acesso de longo prazo](#).

ID da verificação

c2v1fg0f4h

Critérios de alerta

Vermelho: a chave de acesso do usuário root está presente

Verde: a chave de acesso do usuário raiz não está presente

Recommended Action (Ação recomendada)

Exclua a (s) chave (s) de acesso do usuário root. Consulte [Excluindo chaves de acesso para o usuário root](#). Essa tarefa deve ser executada pelo usuário root. Não é possível executar essas etapas como usuário ou perfil do IAM.

Recursos adicionais

[Tarefas que exigem credenciais de usuário root](#)

[Redefinindo uma senha de usuário root perdida ou esquecida](#)

Report columns (Colunas do relatório)

- Status
- ID da conta
- Hora da última atualização

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 somente os grupos de segurança que você cria e suas regras de entrada para IPv4 endereços. Os grupos de segurança criados por AWS Directory Service são marcados como vermelhos ou amarelos, mas não representam um risco de segurança e podem ser excluídos. Para obter mais informações, consulte as [Perguntas frequentes sobre o Trusted Advisor](#).

ID da verificação

HCP4007jGY

Critérios de alerta

- Verde: o Security Group fornece acesso irrestrito às portas 80, 25, 443 ou 465.
- Vermelho: o grupo de segurança está conectado a um recurso e fornece acesso irrestrito às portas 20, 21, 22, 1433, 1434, 3306, 3389, 4333, 5432 ou 5500.
- Amarelo: o Security Group fornece acesso irrestrito a qualquer outra porta.
- Amarelo: o Grupo de Segurança não está vinculado a nenhum recurso e fornece acesso 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.

Revise e exclua grupos de segurança não utilizados. Você pode usar AWS Firewall Manager para configurar e gerenciar centralmente grupos de segurança em Contas da AWS grande escala. Para obter mais informações, consulte a [AWS Firewall Manager documentação](#).

Considere usar o Systems Manager Sessions Manager para acesso SSH (porta 22) e RDP (porta 3389) às instâncias. EC2 Com o gerenciador de sessões, você pode acessar suas EC2 instâncias sem habilitar as portas 22 e 3389 no grupo de segurança.

Recursos adicionais

- [Grupos EC2 de segurança da Amazon](#)
- [List of TCP and UDP port numbers](#) (Lista de números de portas TCP e UDP)
- [Classless Inter-Domain Routing](#) (Roteamento sem classe entre domínios)
- [Trabalhando com o Session Manager](#)
- [AWS Firewall Manager](#)

Colunas do relatório

- Status
- Região
- Nome do grupo de segurança
- ID do grupo de segurança
- Protocolo
- Porta de origem
- Porta de destino
- Associação

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 somente os grupos de segurança que você cria e suas regras de entrada para IPv4 endereços. Os grupos de segurança criados por AWS Directory Service são marcados como vermelhos ou amarelos, mas não representam um risco de segurança e podem ser excluídos. Para obter mais informações, consulte as [Perguntas frequentes sobre o Trusted Advisor](#).

ID da verificação

1iG5NDGVre

Critérios de alerta

- Verde: uma regra de grupo de segurança tem um endereço IP de origem com um sufixo /0 para as portas 25, 80 ou 443.
- Amarelo: uma regra de grupo de segurança tem um endereço IP de origem com um sufixo /0 para portas diferentes de 25, 80 ou 443 e o grupo de segurança está anexado a um recurso.
- 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 e o grupo de segurança não está vinculado a um recurso.

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.

Revise e exclua grupos de segurança não utilizados. Você pode usar AWS Firewall Manager para configurar e gerenciar centralmente grupos de segurança em Contas da AWS grande escala. Para obter mais informações, consulte a [AWS Firewall Manager documentação](#).

Considere usar o Systems Manager Sessions Manager para acesso SSH (porta 22) e RDP (porta 3389) às instâncias. EC2 Com o gerenciador de sessões, você pode acessar suas EC2 instâncias sem habilitar as portas 22 e 3389 no grupo de segurança.

Recursos adicionais

- [Grupos EC2 de segurança da Amazon](#)
- [Classless Inter-Domain Routing](#) (Roteamento sem classe entre domínios)
- [Trabalhando com o Session Manager](#)
- [AWS Firewall Manager](#)

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
- Associação

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 DynamoDB Point-in-time](#)

- [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 o ELB Health Check ativado](#)
- [O Amazon EC2 Auto Scaling Group tem o rebalanceamento de capacidade ativado](#)
- [O Amazon EC2 Auto Scaling não está implantado em vários AZs ou não atende ao número mínimo de AZs](#)
- [Saldo da zona de EC2 disponibilidade da Amazon](#)
- [Monitoramento EC2 detalhado da Amazon não ativado](#)
- [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](#)
- [ElastiCache Backup automático de clusters \(Redis OSS\)](#)
- [Clusters multi-AZ do Amazon MemoryDB](#)
- [Agentes do Amazon MSK que hospedam muitas partições](#)
- [Cluster Amazon MSK Multi-AZ](#)
- [Domínios do Amazon OpenSearch Service com menos de três nós de dados](#)
- [Amazon RDS Backups](#)
- [Backup contínuo do Amazon RDS não ativado](#)
- [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](#)
- [Auto Scaling disponível em sub-redes IPs](#)
- [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 Resiliência de localização](#)
- [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 Outposts Implantação de rack único](#)
- [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](#)
- [AWS STS uso global de endpoints em Regiões da AWS](#)
- [Problemas de alto risco do AWS Well-Architected em relação à confiabilidade](#)
- [O Classic Load Balancer não tem vários configurados AZs](#)
- [CLB Connection Draining](#)
- [Desequilíbrio da meta do ELB](#)
- [GWLB - independência do endpoint AZ](#)
- [Otimização do Load Balancer](#)
- [Independência da AZ do NAT Gateway](#)
- [Endpoint de Firewall de Rede AZ Independence](#)
- [Firewall de Rede Multi-AZ](#)
- [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 vários 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

ID da verificação

c1dfprch08

Critérios de alerta

Amarelo: ALB está em um único AZ.

Verde: o ALB tem dois 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 `BacktrackWindowInHours` parâmetro 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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

`xuy7H1avt1`

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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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

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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusionAPI](#) para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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
- Zona de disponibilidade
- DB Cluster Identifier
- ARN do cluster de banco de dados
- Hora da última atualização

Recuperação do Amazon DynamoDB Point-in-time

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 [Point-in-time recuperação para o 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

ID da verificação

c18d2gz138

Origem

AWS Config Managed Rule: dynamodb-pitr-enabled

Critérios de alerta

Amarelo: Point-in-time a recuperação 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 [Point-in-time Recuperação: Como funciona](#).

Recursos adicionais

[Point-in-time recuperação para o 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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 AWS Backupé](#)

[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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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 AWS Backupé](#)

[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 dos seus volumes do Amazon EBS (disponíveis ou em uso). Falhas podem ocorrer mesmo se os volumes do Amazon EBS forem replicados. Os snapshots são mantidos no 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).

Para automatizar a criação de snapshots do EBS, você pode considerar usar o [Amazon Data Backup Lifecycle Manager](#).

Recursos adicionais

[Amazon Elastic Block Store \(Amazon EBS\)](#)

[Snapshots do Amazon EBS](#)

[AWS Backup](#)

[Amazon Data Lifecycle Manager](#)

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 o ELB Health Check ativado

Descrição

Verifica se seus grupos do Amazon EC2 Auto Scaling associados a um Classic Load Balancer estão usando as verificações de saúde do Elastic Load Balancing. As verificações de saúde padrão para um grupo do Auto Scaling são somente verificações de EC2 status da Amazon. Se uma instância falhar nessas verificações de status, ela será marcada como não íntegra e será encerrada. O Amazon EC2 Auto Scaling lança uma nova instância substituta. A verificação de integridade do Elastic Load Balancing monitora periodicamente as EC2 instâncias da Amazon 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

ID da verificação

c18d2gz104

Origem

AWS Config Managed Rule: autoscaling-group-elb-healthcheck-required

Critérios de alerta

Amarelo: o grupo Amazon EC2 Auto Scaling vinculado ao Classic Load Balancer não habilitou as verificações de saúde 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 Amazon EC2 Auto Scaling Group tem o rebalanceamento de capacidade ativado

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 da EC2 Amazon 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

ID da verificação

AWS Config c18d2gz103

Origem

AWS Config Regra gerenciada: autoscaling-capacity-rebalancing

Critérios de alerta

Amarelo: o rebalanceamento de capacidade de grupos do Amazon EC2 Auto Scaling não está habilitado.

Recommended Action (Ação recomendada)

Certifique-se de que o rebalanceamento de capacidade esteja habilitado para seus 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 vários AZs ou não atende ao número mínimo de AZs

Descrição

Verifica se o grupo Amazon EC2 Auto Scaling está implantado em várias zonas de disponibilidade ou no número mínimo de zonas de disponibilidade especificado. Implante EC2 instâncias da Amazon em várias zonas de disponibilidade para garantir alta disponibilidade.

Você pode ajustar o número mínimo de zonas de disponibilidade usando o `minAvailabilityZones` parâmetro 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 Amazon EC2 Auto Scaling não tem vários AZs configurados ou não atende ao número mínimo especificado. AZs

Recommended Action (Ação recomendada)

Certifique-se de que seu grupo Amazon EC2 Auto Scaling esteja configurado com vários. AZs Implante EC2 instâncias da Amazon em várias zonas de disponibilidade para garantir 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 EC2 disponibilidade da Amazon

Descrição

Verifica a distribuição das instâncias do Amazon Elastic Compute Cloud (Amazon EC2) entre as zonas de disponibilidade em 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 EC2 instâncias da Amazon uniformemente em 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](#)
- [Grupos de posicionamento para suas EC2 instâncias da Amazon](#)
- [Tipos de EC2 instância da Amazon](#)

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 EC2 detalhado da Amazon não ativado

Descrição

Verifica se o monitoramento detalhado está habilitado para suas EC2 instâncias da Amazon.

O monitoramento EC2 detalhado da Amazon fornece métricas mais frequentes, publicadas em intervalos de um minuto, em vez dos intervalos de cinco minutos usados no monitoramento básico da Amazon. EC2 Habilitar o monitoramento detalhado da Amazon EC2 ajuda você a gerenciar melhor seus EC2 recursos da Amazon, para que você possa encontrar tendências e agir 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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 EC2 instâncias da Amazon.

Recommended Action (Ação recomendada)

Ative o monitoramento detalhado de suas EC2 instâncias da Amazon para aumentar a frequência com que os dados EC2 métricos da Amazon são publicados na Amazon CloudWatch (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

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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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 bloqueadora para não bloqueadora. 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 a conectividade de rede barata e de baixa latência entre os AZs mesmos. Região da AWS Ao iniciar instâncias AZs em várias na mesma região, você pode ajudar a proteger seus aplicativos contra 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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 tarefas diferentes AZs.

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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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 vários AZs aumentam a disponibilidade ElastiCache do 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, o ElastiCache 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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 ElastiCache \(Redis OSS\)](#) com o Multi-AZ.

Colunas do relatório

- Status
- Região
- Nome do cluster
- Hora da última atualização

ElastiCache Backup automático de clusters (Redis OSS)

Descrição

Verifica se os clusters Amazon ElastiCache (Redis OSS) 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 `snapshotRetentionPeriod` parâmetros de suas AWS Config regras.

Para obter mais informações, consulte [Backup e restauração para ElastiCache \(Redis OSS\)](#).

 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

ID da verificação

c18d2gz178

Origem

AWS Config Managed Rule: `elasticache-redis-cluster-automatic-backup-check`

Critérios de alerta

Vermelho: os clusters da Amazon ElastiCache (Redis OSS) 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 (Redis OSS) 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 para ElastiCache \(Redis OSS\)](#).

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 vários AZs aprimoram a disponibilidade do cluster MemoryDB por meio da replicação 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, 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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

Cluster Amazon MSK Multi-AZ

Descrição

Verifica o número de zonas de disponibilidade (AZs) do seu cluster provisionado do Amazon MSK. O cluster Amazon MSK é formado por vários corretores que trabalham juntos e distribuem os dados e a carga. A produção pode ser interrompida durante problemas de manutenção ou intermediação em um cluster 2-AZ.

ID da verificação

90046ff5b5

Critérios de alerta

- Amarelo: o cluster Amazon MSK é provisionado com corretores em apenas dois AZs
- Verde: o cluster Amazon MSK é provisionado com corretores em três ou mais AZs

Recommended Action (Ação recomendada)

Para aumentar a disponibilidade do cluster, você pode criar outro cluster em uma AZs configuração 3. Em seguida, migre o cluster existente para o novo cluster que você criou. Você pode usar a replicação do Amazon MSK para essa migração.

Recursos adicionais

[Alta disponibilidade do Amazon MSK](#)

[Migração do Amazon MSK](#)

Colunas do relatório

- Status
- Região
- ARN do cluster MSK
- Número de AZs
- Hora da última atualização

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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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

Backup contínuo do Amazon RDS não ativado

Descrição

Verifica se uma instância do Amazon RDS está habilitada com backups automatizados usando o Amazon RDS ou com backups contínuos do AWS Backup. Os backups contínuos reduzem o risco de perda inesperada de dados e permitem a point-in-time recuperação.

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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

ID da verificação

44fde09ab5

CrITÉRIOS de alerta

- Vermelho: a instância não tem backup automático habilitado no Amazon RDS nem backup contínuo em AWS Backup.
- Vermelho: As versões do MySQL abaixo de 5.6 não oferecem suporte a backup automático ou contínuo. Para fornecer resiliência, primeiro atualize a versão do banco de dados e, em seguida, habilite o backup automático ou contínuo.
- Verde: a instância tem o backup automático habilitado no Amazon RDS.
- Verde: a instância tem o backup contínuo ativado em AWS Backup.

Recommended Action (Ação recomendada)

Certifique-se de que as instâncias do Amazon RDS tenham o backup automático configurado definindo um período de retenção maior que 0 no Amazon RDS ou criando um plano de backup contínuo usando AWS Backup.

Recursos adicionais

- [Conceitos básicos do Amazon RDS](#)
- [Gerenciando backups automatizados](#)
- [Introdução aos backups](#)
- [Backups e point-in-time restauração contínuos \(PITR\)](#)
- [AWS Backup disponibilidade de recursos](#)

Colunas do relatório

- Status
- Região
- DB Instance Identifier
- ARN da instância de banco de dados
- Tipo de implantação
- Tipo de backup
- Motivo
- Hora da última atualização

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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

 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 que você distribua a instância primária e as instâncias do leitor em seu cluster de banco de dados em várias AZs para melhorar a disponibilidade do seu 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

 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
- Valores recomendados
- 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

 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 [Preço](#).

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 diminuiu abaixo de um limite operacionalmente razoável.

ID da verificação

Cmsvnj8db2

Critérios de alerta

- Vermelho: FreeStorageSpace tem menos de 10% da capacidade total
- FreeStorageSpace Amarelo: está entre 10% e 20% da capacidade total

- Verde: FreeStorageSpace é mais de 20% 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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
- Valores recomendados
- 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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: os 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
- Valores recomendados
- 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

 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
- Valores recomendados
- 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

 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
- Valores recomendados
- 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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 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 `TrueIfReplicaModeGravavel`.

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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

 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 `TruelfReplica`

Recursos adicionais

O parâmetro `read_only` controla a permissão de gravação dos clientes em uma instância de banco de dados. O valor padrão desse parâmetro é `TruelfReplica`. Para uma instância de réplica, `TruelfReplica` define o valor `read_only` como `ON (1)` e desativa qualquer atividade de gravação dos clientes. Para uma instância mestre/gravadora, `TruelfReplica` define 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
- Valores recomendados
- 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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 os 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:

- [Habilitando backups automatizados](#)
- [Desmistificando os custos de armazenamento de backup do Amazon RDS](#)

Colunas do relatório

- Status
- Região
- Recurso
- Valores recomendados
- 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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
- Valores recomendados
- 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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 problemas recentes que resultam em atrasos ocasionais replaced/launched replica instances from older backups and these replicas requiring substantial time to “catch-up” to the primary database instance and live transactions. This ReplicaLag may dwindle over time as catch-up occurs. Another example could be that the

transaction velocity able to be achieved on the primary database instance is higher than the replication process or replica infrastructure is able to match. This ReplicaLag may grow over time as replication fails to keep pace with the primary database performance. Finally, the workload may be bursty throughout different periods of the day/month/etc 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

 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

- Valores recomendados
- 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. Você não pode desativar instantâneos automatizados para tipos de RA3 nós.

Você pode especificar o período de retenção mínimo e máximo desejado usando o `MaxRetentionPeriod` parâmetro `MinRetentionPeriod` 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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 obter 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 um TTL longo, os resolvedores de DNS demoram mais para solicitar registros DNS atualizados, o que pode causar atrasos desnecessários no redirecionamento do tráfego (por exemplo, quando o DNS Failover detecta e responde a uma falha em um de seus endpoints). Essa verificação examina somente os registros com uma política de Failover ou se há uma verificação de integridade associada.

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.
- Verde: um registro de recurso não tem política de failover ou tem uma política de failover com um TTL menor que 60.

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, onde **###** 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 ver se há redundância. Uma AZ é um local distinto, isolado de falhas em outras zonas. Ao especificar endereços IP em vários AZs na mesma região, você pode ajudar a proteger seus aplicativos contra 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 dois 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 do 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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 facilmente 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 `minAvailabilityZones` parâmetros 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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

Auto Scaling disponível em sub-redes IPs

Descrição

Verifica se há disponibilidade IPs suficiente entre as sub-redes de destino. Ter IPs disponibilidade suficiente 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 saúde do Elastic Load Balancing não for usada, o Auto Scaling só poderá agir sobre a integridade da instância do Amazon Elastic Compute Cloud (EC2Amazon). 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 dos recursos associados às suas configurações de lançamento, modelos de lançamento e seus grupos de Auto Scaling.

Grupos de Auto Scaling que apontam para recursos indisponíveis não podem lançar novas instâncias do Amazon Elastic Compute Cloud (Amazon) EC2. Quando configurado corretamente, o Auto Scaling faz com que o número de EC2 instâncias da Amazon aumente sem problemas durante picos de demanda e diminua automaticamente durante quedas de demanda. Grupos de Auto Scaling e configurações/modelos de lançamento do Auto Scaling que apontam para recursos indisponíveis não funcionam conforme o esperado.

ID da verificação

8CNsS11I5v

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.
- Vermelho: um modelo de lançamento está associado a uma Amazon Machine Image (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 Auto Scaling ou crie um novo grupo de 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 uma nova configuração de execução ou versão do modelo de execução usando uma AMI válida e associe-a a um grupo do Auto Scaling. Para obter informações sobre como criar uma nova configuração de lançamento, consulte [Criar uma configuração de lançamento no Guia](#) do usuário do Amazon EC2 Auto Scaling. Para obter informações sobre como criar um modelo de lançamento, consulte [Criar um modelo de lançamento para um grupo de Auto Scaling](#) no Guia do usuário do Amazon Auto EC2 Scaling.

 Note

Por motivos de segurança, os resultados da verificação não incluem nenhum recurso referenciado usando AWS Systems Manager parâmetros no modelo de lançamento.

Se seus modelos de lançamento incluírem um AWS Systems Manager parâmetro que inclua uma ID de imagem de máquina da Amazon (AMI), revise o modelo de execução para garantir que os parâmetros façam referência a uma ID de AMI válida ou faça as alterações apropriadas no armazenamento de AWS Systems Manager parâmetros. Para obter mais informações, consulte [Usar AWS Systems Manager parâmetros em vez de AMI IDs](#) no Guia do usuário do Amazon EC2 Auto Scaling.

Recursos adicionais

- [Solução de problemas do Auto Scaling: Amazon EC2 AMIs](#)
- [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](#)
- [Use AWS Systems Manager parâmetros em vez de AMI IDs](#)

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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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

[Práticas recomendadas para AWS CloudHSM](#)

Colunas do relatório

- Status
- Região
- ID do cluster
- Número de instâncias do HSM
- Hora da última atualização

AWS Direct Connect Resiliência de localização

Descrição

Verifica a resiliência do AWS Direct Connect usado para conectar seu local a cada gateway Direct Connect ou gateway privado virtual.

Essa verificação alerta se algum gateway Direct Connect ou gateway privado virtual não estiver configurado com interfaces virtuais em pelo menos dois locais distintos do Direct Connect. A falta de resiliência do local pode resultar em tempo de inatividade inesperado durante a manutenção, corte de fibra, falha do dispositivo ou falha total do local.

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.

Note

O Direct Connect é implementado com o Transit Gateway usando o gateway Direct Connect.

ID da verificação

c1dfpnchv2

Critérios de alerta

Vermelho: O gateway Direct Connect ou gateway privado virtual é configurado com uma ou mais interfaces virtuais em um único dispositivo Direct Connect.

Amarelo: o gateway Direct Connect ou gateway privado virtual é configurado com interfaces virtuais em vários dispositivos Direct Connect em um único local do Direct Connect.

Verde: O gateway Direct Connect ou gateway privado virtual é configurado com interfaces virtuais em dois ou mais locais distintos do Direct Connect.

Recommended Action (Ação recomendada)

Para criar resiliência de localização do Direct Connect, você pode configurar o gateway Direct Connect ou o gateway privado virtual 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 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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 Outposts Implantação de rack único

Descrição

Verifica o saldo do Outposts Racks. Isso avalia se as instâncias do Outposts de um cliente estão implantadas em vários Outposts Racks ou em um único Outpost Rack. Um único rack Outposts cria um único ponto de falha para problemas que envolvem um único rack (por exemplo, falhas ambientais). Esses cenários podem ser mitigados com a implantação de postos avançados em vários racks.

ID da verificação

c243hjzrh

Critérios de alerta

- Amarelo: Seu posto avançado é implantado em um único rack
- Verde: Seu Posto Avançado está distribuído em vários racks.

Recommended Action (Ação recomendada)

Se você estiver executando cargas de trabalho de produção em AWS Outposts, é uma prática recomendada usar a seguinte arquitetura resiliente. Um único AWS Outposts rack cria um único ponto de falha. Considere adicionar um segundo AWS Outposts rack a esse local com capacidade suficiente para um evento de failover e depois distribuir as cargas de trabalho entre os racks.

Recursos adicionais

[Modo de falha 4: racks ou data centers](#)

Colunas do relatório

- Status
- Atributo ARN
- AZ
- Número de racks
- 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

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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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

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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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

AWS STS uso global de endpoints em Regiões da AWS

Descrição

Essa verificação identifica um risco de resiliência quando as AWS cargas de trabalho fazem chamadas entre regiões para o endpoint global STS na região Leste dos EUA (Norte da Virgínia). AWS cargas de trabalho que fazem solicitações entre regiões para o endpoint global STS no Leste dos EUA (Norte da Virgínia) podem ser afetadas negativamente se a conectividade com o endpoint STS do Leste dos EUA (Norte da Virgínia) for afetada.

Em abril de 2025, AWS aprimorou o endpoint global para atender automaticamente às chamadas de endpoint global STS na mesma região em que suas cargas de trabalho em execução AWS, para todas Regiões da AWS habilitadas por padrão. No entanto, algumas cargas de trabalho, como aquelas executadas em regiões opcionais ou aquelas que não usam servidores Amazon DNS, não se beneficiam da redução da latência e do [isolamento de falhas](#) oferecidos como parte desse aprimoramento. Para essas cargas de trabalho, as solicitações globais de endpoint STS são atendidas na região Leste dos EUA (Norte da Virgínia), representando um risco de resiliência para seu aplicativo e aumentando a latência das solicitações de STS.

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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

ID da verificação

c15m0mg1d3

Critérios de alerta

Vermelho: As cargas de trabalho estão fazendo chamadas entre regiões para o endpoint AWS STS global na região Leste dos EUA (Norte da Virgínia).

Ação recomendada

Para melhorar a resiliência e o desempenho de suas cargas de trabalho, recomendamos que você migre do endpoint global do STS para o endpoint regional do STS. Ao usar um endpoint regional, você pode usar AWS STS na mesma região que suas cargas de trabalho.

A seguir está uma lista de diretores AWS Identity and Access Management (IAM) que fazem chamadas entre regiões para o endpoint AWS STS global na região Leste dos EUA (Norte da Virgínia). Seguindo as etapas na postagem do blog [Como usar AWS STS endpoints regionais](#), você pode reconfigurar suas cargas de trabalho para usar o endpoint STS regional.

Status	ARN da entidade principal	Tipo principal do IAM	Ação	Hora da última atualização	Região de origem
Vermelha	arn:aws:iam::999999999:função/exemplo	Função	AssumeRole	01/01/2025 ÀS 08:00.000 Z	ca-west-1
Vermelha	arn:aws:iam::123456789012:usuário/JohnDoe	Usuário	GetCallerIdentity	01/01/2025 ÀS 08:00.000 Z	ca-west-1
Vermelha	arn:aws:sts::123456789012:usuário	Usuário federado	GetCallerIdentity	01/01/2025 ÀS 08:00.000 Z	eu-west-2

Status	ARN da entidade principal	Tipo principal do IAM	Ação	Hora da última atualização	Região de origem
	federado/ <Name>				
Vermelha	arn: aws: iam: 123456789 012: root	Raiz	AssumeRole	01/01/2025 ÀS 08:00.000 Z	il-central-1
Vermelha	arn: aws:sts: :0123456789012: assumido-0123456789 exemplo role/aws:ec2-instance/i	EC2 Função de identidade da instância	GetCaller Identity	01/01/2025 ÀS 08:00.000 Z	us-west-1

Recursos adicionais

- [Gerencie AWS STS em um Região da AWS](#)
- [AWS STS Endpoints regionais](#)

Colunas do relatório

- Status
- Diretor Arn
- Ação
- Tipo da entidade principal
- Região de origem
- Hora da última atualização

Problemas de alto risco do AWS Well-Architected em relação à confiabilidade

Descrição

Verifica problemas de alto risco (HRIs) para suas cargas de trabalho no pilar de 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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 identificados HRIs para confiabilidade
- Número de HRIs 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 vários configurados AZs

Descrição

Verifica se o Classic Load Balancer abrange várias zonas de disponibilidade (). AZs

Um balanceador de carga distribui o tráfego de entrada do aplicativo em várias EC2 instâncias da Amazon em várias 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 `minAvailabilityZones` parâmetro 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

ID da verificação

c18d2gz154

Origem

AWS Config Managed Rule: clb-multiple-az

CrITÉRIOS de alerta

Amarelo: O Classic Load Balancer não tem o Multi-AZ configurado ou não atende ao número mínimo especificado. AZs

Recommended Action (Ação recomendada)

Certifique-se de que seus Classic Load Balancers tenham várias zonas de disponibilidade configuradas. Distribua seu balanceador de carga em vários AZs para garantir que você tenha alta disponibilidade do seu aplicativo.

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

CLB Connection Draining

Descrição

Verifica se há balanceadores de carga clássicos que não têm a drenagem de conexão ativada.

Quando a drenagem da conexão não está ativada e você cancela o registro de uma EC2 instância da Amazon em um balanceador de carga clássico, o balanceador de carga clássico interrompe o roteamento do tráfego para essa instância e fecha a conexão. Quando a drenagem da conexão está ativada, o balanceador de carga clássico para de enviar novas solicitações para a instância cancelada, mas mantém a conexão aberta para atender às solicitações ativas.

ID da verificação

7qGXsKIUw

Critérios de alerta

- Amarelo: a drenagem da conexão não está habilitada para um balanceador de carga clássico.
- Verde: a drenagem da conexão está ativada para o balanceador de carga clássico.

Recommended Action (Ação recomendada)

Ative a drenagem da conexão para o balanceador de carga Classic. 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

Desequilíbrio da meta do ELB

Descrição

Verifica a distribuição alvo dos grupos-alvo nas zonas de disponibilidade (AZs) para Application Load Balancer (ALB), Network Load Balancer (NLB) e Gateway Load Balancer (GWLB).

Essa verificação exclui o seguinte:

- Balanceadores de carga configurados com uma única zona de disponibilidade (AZ).

- Balanceadores de carga em que a diferença no número de destinos entre os mais e os menos preenchidos AZs é igual ou menor que 1.
- Grupos-alvo com alvos baseados em IP em que o AvailabilityZone atributo está definido como “todos”.

ID da verificação

b92b83d667

Critérios de alerta

- Vermelho: uma única AZ representa mais de 66% da capacidade do balanceador de carga.
- Amarelo: uma única AZ representa mais de 50% da capacidade do balanceador de carga.
- Verde: Não AZs representa mais de 50% da capacidade do balanceador de carga.

Recommended Action (Ação recomendada)

Para uma melhor resiliência, certifique-se de que seus grupos-alvo tenham o mesmo número de alvos. AZs

Recursos adicionais

[Grupos de destino para seus Application Load Balancers](#)

[Registre alvos com seu grupo-alvo do Application Load Balancer](#)

Colunas do relatório

- Status
- Região
- Nome do balanceador de carga
- Tipo de Load Balancer
- Grupo-alvo ARN (arn)
- Diferença nas metas registradas em AZs
- Hora da última atualização

GWLB - independência do endpoint AZ

Descrição

Verifica se seus endpoints do Gateway Load Balancer (GWLB) estão configurados como destino de rota de outra zona de disponibilidade (AZ).

Os endpoints do Gateway Load Balancer encaminham o tráfego da rede para dispositivos de firewall atrás de um Gateway Load Balancer para inspeção. Cada endpoint do Gateway Load Balancer opera dentro de uma AZ designada e é construído com redundância somente nessa AZ. Portanto, todos os recursos em uma determinada AZ devem usar um endpoint do Gateway Load Balancer na mesma AZ. Isso garante que qualquer possível interrupção de um endpoint do Gateway Load Balancer ou de sua AZ não afete seus recursos em outra AZ.

ID da verificação

528d6f5ee7

Critérios de alerta

- Amarelo: o tráfego da sua sub-rede em uma AZ está sendo roteado por meio de um endpoint do Gateway Load Balancer em outra AZ.
- Verde: o tráfego da sua sub-rede em uma AZ está sendo roteado por meio de um endpoint do Gateway Load Balancer na mesma AZ.

Recommended Action (Ação recomendada)

Verifique a AZ da sua sub-rede e configure sua tabela de rotas para rotear o tráfego por meio de um endpoint do Gateway Load Balancer na mesma AZ.

Se não houver um endpoint do Gateway Load Balancer na AZ, crie um novo e direcione seu tráfego de sub-rede por ele.

Se você tiver a mesma tabela de rotas associada entre sub-redes em diferentes AZs, mantenha essa tabela de rotas associada às sub-redes que residem na mesma AZ do endpoint do Gateway Load Balancer. Para sub-redes na outra AZ, você pode então associar uma tabela de rotas separada a uma rota para um endpoint do Gateway Load Balancer nesta AZ.

É uma prática recomendada escolher uma janela de manutenção para mudanças de arquitetura em sua Amazon VPC.

Recursos adicionais

- [Independência da zona de disponibilidade](#)
- [Configurar o roteamento para o endpoint do Gateway Load Balancer](#)
- [AWS Well-Architected Tool - Use arquiteturas de anteparo para limitar o escopo do impacto](#)

Colunas do relatório

- Status
- Região

- Lista de IDs de sub-rede Cross AZ
- ID do endpoint do Gateway Load Balancer
- ID de sub-rede do endpoint do Gateway Load Balancer
- Sub-rede AZ do VPC Endpoint
- Hora da última atualização

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 executar um número igual de instâncias em várias zonas de disponibilidade em 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 EC2 instâncias da Amazon registradas com um balanceador de carga são 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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 entre 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

Endpoint de Firewall de Rede AZ Independence

Descrição

Verifica se seus AWS Network Firewall endpoints estão configurados como um destino de rota de outra zona de disponibilidade (AZ).

Os endpoints do Firewall de Rede encaminham o tráfego da rede para um Firewall de Rede para inspeção. Cada endpoint do Network Firewall opera dentro de uma AZ designada e é construído com redundância somente nessa AZ. Seus recursos em uma determinada AZ devem usar um endpoint do Network Firewall na mesma AZ. Isso garante que qualquer possível interrupção de um endpoint do Network Firewall ou de sua AZ não afete seus recursos em outra AZ. O tráfego de rede que se origina em uma AZ diferente para inspeção de tráfego incorre em cobranças de transferência de dados entre AZ. É uma prática recomendada garantir que todos os recursos em uma AZ específica usem um Network Firewall na mesma AZ para evitar cobranças de dados entre AZ.

ID da verificação

7040ea389a

Critérios de alerta

- Amarelo: o tráfego de uma sub-rede em uma AZ está sendo roteado por meio de um endpoint do Network Firewall em outra AZ.
- Verde: o tráfego de uma sub-rede em uma AZ está sendo roteado por meio de um endpoint do Network Firewall na mesma AZ.

Recommended Action (Ação recomendada)

Verifique a AZ da sua sub-rede e roteie o tráfego por meio de um endpoint do Firewall de Rede na mesma AZ.

Se não houver um endpoint de Firewall de Rede no AZ, crie um novo Firewall de Rede e direcione seu tráfego de sub-rede por ele.

Se a mesma tabela de rotas estiver associada a várias sub-redes em diferentes AZs, mantenha essa tabela de rotas associada às sub-redes que residem na mesma AZ do endpoint do Firewall de Rede. Para sub-redes em outras AZs, associe uma tabela de rotas separada a uma rota para um endpoint do Firewall de Rede nessa AZ.

É uma prática recomendada escolher uma janela de manutenção para mudanças de arquitetura em sua Amazon VPC.

Recursos adicionais

[Transferência de dados dentro do mesmo Região da AWS](#)

[Entendendo as taxas de transferência de dados](#)

[Independência da zona de disponibilidade](#)

[Etapas de alto nível para implementar um firewall](#)

[Criando um firewall](#)

[AWS Well-Architected Tool - Use arquiteturas de anteparo para limitar o escopo do impacto](#)

Colunas do relatório

- Status
- Região
- ID do endpoint do Firewall de Rede
- Braço de Firewall de Rede
- Sub-rede de endpoint do Firewall de Rede
- Firewall de Rede Endpoint AZ
- Lista de sub-redes Cross AZ
- Hora da última atualização

Firewall de Rede Multi-AZ

Descrição

Verifica se seus firewalls de rede estão configurados para usar mais de uma zona de disponibilidade (AZ) para endpoints de firewall.

Uma AZ é um local distinto, isolado de falhas em outras zonas. Se o endpoint do Firewall de Rede for implantado em apenas 1 AZ, ele poderá ser um único ponto de falha e prejudicar as cargas de trabalho de outras pessoas que usam o Firewall de AZs Rede para inspeção de tráfego. É uma prática recomendada configurar seus firewalls de rede em vários AZs na mesma região para melhorar a disponibilidade da carga de trabalho.

ID da verificação

c2v1fg0gqd

CrITÉRIOS de alerta

- Amarelo: o endpoint do Network Firewall é implantado em 1 AZ.
- Verde: os endpoints do Network Firewall são implantados em pelo menos dois. AZs

Recommended Action (Ação recomendada)

Certifique-se de que seu Firewall de Rede esteja configurado com pelo menos duas AZs para cargas de trabalho de produção.

Recursos adicionais

[Configuração de sub-rede VPC para AWS Network Firewall](#)

[Criando um firewall](#)

[Zona de disponibilidade](#)

[AWS Well-Architected Tool - Implante a carga de trabalho em vários locais](#)

[Dispositivo em uma VPC de serviços compartilhados](#)

Colunas do relatório

- Status
- Região
- Braço de Firewall de Rede
- Id da VPC

- Sub-redes do Firewall de Rede
- Sub-redes do Firewall de Rede AZs
- 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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 vários 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

ID da verificação

c1dfprch09

CrITÉRIOS de alerta

Amarelo: o NLB está em um único AZ.

Verde: o NLB tem dois 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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 por vários AZs, você limita o raio de explosão de uma falha no 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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 a conectividade de rede barata e de baixa latência entre a mesma AZs AWS região. 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

ID da verificação

c1dfprch10

CrITÉrios de alerta

Amarelo: o VPC endpoint est em uma nica AZ.

Verde: o VPC endpoint est em pelo menos dois. AZs

Recommended Action (Ao recomendada)

Certifique-se de que seu endpoint de interface VPC esteja configurado com pelo menos duas zonas de disponibilidade.

Recursos adicionais

Para obter mais informaes, consulte a seguinte documentao do :

- [Acesse e AWS service \(Servio da AWS\) use uma interface VPC endpoint](#)
- [Endereo IP privado da interface de rede do endpoint](#)
- [AWS PrivateLink conceitos](#)
- [Regies e zonas de disponibilidade](#)

Colunas do relatrio

- Status
- Regio
- ID do VPC Endpoint
-  Multi AZ
- Hora da ltima atualizao

Redundncia de tnel da VPN

Descrio

Verifica o nmero de tneis ativos para cada um dos seus. Site-to-Site VPNs

Uma VPN sempre deve ter dois tneis configurados. Isso fornece redundncia em caso de interrupo ou manuteno planejada dos dispositivos no endpoint AWS . Para alguns hardware, apenas um tnel fica ativo de cada vez. Se uma VPN no tiver tneis ativos, as cobranas da

VPN ainda poderão ser aplicadas. Para obter mais informações, consulte o [Guia do usuário do AWS Site-to-Site 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 [Seu dispositivo de gateway do cliente](#) ou [Excluir uma conexão Site-to-Site VPN](#).

Recursos adicionais

- [AWS Site-to-Site Guia do usuário da VPN](#)
- [Crie um gateway de destino](#)

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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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: não Trusted Advisor foi possível recuperar a utilização ou os limites em um 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 pode abrir 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 agregado de volume SSD de IOPS provisionadas do EBS \(io1\)](#)
- [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](#)
- [EC2 Instâncias sob demanda](#)
- [EC2 Concessões de instâncias reservadas](#)
- [EC2-Endereços IP elásticos clássicos](#)
- [EC2-Endereço IP elástico da 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

fW7HH017J9

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

aW7HH017J9

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

gW7HH017J9

Recursos adicionais

[AWS CloudFormation cotas](#)

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

eI7KK017J9

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

dH7RR016J9

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

dH7RR016J3

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

cG7HH017J9

Recursos adicionais

[Amazon EBS limits](#) (Limites do Amazon EBS)

IOPS agregado de volume SSD de IOPS provisionadas do EBS (io1)

Descrição

Verifica o uso de mais de 80% da cota de IOPS agregada do volume EBS Provisioned IOPS SSD (io1).

ID da verificação

tV7YY017J9

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

gI7MM017J9

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

gI7MM017J2

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

wH7DD013J9

Recursos adicionais

[Amazon EBS limits](#) (Limites do Amazon EBS)

EC2 Instâncias sob demanda

Descrição

Verifica o uso de mais de 80% da cota de instâncias EC2 sob demanda.

ID da verificação

0Xc6LMYG8P

Recursos adicionais

[EC2 Cotas da Amazon](#)

EC2 Concessões de instâncias reservadas

Descrição

Verifica o uso de mais de 80% da cota de leasing da Instância EC2 Reservada.

ID da verificação

iH7PP017J9

Recursos adicionais

[EC2 Cotas da Amazon](#)

EC2-Endereços IP elásticos clássicos

Descrição

Verifica o uso de mais de 80% da cota EC2 de endereços IP elásticos clássicos.

ID da verificação

aW9HH018J6

Recursos adicionais

[EC2 Cotas da Amazon](#)

EC2-Endereço IP elástico da VPC

Descrição

Verifica o uso de mais de 80% da cota de endereço IP elástico EC2 -VPC.

ID da verificação

1N7RR017J9

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

EM8b3yLRTx

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

iK700017J9

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

sU7XX017J9

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

n07SS017J9

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

pR7UU017J9

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

oQ7TT017J9

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

rT7WW017J9

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

qS7VV017J9

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

bW7HH017J9

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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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 pode abrir 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

jt1IM03qZM

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

gfZAn3W7w1

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

3Njm0DJQ09

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

hJ7NN017J9

Recursos adicionais

[Amazon SES quotas](#) (Cotas do Amazon SES)

VPC

Descrição

Verifica o uso superior a 80% da cota da VPC.

ID da verificação

jL7PP017J9

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

kM7QQ017J9

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](#)
- [Amazon API Gateway REST APIs sem rastreamento de raio-X ativado](#)
- [Registro de CloudFront acesso da Amazon configurado](#)
- [A ação CloudWatch de alarme da Amazon está desativada](#)
- [EC2 Instância da Amazon não gerenciada por 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](#)
- [Logs de acesso do Amazon S3 habilitados](#)
- [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](#)
- [AWS CloudFormation Notificação de pilha](#)
- [AWS CloudTrail registro de eventos de dados para objetos em um bucket do S3](#)
- [AWS CodeBuild Registro do projeto](#)
- [AWS CodeDeploy Reversão automática e monitor ativados](#)
- [AWS CodeDeploy O Lambda está usando all-at-once a configuração de implantação](#)
- [AWS Elastic Beanstalk O Enhanced Health Reporting não está configurado](#)
- [AWS Elastic Beanstalk com as atualizações gerenciadas da plataforma desativadas](#)
- [AWS Fargate a versão da plataforma não é a mais recente](#)
- [AWS Systems Manager Associação de Gestores Estaduais 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 WebSocket REST ou rotas de API no Amazon API Gateway para coletar registros de execução em CloudWatch registros para solicitações recebidas por você 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 (ERROR, INFO) no parâmetro `loggingLevel` nas regras. 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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 para seu Amazon API Gateway [REST APIs](#) 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
- AWS Config Regra
- Parâmetros de entrada
- Hora da última atualização

Amazon API Gateway REST APIs sem rastreamento de raio-X ativado

Descrição

Verifica se o Amazon API Gateway REST APIs tem AWS X-Ray o rastreamento ativado.

Ative o rastreamento X-Ray para seu REST APIs para permitir que o API Gateway faça amostras de solicitações de invocação de API com informações de rastreamento. Isso permite que você aproveite para rastrear e analisar solicitações AWS X-Ray à medida que elas passam pelo REST do API Gateway APIs até os serviços downstream.

Para obter mais informações, consulte [Rastreando solicitações de usuários para REST APIs usando 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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 seu API Gateway APIs REST.

Para obter mais informações, consulte [Configuração AWS X-Ray com o API Gateway REST APIs](#).

Recursos adicionais

- [Rastreando solicitações de usuários para REST APIs usando X-Ray](#)
- [O que AWS X-Ray é](#)

Colunas do relatório

- Status
- Região
- Recurso
- AWS Config Regra
- 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

ID da verificação

c18d2gz110

Origem

AWS Config Managed Rule: cloudfront-accesslogs-enabled

Crítérios 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
- AWS Config Regra
- 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 o AWS CLI para ativar ou desativar o recurso de ação em seu alarme. Ou você pode desativar ou ativar 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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-actions](#) na Referência de AWS CLI comandos e [func \(*CloudWatch\) EnableAlarmActions](#) na Referência da AWS API SDK for Go.

Colunas do relatório

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

EC2 Instância da Amazon não gerenciada por AWS Systems Manager

Descrição

Verifica se as EC2 instâncias da Amazon em sua conta são gerenciadas por AWS Systems Manager.

O Systems Manager ajuda você a entender e controlar o estado atual da sua EC2 instância Amazon 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 [Como configurar o Systems Manager para EC2 instâncias](#).

 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

ID da verificação

c18d2gz145

Origem

AWS Config Managed Rule: ec2-instance-managed-by-systems-manager

Critérios de alerta

Amarelo: As EC2 instâncias da Amazon não são gerenciadas pelo Systems Manager.

Recommended Action (Ação recomendada)

Configure sua EC2 instância Amazon para ser gerenciada pelo Systems Manager.

Essa verificação não pode ser excluída da exibição no Trusted Advisor console.

Para obter mais informações, consulte [Por que minha EC2 instância não está sendo exibida como um nó gerenciado ou mostrando o status “Conexão perdida” no Systems Manager?](#).

Recursos adicionais

[Configurando o Systems Manager para EC2 instâncias](#)

Colunas do relatório

- Status
- Região
- Recurso
- AWS Config Regra
- 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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
- AWS Config Regra
- 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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
- AWS Config Regra
- 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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
- AWS Config Regra

- 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 registro deseja filtrar (erro, pesquisa, índice) usando o parâmetro logTypes em suas AWS Config regras.

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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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
- AWS Config Regra
- 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

 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

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 de gravador no 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
- Valores recomendados
- Nome do motor

- Hora da última atualização

O monitoramento aprimorado do Amazon RDS está desativado

Descrição

Os 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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

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
- Valores recomendados
- 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 ativar 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

 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

c1qf5bt012

Critérios de alerta

Amarelo: os recursos do Amazon RDS não têm o Performance Insights ativado.

Recommended Action (Ação recomendada)

Ative 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
- Valores recomendados
- 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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

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
- Valores recomendados
- 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 de bucket do Amazon S3 de registro desejado para corresponder ao parâmetro `bucketNames` de suas regras. 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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
- AWS Config Regra
- Parâmetros de entrada
- Hora da última atualização

Logs de acesso do Amazon S3 habilitados

Descrição

Verifica a configuração de registro dos buckets do Amazon Simple Storage Service.

A ativação do registro de acesso ao servidor fornece registros detalhados de acesso por hora a um bucket específico do Amazon S3. Os registros de acesso contêm detalhes da solicitação, incluindo tipo, recursos especificados e hora/data de processamento. O registro está desativado por padrão. Os clientes devem ativar o registro de acesso para realizar auditorias de segurança ou analisar o comportamento e os padrões de uso do usuário.

Quando o registro é ativado inicialmente, a configuração é validada automaticamente. No entanto, modificações futuras podem resultar em falhas de registro. Observe que, atualmente, essa verificação não examina as permissões de gravação no bucket do Amazon S3.

ID da verificação

c1fd6b9614

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 root, portanto, o Trusted Advisor não consegue verificá-la.
- Vermelho: o bucket de destino não existe.
- Vermelho: o bucket de destino e o bucket de origem têm proprietários diferentes.
- Verde: o bucket tem o registro de acesso ao servidor ativado, o destino existe e as permissões para gravar no destino existem

Recommended Action (Ação recomendada)

Ative o registro de acesso ao servidor para todos os buckets relevantes do Amazon S3. Os registros de acesso ao servidor fornecem uma trilha de auditoria que pode ser usada para entender os padrões de acesso ao bucket e investigar atividades suspeitas. A ativação do registro em todos os buckets aplicáveis melhorará a visibilidade dos eventos de acesso em todo o seu ambiente Amazon S3. 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 root e você quiser que o Trusted Advisor verifique o status do registro em log, adicione a conta root como beneficiária da concessão. 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).

Recursos adicionais

[Trabalhando com baldes](#)

[Server access logging \(Registro em log de acesso ao servidor\)](#)

[Formato de registro de acesso ao servidor](#)

[Excluindo arquivos de log](#)

Colunas do relatório

- Status
- Região
- Atributo ARN
- Nome do bucket
- Nome do destino
- O destino existe
- Mesmo proprietário
- Gravação habilitada
- Motivo
- 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, tópicos e funções do Amazon SQS. AWS Lambda

Você pode especificar o destino e os tipos de eventos desejados usando os parâmetros `destinationArn` e `eventTypes` de suas regras. 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

ID da verificação

c18d2gz163

Origem

AWS Config Managed Rule: s3-event-notifications-enabled

Critérios de alerta

Amarelo: o Amazon S3 não tem notificações de eventos habilitadas ou não está configurado com o destino 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
- AWS Config Regra
- 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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
- AWS Config Regra
- 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 AWS Config regras.

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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

ID da verificação

c18d2gz122

Origem

AWS Config Managed Rule: vpc-flow-logs-enabled

Critérios de alerta

VPCs Amarelo: não tem Amazon VPC Flow Logs.

Recommended Action (Ação recomendada)

Crie registros de fluxo de VPC para cada um dos seus VPCs

Para obter mais informações, consulte [Criar um log de fluxo](#)

Colunas do relatório

- Status
- Região
- Recurso
- AWS Config Regra
- 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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
- AWS Config Regra
- Parâmetros de entrada
- Hora da última atualização

AWS CloudFormation Notificação de pilha

Descrição

Verifica se todas as suas AWS CloudFormation pilhas usam o Amazon SNS para receber notificações quando ocorre um evento.

Você pode configurar essa verificação para procurar um tópico específico do Amazon SNS ARNs usando parâmetros em suas AWS Config regras.

Para obter mais informações, consulte [Configuração das opções AWS CloudFormation de pilha](#).

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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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 AWS CloudFormation pilhas não estão ativadas.

Recommended Action (Ação recomendada)

Certifique-se de que suas AWS CloudFormation pilhas usem o Amazon SNS para receber notificações quando um evento ocorrer.

O monitoramento de eventos da pilha ajuda você a responder rapidamente a ações não autorizadas que podem alterar seu AWS ambiente.

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
- AWS Config Regra
- Parâmetros de entrada
- Hora da última atualização

AWS CloudTrail registro de eventos de dados para objetos em um bucket do S3

Descrição

Verifica se pelo menos uma AWS CloudTrail trilha 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

ID da verificação

c18d2gz166

Origem

AWS Config Managed Rule: cloudtrail-s3-dataevents-enabled

Critérios de alerta

Amarelo: o registro de AWS CloudTrail eventos 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
- AWS Config Regra
- Parâmetros de entrada
- Hora da última atualização

AWS CodeBuild Registro do projeto

Descrição

Verifica se o ambiente AWS CodeBuild do projeto 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 ou grupo de CloudWatch registros do Amazon S3 para armazenar os registros, usando o parâmetro s3 BucketNames ou cloudWatchGroupNames em suas regras. AWS Config

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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

ID da verificação

c18d2gz113

Origem

AWS Config Managed Rule: codebuild-project-logging-enabled

CrITÉRIOS de alerta

Amarelo: o registro AWS CodeBuild do projeto não está ativado.

Recommended Action (Ação recomendada)

Certifique-se de que o registro esteja ativado em seu AWS CodeBuild projeto. Essa verificação não pode ser excluída da exibição no AWS Trusted Advisor console.

Para obter mais informações, consulte [Registro e monitoramento em AWS CodeBuild](#).

Colunas do relatório

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

AWS CodeDeploy Reversão automática e monitor ativados

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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

ID da verificação

c18d2gz114

Origem

AWS Config Managed Rule: codedeploy-auto-rollback-monitor-enabled

Critérios de alerta

Amarelo: a reversão AWS CodeDeploy automática da implantação e o monitoramento da implantação 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
- AWS Config Regra
- Parâmetros de entrada
- Hora da última atualização

AWS CodeDeploy O 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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
- AWS Config Regra
- Parâmetros de entrada
- Hora da última atualização

AWS Elastic Beanstalk O Enhanced Health Reporting não está configurado

Descrição

Verifica se um AWS Elastic Beanstalk ambiente está configurado para relatórios de integridade aprimorados.

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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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
- AWS Config Regra
- Parâmetros de entrada
- Hora da última atualização

AWS Elastic Beanstalk com as atualizações gerenciadas da plataforma desativadas

Descrição

Verifica se as atualizações de plataforma gerenciadas nos ambientes e modelos de configuração do Elastic Beanstalk estão habilitadas.

AWS Elastic Beanstalk lança regularmente atualizações de 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 `UpdateLevel` parâmetros 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

ID da verificação

c18d2gz177

Origem

AWS Config Managed Rule: elastic-beanstalk-managed-updates-enabled

Critérios de alerta

Amarelo: as atualizações AWS Elastic Beanstalk gerenciadas da plataforma não estão configuradas de forma 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
- AWS Config Regra
- Parâmetros de entrada
- Hora da última atualização

AWS Fargate a versão da plataforma 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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
- AWS Config Regra
- Parâmetros de entrada
- Hora da última atualização

AWS Systems Manager Associação de Gestores Estaduais em Status de Não Conformidade

Descrição

Verifica se o status da conformidade da AWS Systems Manager associação é COMPATÍVEL ou NÃO COMPATÍVEL após a execução da associação na instância.

O State Manager, um recurso do AWS Systems Manager, é um serviço de gerenciamento de configuração seguro e escalável que automatiza o processo de manter seus nós gerenciados e outros AWS recursos em um estado definido por você. Uma associação do State Manager é uma configuração que você atribui aos seus AWS recursos. A configuração define o estado que você deseja manter em seus recursos, por isso ajuda você a atingir a meta, como evitar desvios de configuração em suas instâncias da 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

ID da verificação

c18d2gz147

Origem

AWS Config Managed Rule: ec2-managedinstance-association-compliance-status-check

Critérios de alerta

Amarelo: o status da conformidade da AWS Systems Manager associação 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

[AWS Systems Manager State Manager](#)

Colunas do relatório

- Status
- Região
- Recurso
- AWS Config Regra
- 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 capturados AWS 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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
- AWS Config Regra
- 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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
- AWS Config Regra
- 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 Amazon Aurora e RDS para MySQL, RDS para MariaDB, RDS para Oracle, RDS para PostgreSQL e RDS para SQL Server em todas as regiões. 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

Recursos adicionais

[Proteção contra exclusão para clusters do Aurora.](#)

Colunas do relatório

- Status
- Região
- Recurso
- AWS Config Regra
- 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.

Para clientes Business, Enterprise On-Ramp ou Enterprise Support, você pode usar a [BatchUpdateRecommendationResourceExclusion](#) API para incluir ou excluir um ou mais recursos dos seus Trusted Advisor resultados.

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
- AWS Config Regra
- 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 uma verificação removida, como especificar o ID da verificação em uma operação de AWS Support API ou seu código, receberá erros de chamada de API. Remova essas verificações para evitar erros.

Para obter mais informações sobre as verificações disponíveis, consulte o [AWS Trusted Advisor verifique a referência](#).

Verificações novas e atualizadas

A seguir estão as verificações novas e atualizadas:

Nome da verificação	ID da verificação	Descrição
Recomendações de otimização de custos do Amazon Aurora para armazenamento em cluster de banco de dados	c1z7kmr17n	Novo cheque
AWS STS uso global de endpoints em Regiões da AWS	c15m0mg1d3	Verificação atualizada: essa verificação agora está disponível em todos os níveis do AWS Support plano.

Nova verificação - uso AWS STS global de endpoints em Regiões da AWS

A seguinte verificação foi adicionada:

Nome da verificação	ID da verificação	Descrição
AWS STS uso global de endpoints em Regiões da AWS	c15m0mg1d3	Novo cheque

Novas verificações do Cust Optimization Hub

AWS Trusted Advisor adicionou as seguintes Hub de Otimização de Custos da AWS verificações:

Verifique o nome	ID da verificação
Recomendações de compra de capacidade reservada do Amazon DynamoDB	c1z7kmr15n
Recomendações de otimização de custos do Amazon EBS para volumes	c1z7kmr02n
Recomendações de otimização de EC2 custos da Amazon para grupos do Amazon EC2 Auto Scaling	c1z7kmr01n
Recomendações EC2 de otimização de custos da Amazon para instâncias	c1z7kmr00n
Recomendações de compra de nós ElastiCache reservados da Amazon	c1z7kmr13n
Recomendações de compra de nós reservados do Amazon MemoryDB	c1z7kmr16n
Recomendações de compra de instâncias reservadas do Amazon OpenSearch Service	c1z7kmr14n
Recomendações de otimização de custos do Amazon RDS para armazenamento de instâncias de banco de dados	c1z7kmr04n

Verifique o nome	ID da verificação
Recomendações de otimização de custos do Amazon RDS para instâncias de banco de dados	c1z7kmr03n
Recomendações de compra de instâncias reservadas do Amazon RDS	c1z7kmr11n
Recomendações de compra de nós reservados do Amazon Redshift	c1z7kmr12n
AWS Fargate recomendações de otimização de custos para o Amazon ECS	c1z7kmr06n
AWS Lambda recomendações de otimização de custos para funções	c1z7kmr05n
AWS Recomendações de compra de Savings Plans para Amazon SageMaker AI	c1z7kmr08n
AWS Recomendações de compra da Savings Plans para computação	c1z7kmr09n

CloudFront verificações específicas revisadas

As seguintes verificações foram revisadas:

Nome da verificação	ID da verificação	Descrição
CloudFront Nomes de domínio alternativos	N420c450f2	Foi adicionada uma nota indicando que essa verificação se aplica às CloudFront distribuições clássicas da Amazon.

Nome da verificação	ID da verificação	Descrição
CloudFront Certificados SSL personalizados no IAM Certificate Store	N425c450f2	Foi adicionada uma nota indicando que essa verificação se aplica às CloudFront distribuições clássicas da Amazon.
CloudFront Encaminhamento de cabeçalho e taxa de acertos de cache	N415c450f2	Foi adicionada uma nota indicando que essa verificação se aplica às CloudFront distribuições clássicas da Amazon.

Verificações revisadas

As seguintes verificações foram revisadas:

Nome da verificação	ID da verificação
Otimização do modo throughput do Amazon EFS	c1dfprch02
Fim do suporte às EC2 instâncias da Amazon com Microsoft Windows Server	Qsdfp3A4L4

A descrição dessa verificação foi alterada. Para obter mais informações, consulte:

- [Fim do suporte às EC2 instâncias da Amazon com Microsoft Windows Server](#)

A descrição e a recomendação dessa verificação foram alteradas. Para obter mais informações, consulte:

- [Otimização do modo de taxa de transferência do Amazon EFS](#)

Verificações obsoletas AWS Security Hub

As seguintes AWS Security Hub verificações estão obsoletas:

Nome da verificação	ID da verificação
S3.10 - Os buckets de uso geral do S3 com versionamento ativado devem ter configurações de ciclo de vida	Hs4Ma3G211
S3.11 - Os buckets de uso geral do S3 devem ter as notificações de eventos ativadas	Hs4Ma3G212
CodeBuild.5 - os ambientes CodeBuild do projeto não devem ter o modo privilegiado ativado	Hs4Ma3G218
CloudFormation.1 - CloudFormation as pilhas devem ser integradas ao Amazon Simple Notification Service (SNS)	Hs4Ma3G245
SNS.2 - O registro do status de entrega deve ser ativado para mensagens de notificação enviadas para um tópico	Hs4Ma3G263
Athena.1 - Os grupos de trabalho do Athena devem ser criptografados em repouso	Hs4Ma3G294

Nova verificação: Amazon RDS Continuous Backup não habilitado

Trusted Advisor adicionou a seguinte verificação em 23 de dezembro de 2024.

Nome da verificação	Categoria da verificação	ID da verificação
Backup contínuo do Amazon RDS não ativado	Tolerância a falhas	44fde09ab5

Verifica se uma instância do Amazon RDS está habilitada com backups automatizados usando o Amazon RDS ou com backups contínuos do. AWS Backup Os backups contínuos reduzem o risco de perda inesperada de dados e permitem a point-in-time recuperação.

Para obter mais informações, consulte [Backup contínuo do Amazon RDS não ativado](#).

Nova verificação: Registro AWS CloudTrail de eventos de gerenciamento

Trusted Advisor adicionou a seguinte verificação em 23 de dezembro de 2024.

Nome da verificação	Categoria da verificação	ID da verificação
AWS CloudTrail Registro de eventos de gerenciamento	Segurança	c25hn9x03v

Verifica seu uso de AWS CloudTrail.

Para obter mais informações, consulte [AWS CloudTrail Registro de eventos de gerenciamento](#).

Atualização da verificação de recursos do grupo Auto Scaling

Trusted Advisor atualizou a seguinte verificação em 23 de dezembro de 2024.

Nome da verificação	Categoria da verificação	ID da verificação
Recursos do grupo do Auto Scaling	Tolerância a falhas	8CNsS11I5v

A descrição dessa verificação foi atualizada para incluir configurações e modelos de lançamento.

Um novo critério de alerta Red: A launch template is associated with a deleted Amazon Machine Image (AMI). foi adicionado.

Para obter mais informações, consulte [Recursos do grupo do Auto Scaling](#).

Atualização da verificação de acesso externo do IAM Access Analyzer

Trusted Advisor atualizou a seguinte verificação em 23 de dezembro de 2024.

Nome da verificação	Categoria da verificação	ID da verificação
Acesso externo ao IAM Access Analyzer	Segurança	07602fcad6

A descrição dessa verificação é atualizada para indicar que ela analisa o acesso do IAM no nível da conta. Para obter mais informações, consulte [Acesso externo ao IAM Access Analyzer](#).

Adicionado 1 novo cheque

Trusted Advisor adicionou 1 novo cheque em 22 de novembro de 2024:

- [8604e947f2 - Grupos de segurança do Application Load Balancer](#)

3 verificações atualizadas

Trusted Advisor 3 verificações atualizadas em 7 de novembro de 2024:

- [b92b83d667 - Desequilíbrio da meta do ELB](#)
- [8 CNs SLLI5v - Recursos do Auto Scaling Group](#)
- [WUY7G1zxQL - Equilíbrio da zona de disponibilidade da Amazon EC2](#)

Foram adicionadas 4 verificações

Trusted Advisor adicionou 4 novas verificações em 11 de outubro de 2024:

- 07602fcad6 - IAM Access Analyzer - acesso externo
- 528d6f5ee7 - GWLB - Ponto final AZ
- c2vlfg0jp6 - Endpoints de interface VPC inativos
- c2vlfg0k35 - Endpoints inativos do Load Balancer do Gateway

3 verificações atualizadas

Trusted Advisor 3 verificações atualizadas em 2 de outubro de 2024:

- O ID de verificação 7040ea389a passou do pilar Otimização de Custos para o pilar de Tolerância a Falhas
- ID de verificação atualizada: 7 DAFEmo dias
- ID de verificação atualizada cmSvnj8db2

Foram adicionados 9 novos cheques

Trusted Advisor adicionou 9 novos cheques em 23 de agosto de 2024:

- c2vlf0p86 - [IAM] - Provedor de identidade SAML 2.0
- 7040ea389a - Transferência de dados entre AZ do endpoint do Firewall de Rede
- c2vlf0bfbw - Firewall de rede de baixa utilização
- c2vlf0gqgd - Firewall de Rede Multi-AZ
- c2vlf0p1w - Protocolo criptografado do Application Load Balancer Target Groups
- c2vlf022t - [NAT Gateway] - Recurso subutilizado
- c243hjzrh - Implantação de rack único AWS Outposts
- b92b83d667 - Desequilíbrio da meta do ELB
- 90046ff5b5 - A disponibilidade do MSK é limitada a duas zonas

Para obter mais informações, consulte o [AWS Trusted Advisor verifique a referência](#).

Atualizou 1 verificação de segurança e adicionou 1 verificação de segurança

Trusted Advisor 1 verificações de excelência operacional atualizadas em 22 de agosto de 2024:

- c1fd6b96l4

Trusted Advisor adicionou 1 verificação de segurança em 22 de agosto de 2024:

- c2vlf0f4h

Para obter mais informações, consulte o [AWS Trusted Advisor verifique a referência](#).

6 verificações de segurança atualizadas

Trusted Advisor 6 verificações de segurança atualizadas em 20 de agosto de 2024:

- nNauJisYIT
- C9D319E7sg
- A2sec6 ILx
- HCP40,07 jGy
- 1iG5 NDGVre
- Yw2k9puPzl

Para obter mais informações, consulte o [AWS Trusted Advisor verifique a referência](#).

1 verificações de tolerância a falhas atualizadas

Trusted Advisor atualizou a 1 verificação de tolerância a falhas e 1 segurança em 12 de agosto de 2024:

- Redundância de túnel da VPN
- É necessário atualizar a versão secundária do mecanismo Amazon RDS

Para obter mais informações, consulte o [AWS Trusted Advisor verifique a referência](#).

9 cheques atualizados

Trusted Advisor atualizou as 9 verificações em 21 de julho de 2024:

- 7q GXs KIUw
- ZRxQIPsb6c
- N425c450f2
- 7 DAFEmo cães
- Pfx0 RwqBli
- H7 IgTzj TYb
- C056F80Cr3

- Yw2k9puPzl
- XSqx82FQu

Para obter mais informações, consulte o [AWS Trusted Advisor verifique a referência](#).

Foram removidas 5 verificações e adicionadas 1 cheque

Trusted Advisor descontinuaram 3 verificações de tolerância a falhas, 1 verificação de desempenho e 1 verificação de segurança em 15 de maio de 2024:

- Uso do IAM
- Balanceamento de carga entre zonas do ELB
- Volumes magnéticos do Amazon EBS utilizados em excesso
- Grande número de regras de grupo de EC2 segurança aplicadas a uma instância
- Grande número de regras em um grupo EC2 de segurança

Trusted Advisor adicionou 1 nova verificação de segurança em 15 de maio de 2024:

- Logs de acesso ao servidor Amazon S3 habilitados

Para obter mais informações, consulte o [AWS Trusted Advisor verifique a referência](#).

Verificações de tolerância a falhas removidas

Trusted Advisor verificação obsoleta de tolerância a falhas 3 em 25 de abril de 2024:

- AWS Direct Connect Redundância de conexão
- AWS Direct Connect Redundância de localização
- AWS Direct Connect Redundância de interface virtual

Para obter mais informações, consulte o [AWS Trusted Advisor verifique a referência](#).

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 o [AWS Trusted Advisor verifique a referência](#).

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 o [AWS Trusted Advisor verifique a referência](#).

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 o [AWS Trusted Advisor verifique a referência](#).

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 o [AWS Trusted Advisor verifique a referência](#).

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 o [AWS Trusted Advisor verifique a referência](#).

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 EC2 instâncias da Amazon com Ubuntu LTS

Para obter mais informações, consulte o [AWS Trusted Advisor verifique a referência](#).

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 o [AWS Trusted Advisor verifique a referência](#).

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 o [AWS Trusted Advisor verifique a referência](#).

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 o [AWS Trusted Advisor verifique a referência](#).

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 o [AWS Trusted Advisor verifique a referência](#).

Nova AWS Trusted Advisor API

AWS Trusted Advisor apresenta novidades APIs para permitir que você acesse programaticamente as verificações, recomendações e recomendações priorizadas de melhores práticas do Trusted Advisor. Trusted Advisor APIs permitem que você se integre programaticamente Trusted Advisor à sua ferramenta operacional preferida para automatizar e otimizar suas cargas de trabalho em grande escala. Disponível para clientes Business, Enterprise On-Ramp ou Enterprise Support, o novo APIs fornece 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.

O novo Trusted Advisor APIs substituirá as 3 funcionalidades oferecidas anteriormente por meio da AWS Support API (SAPI). A SAPI continuará oferecendo casos e outras informações de suporte.

Trusted Advisor 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 EC2	Segurança	Hs4Ma3G119

Nome da verificação	Categoria da verificação	ID da verificação
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 o [Exibir AWS Trusted Advisor cheques fornecidos por 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
- Auto Scaling disponível em sub-redes IPs
- 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](#)

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 AWS Config em uma região](#)
- [Meu controle está arquivado no Security Hub, mas ainda vejo as descobertas em 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 obter mais informações, consulte o [Guia do usuário do AWS Resilience Hub](#).

Para receber resultados Trusted Advisor para seus clusters ElastiCache e para o 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 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 Suporte API normalmente.

Para obter mais informações, consulte [Conceitos básicos das recomendações do Trusted Advisor](#).

Novos cheques para a Amazon EC2

Trusted Advisor adicionou a seguinte verificação em 1º de setembro de 2022.

- Fim do suporte às EC2 instâncias da Amazon com 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 [Visualizando AWS Security Hub controles em 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	C0r6dfpM03
Volumes subprovisionados do Amazon EBS	Performance	C0r6dfpM04
AWS Lambda funções superprovisionadas para o tamanho da memória	Otimização de custo	C0r6dfpM05
AWS Lambda funções subprovisionadas para o tamanho da memória	Performance	C0r6dfpM06

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 obter mais informações, consulte [Opte por receber Trusted Advisor cheques 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	12Fnkp18Y5

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 [Visualizando AWS Security Hub controles em AWS Trusted Advisor](#).

Novas verificações para Amazon EC2 e AWS Well-Architected

Trusted Advisor adicionou as seguintes verificações em 20 de dezembro de 2021.

- Consolidação de EC2 instâncias da Amazon para Microsoft SQL Server
- EC2 Instâncias da Amazon provisionadas em excesso para o Microsoft SQL Server
- Fim do suporte às EC2 instâncias da Amazon com 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 [Criação de CloudWatch alarmes da Amazon para monitorar métricas 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	dH7RR016J3

Nome da verificação	Categoria da verificação	ID da verificação
Armazenamento de volumes SSD de IOPS provisionadas (io2) do EBS	Limites do serviço	gI7MM017J2

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
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
EC2 Endereços IP elásticos	Limites do serviço	aW9HH018J6

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 para essas cinco verificações também são atualizados. Para obter mais informações, consulte [Criação de CloudWatch alarmes da Amazon para monitorar métricas 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	dH7RR016J9	Armazenamento de volume (gp2) de uso geral SSD (TiB)
Armazenamento de volume (padrão) magnético EBS	Limites do serviço	cG7HH017J9	Armazenamento de volume (padrão) magnético (TiB)
Armazenamento de volumes SSD de IOPS provisionadas (io1) do EBS	Limites do serviço	gI7MM017J9	Armazenamento (SSD) de IOPS provisionadas (TiB)

Nome da verificação	Categoria da verificação	ID da verificação	CloudWatch Métrica atualizada para ServiceLimit
Armazenamento de volume HDD otimizados para throughput (st1) EBS	Limites do serviço	wH7DD013J9	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
EC2Serviço de configuração para instâncias do Windows EC2	Tolerância a falhas	V77i0L1Bqz
ENAVersão do driver para instâncias EC2 do Windows	Tolerância a falhas	TyfdMXG69d
NVMeVersão do driver para instâncias EC2 do Windows	Tolerância a falhas	yHAGQJV9K5
Versão do driver PV para instâncias EC2 do Windows	Tolerância a falhas	Wnwm9I15bG
Volumes ativos do EBS	Limites do serviço	fH7LL017J9

O Amazon Elastic Block Store não tem mais um limite no número de volumes que você pode provisionar.

Você pode monitorar suas EC2 instâncias da Amazon e verificar se elas estão atualizadas usando o [AWS Systems Manager Distributor](#), 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	eW7HH017J9

AWS Support Aplicativo no Slack

Você pode usar o AWS Support aplicativo para gerenciar seus casos de AWS suporte no Slack. Convide os membros da sua equipe para canais de bate-papo, responda às atualizações de casos e converse diretamente com os agentes de suporte. Use o AWS Support aplicativo para gerenciar casos de suporte rapidamente no Slack.

Use o AWS Support aplicativo 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 aplicativo, 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](#)

- [Participe de uma sessão de bate-papo ao vivo com Suporte](#)
- [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](#)
- [AWS Support Comandos do aplicativo no Slack](#)
- [Visualizar correspondências do aplicativo AWS Support no AWS Support Center Console](#)
- [Criação de AWS Support aplicativos nos recursos do Slack com AWS CloudFormation](#)

Pré-requisitos

Você deve atender aos seguintes requisitos para usar o AWS Support aplicativo 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 AWS Support planos](#).
- 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).
- Você faz login no Conta da AWS como usuário ou função AWS Identity and Access Management (IAM) com as permissões necessárias. Para obter mais informações, consulte [Gerenciando o acesso ao widget do AWS Support aplicativo](#).
- É preciso criar um perfil do IAM que tenha as permissões necessárias para executar as ações para você. O AWS Support aplicativo usa essa função para fazer chamadas de API para diferentes serviços. Para obter mais informações, consulte [Gerenciando o acesso ao AWS Support aplicativo](#).

Tópicos

- [Gerenciando o acesso ao widget do AWS Support aplicativo](#)
- [Gerenciando o acesso ao AWS Support aplicativo](#)

Gerenciando o acesso ao widget do AWS Support aplicativo

Você pode anexar uma política AWS Identity and Access Management (IAM) para conceder permissão ao usuário do IAM para configurar o widget do AWS Support aplicativo 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 root no seu Conta da AWS, mas não recomendamos que você 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

O AWS Support aplicativo inclui ações somente com permissão que não correspondem diretamente a uma operação de API. Essas ações são indicadas na [Referência de autorização de serviço](#) com [permission only].

O AWS Support aplicativo 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. Portanto, essas ações de API não estão incluídas no AWS CLI AWS SDKs e.

Gerenciando o acesso ao AWS Support aplicativo

Depois de ter permissões para o widget do AWS Support aplicativo, você também deve criar uma função AWS Identity and Access Management (IAM). Essa função executa ações de outros Serviços da AWS para você, como a AWS Support API e as 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 bate-papo ao vivo com um agente de suporte e escolhe um novo canal privado como sua preferência de canal de bate-papo ao vivo, o AWS Support aplicativo cria um canal separado no Slack. Esse canal do Slack tem as mesmas permissões do canal em que você criou o caso ou iniciou o chat.

Se você alterar a função do IAM ou a política do IAM, suas alterações se aplicarão ao canal do Slack que você configurou e a todos os novos canais do Slack de chat ao vivo que o AWS Support aplicativo criar para você.

Siga esses procedimentos para criar seu perfil e sua política do IAM.

Tópicos

- [Use uma política AWS gerenciada ou crie uma política gerenciada pelo cliente](#)
- [Criar um perfil do IAM](#)
- [Solução de problemas](#)

Use uma política AWS gerenciada ou crie uma política gerenciada pelo cliente

Para conceder permissões à sua função, você pode usar uma política AWS gerenciada 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 automaticamente as permissões necessárias para o AWS Support aplicativo. 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.

Para criar uma política gerenciada pelo cliente para o AWS Support aplicativo

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, selecione Políticas.
3. Escolha 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 Próximo: tags.
7. (Opcional) É possível usar tags como pares de chave-valor para adicionar metadados à política.
8. Escolha 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 a função tenha permissões completas para todas as ações necessárias para o AWS Support aplicativo. Depois de configurar um canal do Slack com o perfil, qualquer usuário em seu canal terá as mesmas permissões.

Note

Para obter uma lista de políticas AWS gerenciadas, consulte [AWS políticas gerenciadas para AWS Support aplicativos no Slack](#).

Você pode atualizar a política para remover uma permissão do AWS Support aplicativo.

```
{
  "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 AWS Identity and Access Management](#)

Criar um perfil 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.

Para criar uma função para o AWS Support aplicativo

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 Próximo: Permissões.
6. Insira o nome da política. Você pode escolher a política AWS gerenciada ou escolher uma política gerenciada pelo cliente que você criou, 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 Próximo: revisar.
10. Em Role name (Nome do perfil), digite um nome, como *AWSSupportAppRole*.
11. (Opcional) Em 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 [Criação de uma função para um AWS serviço](#) no Guia do usuário do IAM.

Solução de problemas

Consulte os tópicos a seguir para gerenciar o acesso ao AWS Support aplicativo.

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 AWS Support aplicativo diz que estou perdendo uma função do IAM para 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 aos seus casos de suporte, independentemente de ter Conta da AWS ou não um usuário do IAM.

Recomendamos seguir estas práticas recomendadas:

- Configure canais privados do Slack com o AWS Support aplicativo
- 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 sua função do IAM não aparecer na função do IAM da lista de AWS Support aplicativos, isso significa que a função não tem o AWS Support aplicativo como uma entidade confiável ou que a função foi excluída. É possível atualizar um perfil existente ou criar um. Consulte [Criar um perfil 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 AWS Support aplicativo assume essa função para realizar essas ações para você.

Se você receber um erro sobre a falta de uma permissão do AWS Support aplicativo, verifique se a política anexada à sua função 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 na página AWS Support Center Console at <https://console.aws.amazon.com/support/app#/config>.
2. Escolha o canal que você configurou com o AWS Support aplicativo.
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 AWS Support aplicativo diz que estou perdendo uma função do IAM para 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. Depois, você pode usar o AWS Support aplicativo para solicitar aumentos de cota 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 [Exemplo de política do IAM](#) permite que o AWS Support aplicativo crie a função Service Quotas para você.

```
{
  "Effect": "Allow",
  "Action": "iam:CreateServiceLinkedRole",
  "Resource": "*",
  "Condition": {
    "StringEquals": {"iam:AWSServiceName": "servicequotas.amazonaws.com"}
  }
}
```

Se você excluir a função do IAM que configura para seu canal, deverá criar a função manualmente ou atualizar a política do IAM para permitir que o AWS Support aplicativo crie uma para você.

Autorizar um espaço de trabalho do Slack

Depois de autorizar seu espaço de trabalho e dar permissão ao AWS Support aplicativo para acessá-lo, você precisará de uma função AWS Identity and Access Management (IAM) para seu. Conta da AWS O AWS Support aplicativo usa essa função para chamar operações de API [AWS Support Service Quotas](#) para você. Por exemplo, o AWS Support aplicativo usa a função para chamar a CreateCase operação 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, deverá 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 seu 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 AWS Support Está solicitando permissão para acessar a página do your-workspace-name Slack, escolha Permitir.

 Note

Se você não puder permitir que o Slack acesse seu espaço de trabalho, certifique-se de ter permissões do administrador do Slack para adicionar o AWS Support aplicativo 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 trabalho).

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, seu número de Conta da AWS identificação aparece como o nome da conta no 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 AWS Support aplicativo usa esse nome para identificar sua conta no canal do Slack. É possível atualizá-lo a qualquer momento.

Edit account name ✕

Choose an account name that you can easily recognize in Slack. This name won't appear in your AWS account settings.

Account name

aws-administrator-account

Maximum 30 characters (5 remaining)

Example Usage:

Account name being used by Support Slack App Bot

- **AWS account:** aws-administrator-account (ID: 123456789012)

Cancel Save

Seu espaço de trabalho e o nome da conta aparecem na página Slack configuration (Configuração do Slack).

Slack configuration

Workspaces

Delete Authorize workspace Add multiple accounts ↺

Workspace

troubleshooting

Account name

Delete Edit

Name used in Slack

aws-administrator-account

Autorizar várias contas

Para autorizar vários Contas da AWS a usar os espaços de trabalho do Slack, você pode usar o [Terraform AWS CloudFormation](#) para criar seus recursos do aplicativo. AWS Support

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 AWS Support aplicativo é onde você pode criar e pesquisar casos 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.

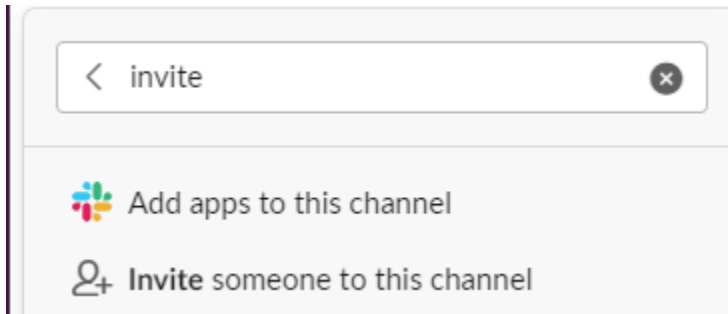
Cada um Conta da AWS deve configurar um canal do Slack separadamente no AWS Support aplicativo. Dessa forma, o AWS Support aplicativo pode acessar os casos de suporte dessa forma Conta da AWS. Se outra pessoa Conta da AWS da sua organização já convidou o AWS Support aplicativo para esse canal do Slack, vá 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 um Conta da AWS pode usar o AWS Support aplicativo. O AWS Support aplicativo retornará uma mensagem de erro se você tentar configurar o mesmo canal do Slack para outro workspace.

Para configurar um canal do Slack

1. No seu aplicativo Slack, escolha o canal do Slack que você deseja usar com o AWS Support aplicativo.
2. Conclua as etapas a seguir para convidar o AWS Support aplicativo para 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.

Slack workspace

Workspace

Choose a Slack workspace to use with the AWS Support App. If your workspace doesn't appear below, you can [add a workspace in Slack](#) so that the AWS Support App can access your workspace.

troubleshooting ▼

↻

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.
 - Privado — em ID do canal, insira o ID ou o URL do canal do Slack para o qual você convidou o AWS Support aplicativo.

 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 seu canal é o valor que parece **C01234A5BCD**.

7. Em Nome da configuração do canal, insira um nome que identifique facilmente sua configuração de canal do Slack para o AWS Support aplicativo. Esse nome aparece somente no seu 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.

▼ Slack channel

Channel Type

- ☐ Public
Choose a public channel from the list.
- ☒ Private
A channel member must invite a user to join or view.

Channel ID

Channel configuration name

Choose a name that you can easily identify. You can change the name at any time.



Tip

Tip To find the channel ID, right-click your channel name in Slack, choose **Copy** and then choose **Copy link**. Your channel ID is the value that looks like **C01234A5BCD**.

8. Em Permissões, para a função do IAM para o AWS Support aplicativo no Slack, escolha uma função que você criou para o AWS Support aplicativo. Somente funções que têm o AWS Support aplicativo como uma entidade confiável aparecem na lista.

▼ Permissions

IAM role for the AWS Support App

Choosing another IAM role for this Slack channel configuration can affect the permissions for any chat channels created from this troubleshooting channel. You can verify that your role has the required permissions. [Learn more](#)



 Note

Se você não criou um perfil ou não encontra seu perfil na lista, consulte [Gerenciando o acesso ao AWS Support aplicativo](#).

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 [Escolha do nível inicial de gravidade do caso de suporte](#).
 - 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.

▼ Notifications

Additional case notifications

Choose when to get notified for cases created and updated.

☒ All cases

☐ High-severity cases

☐ None

Notification types

Get notified for the following types of cases that are created.

☒ New and reopened cases

☒ Case correspondences

☒ Resolved cases

Note: You will receive notifications in your Slack channel for all case updates for this account.

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 **channelName** página, você pode realizar as seguintes tarefas:
 - Escolha Rename (Renomear) para atualizar o nome da configuração do seu canal. Esse nome só aparece no seu Conta da AWS e não aparecerá no Slack.
 - Escolha Excluir para excluir a configuração do canal do AWS Support aplicativo. 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

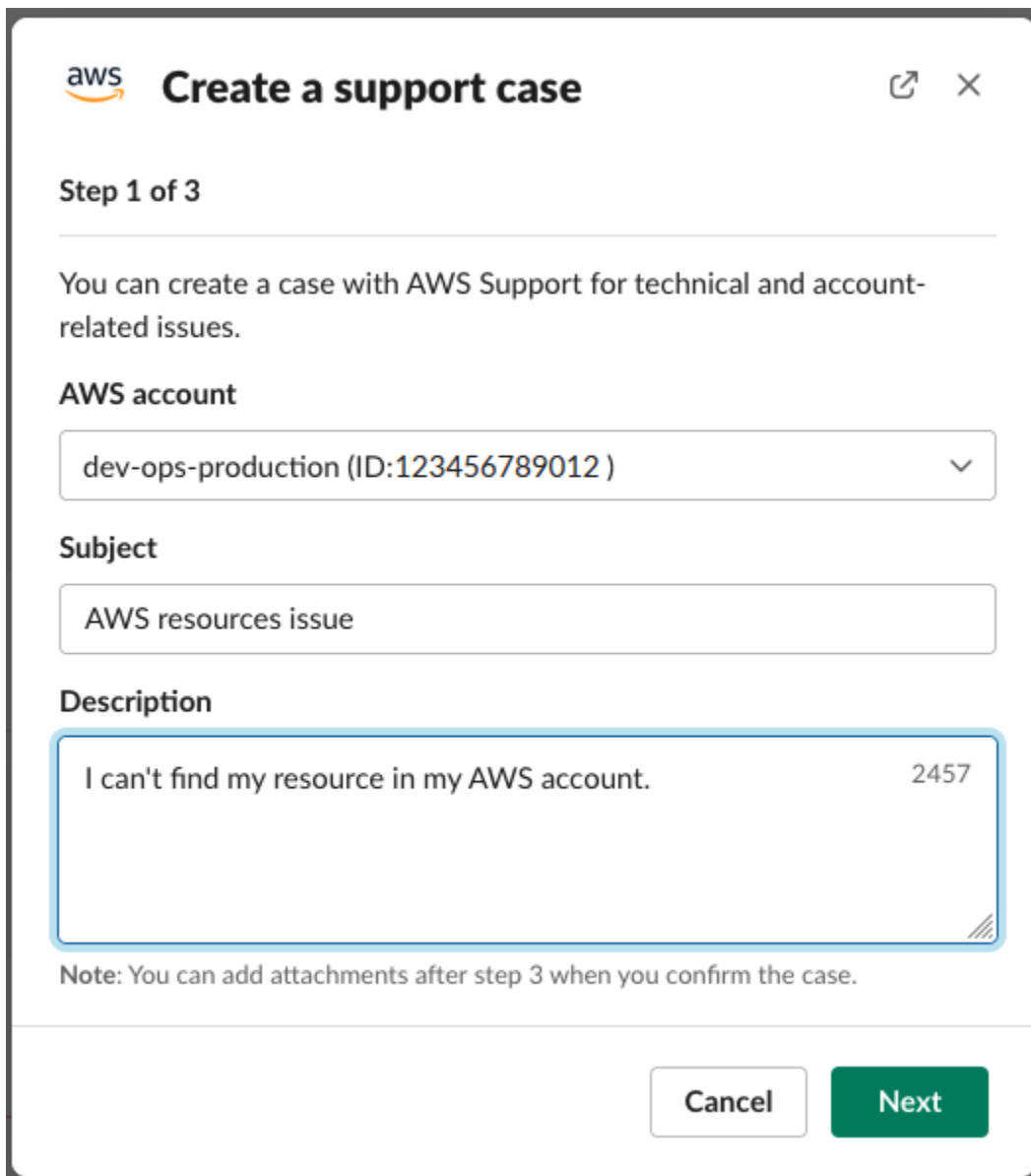
Depois de autorizar seu espaço de trabalho do Slack e adicionar um canal, você pode criar um caso de suporte em seu canal do Slack.

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, como como você está usando um AWS service (Serviço da AWS) e quais etapas de solução de problemas você tentou.



aws **Create a support case**

Step 1 of 3

You can create a case with AWS Support for technical and account-related issues.

AWS account

dev-ops-production (ID:123456789012)

Subject

AWS resources issue

Description

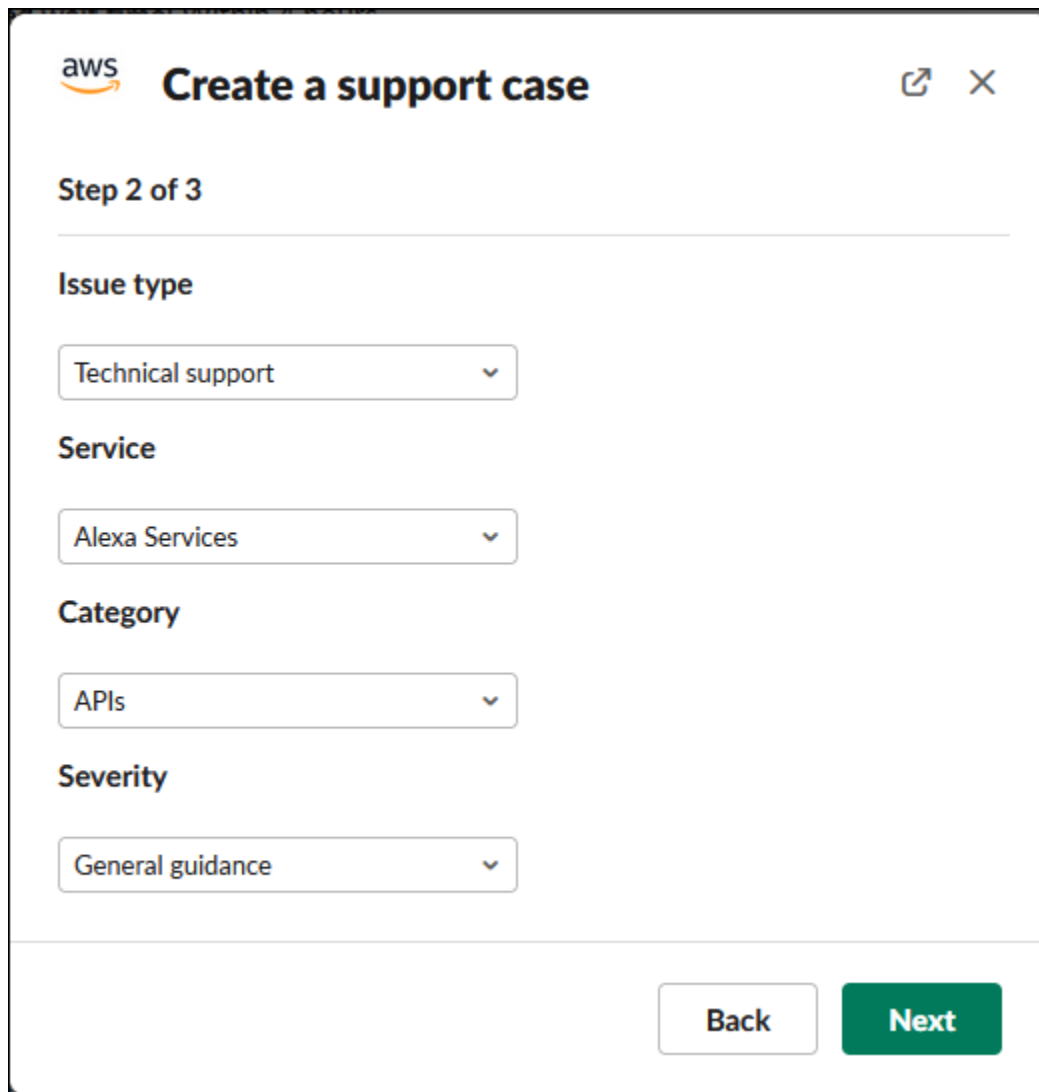
I can't find my resource in my AWS account. 2457

Note: You can add attachments after step 3 when you confirm the case.

Cancel Next

3. Escolha 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 Alexa Serviços.



The screenshot shows the 'Create a support case' interface in the AWS Support console. It is titled 'Step 2 of 3'. The form contains four dropdown menus: 'Issue type' set to 'Technical support', 'Service' set to 'Alexa Services', 'Category' set to 'APIs', and 'Severity' set to 'General guidance'. At the bottom right, there are two buttons: 'Back' and 'Next'.

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.

 **Create a support case** ✕

Step 3 of 3

Contact language

English ▾

Contact method

☒ Live chat in Slack

☐ Email and Slack notifications

Live chat channel preference

New private channel ▾

 A new channel will be created for your live chat session, and anyone who is invited to the channel can see previous chat history.

Additional chat members (optional)

Add chat members

You will be added to the live chat automatically.

Back

Review

- 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 AWS Support agente, e o canal atual usará um tópico no canal atual para você conversar com o AWS Support agente.
- 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 aplicativo adicionará automaticamente você e os membros selecionados ao novo canal. Para o canal atual, o AWS Support aplicativo marcará automaticamente você e os membros selecionados no tópico de bate-papo quando o AWS Support agente entrar.

 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.
- Se você iniciar uma nova sessão de bate-papo ao vivo para um caso de suporte existente, o AWS Support aplicativo usará o mesmo canal de bate-papo ou tópico usado em um bate-papo ao vivo anterior. O AWS Support aplicativo também usa a mesma preferência de canal de bate-papo 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

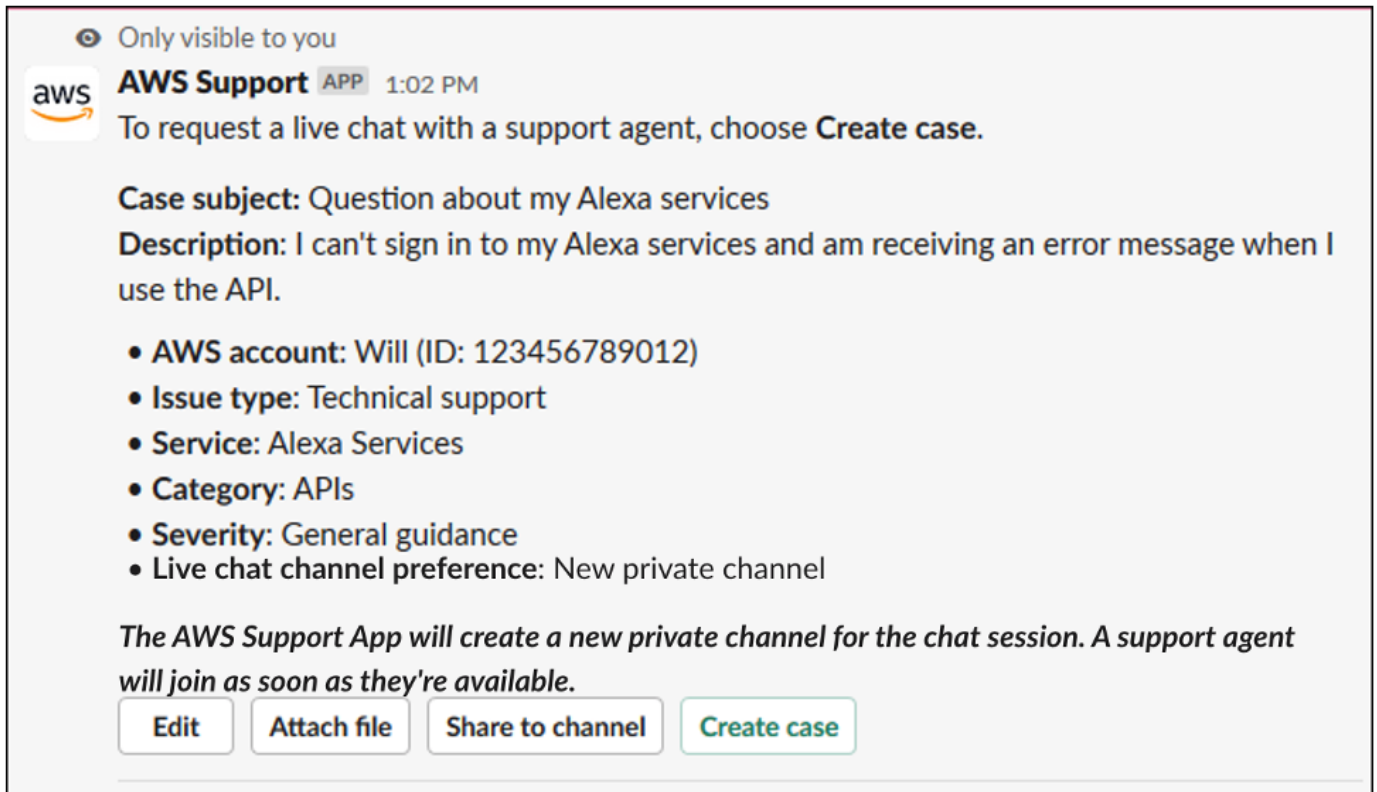
- É possível anexar até três arquivos. Cada arquivo pode ter até 5 MB.

- 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 Alexa Serviços.



The screenshot shows a Slack message from the AWS Support App. At the top, it says "Only visible to you". Below that is the AWS logo and the text "AWS Support APP 1:02 PM". The main text says "To request a live chat with a support agent, choose **Create case**." Below this is a form with the following fields:

- Case subject:** Question about my Alexa services
- Description:** I can't sign in to my Alexa services and am receiving an error message when I use the API.
- Details:**
 - **AWS account:** Will (ID: 123456789012)
 - **Issue type:** Technical support
 - **Service:** Alexa Services
 - **Category:** APIs
 - **Severity:** General guidance
 - **Live chat channel preference:** New private channel

Below the form, there is a note: "The AWS Support App will create a new private channel for the chat session. A support agent will join as soon as they're available." At the bottom, there are four buttons: "Edit", "Attach file", "Share to channel", and "Create case".

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. Depois, será possível 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 agentes de suporte. Para obter mais informações, consulte [Atualizar, resolver e reabrir um caso](#).
- Você não pode adicionar correspondências a casos de canais de bate-papo criados pelo AWS Support aplicativo. 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

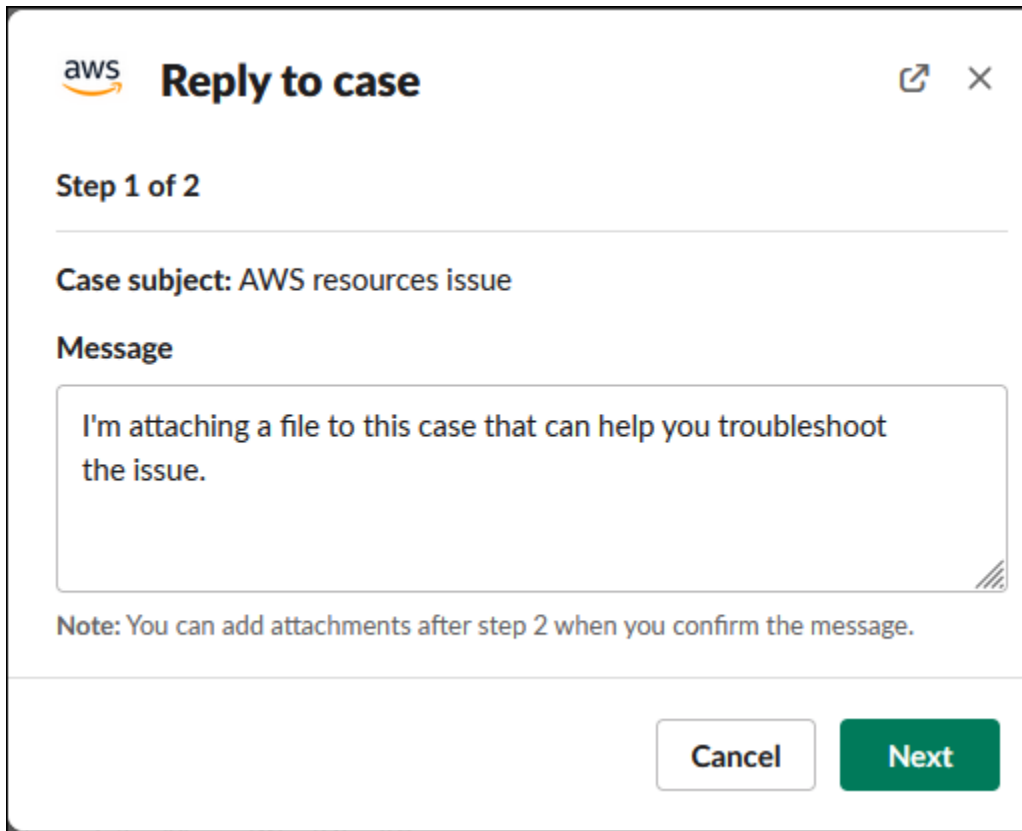
1. No seu canal do Slack, escolha o caso ao qual você quer responder. Você pode inserir `/awssupport search` para encontrar o seu caso de suporte.
2. Escolha See details (Visualizar detalhes) ao lado do caso que você deseja.
3. Na parte inferior dos detalhes de caso, escolha Reply (Responder).

Share to channel

Reply

Resolve case

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).



The screenshot shows a dialog box titled "aws Reply to case" with a close button (X) and a share icon. It is labeled "Step 1 of 2". The "Case subject" is "AWS resources issue". The "Message" field contains the text: "I'm attaching a file to this case that can help you troubleshoot the issue." Below the message field is a note: "Note: You can add attachments after step 2 when you confirm the message." At the bottom right are "Cancel" and "Next" buttons.

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

Only visible to you

 **AWS Support** APP 10:53 AM

To respond to this case, review and then choose **Send message**.

Case subject: AWS resources issue

Message: I'm attaching a file to this case that can help you troubleshoot the issue.

We will contact you by email and Slack notifications within 24 hours.

Additional contacts to notify: None

[Edit](#) [Attach file](#) [Share to channel](#) [Send message](#)

Attachments: error-log

[Delete files](#)

✓ You successfully attached 1 file. Choose **Create case** within 1 hour to include the file with your case.

Participe de uma sessão de bate-papo ao vivo com Suporte

Ao solicitar um bate-papo ao vivo para seu caso, você opta por usar um novo canal de bate-papo ou um tópico no canal atual para você e o AWS Support agente. 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. É uma prática recomendada adicionar somente usuários que precisam de acesso aos seus casos de suporte. Qualquer membro de um canal ou thread de chat também pode participar de um chat ativo.

ℹ Note

Os canais e tópicos de bate-papo ao vivo também recebem notificações quando uma correspondência é adicionada ao caso fora da sessão de bate-papo ao vivo. Isso ocorre antes, durante e depois de uma sessão de bate-papo, então você pode usar um canal ou

discussão de bate-papo para monitorar todas as atualizações de um caso. Se você optar por usar um novo canal de bate-papo, use o canal de configuração que você convidou o AWS Support aplicativo para responder a essas correspondências.

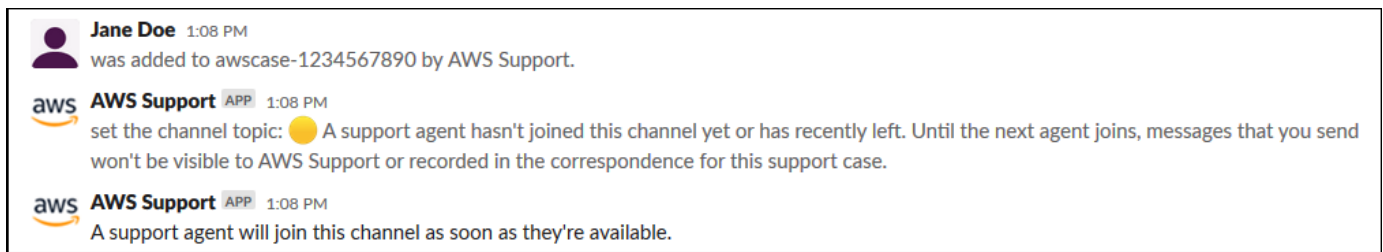
Para participar de uma sessão de bate-papo ao vivo Suporte em um novo canal

1. No aplicativo Slack, navegue até o canal que o AWS Support aplicativo cria para você. O nome do canal inclui seu ID de caso de suporte, como **aws-case-1234567890**.

 Note

O AWS Support aplicativo adiciona uma mensagem fixa ao canal de bate-papo ao vivo que contém detalhes sobre 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. Até que um agente de suporte entre no canal, o agente não verá as mensagens nesse bate-papo e as mensagens não aparecerão na sua correspondência de 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 AWS Support aplicativo salva automaticamente seus arquivos e o registro de bate-papo na correspondência do seu caso.

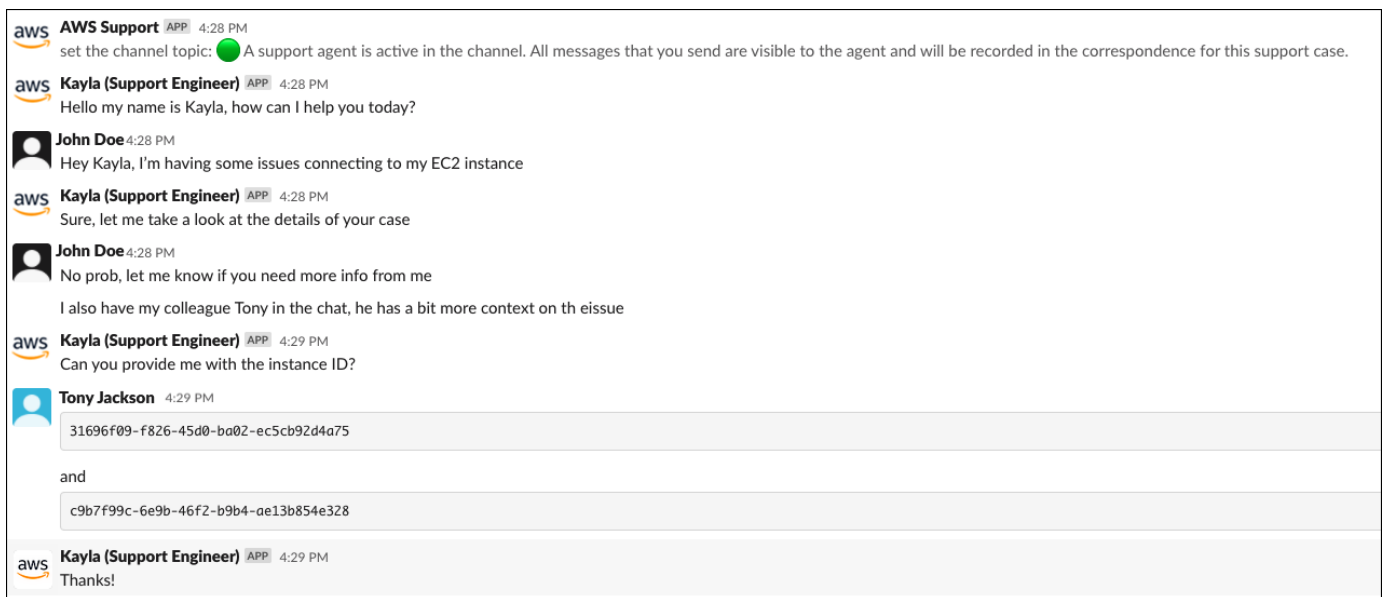
 Note

Ao conversar com um agente de suporte, observe as seguintes diferenças no Slack para o AWS Support aplicativo:

- 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

Veja a seguir um exemplo de uma sessão de bate-papo ao vivo com um agente de suporte para corrigir um problema de conectividade em duas instâncias do Amazon Elastic Compute Cloud (Amazon EC2).



5. (Opcional) Para interromper o chat ao vivo, escolha End chat (Encerrar chat). O agente de suporte sai do canal e o AWS Support aplicativo para de gravar o bate-papo 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 fixa a seguir mostra os detalhes do caso sobre uma EC2 instância da Amazon. É possível encontrar as mensagens fixadas abaixo do nome do canal do Slack.



 **AWS Support** APP 2:33 PM

This is a live chat channel for the following case.

Case subject: Cannot connect to ec2 instance (Case ID: 6887208841)

Description: The ec2 instance i-09f00da444 was unable to lookup our dns region. We had full access yesterday. Now we get "Access denied" message.

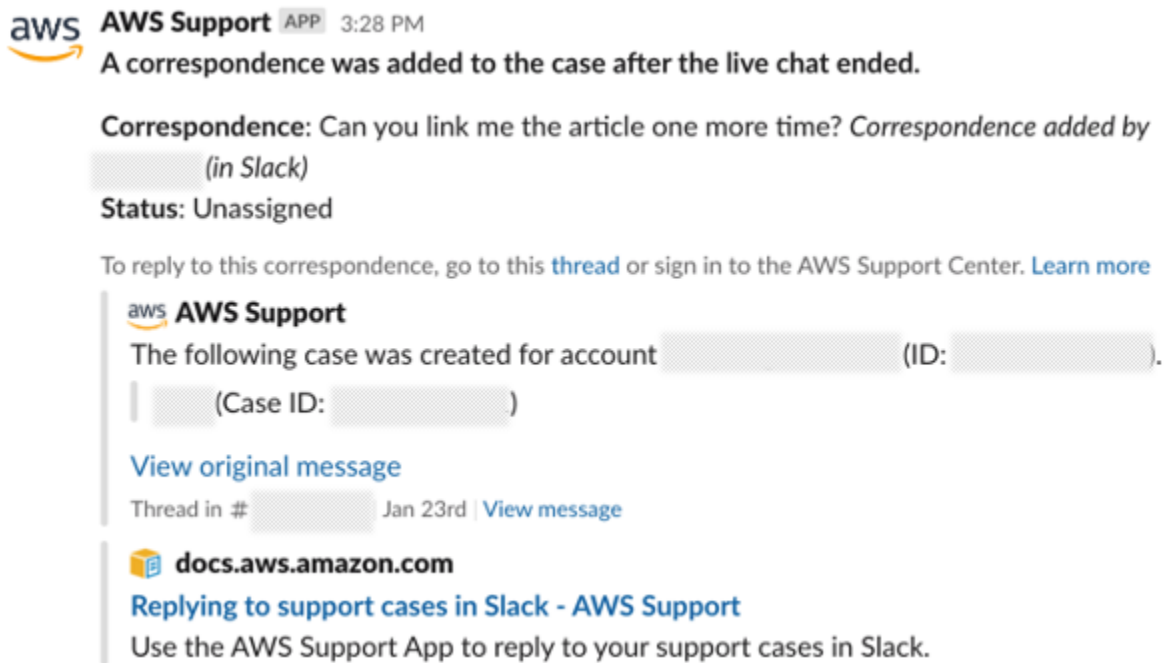
Case created by Jane Doe (in Slack)

- **Status:** Unassigned
- **Created:** 02/16/2021, 2:33PM PST
- **AWS account:** Instance Management (ID: 111122223333)
- **Issue type:** Technical support
- **Service:** Elastic Compute Cloud (EC2-Linux)
- **Category:** SSH Issue
- **Severity:** Production system impaired

End chat Resolve case

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 bate-papo ao vivo com Suporte o canal atual

1. No aplicativo Slack, navegue até o tópico no canal atual que o AWS Support aplicativo usa para o bate-papo. 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 da conversa de bate-papo nunca são vistas Suporte, mesmo quando o bate-papo está ativo.

Thread aws-support-communications**AWS Support** APP < 1 minute ago

The following case was created for account [REDACTED].

Question about my Alexa services (Case ID: [REDACTED])



A support agent hasn't joined this chat session yet or has recently left

Get updates

See details

End chat

Reply

Resolve case

7 replies

**AWS Support** APP < 1 minute ago

@Jane Doe requested a chat for this case.

Question about my Alexa services (Case ID: [REDACTED])

**AWS Support** APP < 1 minute ago

A support agent will join this chat session as soon as they're available.

**Tip:** Editing and deleting messages is not supported during the chat session. Support agents will still see original messages.

3. (Opcional) Marque outros membros do canal para notificá-los no thread do chat.
4. Depois que o agente de suporte entra no bate-papo, o tópico fica ativo e o AWS Support aplicativo grava o bate-papo. 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 AWS Support aplicativo salva automaticamente seus arquivos e o registro de bate-papo na correspondência do seu caso.
5. (Opcional) Para interromper o chat ao vivo, escolha Encerrar chat na mensagem inicial desse thread. O agente de suporte deixa o tópico e o AWS Support aplicativo para de gravar o bate-papo 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.

Thread  aws-support-communications

 **AWS Support** APP < 1 minute ago

The following case was created for account [REDACTED].

Question about my Alexa services (Case ID: [REDACTED])

 A support agent hasn't joined this chat session yet or has recently left

[Get updates](#) [See details](#) [End chat](#) [Reply](#) [Resolve case](#)

7 replies

Como procurar casos de suporte no Slack

No seu canal do Slack, você pode pesquisar casos de suporte em sua conta Conta da AWS e em outras contas que configuraram o mesmo canal e espaço de trabalho. Por exemplo, se 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, você poderá usar o aplicativo para pesquisar os casos de suporte uns dos outros. AWS Support

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.

👁 Only visible to you

 **AWS Support** APP 1:07 PM

Search for cases created by account **aws-administrator-account** (ID: 123456789012).

I want to search for cases by:

☒ Filter options

☐ Case ID

Date range:

 10/01/2022 

 Today 

Case status:

All cases 

Case created in:

English 

Search

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. Selecione a opção 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.

 Only visible to you

 **AWS Support** APP 1:51 PM

3 results found for cases created from 10/01/2022 to 12/28/2022 with AWS account aws-administrator-account (ID:123456789012).

Case subject: Can't retrieve info about my certificate (Case ID: 1234567890)

Created: 10/25/2022, 10:30 PM UTC

Status: Resolved

[See details](#)

Case subject: Question about my AWS account bill (Case ID: 4445556660)

Created: 10/14/2022, 7:35 PM UTC

Status: Resolved

[See details](#)

Case subject: Technical support for EC2 instances (Case ID: 9087654321)

Created: 10/13/2022, 2:28 PM UTC

Status: In progress

[See details](#)

[Edit Search](#) [Share to channel](#)

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).

 Only visible to you

This case was created on 10/14/2022, 10:30 PM UTC.

Case subject: Question about my AWS account bill (Case ID: 4445556660)

Description: I have a question about a charge for my last statement

- **Status:** Resolved
- **AWS account:** aws-administrator-account (ID: 123456789012)
- **Issue type:** Account and billing support
- **Service:** Academy
- **Category:** Account/Lab access issue
- **Severity:** General question
- **Language:** English

Correspondence:

Amazon Web Services, 10/25/2022, 10:30 PM UTC

This case has been resolved. Please contact us again if you need further assistance.

Share to channel

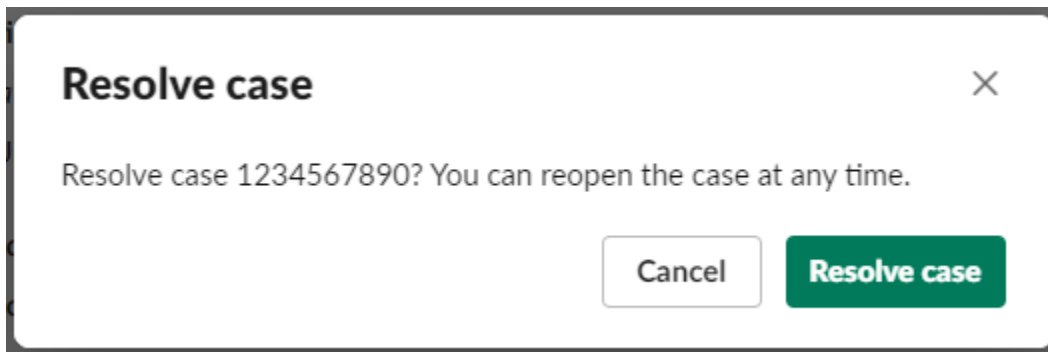
Reopen case

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.

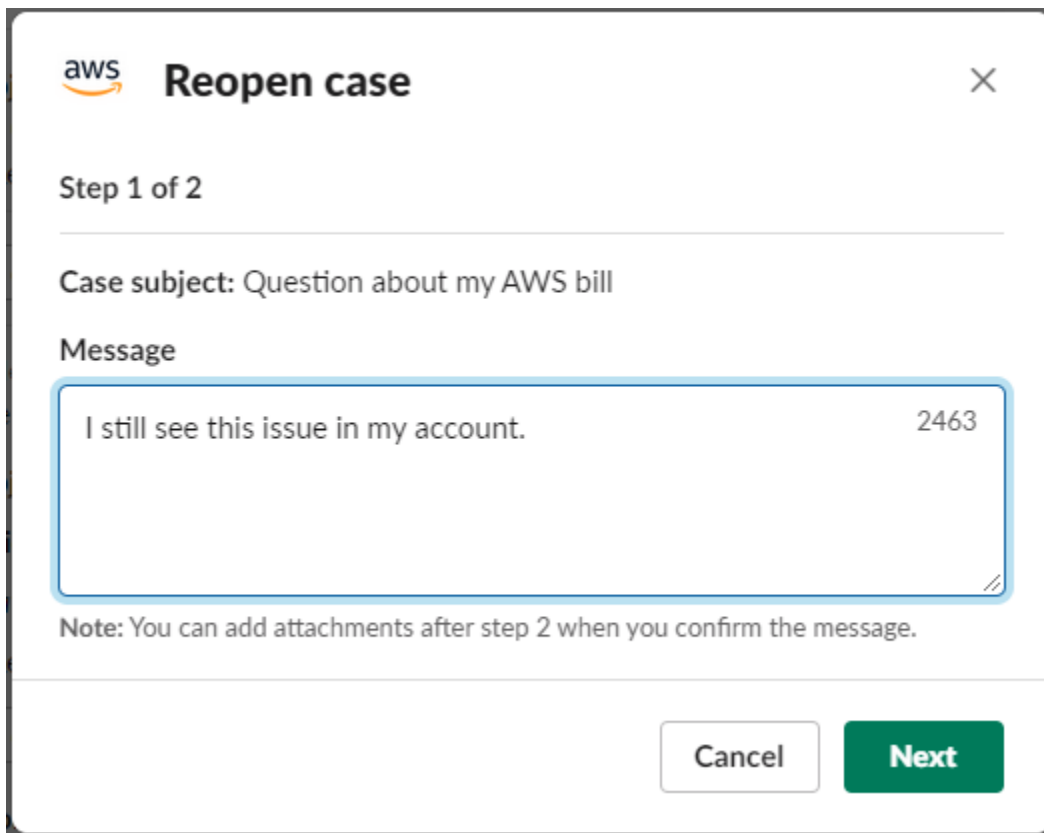


Como reabrir um caso de suporte no Slack

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 Próximo.



aws Reopen case X

Step 1 of 2

Case subject: Question about my AWS bill

Message

I still see this issue in my account. 2463

Note: You can add attachments after step 2 when you confirm the message.

Cancel Next

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.

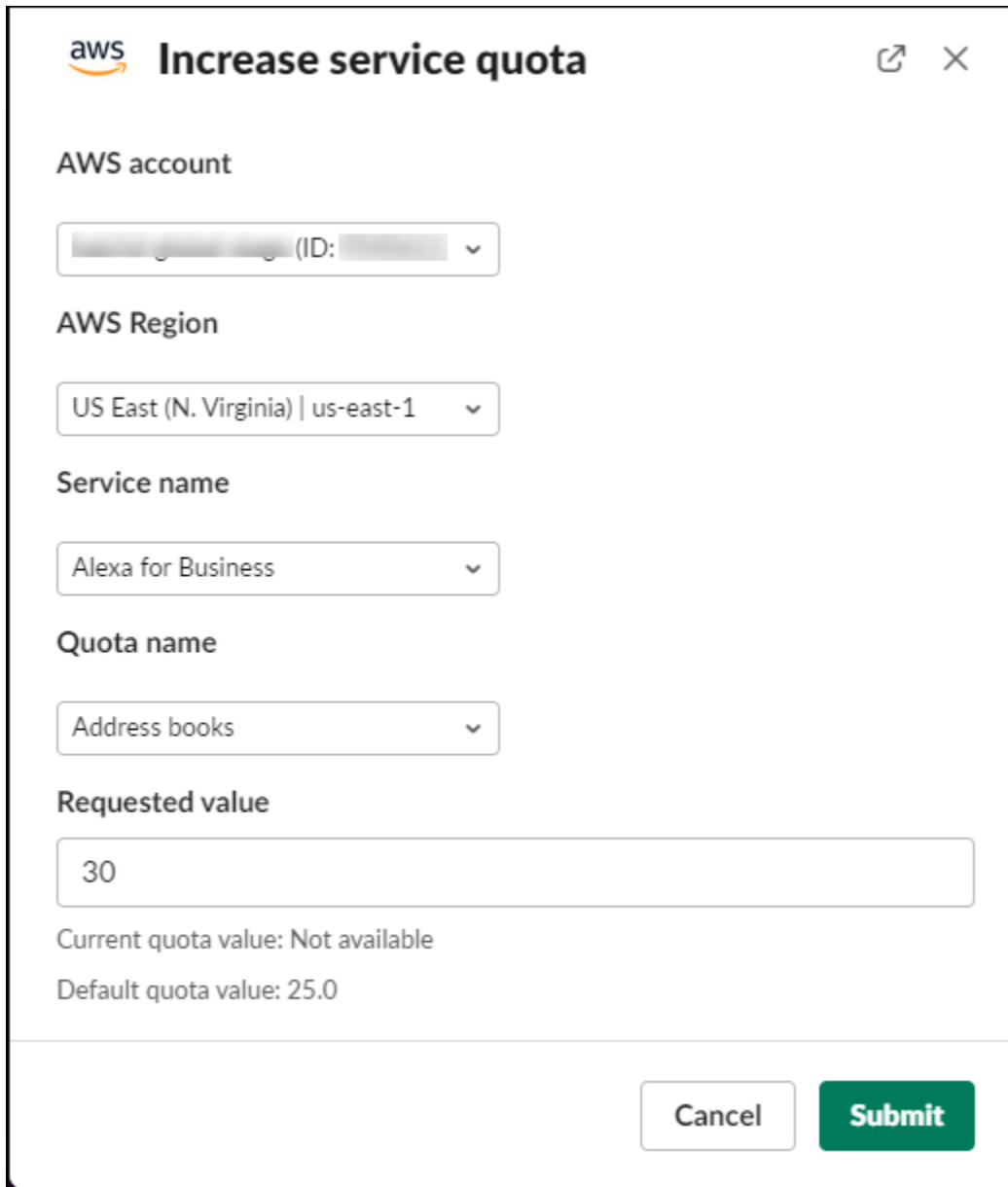
Para solicitar aumentos de cota de serviço

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



The screenshot shows the 'Increase service quota' form in the AWS console. The form is titled 'Increase service quota' with the AWS logo. It contains several dropdown menus and a text input field. The 'AWS account' dropdown is partially obscured. The 'AWS Region' dropdown is set to 'US East (N. Virginia) | us-east-1'. The 'Service name' dropdown is set to 'Alexa for Business'. The 'Quota name' dropdown is set to 'Address books'. The 'Requested value' text input field contains the number '30'. Below the input field, it says 'Current quota value: Not available' and 'Default quota value: 25.0'. At the bottom right, there are two buttons: 'Cancel' and 'Submit'.

aws Increase service quota

AWS account

(ID:)

AWS Region

US East (N. Virginia) | us-east-1

Service name

Alexa for Business

Quota name

Address books

Requested value

30

Current quota value: Not available

Default quota value: 25.0

Cancel Submit

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).

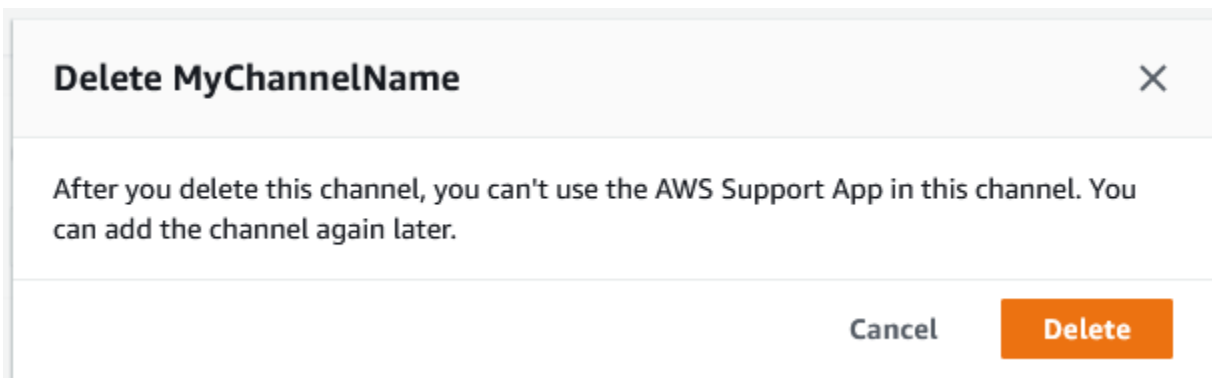
Como excluir uma configuração de canal do Slack do aplicativo AWS Support

Você pode excluir uma configuração de canal do AWS Support aplicativo se não precisar dela. Essa ação remove apenas o canal do AWS Support aplicativo 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 AWS Support aplicativo novamente mais tarde.



Como excluir uma configuração de espaço de trabalho do Slack no aplicativo AWS Support

Você pode excluir uma configuração do espaço de trabalho do AWS Support aplicativo se não precisar dela. Essa ação remove apenas o espaço de trabalho do AWS Support aplicativo e do AWS Support Center Console. O seu espaço de trabalho não é excluído do Slack.

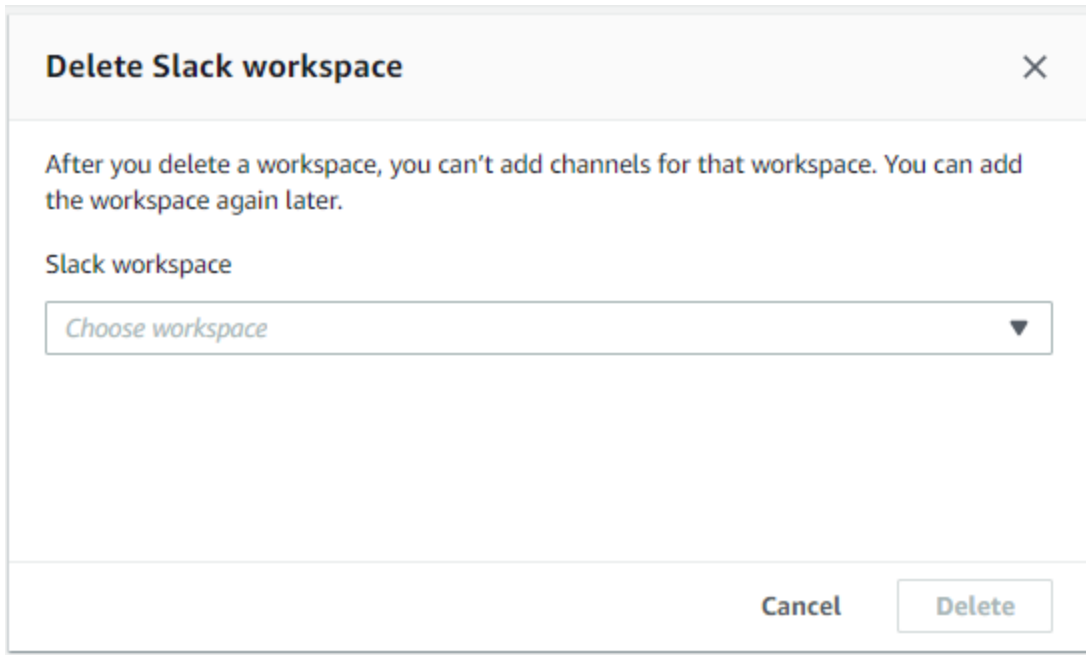
É possível adicionar até 5 espaços de trabalho em sua Conta da AWS. Se você já atingiu essa cota, exclua um espaço de trabalho do Slack antes de adicionar outro.

Note

Se você adicionou canais desse espaço de trabalho ao AWS Support aplicativo, primeiro exclua 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 ao seu Conta da AWS novamente mais tarde.



Delete Slack workspace [X]

After you delete a workspace, you can't add channels for that workspace. You can add the workspace again later.

Slack workspace

Choose workspace ▼

Cancel Delete

AWS Support Comandos do aplicativo no 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 pesquisar casos de suporte para quem configurou Contas da AWS o AWS Support aplicativo 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 aplicativo cria para você se você escolher um novo canal para o seu bate-papo Suporte. Os canais de bate-papo incluem seu ID de caso de suporte, como **aws-case-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.

Correspondence	
MyIAMRole (Role) Thu Feb 24 2022 09:09:33 GMT-0800 (Pacific Standard Time)	I am having difficulty retrieving information about my certificates. _Case created by JaneDoe (in Slack)_

Criação de AWS Support aplicativos nos recursos do Slack com AWS CloudFormation

AWS Support O aplicativo no Slack é integrado com AWS CloudFormation, um serviço que ajuda você a modelar e configurar seus AWS recursos para que você possa gastar menos tempo criando e gerenciando seus recursos e infraestrutura. Você cria um modelo que descreve todos os AWS recursos que você deseja (como o seu AccountAlias e SlackChannelConfiguration) e AWS CloudFormation provisiona e configura esses recursos para você.

Ao usar AWS CloudFormation, você pode reutilizar seu modelo para configurar os recursos do AWS Support aplicativo de forma consistente e repetida. Descreva seus recursos uma vez e, em seguida, provisione os mesmos recursos repetidamente em várias Contas da AWS regiões.

AWS Support Aplicativo e AWS CloudFormation modelos

Para provisionar e configurar recursos para AWS Support aplicativos e serviços relacionados, você deve entender [AWS CloudFormation os modelos](#). Os modelos são arquivos de texto formatados em JSON ou YAML. Esses modelos descrevem os recursos que você deseja provisionar em suas AWS CloudFormation pilhas. Se você não estiver familiarizado com JSON ou YAML, você pode usar o AWS CloudFormation Designer para ajudá-lo a começar a usar modelos. AWS CloudFormation Para obter mais informações, consulte [O que é AWS CloudFormation Designer?](#) no Guia do AWS CloudFormation usuário.

AWS Support O aplicativo suporta a criação de seu AccountAlias e SlackChannelConfiguration em AWS CloudFormation. Para obter mais informações, incluindo exemplos de modelos JSON e YAML para os SlackChannelConfiguration recursos AccountAlias e, consulte a [referência do tipo de recurso do AWS Support aplicativo](#) no Guia do AWS CloudFormation usuário.

Criar recursos de configuração do Slack para a organização

Você pode usar CloudFormation modelos para criar os recursos necessários para o AWS Support aplicativo. 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, você pode 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 canal do Slack para unidades específicas Contas da AWS ou

organizacionais (). OUs 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 modelos do CloudFormation ou não. Se não usar modelos do CloudFormation, você poderá concluir as seguintes etapas manuais em vez disso:

- Crie os recursos do AWS Support aplicativo no AWS Support Center Console.
- Crie um caso de suporte AWS Support para [autorizar várias contas](#) a usar o AWS Support aplicativo.
- Ligue para o [RegisterSlackWorkspaceForOrganization](#) Operação de API para registrar um espaço de trabalho do Slack para sua conta. A CloudFormation pilha chama essa operação de API para você.

Siga estes procedimentos para carregar o CloudFormation modelo em sua organização. Você pode usar os modelos de exemplo da página de [referência dos tipos de recursos do AWS Support App](#).

Os modelos CloudFormation instruem a criação dos 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 ferramenta `AWSSupportAppFullAccess` AWS a política gerenciada está anexada.

Sumário

- [Atualize seus CloudFormation modelos para o Slack](#)
- [Criar uma pilha para a conta de gerenciamento](#)
- [Criar um conjunto de pilhas para a organização](#)

Atualize seus CloudFormation modelos 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 o uso do modelo para criar um [AccountAlias](#) recurso para sua organização. A ferramenta AccountAlias Um recurso identifica exclusivamente um Conta da AWS no aplicativo. AWS Support 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](#).

Para atualizar seus CloudFormation modelos para o Slack

1. Se você for a conta de gerenciamento de uma organização, deverá autorizar manualmente um espaço de trabalho do Slack para sua conta antes que suas contas de membros possam usar 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 workspace e o canal IDs, 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/T012ABCDEFGF/C01234A5BCD>, T012ABCDEFGF 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 o [RegisterSlackWorkspaceForOrganization](#) Operação de API 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. Você não precisa fazer o upload do modelo de configuração do canal Slack, a menos que também esteja configurando a conta de gerenciamento para usar o AWS Support aplicativo.

Crie uma pilha para a conta de gerenciamento

1. Faça login AWS Management Console como a conta de gerenciamento da sua organização.
2. Abra o AWS CloudFormation console em <https://console.aws.amazon.com/cloudformation>.
3. Caso ainda não tenha feito isso, no seletor de região, escolha uma das seguintes opções:
Regiões da AWS
 - Europa (Frankfurt)
 - Europa (Irlanda)
 - Europa (Londres)
 - Leste dos EUA (Norte 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 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`. Você pode usar conjuntos de pilhas para criar a pilha para toda a sua organização ou especificar a OUs que você deseja. Para obter mais informações, consulte [Criar um conjunto de pilhas](#).

Esse procedimento também chama o [RegisterSlackWorkspaceForOrganization](#) Operação de API 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 AWS Management Console como a conta de gerenciamento da sua organização.
2. Abra o AWS CloudFormation console em <https://console.aws.amazon.com/cloudformation>.
3. Se ainda não o fez, no seletor de região, escolha o mesmo Região da AWS que você usou no procedimento anterior.
4. No painel de navegação, escolha StackSets.
5. Escolha 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 Especificar StackSet detalhes, insira um nome de pilhas **support-app-slack-workspace**, como, insira uma descrição e escolha Avançar.
10. Na página Configurar StackSet opções, mantenha as opções padrão e escolha Avançar.
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 destinos de implantação, escolha se você deseja criar a pilha para toda a organização ou para uma específica OUs. Se escolher uma UO, insira o ID da UO.
13. Em Especificar regiões, insira somente uma das seguintes opções Regiões da AWS:
 - Europa (Frankfurt)
 - Europa (Irlanda)
 - Europa (Londres)
 - Leste dos EUA (Norte da Virgínia)
 - Leste dos EUA (Ohio)
 - Oeste dos EUA (Oregon)
 - Ásia-Pacífico (Singapura)
 - Ásia-Pacífico (Tóquio)
 - Canadá (Central)

 Observações:

- Para simplificar seu fluxo de trabalho, recomendamos que você use o mesmo Região da AWS que escolheu na etapa 3.
- Escolher mais de um Região da AWS pode causar conflitos na criação de sua pilha.

14. Para opções de implantação, para Tolerância a falhas - opcional, insira o número de contas em que as pilhas podem falhar antes de CloudFormation interromper 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 CloudFormation falhe 9 vezes, pelo menos uma conta será bem-sucedida.
15. Escolha 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 a função do IAM e anexa uma política AWS gerenciada. Essa função tem as permissões necessárias para acessar outros serviços por você. Para obter mais informações, consulte [Gerenciando o acesso ao AWS Support aplicativo](#).

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 de CloudFormation criar as pilhas, cada conta membro pode entrar no console do Support Center e encontrar seus espaços de trabalho e canais configurados do Slack. Eles podem então usar o AWS Support aplicativo para seus 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 CloudFormation

Para saber mais sobre isso CloudFormation, consulte os seguintes recursos:

- [AWS CloudFormation](#)
- [AWS CloudFormation Guia do usuário](#)
- [AWS CloudFormation API Reference](#)
- [AWS CloudFormation Guia do usuário da interface de linha de comando](#)

Crie recursos de AWS Support aplicativos usando o Terraform

Você também pode usar o [Terraform](#) para criar os recursos do AWS Support aplicativo para o seu Conta da AWS. O Terraform é uma infrastructure-as-code ferramenta que você pode usar para seus aplicativos em nuvem. Você pode usar o Terraform para criar recursos de AWS Support aplicativos em vez de implantar uma CloudFormation pilha em uma conta.

Depois de instalar o Terraform, você pode especificar os recursos do AWS Support aplicativo que deseja. O Terraform chama o [RegisterSlackWorkspaceForOrganization](#) Operação de API para registrar um espaço de trabalho do Slack para você e criar 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 CloudFormation pilhas, você não pode usar o Terraform para criar os recursos do AWS Support aplicativo para uma OU em 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 [Registrando AWS Support o aplicativo em chamadas de API do Slack usando AWS CloudTrail](#).

Saiba mais

Para saber mais sobre o Terraform, consulte os tópicos a seguir:

- [Instalação do Terraform](#)
- [Tutorial do Terraform: Crie infraestrutura para 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 [AWS programas](#) de 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 service (Serviço da AWS) 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 Suporte. Os tópicos a seguir mostram como configurar para atender Suporte aos seus objetivos de segurança e conformidade. Você também aprende a usar outros Amazon Web Services que ajudam você a monitorar e proteger seus Suporte 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 Suporte](#)

Proteção de dados em AWS Support

O modelo de [responsabilidade AWS compartilhada modelo](#) se aplica à proteção de dados em Suporte. 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 o conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para obter mais informações sobre a privacidade de dados, consulte as [Data Privacy FAQ](#). Para obter mais informações sobre a proteção de dados na Europa, consulte a postagem do blog [AWS Shared Responsibility Model and RGPD](#) 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. Para obter informações sobre o uso de CloudTrail trilhas para capturar AWS atividades, consulte Como [trabalhar com CloudTrail trilhas](#) no Guia AWS CloudTrail do usuário.
- 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 140-3 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para obter mais informações sobre os endpoints FIPS disponíveis, consulte [Federal Information Processing Standard \(FIPS\) 140-3](#).

É altamente recomendável que nunca sejam colocadas informações confidenciais ou sigilosas, como endereços de e-mail de clientes, em tags 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 SDKs. AWS CLI Quaisquer dados inseridos em tags ou em 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, é fortemente recomendável que não sejam incluídas informações de credenciais no URL para validar a solicitação nesse servidor.

 Important

No caso de correspondência, nunca compartilhe informações confidenciais, como credenciais, cartões de crédito, informações assinadas URLs ou de identificação pessoal.

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](#): `AWSSupport ServiceRolePolicy`
- 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. Você pode ver os detalhes do caso por até 24 meses após a criação do caso. Para obter mais informações, consulte [DescribeCases](#) na Referência de APIs do AWS Support .
- 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 o [AWS Support FAQs](#).

- 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 Suporte os recursos. O IAM é um AWS service (Serviço da AWS) que você pode usar sem custo adicional.

Tópicos

- [Público](#)
- [Autenticação com identidades](#)
- [Gerenciar o acesso usando políticas](#)
- [Como AWS Support funciona com o IAM](#)
- [AWS Support exemplos de políticas baseadas em identidade](#)
- [Uso de perfis vinculados ao serviço](#)
- [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 Suporte.

Usuário do serviço — Se você usar o Suporte serviço para realizar seu trabalho, seu administrador fornecerá as credenciais e as permissões de que você precisa. À medida que você usa mais Suporte 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 Suporte, consulte [Solução de problemas AWS Support de identidade e acesso](#).

Administrador de serviços — Se você é responsável pelos Suporte recursos da sua empresa, provavelmente tem acesso total Suporte a. É seu trabalho determinar quais Suporte recursos e recursos seus usuários do serviço devem acessar. Envie as solicitações ao administrador do IAM para alterar as permissões dos usuários de serviço. Revise as informações nesta página para compreender os conceitos básicos do IAM. Para saber mais sobre como sua empresa pode usar o IAM com Suporte, consulte [Como 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 Suporte. Para ver exemplos de políticas Suporte baseadas em identidade que você pode usar no IAM, consulte [AWS Support exemplos de políticas baseadas em identidade](#)

Autenticação com identidades

A autenticação é a forma 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 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 designar solicitações por conta própria, consulte [Versão 4 do AWS Signature para solicitações de API](#) no Guia do usuário do IAM.

Independente do método de autenticação usado, também pode ser necessário fornecer informações adicionais de segurança. Por exemplo, AWS recomenda que você use a autenticação multifator (MFA) para aumentar a segurança da sua conta. Para saber mais, consulte [Autenticação multifator](#) no Guia do usuário do AWS IAM Identity Center e [Usar a autenticação multifator da AWS no IAM](#) no Guia do usuário do IAM.

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 puder executar. Para obter a lista completa das tarefas que exigem login como usuário-raiz, consulte [Tarefas que exigem credenciais de usuário-raiz](#) no Guia do Usuário do IAM.

Usuários e grupos 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, é recomendável contar com credenciais temporárias em vez de criar usuários do IAM com credenciais de longo prazo, como senhas e chaves de acesso. No entanto, se você tiver casos de uso específicos que exijam credenciais de longo prazo com usuários do IAM, é recomendável alternar as chaves de acesso. Para obter mais informações, consulte [Alternar as chaves de acesso regularmente para casos de uso que exijam credenciais de longo prazo](#) no Guia do Usuário do IAM.

Um [grupo do IAM](#) é uma identidade que especifica uma coleção de usuários do IAM. Não é possível fazer login como um grupo. É possível usar grupos para especificar permissões para vários usuários de uma vez. Os grupos facilitam o gerenciamento de permissões para grandes conjuntos de usuários. Por exemplo, você pode ter um grupo chamado IAMAdminse conceder a esse grupo permissões para administrar recursos do IAM.

Usuários são diferentes de perfis. Um usuário é exclusivamente associado a uma pessoa ou a uma aplicação, mas um perfil pode ser assumido por qualquer pessoa que precisar dele. Os usuários

têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte [Casos de uso para usuários do IAM](#) no Guia do usuário do IAM.

Perfis do IAM

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. Para assumir temporariamente uma função do IAM no AWS Management Console, você pode [alternar de um usuário para uma função do IAM \(console\)](#). Você pode assumir uma função chamando uma operação de AWS API AWS CLI ou usando uma URL personalizada. Para obter mais informações sobre métodos para usar perfis, consulte [Métodos para assumir um perfil](#) no Guia do usuário do IAM.

Perfis do IAM com credenciais temporárias são úteis nas seguintes situações:

- **Acesso de usuário federado:** para atribuir permissões a identidades federadas, é possível criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas por ele. Para ter mais informações sobre perfis para federação, consulte [Criar um perfil para um provedor de identidade de terceiros \(federação\)](#) no Guia do usuário do IAM. Se usar o Centro de Identidade do IAM, configure um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o Centro de Identidade do IAM correlaciona o conjunto de permissões a um perfil no IAM. Para obter informações sobre conjuntos de permissões, consulte [Conjuntos de Permissões](#) no Guia do Usuário do AWS IAM Identity Center .
- **Permissões temporárias para usuários do IAM:** um usuário ou um perfil do IAM pode presumir um perfil do IAM para obter temporariamente permissões diferentes para uma tarefa específica.
- **Acesso entre contas:** é possível usar um perfil do IAM para permitir que alguém (uma entidade principal confiável) em outra conta acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto, com alguns Serviços da AWS, você pode anexar uma política diretamente a um recurso (em vez de usar uma função como proxy). Para conhecer a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte [Acesso a recursos entre contas no IAM](#) no Guia do usuário do IAM.
- **Acesso entre serviços** — Alguns Serviços da AWS usam recursos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicativos na Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões da entidade principal da chamada, usando um perfil de serviço ou um perfil vinculado ao serviço.

- **Sessões de acesso direto (FAS)** — Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado 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 [Sessões de acesso direto](#).
- **Perfil de serviço:** um perfil de serviço é um [perfil do IAM](#) que um serviço assume para executar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte [Criar um perfil para delegar permissões a um AWS service \(Serviço da AWS\)](#) no Guia do Usuário do IAM.
- **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 presumir 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 editar as permissões para perfis vinculados a serviço.
- **Aplicativos em execução na Amazon EC2** — Você pode usar uma função do IAM para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma EC2 instância e fazendo solicitações AWS CLI de AWS API. Isso é preferível a armazenar chaves de acesso na EC2 instância. Para atribuir uma AWS função a uma EC2 instância e disponibilizá-la para todos os aplicativos, você cria um perfil de instância anexado à instância. Um perfil de instância contém a função e permite que programas em execução na EC2 instância recebam credenciais temporárias. Para obter mais informações, consulte [Usar uma função do IAM para conceder permissões a aplicativos executados em EC2 instâncias da Amazon](#) no Guia do usuário do IAM.

Gerenciar o 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 obter mais

informações sobre a estrutura e o conteúdo de documentos de políticas JSON, consulte [Visão geral das políticas JSON](#) no Guia do usuário do IAM.

Os administradores podem usar 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 perfis não têm permissões. Para conceder permissão aos usuários para executar ações nos recursos que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM aos perfis e os usuários podem assumir os perfis.

As políticas do IAM definem permissões para uma ação independentemente do método usado para executar a operação. Por exemplo, suponha que você tenha uma política que permite a ação `iam:GetRole`. Um usuário com essa política pode obter informações de 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 perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte [Definir permissões personalizadas do IAM com as políticas gerenciadas pelo cliente](#) no Guia do Usuário do IAM.

As políticas baseadas em identidade podem ser categorizadas como políticas em linha ou políticas gerenciadas. As políticas em linha são anexadas diretamente a um único usuário, grupo ou perfil. As políticas gerenciadas são políticas 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 recurso avançado no qual você define o máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM (usuário ou perfil do IAM). É possível definir um limite de permissões para uma entidade.

As permissões resultantes são a interseção das políticas baseadas em identidade de uma entidade com seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou o perfil no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte [Limites de permissões para identidades do IAM](#) no Guia do usuário do IAM.

- Políticas de controle de serviço (SCPs) — SCPs são políticas JSON que especificam as permissões máximas para uma organização ou unidade organizacional (OU) em AWS Organizations. AWS Organizations é um serviço para agrupar e gerenciar centralmente várias Contas da AWS que sua empresa possui. Se você habilitar todos os recursos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as suas contas. O SCP limita as permissões para entidades nas contas dos membros, incluindo cada um Usuário raiz da conta da AWS. Para obter mais informações sobre Organizations e SCPs, consulte [Políticas de controle de serviços](#) no Guia AWS Organizations do Usuário.
- Políticas de controle de recursos (RCPs) — RCPs são políticas JSON que você pode usar para definir o máximo de permissões disponíveis para recursos em suas contas sem atualizar as políticas do IAM anexadas a cada recurso que você possui. O RCP limita as permissões para recursos nas contas dos membros e pode afetar as permissões efetivas para identidades, incluindo a Usuário raiz da conta da AWS, independentemente de pertencerem à sua organização. Para obter mais informações sobre Organizations e RCPs, incluindo uma lista Serviços da AWS desse suporte RCPs, consulte [Políticas de controle de recursos \(RCPs\)](#) no Guia AWS Organizations 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 recursos. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, consulte [Políticas de sessão](#) no Guia do usuário do IAM.

Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Para saber como 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 Suporte, você deve entender quais recursos do IAM estão disponíveis para uso Suporte. Para ter uma visão de alto nível de como Suporte 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 Suporte usar o IAM, consulte [Gerenciar acesso para Suporte](#).

Tópicos

- [Políticas baseadas em identidade do Suporte](#)
- [Suporte Funções do IAM](#)

Políticas baseadas em identidade do Suporte

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 Suporte 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 podem ser usadas 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. Algumas operações também exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

Incluem ações em uma política para conceder permissões para executar a operação associada.

As ações políticas Suporte usam o seguinte prefixo antes da ação: `support:`. Por exemplo, para conceder permissão a alguém para executar uma EC2 instância da Amazon com a operação de EC2 `RunInstances` API da Amazon, você inclui a `ec2:RunInstances` ação na política dessa pessoa. As declarações de política devem incluir um elemento `Action` ou Suporte. 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 Suporte ações, consulte [Ações definidas por AWS Support](#) no Guia do usuário do IAM.

Exemplos

Para ver exemplos de políticas Suporte baseadas em identidade, consulte. [AWS Support exemplos de políticas baseadas em identidade](#)

Suporte Funções do IAM

Uma [função do IAM](#) é uma entidade dentro da sua AWS conta que tem permissões específicas.

Usando credenciais temporárias com Suporte

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 [AssumeRole](#) ou [GetFederationToken](#).

Suporte suporta o uso de credenciais temporárias.

Perfis vinculados a 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 em 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.

Suporte suporta funções vinculadas a serviços. Para obter detalhes sobre como criar ou gerenciar funções Suporte 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 significa que um administrador do IAM pode alterar as permissões para esse perfil. Porém, fazer isso pode alterar a funcionalidade do serviço.

Suporte 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 Suporte. 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 Suporte](#)
- [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 Suporte 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 Suporte rapidamente, use políticas AWS gerenciadas para dar aos 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 Suporte

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 Suporte 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 Suporte 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 criar uma política que permita 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": "*"
    }
  ]
}
```

Uso de perfis vinculados ao serviço

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. Suporte Trusted Advisor Em cada caso, a função vinculada ao serviço é uma função predefinida. Essa função inclui todas as permissões necessárias Suporte 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. Suporte 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, Suporte 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. Suporte Essa função vinculada ao serviço é predefinida e inclui as permissões Suporte necessárias para chamar outros AWS serviços em seu nome.

O perfil vinculado ao serviço `AWSServiceRoleForSupport` confia no serviço `support.amazonaws.com` para presumir o perfil.

Para fornecer esses serviços, as permissões predefinidas da função dão Suporte acesso aos metadados do recurso, não aos dados do cliente. Somente Suporte 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 [GetExecutionHistory](#) para a chamada de AWS Step Functions API não estão visíveis para Suporte. 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 obter 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 Suporte executadas em seu nome. Para obter informações sobre CloudTrail, consulte o [Guia AWS CloudTrail do usuário](#).

Permissões de função vinculada ao serviço Suporte

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 — Suporte 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 Suporte 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 — Suporte 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 obter mais informações, consulte [AWS políticas gerenciadas para AWS Support](#).

Criação de uma função vinculada ao serviço para Suporte

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 Suporte 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 Suporte

É possível usar o IAM para editar a descrição da função vinculada ao serviço `AWSServiceRoleForSupport`. Para obter mais informações, consulte [Editar um perfil vinculado ao serviço](#) no Guia do usuário do IAM.

A `AWSServiceRoleForSupport` função é necessária Suporte 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 [Suporte](#).

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 sua instância Amazon Elastic Compute Cloud EC2 (Amazon) 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](#)
- [Criação de uma função vinculada ao serviço para o Trusted Advisor](#)
- [Editar um perfil vinculado ao serviço para o Trusted Advisor](#)
- [Excluir um perfil vinculado 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 [Visão 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 um perfil vinculado 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.

Criação de 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 em <https://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 um perfil vinculado 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 um perfil vinculado 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 em <https://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 estão disponíveis para uso de todos os AWS clientes. Recomendamos que você reduza ainda mais as permissões definindo as [políticas gerenciadas pelo cliente](#) que são específicas para seus casos de uso.

Você não pode alterar as permissões definidas 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) é lançada ou novas operações de API são 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 Partner-Led Support](#)

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 Suporte](#).

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 88 novas permissões aos seguintes serviços para realizar ações que ajudam a solucionar problemas de clientes relacionados ao faturamento, suporte administrativo e técnico: • Amazon Bedrock — Para solucionar problemas relacionados ao Amazon Bedrock. • Amazon Connect — Para depurar problemas	25 de novembro de 2024

Alteração	Descrição	Data
	relacionados ao Amazon Connect. • Amazon DataZone — Para depurar problemas relacionados à Amazon DataZone. • Amazon EC2 — Para solucionar problemas relacionados à Amazon EC2. • Amazon EKS — Para depurar problemas relacionados ao Amazon EKS. • AWS Glue — Para solucionar problemas relacionados a. AWS Glue • Amazon Managed Service para Apache Flink — Para solucionar problemas relacionados ao Amazon Managed Service para Apache Flink. • AWS Lambda — Para depurar problemas relacionados ao AWS Lambda.	

Alteração	Descrição	Data
AWSSupportServiceRolePolicy : atualização para uma política existente	Foram adicionadas 79 novas permissões aos seguintes serviços para realizar ações que ajudam a solucionar problemas de clientes relacionados ao faturamento, suporte administrativo e técnico: • Amazon OpenSearch Serverless — Para solucionar problemas relacionados ao Amazon OpenSearch Serverless. • AWS AppConfig — Para depurar problemas relacionados a. AWS AppConfig • Sinais do aplicativo — Para depurar problemas relacionados aos sinais do aplicativo. • Amazon Athena — Para solucionar problemas relacionados ao Amazon Athena. • Amazon CloudWatch — Para depurar problemas relacionados à Amazon CloudWatch. • Amazon DynamoDB — Para solucionar problemas relacionados ao Amazon DynamoDB.	8 de outubro de 2024

Alteração	Descrição	Data
	• Amazon EC2 — Para solucionar problemas relacionados à Amazon EC2. • AWS IoT — Para depurar problemas relacionados ao AWS IoT. • AWS Lambda — Para solucionar problemas relacionados ao AWS Lambda. • AWS Launch Wizard — Para solucionar problemas relacionados ao AWS Launch Wizard. • AWS Security Hub — Para depurar problemas relacionados a. AWS Security Hub • Amazon WorkSpaces — Para depurar problemas relacionados à Amazon WorkSpaces.	

Alteração	Descrição	Data
AWSSupportServiceRolePolicy : atualização para uma política existente	Foram adicionadas 79 novas permissões aos seguintes serviços para realizar ações que ajudam a solucionar problemas de clientes relacionados ao faturamento, suporte administrativo e técnico: • Conta da AWS — Para solucionar problemas relacionados ao Conta da AWS. • AWS Auto Scaling — Para depurar problemas relacionados a. AWS Auto Scaling • Amazon Bedrock — Para depurar problemas relacionados ao Amazon Bedrock. • AWS CodeConnections — Para solucionar problemas relacionados ao AWS CodeConnections. • AWS Deadline Cloud — Para depurar problemas relacionados ao AWS Deadline Cloud. • Amazon Elastic Kubernetes Service: para solucionar problemas relativos ao Amazon Elastic Kubernetes Service.	5 de agosto de 2024

Alteração	Descrição	Data
	• Elastic Load Balancing — Para solucionar problemas relacionados ao Elastic Load Balancing. • AWS Nível gratuito — Para depurar problemas relacionados ao nível AWS gratuito. • Amazon Inspector — Para solucionar problemas relacionados ao Amazon Inspector. • OpenSearch Ingestão da Amazon — Para solucionar problemas relacionados à ingestão da Amazon OpenSearch . • Amazon WorkSpaces — Para depurar problemas relacionados à Amazon WorkSpaces. • AWS X-Ray — Para depurar problemas relacionados ao AWS X-Ray.	

Alteração	Descrição	Data
AWSSupportServiceRolePolicy : atualização para uma política existente	Foram adicionadas 17 novas permissões aos seguintes serviços para realizar ações que ajudam a solucionar problemas de clientes relacionados ao faturamento, 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.	22 de março de 2024

Alteração	Descrição	Data
AWSSupportServiceRolePolicy : atualização para uma política existente	Foram adicionadas 63 novas permissões aos seguintes serviços para realizar ações que ajudam 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 AI — Para solucionar problemas relacionados ao serviço Amazon SageMaker AI. • 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 à 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 Edge — Para solucionar problemas relacionados a. AWS Snowball Edge • 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 relacionados ao EC2 serviço da Amazon. • 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 AWS EC2 Image 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 relacionados 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 AI — Para depurar problemas relacionados à Amazon SageMaker AI.	

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 solucionar problemas relacionados ao Elastic Disaster Recovery. • Amazon CloudWatch — Para solucionar problemas de configuração da Amazon. CloudWatch • Amazon EC2 — Para depurar problemas relacionados ao EC2 serviço. • AWS Certificate Manager — Para solucionar problemas relacionados ao Certificate Manager.	

Alteração	Descrição	Data
	• Amazon EventBridge Scheduler — Para solucionar 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 relacionados ao serviço 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 CloudWatch 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 AWS Support desenvolvimento de ferramentas para apoiar a importação e exportação para um repositório de FSx dados da Amazon. • GameLift Servidores Amazon — Para solucionar problemas relacionados aos GameLift servidores Amazon. • 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	

Alteração	Descrição	Data
	Managed Service for Prometheus. • 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 a. AWS Mainframe Modernization • 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 resolvidor 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 ao CloudWatch Logs. • Amazon Interactive Video Service — Para ajudar a Suporte 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 solucionar	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. • Amazon EC2 Recycle Bin — 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 ver a descrição dos FSx instantâneos da Amazon.	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 informações, consulte Alterações de permissão do AWSSupportServiceRolePolicy.	
Publicação do log de alterações	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:GetAnalyticsConfiguration
	s3.ListBucketAnalyticsConfiguration	
	s3.GetBucketNotificationConfiguration	s3:GetBucketNotification
	s3.GetBucketEncryption	s3:GetEncryptionConfiguration
	s3.GetBucketIntelligentTieringConfiguration	s3:GetIntelligentTieringConfiguration
	s3.ListBucketIntelligentTieringConfiguration	
	s3.GetBucketInventoryConfiguration	s3:GetInventoryConfiguration
	s3.ListBucketInventoryConfiguration	
	s3.GetBucketLifecycleConfiguration	s3:GetLifecycleConfiguration

Data	Nome da operação da API	Permissões do IAM necessárias
	s3.GetBucketMetricsConfiguration	s3:GetMetricsConfiguration
	s3.ListBucketMetricsConfiguration	
	s3.GetBucketReplication	s3:GetReplicationConfiguration
	s3.HeadBucket	s3:ListBucket
	s3.ListObjects	
	s3.ListBuckets	s3:ListAllMyBuckets
	s3.ListMultipartUploads	s3:ListBucketMultipartUploads
	s3.ListObjectVersions	s3:ListBucketVersions
	s3.ListParts	s3:ListMultipartUploadParts

AWS políticas gerenciadas para AWS Support aplicativos no Slack

Note

Para acessar e visualizar casos de suporte no AWS Support Center Console, consulte [Gerencie 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 [AWS Support Aplicativo 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 permissões

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 [Gerenciando o acesso ao AWS Support aplicativo](#).

AWS política gerenciada: AWSSupportAppReadOnlyAccess

A [AWSSupportAppReadOnlyAccess](#) política concede permissões que permitem que a entidade execute ações do AWS Support aplicativo somente para leitura. Para obter mais informações, consulte [AWS Support Aplicativo no Slack](#).

Detalhes de permissões

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
AWSSupportAppFullAccess e 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 informações, consulte Gerenciando o acesso ao AWS Support aplicativo .	19 de agosto de 2022
Publicação do log de alterações	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 [AWSTrustedAdvisorPriorityFullAccess](#) política 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 das permissões

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 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 [AWSTrustedAdvisorPriorityReadOnlyAccess](#) política concede permissões somente de leitura à Trusted Advisor Priority, incluindo permissão para visualizar as contas de administrador delegado.

Detalhes das permissões

Na primeira declaração, a política inclui as seguintes permissões para `trustedadvisor`:

- Descreve sua Trusted Advisor conta e 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.

- `accessanalyzer`— Descreve AWS Identity and Access Management Access Analyzer os recursos
- `AutoScaling`— Descreve as cotas e os recursos da conta 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
- `dynamodbaccelerator`— Descreve os recursos do DynamoDB Accelerator
- `ec2`— Descreve as cotas e os recursos da conta 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
- `networkfirewall`— Descreve AWS Network Firewall os recursos
- `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": [
    {
      "Sid" : "TrustedAdvisorServiceRolePermissions",
      "Effect": "Allow",
      "Action": [
        "access-analyzer:ListAnalyzers",
        "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",
        "cloudwatch:ListMetrics",
        "dax:DescribeClusters",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeTable",
        "dynamodb:ListTables",
        "ec2:DescribeAddresses",
        "ec2:DescribeReservedInstances",
        "ec2:DescribeInstances",
        "ec2:DescribeVpcs",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeImages",
        "ec2:DescribeNatGateways",
        "ec2:DescribeVolumes",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeRegions",
        "ec2:DescribeReservedInstancesOfferings",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVpcEndpoints",
```

```
"ec2:DescribeVpnConnections",
"ec2:DescribeVpnGateways",
"ec2:DescribeLaunchTemplateVersions",
"ec2:GetManagedPrefixListEntries",
"ecs:DescribeTaskDefinition",
"ecs:ListTaskDefinitions"
"elasticloadbalancing:DescribeAccountLimits",
"elasticloadbalancing:DescribeInstanceHealth",
"elasticloadbalancing:DescribeLoadBalancerAttributes",
"elasticloadbalancing:DescribeLoadBalancerPolicies",
"elasticloadbalancing:DescribeLoadBalancerPolicyTypes",
"elasticloadbalancing:DescribeLoadBalancers",
"elasticloadbalancing:DescribeListeners",
"elasticloadbalancing:DescribeRules",
"elasticloadbalancing:DescribeTargetGroups",
"elasticloadbalancing:DescribeTargetHealth",
"iam:GenerateCredentialReport",
"iam:GetAccountPasswordPolicy",
"iam:GetAccountSummary",
"iam:GetCredentialReport",
"iam:GetServerCertificate",
"iam:ListServerCertificates",
"iam:ListSAMLProviders",
"kinesis:DescribeLimits",
"kafka:DescribeClusterV2",
"kafka:ListClustersV2",
"kafka:ListNodes",
"network-firewall:ListFirewalls",
"network-firewall:DescribeFirewall",
"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:GetQueueAttributes",
        "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 obter 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 Atualize para uma política existente.	Trusted Advisor adicionou novas ações para conceder elasticloadbalancing:DescribeListeners, as elasticloadbalancing:DescribeRules permissões e.	30 de outubro de 2024
AWSTrustedAdvisorServiceRolePolicy Atualize para uma política existente.	Trusted Advisor adicionou novas ações para conceder as sqs:GetQueueAttributes permissões access-analyzer:ListAnalyzers cloudwatch:ListMetrics dax:DescribeClusters ,ec2:DescribeNatGateways ,ec2:DescribeRouteTables ,ec2:DescribeVpcEndpoints , ec2:GetManagedPrefixListEntries elasticlo	11 de junho de 2024

Alteração	Descrição	Data
	adbalanci ng:DescribeTargetH ealth ,iam:ListS AMLProviders ,, kafka:DescribeClus terV2 network-f irewall:ListFirewa lls network-f irewall:DescribeFi rewall e.	
AWSTrustedAdvisorServiceRolePolicy Atualize para uma política existente.	Trusted Advisor adicionou novas ações para conceder o cloudtrail:GetTrail cloudtrail:ListTrails cloudtrail:GetEventSelectors outposts:GetOutposts ,outposts:ListAssets e outposts:ListOutposts permissões.	18 de janeiro de 2024
AWSTrustedAdvisorPriorityFullAccess Atualize para uma política existente.	Trusted Advisor atualizou a política AWSTrustedAdvisorPriorityFullAccess AWS gerenciada para incluir a declaração IDs.	6 de dezembro de 2023
AWSTrustedAdvisorPriorityReadOnlyAccess Atualize para uma política existente.	Trusted Advisor atualizou a política AWSTrustedAdvisorPriorityReadOnlyAccess AWS gerenciada para incluir a declaração IDs.	6 de dezembro de 2023

Alteração	Descrição	Data
AWSTrustedAdvisorServiceRolePolicy : atualização para uma política existente	Trusted Advisor adicionou novas ações para conceder <code>ec2:DescribeRegions</code> , <code>s3:GetLifecycleConfiguration</code> , <code>ecs:DescribeTaskDefinition</code> , <code>ecs:ListTaskDefinitions</code> permissões e.	9 de novembro de 2023
AWSTrustedAdvisorServiceRolePolicy : atualização para uma política existente	Trusted Advisor adicionou novas ações do <code>IAMroute53resolver:ListResolverEndpoints</code> , <code>route53resolver:ListResolverEndpointIpAddresses</code> , <code>ec2:DescribeSubnets</code> , <code>kafka:ListClustersV2</code> e <code>kafka:ListNodes</code> para integrar novas verificações de resiliência.	14 de setembro de 2023
AWSTrustedAdvisorReportingServiceRolePolicy V2 da política gerenciada anexada à função vinculada ao Trusted Advisor <code>AWSServiceRoleForTrustedAdvisorReporting</code> serviço	Atualize a política AWS gerenciada para V2 para a função vinculada ao Trusted Advisor <code>AWSServiceRoleForTrustedAdvisorReporting</code> serviço. A V2 adicionará mais uma ação <code>organizations:ListDelegatedAdministrators</code> do IAM	28 de fevereiro de 2023

Alteração	Descrição	Data
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
AWSTrustedAdvisorServiceRolePolicy: atualização para uma política existente	Trusted Advisor adicionou novas ações para conceder <code>DescribeTargetGroups</code> as <code>GetAccountPublicAccessBlock</code> permissões e. <code>DescribeTargetGroup</code> é necessário para a permissão <code>Auto Scaling Group Health Check</code> (Verificação de integridade do grupo do Auto Scaling) para recuperar balanceadores de carga não clássicos anexados a um grupo do Auto Scaling. <code>GetAccountPublicAccessBlock</code> é necessário para a permissão <code>Amazon S3 Bucket Permissions</code> (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

Alteração	Descrição	Data
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
- Veja uma lista de todos os modificadores do plano de suporte para seu Conta da AWS

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "supportplans:GetSupportPlan",
        "supportplans:GetSupportPlanUpdateStatus",
        "supportplans:StartSupportPlanUpdate",
```

```

        "supportplans:CreateSupportPlanSchedule"
        "supportplans:ListSupportPlanModifiers"
    ],
    "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
- Veja uma lista de todos os modificadores do plano de suporte para seu Conta da AWS

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "supportplans:GetSupportPlan",
        "supportplans:GetSupportPlanUpdateStatus",
        "supportplans:ListSupportPlanModifiers"
      ],
      "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
AWSSupportPlansReadOnlyAccess - Atualização em uma política existente AWSSupportPlansFullAccess - Atualização em uma política existente	Adicione ListSupportPlanModifiers ações AWSSupportPlansFullAccess e políticas AWSSupportPlansReadOnlyAccess gerenciadas.	9 de setembro de 2024
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

AWS políticas gerenciadas para AWS Partner-Led 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 estão disponíveis para uso de todos os AWS

clientes. Recomendamos que você reduza ainda mais as permissões definindo as [políticas gerenciadas pelo cliente](#) que são específicas para seus casos de uso.

Você não pode alterar as permissões definidas 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) é lançada ou novas operações de API são disponibilizadas para serviços existentes.

Para mais informações, consulte [Políticas gerenciadas pela AWS](#) no Manual do usuário do IAM.

AWS política gerenciada: `AWSPartnerLedSupportReadOnlyAccess`

Você pode anexar `AWSPartnerLedSupportReadOnlyAccess` aos seus usuários, grupos e funções.

Essa política pode ser usada para conceder acesso somente de leitura aos metadados de serviços da sua conta APIs que podem ler. AWS Você pode usar essa política para fornecer aos seus parceiros do AWS Partner-Led Support Program acesso aos serviços especificados na seção de detalhes de permissões abaixo.

Detalhes das permissões

Esta política inclui as seguintes permissões.

- `acm`— Permita que os diretores solucionem casos de suporte técnico relacionados a. AWS Certificate Manager
- `acm-pca`— Permita que os diretores solucionem casos de suporte técnico relacionados a. AWS Private Certificate Authority
- `apigateway`— Permita que os diretores solucionem casos de suporte técnico relacionados ao Amazon API Gateway.
- `athena`— Permita que os diretores solucionem casos de suporte técnico relacionados ao Amazon Athena.

- `backup`— Permita que os diretores solucionem casos de suporte técnico relacionados a. AWS Backup
- `backup-gateway`— Permita que os diretores solucionem casos de suporte técnico relacionados ao AWS Backup Gateway.
- `cloudformation`— Permita que os diretores solucionem casos de suporte técnico relacionados a. AWS CloudFormation
- `cloudfront`— Permita que os diretores solucionem casos de suporte técnico relacionados à Amazon. CloudFront
- `cloudtrail`— Permita que os diretores solucionem casos de suporte técnico relacionados a. AWS CloudTrail
- `cloudwatch`— Permita que os diretores solucionem casos de suporte técnico relacionados à Amazon. CloudWatch
- `codepipeline`— Permita que os diretores solucionem casos de suporte técnico relacionados a. AWS CodePipeline
- `cognito-identity`— Permita que os diretores solucionem casos de suporte técnico relacionados à Identidade do Amazon Cognito.
- `cognito-idp`— Permita que os diretores solucionem casos de suporte técnico relacionados aos grupos de usuários do Amazon Cognito.
- `cognito-sync`— Permita que os diretores solucionem casos de suporte técnico relacionados ao Amazon Cognito Sync.
- `connect`— Permita que os diretores solucionem casos de suporte técnico relacionados ao Amazon Connect.
- `directconnect`— Permita que os diretores solucionem casos de suporte técnico relacionados a. AWS Direct Connect
- `dms`— Permita que os diretores solucionem casos de suporte técnico relacionados a. AWS Database Migration Service
- `ds`— Permita que os diretores solucionem casos de suporte técnico relacionados a. AWS Directory Service
- `ec2`— Permita que os diretores solucionem casos de suporte técnico relacionados ao Amazon Elastic Compute Cloud. Isso inclui categorias de suporte técnico em EC2 (Windows e Linux), Virtual Private Cloud (VPC) e VPC.
- `ecs`— Permita que os diretores solucionem casos de suporte técnico relacionados ao Amazon Elastic Container Service.

- `eks`— Permita que os diretores solucionem casos de suporte técnico relacionados ao Amazon Elastic Kubernetes Service.
- `elasticache`— Permita que os diretores solucionem casos de suporte técnico relacionados à Amazon. ElastiCache
- `elasticbeanstalk`— Permita que os diretores solucionem casos de suporte técnico relacionados a. AWS Elastic Beanstalk
- `elasticfilesystem`— Permita que os diretores solucionem casos de suporte técnico relacionados ao Amazon Elastic File System.
- `elasticloadbalancing`— Permita que os diretores solucionem casos de suporte técnico relacionados ao Elastic Load Balancing.
- `emr-containers`— Permita que os diretores solucionem casos de suporte técnico relacionados ao Amazon EMR no EKS.
- `emr-serverless`— Permita que os diretores solucionem casos de suporte técnico relacionados ao Amazon EMR Serverless.
- `es`— Permita que os diretores solucionem casos de suporte técnico relacionados ao Amazon OpenSearch Service. Isso inclui categorias de suporte técnico, como OpenSearch Service Managed Cluster.
- `events`— Permita que os diretores solucionem casos de suporte técnico relacionados à Amazon. EventBridge
- `fsx`— Permita que os diretores solucionem casos de suporte técnico relacionados à Amazon. FSx. Isso inclui categorias de suporte técnico, como FSX for Windows File Server.
- `glue`— Permita que os diretores solucionem casos de suporte técnico relacionados a. AWS Glue
- `guardduty`— Permita que os diretores solucionem casos de suporte técnico relacionados à Amazon. GuardDuty
- `iam`— Permita que os diretores solucionem casos de suporte técnico relacionados a. AWS Identity and Access Management
- `kafka`— Permita que os diretores solucionem casos de suporte técnico relacionados ao Amazon Managed Streaming for Apache Kafka.
- `kafkaconnect`— Permita que os diretores solucionem casos de suporte técnico relacionados ao Amazon Managed Streaming for Apache Kafka Connect.
- `lambda`— Permita que os diretores solucionem casos de suporte técnico relacionados a. AWS Lambda

- `logs`— Permite que os diretores solucionem casos de suporte técnico relacionados ao Amazon CloudWatch Logs.
- `medialive`— Permite que os diretores solucionem casos de suporte técnico relacionados a. AWS Elemental MediaLive
- `mobiletargeting`— Permite que os diretores solucionem casos de suporte técnico relacionados ao Amazon Pinpoint.
- `pipes`— Permite que os diretores solucionem casos de suporte técnico relacionados ao Amazon EventBridge Pipes.
- `polly`— Permite que os diretores solucionem casos de suporte técnico relacionados ao Amazon Polly.
- `quicksight`— Permite que os diretores solucionem casos de suporte técnico relacionados à Amazon. QuickSight
- `rds`— Permite que os diretores solucionem casos de suporte técnico relacionados ao Amazon Relational Database Service. Isso inclui categorias de suporte técnico, como: Relational Database Service (Aurora - MySQL-compat), Relational Database Service (Aurora - PostgreSQL-C), Relational Database Service (PostgreSQL), Relational Database Service (SQL Server), Relational Database Service (MySQL) e Relational Database Service (Oracle).
- `redshift`— Permite que os diretores solucionem casos de suporte técnico relacionados ao Amazon Redshift.
- `redshift-data`— Permite que os diretores solucionem casos de suporte técnico relacionados à API de dados do Amazon Redshift.
- `redshift-serverless`— Permite que os diretores solucionem casos de suporte técnico relacionados ao Amazon Redshift Serverless.
- `route53`— Permite que os diretores solucionem casos de suporte técnico relacionados ao Amazon Route 53.
- `route53domains`— Permite que os diretores solucionem casos de suporte técnico relacionados aos domínios do Amazon Route 53.
- `route53-recovery-cluster`— Permite que os diretores solucionem casos de suporte técnico relacionados ao cluster de recuperação do Amazon Route 53.
- `route53-recovery-control-config`— Permite que os diretores solucionem casos de suporte técnico relacionados aos controles de recuperação do Amazon Route 53.
- `route53-recovery-readiness`— Permite que os diretores solucionem casos de suporte técnico relacionados à prontidão de recuperação do Amazon Route 53.

- `route53resolver`— Permita que os diretores solucionem casos de suporte técnico relacionados ao Amazon Route 53 Resolver.
- `s3`— Permita que os diretores solucionem casos de suporte técnico relacionados ao Amazon Simple Storage Service.
- `s3express`— Permita que os diretores solucionem casos de suporte técnico relacionados ao Amazon S3 Express.
- `sagemaker`— Permita que os diretores solucionem casos de suporte técnico relacionados à Amazon SageMaker AI.
- `scheduler`— Permita que os diretores solucionem casos de suporte técnico relacionados ao Amazon EventBridge Scheduler.
- `servicequotas`— Permita que os diretores solucionem casos de suporte técnico relacionados às Quotas de Serviço.
- `ses`— Permita que os diretores solucionem casos de suporte técnico relacionados ao Amazon Simple Email Service.
- `sns`— Permita que os diretores solucionem casos de suporte técnico relacionados ao Amazon Simple Notification Service.
- `ssm`— Permita que os diretores solucionem casos de suporte técnico relacionados a. AWS Systems Manager
- `ssm-contacts`— Permita que os diretores solucionem casos de suporte técnico relacionados aos AWS Systems Manager Incident Manager Contatos.
- `ssm-incidents`— Permita que os diretores solucionem casos de suporte técnico relacionados a. AWS Systems Manager Incident Manager
- `ssm-sap`— permita que os diretores solucionem casos de suporte técnico relacionados ao SAP AWS Systems Manager .
- `swf`— Permita que os diretores solucionem casos de suporte técnico relacionados ao Amazon Simple Workflow Service.
- `vpc-lattice`— Permita que os diretores solucionem casos de suporte técnico relacionados ao Amazon VPC Lattice. Isso inclui categorias de suporte técnico, como VPC - Transit Gateway.
- `waf`— Permita que os diretores solucionem casos de suporte técnico relacionados a. AWS WAF
- `waf-regional`— Permita que os diretores solucionem casos de suporte técnico relacionados ao AWS WAF Regional.
- `wafv2`— Permita que os diretores solucionem casos de suporte técnico relacionados à AWS WAF V2.

- `workspaces`— Permita que os diretores solucionem casos de suporte técnico relacionados à Amazon. WorkSpaces Isso inclui categorias de suporte técnico, como Espaços de trabalho (Windows).
- `workspaces-web`— Permita que os diretores solucionem casos de suporte técnico relacionados ao Amazon WorkSpaces Secure Browser. Isso inclui categorias de suporte técnico, como Espaços de trabalho (Windows).

Para visualizar as permissões para esta política, consulte [AWSPartnerLedSupportReadOnlyAccess](#) na Referência de políticas gerenciadas pela AWS .

AWS Atualizações do Partner-Led Support para políticas AWS gerenciadas

Veja detalhes sobre as atualizações das políticas AWS gerenciadas do AWS Partner-Led Support desde que esse serviço começou a monitorar essas mudanças. Para receber alertas automáticos sobre alterações nessa página, assine o feed RSS na página de histórico do AWS Partner-Led Support Document.

Alteração	Descrição	Data
AWSPartnerLedSupportReadOnlyAccess – Nova política	Foi adicionada uma nova política AWS gerenciada que contém permissões que podem ler metadados de serviços em sua AWS conta.	22 de novembro de 2024
AWS O Partner-Led Support começou a monitorar as mudanças	AWS O Partner-Led Support começou a monitorar as mudanças em suas políticas AWS gerenciadas.	22 de novembro de 2024

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:

- Uso AWS Identity and Access Management (IAM).
- Use o endereço de e-mail e a senha associados à sua AWS conta. Essa identidade é chamada de usuário raiz da AWS conta (não recomendado).

Se você tiver um plano Business, Enterprise On-Ramp ou Enterprise Support, também poderá usar a [Suporte API](#) para acessar Suporte e Trusted Advisor operar programaticamente. Para obter mais informações, consulte a [Referência da API do AWS Support](#).

 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 (não recomendada)

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 Suporte ações no console. Você também pode especificar essas Suporte ações em uma política do IAM para permitir ou negar ações específicas.

 Note

Negar qualquer uma das ações a seguir em suas políticas do IAM pode resultar em um comportamento não intencional no Support Center ao criar ou interagir com um caso de suporte.

Ação	Descrição
AddAttachmentsToSet	Concede permissão para adicionar um ou mais anexos a um conjunto de anexos. Um conjunto de anexos é um contêiner temporário para anexos que você adiciona a um caso ou comunicação de caso. O conjunto fica disponível por 1 hora após sua criação. O expiryTime retornado na resposta é quando o conjunto expira.
AddCommunicationToCase	Concede permissão para adicionar mais comunicação com o cliente a um Suporte caso, incluindo um conjunto de endereços de e-mail para copiar na comunicação.
CreateCase	Concede permissão para criar um caso.
DescribeAttachment	Concede permissão para recuperar um anexo em um caso.
DescribeCaseAttributes	Concede permissão para que os serviços secundários leiam os atributos do caso do Suporte . *Isso é usado internamente pelo Suporte Center para obter atributos marcados em seu caso.
DescribeCases	Concede permissão para retornar uma lista de Suporte casos que corresponda a um ID de caso ou caso IDs.
DescribeCommunication	Concede permissão para obter uma única comunicação e anexos para um único AWS Suporte caso.
DescribeCommunications	Concede permissão para devolver comunicações e anexos de um ou mais Suporte casos.

Ação	Descrição
<code>DescribeCreateCaseOptions</code>	Concede permissão para retornar uma lista de <code>CreateCaseOption</code> tipos junto com os horários suportados correspondentes e a disponibilidade do idioma.
<code>DescribeIssueTypes</code>	Concede permissão para retornar tipos de problemas para casos do Suporte . Isso é usado internamente pelo Suporte Center para obter os tipos de problemas disponíveis para sua conta.
<code>DescribeServices</code>	Concede permissão para retornar a lista atual de AWS serviços e uma lista de categorias de serviço para cada serviço. Em seguida, você usa nomes e categorias de serviços para criar um caso. Cada AWS serviço tem seu próprio conjunto de categorias.
<code>DescribeSeverityLevels</code>	Concede permissão para retornar a lista de níveis de gravidade que você pode atribuir a um Suporte caso.
<code>DescribeSupportedLanguages</code>	Concede permissão para retornar uma lista de idiomas compatíveis para um <code>CategoryCode</code> , <code>IssueType</code> e <code>ServiceCode</code> especificado.
<code>DescribeSupportLevel</code>	Concede permissão para retornar o nível de suporte de um identificador de AWS conta. Isso é usado internamente pelo Suporte Center para identificar seu nível de suporte.
<code>DescribeTrustedAdvisorCheckRefreshStatuses</code>	Concede permissão para retornar o status de atualização das AWS Trusted Advisor verificações que têm a verificação IDs especificada.

Ação	Descrição
<code>DescribeTrustedAdvisorCheckResult</code>	Concede permissão para retornar os resultados da AWS Trusted Advisor verificação que tem a ID de verificação especificada.
<code>DescribeTrustedAdvisorChecks</code>	Concede permissão para retornar informações sobre todos os AWS Trusted Advisor cheques disponíveis, incluindo nome, ID, categoria, descrição e metadados.
<code>DescribeTrustedAdvisorCheckSummaries</code>	Concede permissão para retornar os resultados dos AWS Trusted Advisor resumos da verificação IDs especificada.
<code>GetInteraction</code>	Concede permissão para recuperar detalhes sobre uma interação específica por meio de seu identificador exclusivo. Isso é usado internamente pelo Suporte Center para recuperar recomendações personalizadas.
<code>InitiateCallForCase</code>	Concede permissão para iniciar uma chamada no Suporte Center. Isso é usado internamente pelo Suporte Center para iniciar uma chamada em seu nome.
<code>InitiateChatForCase</code>	Concede permissão para iniciar uma chamada no Suporte Center. Isso é usado internamente pelo Suporte Center para iniciar um bate-papo em seu nome.
<code>PutCaseAttributes</code>	Concede permissão para permitir que serviços secundários anexem atributos aos Suporte casos. Isso é usado internamente pelo Suporte Center para adicionar tags operacionais aos seus Suporte casos.

Ação	Descrição
RateCaseCommunication	Concede permissão para avaliar a comunicação de um Suporte caso.
RefreshTrustedAdvisorCheck	Concede permissão para atualizar o AWS Trusted Advisor cheque que você especifica usando a ID do cheque.
ResolveCase	Concede permissão para resolver um Suporte caso.
SearchForCases	Concede permissão para retornar uma lista de Suporte casos que corresponda às entradas fornecidas. Isso é usado internamente pelo Suporte Center para encontrar casos pesquisados.
StartInteraction	Concede permissão para iniciar uma nova interação e receber assistência personalizada para solução de problemas técnicos e de conta. Isso é usado internamente pelo Suporte Center para iniciar o processo de solução de problemas.

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 Suporte 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 no seu e trabalhar Conta da AWS 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 [Fazer login no AWS Management Console como usuário do IAM](#) no Guia do usuário do IAM.

A maneira mais fácil de conceder permissões é anexar a política AWS gerenciada [AWSSupportAccess](#) ao 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 Suporte ações

A política AWS gerenciada [AWSSupportAccess](#) concede acesso a um usuário do IAM Suporte 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 \(console\)](#) no Manual 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 Suporte, 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 Suporte API, o namespace `support` do IAM controla o acesso a. Trusted Advisor Para obter 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
<code>GetSupportPlan</code>	Concede permissão para visualizar detalhes sobre o plano de suporte atual para esta Conta da AWS.
<code>GetSupportPlanUpdateStatus</code>	Concede permissão para visualizar detalhes sobre o status de uma solicitação de atualização de um plano de suporte.
<code>StartSupportPlanUpdate</code>	Concede permissão para iniciar a solicitação de atualização do plano de suporte para esta Conta da AWS.
<code>CreateSupportPlanSchedule</code>	Concede permissão para criar agendamentos de planos de suporte para esta Conta da AWS.

Ação	Descrição
<code>ListSupportPlanModifiers</code>	Concede permissão para visualizar uma lista de todos os modificadores do plano de suporte para isso 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": "*"
    },
    {
      "Effect": "Allow",
      "Action": "supportplans:List*",
      "Resource": "*"
    }
  ]
}
```

```
        "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 obter 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). SCPs são um tipo de política que gerencia 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 AWS Organizations do usuário.
- [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. Todas as Contas da AWS têm acesso a uma seleção de [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 [AWS Trusted Advisor verifique a referência](#).

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 Suporte API. Em vez disso, use o namespace `support` para Suporte.

Note

Se você tiver permissões para a [AWS Support](#) API, 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 Suporte plano e várias Trusted Advisor preferências.
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 .
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.

Ação	Descrição
<code>DescribeCheckStatusHistoryChanges</code>	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 [Visão organizacional para AWS Trusted Advisor](#).

Ação	Descrição
<code>DescribeOrganization</code>	Concede permissão para ver se Conta da AWS ele atende aos requisitos para ativar o recurso de visualização organizacional.
<code>DescribeOrganizationAccounts</code>	Concede permissão para visualizar as AWS contas vinculadas que estão na organização.
<code>DescribeReports</code>	Concede permissão para visualizar detalhes para relatórios de visualização organizacional, como o nome do relatório, o runtime, a data de criação, o status e o formato
<code>DescribeServiceMetadata</code>	Concede permissão para visualizar informações sobre relatórios de exibição organizacional, como categorias de verificação Regiões da AWS, nomes de cheques e status de recursos.
<code>GenerateReport</code>	Concede permissão para criar um relatório para Trusted Advisor cheques em sua organização.
<code>ListAccountsForParent</code>	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).

Ação	Descrição
ListOrganizationalUnitsForParent	Concede permissão para visualizar, no Trusted Advisor console, todas as unidades organizacionais (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 [Comece com o AWS Trusted Advisor Priority](#).

Ação	Descrição
DescribeRisks	Concede permissão para visualizar riscos em Trusted Advisor Prioridade.

Ação	Descrição
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.
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, consulte [Exemplos de políticas do IAM para o Trusted Advisor Engage](#).

Para obter mais informações, consulte [Comece a usar o AWS Trusted Advisor Engage \(versão prévia\)](#).

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.
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 Suporte 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 Suporte 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 Suporte API. Em vez disso, use o namespace `support`. Você precisa ter permissões na Suporte API para fazer chamadas Trusted Advisor programaticamente.

Por exemplo, se você quiser chamar a [RefreshTrustedAdvisorCheck](#) operação, 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 Suporte API Trusted Advisor, mas não o resto das operações da Suporte 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 Suporte e Trusted Advisor, consulte [Ações](#).

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 [Comece com o 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 serviço (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](#). SCPs oferece controle central sobre o máximo de permissões disponíveis para todas as contas em sua 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 SCPs, você deve primeiro fazer o seguinte:

- Ativar todos os recursos em sua organização. Para obter mais informações, consulte [Habilitar todos os recursos em sua organização](#) no Manual do usuário do AWS Organizations .

- Habilite SCPs para uso em sua organização. Para obter mais informações, consulte [Habilitar e desabilitar tipos de política](#) no Guia do usuário do AWS Organizations .
- Crie o SCPs que você precisa. Para obter mais informações sobre a criação SCPs, consulte [Criação, atualização e exclusão de políticas de controle de serviços](#) no Guia do AWS Organizations usuário.

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 Suporte 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 Suporte](#)
- [Quero permitir que pessoas fora da minha AWS conta acessem meus Suporte 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 Suporte.

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 Suporte. 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 Suporte

Para permitir que outras pessoas acessem Suporte, você deve conceder permissão às pessoas ou aplicativos que precisam de acesso. Se você estiver usando o AWS IAM Identity Center para gerenciar pessoas e aplicações, atribua conjuntos de permissões a usuários ou grupos para definir o nível de acesso. Os conjuntos de permissões criam e atribuem automaticamente políticas do IAM aos perfis do IAM associados à pessoa ou aplicação. Para ter mais informações, consulte [Conjuntos de permissões](#) no Guia do usuário do AWS IAM Identity Center .

Se você não estiver usando o Centro de Identidade do IAM, deverá criar entidades do IAM (usuários ou perfis) para as pessoas ou aplicações que precisam de acesso. Você deve anexar uma política à entidade que concede a eles as permissões corretas no Suporte. Depois que as permissões forem concedidas, forneça as credenciais ao usuário ou desenvolvedor da aplicação. Eles usarão essas credenciais para acessar AWS. Para saber mais sobre como criar grupos, políticas, permissões e usuários do IAM, consulte [Identities do IAM](#) e [Políticas e permissões no IAM](#) no Guia do usuário do IAM.

Quero permitir que pessoas fora da minha AWS conta acessem meus Suporte recursos

Você pode criar um perfil que os usuários de outras contas ou pessoas fora da organização podem usar para acessar seus recursos. É possível especificar quem é confiável para assumir o perfil. Para serviços que oferecem 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 Suporte compatível com esses recursos, consulte [Como AWS Support funciona com o IAM](#).
- Para saber como fornecer acesso aos seus recursos em todas as Contas da AWS que você possui, consulte Como [fornecer acesso a um usuário do IAM em outra 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 perfis e políticas baseadas em recurso para acesso entre contas, consulte [Acesso a recursos entre contas no IAM](#) no Guia do usuário do IAM.

Resposta a incidentes

A resposta a incidentes Suporte 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. Você pode 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 rastrear 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 CloudTrail captura 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 obter mais informações, consulte o [Guia do usuário do AWS CloudTrail](#).

Para obter mais informações, consulte [Monitoramento e registro para AWS Support](#) e [Monitoramento e registro para 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 regulamentos aplicáveis. AWS fornece os seguintes recursos para ajudar na conformidade:

- [Governança e conformidade de segurança](#): esses guias de implementação de solução abordam considerações sobre a arquitetura e fornecem etapas para implantar recursos de segurança e conformidade.
- [Referência de serviços qualificados para HIPAA](#): lista os serviços qualificados para HIPAA. Nem todos Serviços da AWS são elegíveis para a 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](#).
- [Amazon GuardDuty](#) — Isso AWS service (Serviço da AWS) detecta possíveis ameaças às suas cargas de trabalho Contas da AWS, contêineres e dados monitorando seu ambiente em busca de atividades suspeitas e maliciosas. GuardDuty pode ajudá-lo a atender a vários requisitos de conformidade, como o PCI DSS, atendendo aos requisitos de detecção de intrusões exigidos por determinadas estruturas de conformidade.
- [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 altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center 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 Suporte 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 compatibilidade com 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 compatibilidade com esses modos.

Além disso, as solicitações devem ser assinadas usando 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 Suporte

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 Suporte usar AWS SDKs

Os exemplos de código a seguir mostram como usar Suporte com um kit AWS de desenvolvimento de software (SDK).

As noções básicas são exemplos de código que mostram como realizar as operações essenciais em um serviço.

Ações são trechos de código de programas maiores e devem ser executadas em contexto. Embora as ações mostrem como chamar perfis de serviço individuais, você pode ver as ações no contexto em seus cenários relacionados.

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulte [Usando AWS Support com um AWS SDK](#). Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Conceitos básicos

Olá Suporte

O exemplo de código a seguir mostra como começar a usar o Suporte.

.NET

SDK para .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($"{response.Services.Count} services available.");
}
```

- Para obter detalhes da API, consulte [DescribeServices](#) a Referência AWS SDK para .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 [DescribeServices](#) a 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.",
      );
    }
    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 [DescribeServices](#) a Referência AWS SDK para JavaScript da API.

Kotlin

SDK para 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 [DescribeServices](#) referência 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 [DescribeServices](#) Referência da API AWS SDK for Python (Boto3).

Exemplos de código

- [Exemplos básicos de Suporte uso AWS SDKs](#)
- [Olá Suporte](#)
- [Aprenda o básico Suporte com um SDK AWS](#)

- [Ações para Suporte usar AWS SDKs](#)
 - [Use AddAttachmentsToSet com um AWS SDK ou CLI](#)
 - [Use AddCommunicationToCase com um AWS SDK ou CLI](#)
 - [Use CreateCase com um AWS SDK ou CLI](#)
 - [Use DescribeAttachment com um AWS SDK ou CLI](#)
 - [Use DescribeCases com um AWS SDK ou CLI](#)
 - [Use DescribeCommunications com um AWS SDK ou CLI](#)
 - [Use DescribeServices com um AWS SDK ou CLI](#)
 - [Use DescribeSeverityLevels com um AWS SDK ou CLI](#)
 - [Usar DescribeTrustedAdvisorCheckRefreshStatuses com uma CLI](#)
 - [Usar DescribeTrustedAdvisorCheckResult com uma CLI](#)
 - [Usar DescribeTrustedAdvisorCheckSummaries com uma CLI](#)
 - [Usar DescribeTrustedAdvisorChecks com uma CLI](#)
 - [Usar RefreshTrustedAdvisorCheck com uma CLI](#)
 - [Use ResolveCase com um AWS SDK ou CLI](#)

Exemplos básicos de Suporte uso AWS SDKs

Os exemplos de código a seguir mostram como usar o básico do AWS Support with AWS SDKs.

Exemplos

- [Olá Suporte](#)
- [Aprenda o básico Suporte com um SDK AWS](#)
- [Ações para Suporte usar AWS SDKs](#)
 - [Use AddAttachmentsToSet com um AWS SDK ou CLI](#)
 - [Use AddCommunicationToCase com um AWS SDK ou CLI](#)
 - [Use CreateCase com um AWS SDK ou CLI](#)
 - [Use DescribeAttachment com um AWS SDK ou CLI](#)
 - [Use DescribeCases com um AWS SDK ou CLI](#)
 - [Use DescribeCommunications com um AWS SDK ou CLI](#)
 - [Use DescribeServices com um AWS SDK ou CLI](#)

- [Use DescribeSeverityLevels com um AWS SDK ou CLI](#)
- [Usar DescribeTrustedAdvisorCheckRefreshStatuses com uma CLI](#)
- [Usar DescribeTrustedAdvisorCheckResult com uma CLI](#)
- [Usar DescribeTrustedAdvisorCheckSummaries com uma CLI](#)
- [Usar DescribeTrustedAdvisorChecks com uma CLI](#)
- [Usar RefreshTrustedAdvisorCheck com uma CLI](#)
- [Use ResolveCase com um AWS SDK ou CLI](#)

Olá Suporte

O exemplo de código a seguir mostra como começar a usar o Suporte.

.NET

SDK para .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($"{response.Services.Count} services available.");
}
}
```

- Para obter detalhes da API, consulte [DescribeServices](#) a Referência AWS SDK para .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 [DescribeServices](#) a 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](#).

Invoke `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.",
      );
    }
    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 [DescribeServices](#) a Referência AWS SDK para JavaScript da API.

Kotlin

SDK para 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 [DescribeServices](#) referência 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 [DescribeServices](#) Referência da API AWS SDK for Python (Boto3).

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulte [Usando AWS Support com um AWS SDK](#). Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Aprenda o básico Suporte com um SDK AWS

Os exemplos de código a seguir mostram como:

- Obtenha e exiba os serviços disponíveis e os níveis de gravidade dos casos.
- Criar um caso de suporte usando um serviço, uma categoria e um nível de gravidade selecionados.
- Obter e exibir uma lista de casos em aberto para o dia atual.
- Adicionar um conjunto de anexos e uma comunicação ao novo caso.
- Descrever o novo anexo e a comunicação para o caso.
- Resolver o caso.

- Obtenha e exiba uma lista de casos resolvidos para o dia atual.

.NET

SDK para .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 Suporte 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 AWS SDK para .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 Suporte 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 = "C:\\AWS\\test.txt" ; //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 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 * as inquirer from "@inquirer/prompts";
import { retry } from "@aws-doc-sdk-examples/lib/utils/util-timers.js";

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.",
      );
    }
    throw err;
  }
};

/**
 * Select a service from the list returned from DescribeServices.
 */
export const getService = async () => {
  const { services } = await client.send(new DescribeServicesCommand({}));
  const selectedService = await inquirer.select({
    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;
};
```

```
/**
 * @param {{ categories: import('@aws-sdk/client-support').Category[]}} service
 */
export const getCategory = async (service) => {
  const selectedCategory = await inquirer.select({
    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.select({
    message: "Select a severity level.",
    choices: severityLevels.map((s) => ({ name: s.name, value: s })),
  });
  return selectedSeverityLevel;
};

/**
 * Create a new support case
 * @param {{
 *   selectedService: import('@aws-sdk/client-support').Service
 *   selectedCategory: import('@aws-sdk/client-support').Category
 *   selectedSeverityLevel: import('@aws-sdk/client-support').SeverityLevel
 * }} selections
 * @returns
 */
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 startOfDay = new Date(d.getFullYear(), d.getMonth(), d.getDate());
  const command = new DescribeCasesCommand({
    includeCommunications: false,
    afterTime: startOfDay.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;
};

/**
 * @param {import('@aws-sdk/client-support').Communication[]} communications
 */
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.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.
   * @param {{
   *   caseId: string,
   *   cases: import('@aws-sdk/client-support').CaseDetails[]
   *   nextToken: string
   * }} options
   * @returns
   */
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 getTodayResolvedCases = 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 AWS SDK para JavaScript .
 - [AddAttachmentsToSet](#)
 - [AddCommunicationToCase](#)
 - [CreateCase](#)
 - [DescribeAttachment](#)
 - [DescribeCases](#)
 - [DescribeCommunications](#)
 - [DescribeServices](#)
 - [DescribeSeverityLevels](#)
 - [ResolveCase](#)

Kotlin

SDK para 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 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.")

```

Defina 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 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, consulte [Usando AWS Support com um AWS SDK](#). Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Ações para Suporte usar AWS SDKs

Os exemplos de código a seguir demonstram como realizar Suporte ações individuais com AWS SDKs. 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 CLI](#)
- [Use AddCommunicationToCase com um AWS SDK ou CLI](#)
- [Use CreateCase com um AWS SDK ou CLI](#)
- [Use DescribeAttachment com um AWS SDK ou CLI](#)
- [Use DescribeCases com um AWS SDK ou CLI](#)
- [Use DescribeCommunications com um AWS SDK ou CLI](#)
- [Use DescribeServices com um AWS SDK ou CLI](#)
- [Use DescribeSeverityLevels com um AWS SDK ou CLI](#)
- [Usar DescribeTrustedAdvisorCheckRefreshStatuses com uma CLI](#)
- [Usar DescribeTrustedAdvisorCheckResult com uma CLI](#)
- [Usar DescribeTrustedAdvisorCheckSummaries com uma CLI](#)
- [Usar DescribeTrustedAdvisorChecks com uma CLI](#)
- [Usar RefreshTrustedAdvisorCheck com uma CLI](#)
- [Use ResolveCase com um AWS SDK ou CLI](#)

Use **AddAttachmentsToSet** com um AWS SDK ou CLI

Os exemplos de código a seguir mostram como usar o AddAttachmentsToSet.

Exemplos de ações são trechos de código de programas maiores e devem ser executados em contexto. É possível ver essa ação em contexto no seguinte exemplo de código:

- [Conheça os conceitos básicos](#)

.NET

SDK para .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 [AddAttachmentsToSet](#) na Referência AWS SDK para .NET da API.

CLI

AWS CLI

Para adicionar um anexo a um conjunto

O `add-attachments-to-set` exemplo a seguir adiciona uma imagem a um conjunto que você pode especificar para um caso de suporte em sua AWS conta.

```
aws support add-attachments-to-set \
  --attachment-set-id "as-2f5a6faa2a4a1e600-mu-nk5xQlBr70-
  G1cUos5LZkd38K0AHZa9BMDVzNEXAMPLE" \
  --attachments fileName=troubleshoot-screenshot.png,data=base64-encoded-string
```

Saída:

```
{
  "attachmentSetId": "as-2f5a6faa2a4a1e600-mu-nk5xQlBr70-
  G1cUos5LZkd38K0AHZa9BMDVzNEXAMPLE",
  "expiryTime": "2020-05-14T17:04:40.790+0000"
}
```

Para obter mais informações, consulte [Case management](#) no Guia do usuário do AWS Support.

- Para obter detalhes da API, consulte [AddAttachmentsToSet](#) na 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 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 [AddAttachmentsToSet](#) 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 [AddAttachmentsToSet](#) Referência AWS SDK para JavaScript da API.

Kotlin

SDK para 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 [AddAttachmentsToSet](#) referência 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 [AddAttachmentsToSet](#) Referência da API AWS SDK for Python (Boto3).

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulte [Usando AWS Support com um AWS SDK](#). Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **AddCommunicationToCase** com um AWS SDK ou CLI

Os exemplos de código a seguir mostram como usar o AddCommunicationToCase.

Exemplos de ações são trechos de código de programas maiores e devem ser executados em contexto. É possível ver essa ação em contexto no seguinte exemplo de código:

- [Conheça os conceitos básicos](#)

.NET

SDK para .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 [AddCommunicationToCase](#) a Referência AWS SDK para .NET da API.

CLI

AWS CLI

Para adicionar uma comunicação a um caso

O `add-communication-to-case` exemplo a seguir adiciona comunicações a um caso de suporte em sua AWS conta.

```
aws support add-communication-to-case \
  --case-id "case-12345678910-2013-c4c1d2bf33c5cf47" \
  --communication-body "I'm attaching a set of images to this case." \
  --cc-email-addresses "myemail@example.com" \
  --attachment-set-id "as-2f5a6faa2a4a1e600-mu-nk5xQlBr70-
G1cUos5LZkd38K0AHZa9BMDVzNEXAMPLE"
```

Saída:

```
{
  "result": true
}
```

Para obter mais informações, consulte [Case management](#) no Guia do usuário do AWS Support.

- Para obter detalhes da API, consulte [AddCommunicationToCase](#) na 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 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 [AddCommunicationToCase](#) a 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 [AddCommunicationToCase](#) a Referência AWS SDK para JavaScript da API.

Kotlin

SDK para 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 [AddCommunicationToCase](#) referência da API AWS SDK for Kotlin.

PowerShell

Ferramentas para PowerShell V4

Exemplo 1: adiciona o corpo de uma comunicação por e-mail ao caso especificado.

```
Add-ASACommunicationToCase -CaseId "case-12345678910-2013-c4c1d2bf33c5cf47" -
CommunicationBody "Some text about the case"
```

Exemplo 2: adiciona o corpo de uma comunicação por e-mail ao caso especificado mais um ou mais endereços de e-mail contidos na linha CC do e-mail.

```
Add-ASACommunicationToCase -CaseId "case-12345678910-2013-c4c1d2bf33c5cf47" -
CcEmailAddress @"email1@address.com", "email2@address.com") -CommunicationBody
"Some text about the case"
```

- Para obter detalhes da API, consulte [AddCommunicationToCase](#) em Referência de Ferramentas da AWS para PowerShell cmdlet (V4).

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 [AddCommunicationToCase](#) Referência da API AWS SDK for Python (Boto3).

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulte [Usando AWS Support com um AWS SDK](#). Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **CreateCase** com um AWS SDK ou CLI

Os exemplos de código a seguir mostram como usar o `CreateCase`.

Exemplos de ações são trechos de código de programas maiores e devem ser executados em contexto. É possível ver essa ação em contexto no seguinte exemplo de código:

- [Conheça os conceitos básicos](#)

.NET

SDK para .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 [CreateCase](#) na Referência AWS SDK para .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 [CreateCase](#) na 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 [CreateCase](#) a 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 [CreateCase](#) Referência AWS SDK para JavaScript da API.

Kotlin

SDK para 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 [CreateCase](#) referência da API AWS SDK for Kotlin.

PowerShell

Ferramentas para PowerShell V4

Exemplo 1: Cria um novo caso no AWS Support Center. Os valores dos CategoryCode parâmetros - ServiceCode e - podem ser obtidos usando o Get-ASAService cmdlet. O valor do SeverityCode parâmetro - pode ser obtido usando o Get-ASASeverityLevel cmdlet. 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 [CreateCase](#) em Referência de Ferramentas da AWS para PowerShell cmdlet (V4).

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 [CreateCase](#)Referência da API AWS SDK for Python (Boto3).

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulte [Usando AWS Support com um AWS SDK](#). Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **DescribeAttachment** com um AWS SDK ou CLI

Os exemplos de código a seguir mostram como usar o DescribeAttachment.

Exemplos de ações são trechos de código de programas maiores e devem ser executados em contexto. É possível ver essa ação em contexto no seguinte exemplo de código:

- [Conheça os conceitos básicos](#)

.NET

SDK para .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 [DescribeAttachment](#) na Referência AWS SDK para .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-  
gJv9qqDooTipsz3V1Nb19rCfkZneeQeDPgp8X1iVJyHH7UuhZDdNeqGoduZsPrAhyMakq1c60-  
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 [DescribeAttachment](#) na 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 [DescribeAttachment](#) 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 [DescribeAttachment](#) Referência AWS SDK para JavaScript da API.

Kotlin

SDK para 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 [DescribeAttachment](#) referência 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 "
                    "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 [DescribeAttachment](#) Referência da API AWS SDK for Python (Boto3).

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulte [Usando AWS Support com um AWS SDK](#). Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **DescribeCases** com um AWS SDK ou CLI

Os exemplos de código a seguir mostram como usar o DescribeCases.

Exemplos de ações são trechos de código de programas maiores e devem ser executados em contexto. É possível ver essa ação em contexto no seguinte exemplo de código:

- [Conheça os conceitos básicos](#)

.NET

SDK para .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 [DescribeCases](#) a Referência AWS SDK para .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 [DescribeCases](#) na 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 [DescribeCases](#) a 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 [DescribeCases](#) a Referência AWS SDK para JavaScript da API.

Kotlin

SDK para 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 [DescribeCases](#) referência da API AWS SDK for Kotlin.

PowerShell

Ferramentas para PowerShell V4

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")
```

- Para obter detalhes da API, consulte [DescribeCases](#) em Referência de Ferramentas da AWS para PowerShell cmdlet (V4).

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 [DescribeCases](#) Referência da API AWS SDK for Python (Boto3).

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulte [Usando AWS Support com um AWS SDK](#). Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **DescribeCommunications** com um AWS SDK ou CLI

Os exemplos de código a seguir mostram como usar o `DescribeCommunications`.

Exemplos de ações são trechos de código de programas maiores e devem ser executados em contexto. É possível ver essa ação em contexto no seguinte exemplo de código:

- [Conheça os conceitos básicos](#)

.NET

SDK para .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 [DescribeCommunications](#) a Referência AWS SDK para .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":
    "eyJhZG90VG9rZW4iOiBudWxsLCAiYm90b190cnVuY2F0ZV9hbW91bnQEXAMPLE=="
}
```

Para obter mais informações, consulte [Case management](#) no Guia do usuário do AWS Support.

- Para obter detalhes da API, consulte [DescribeCommunications](#) na 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 [DescribeCommunications](#) a 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 [DescribeCommunications](#) na Referência AWS SDK para JavaScript da API.

Kotlin

SDK para 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 [DescribeCommunications](#) referência da API AWS SDK for Kotlin.

PowerShell

Ferramentas para PowerShell V4

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"
```

- Para obter detalhes da API, consulte [DescribeCommunications](#) em Referência de Ferramentas da AWS para PowerShell cmdlet (V4).

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 [DescribeCommunications](#)Referência da API AWS SDK for Python (Boto3).

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulte [Usando AWS Support com um AWS SDK](#). Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **DescribeServices** com um AWS SDK ou CLI

Os exemplos de código a seguir mostram como usar o `DescribeServices`.

Exemplos de ações são trechos de código de programas maiores e devem ser executados em contexto. É possível ver essa ação em contexto no seguinte exemplo de código:

- [Conheça os conceitos básicos](#)

.NET

SDK para .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 [DescribeServices](#) a Referência AWS SDK para .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 [DescribeServices](#) na 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 [DescribeServices](#) a Referência AWS SDK for Java 2.x da API.

Kotlin

SDK para 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 [DescribeServices](#) referência da API AWS SDK for Kotlin.

PowerShell

Ferramentas para PowerShell V4

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 [DescribeServices](#) em Referência de Ferramentas da AWS para PowerShell cmdlet (V4).

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 [DescribeServices](#) Referência da API AWS SDK for Python (Boto3).

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulte [Usando AWS Support com um AWS SDK](#). Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **DescribeSeverityLevels** com um AWS SDK ou CLI

Os exemplos de código a seguir mostram como usar o `DescribeSeverityLevels`.

Exemplos de ações são trechos de código de programas maiores e devem ser executados em contexto. É possível ver essa ação em contexto no seguinte exemplo de código:

- [Conheça os conceitos básicos](#)

.NET

SDK para .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 [DescribeSeverityLevels](#) na Referência AWS SDK para .NET da API.

CLI

AWS CLI

Para 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 [DescribeSeverityLevels](#) na 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 [DescribeSeverityLevels](#) na 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 [DescribeSeverityLevels](#) Referência AWS SDK para JavaScript da API.

Kotlin

SDK para 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 [DescribeSeverityLevels](#) referência da API AWS SDK for Kotlin.

PowerShell

Ferramentas para PowerShell V4

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 [DescribeSeverityLevels](#) em Referência de Ferramentas da AWS para PowerShell cmdlet (V4).

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 [DescribeSeverityLevels](#)Referência da API AWS SDK for Python (Boto3).

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulte [Usando AWS Support com um AWS SDK](#). Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Usar **DescribeTrustedAdvisorCheckRefreshStatuses** com uma CLI

Os exemplos de código a seguir mostram como usar o `DescribeTrustedAdvisorCheckRefreshStatuses`.

CLI

AWS CLI

Para listar os status de atualização das verificações do AWS Trusted Advisor

O exemplo `describe-trusted-advisor-check-refresh-statuses` a seguir lista os status de atualização de duas verificações do Trusted Advisor: permissões do bucket do Amazon S3 e uso do IAM.

```
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 Guia do usuário do AWS Support.

- Para obter detalhes da API, consulte [DescribeTrustedAdvisorCheckRefreshStatuses](#) na Referência de AWS CLI Comandos.

PowerShell

Ferramentas para PowerShell V4

Exemplo 1: retorna o status atual das solicitações de atualização para as verificações especificadas. Solicitação - ASATrusted AdvisorCheckRefresh pode ser usada para solicitar que as informações de status das verificações sejam atualizadas.

```
Get-ASATrustedAdvisorCheckRefreshStatus -CheckId @"checkid1", "checkid2")
```

- Para obter detalhes da API, consulte [DescribeTrustedAdvisorCheckRefreshStatuses](#) em Referência de Ferramentas da AWS para PowerShell cmdlet (V4).

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulte [Usando AWS Support com um AWS SDK](#). Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Usar **DescribeTrustedAdvisorCheckResult** com uma CLI

Os exemplos de código a seguir mostram como usar o `DescribeTrustedAdvisorCheckResult`.

CLI

AWS CLI

Para listar os resultados de uma verificação do AWS Trusted Advisor

O exemplo `describe-trusted-advisor-check-result` 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 Guia do usuário do AWS Support.

- Para obter detalhes da API, consulte [DescribeTrustedAdvisorCheckResult](#) na Referência de AWS CLI Comandos.

PowerShell

Ferramentas para PowerShell V4

Exemplo 1: Retorna os resultados de uma verificação do Trusted Advisor. A lista de verificações disponíveis do Trusted Advisor pode ser obtida usando `Get-ASATrustedAdvisorChecks`. 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 exclusiva 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 [DescribeTrustedAdvisorCheckResult](#) em Referência de Ferramentas da AWS para PowerShell cmdlet (V4).

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulte [Usando AWS Support com um AWS SDK](#). Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Usar **DescribeTrustedAdvisorCheckSummaries** com uma CLI

Os exemplos de código a seguir mostram como usar o `DescribeTrustedAdvisorCheckSummaries`.

CLI

AWS CLI

Para listar os resumos das verificações do AWS Trusted Advisor

O exemplo `describe-trusted-advisor-check-summaries` a seguir lista os resultados de duas verificações do Trusted Advisor: permissões do bucket do Amazon S3 e uso do IAM.

```
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 Guia do usuário do AWS Support.

- Para obter detalhes da API, consulte [DescribeTrustedAdvisorCheckSummaries](#) na Referência de AWS CLI Comandos.

PowerShell

Ferramentas para PowerShell V4

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 [DescribeTrustedAdvisorCheckSummaries](#) em Referência de Ferramentas da AWS para PowerShell cmdlet (V4).

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulte [Usando AWS Support com um AWS SDK](#). Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Usar **DescribeTrustedAdvisorChecks** com uma CLI

Os exemplos de código a seguir mostram como usar o `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 da verificação. 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 Guia do usuário do AWS Support.

- Para obter detalhes da API, consulte [DescribeTrustedAdvisorChecks](#) na Referência de AWS CLI Comandos.

PowerShell

Ferramentas para PowerShell V4

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 [DescribeTrustedAdvisorChecks](#) em Referência de Ferramentas da AWS para PowerShell cmdlet (V4).

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulte [Usando AWS Support com um AWS SDK](#). Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Usar **RefreshTrustedAdvisorCheck** com uma CLI

Os exemplos de código a seguir mostram como usar o 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 Guia do usuário do AWS Support.

- Para obter detalhes da API, consulte [RefreshTrustedAdvisorCheck](#) na Referência de AWS CLI Comandos.

PowerShell

Ferramentas para PowerShell V4

Exemplo 1: Solicita uma atualização para a verificação especificada do Trusted Advisor.

```
Request-ASATrustedAdvisorCheckRefresh -CheckId "checkid1"
```

- Para obter detalhes da API, consulte [RefreshTrustedAdvisorCheck](#) em Referência de Ferramentas da AWS para PowerShell cmdlet (V4).

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulte [Usando AWS Support com um AWS SDK](#). Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **ResolveCase** com um AWS SDK ou CLI

Os exemplos de código a seguir mostram como usar o `ResolveCase`.

Exemplos de ações são trechos de código de programas maiores e devem ser executados em contexto. É possível ver essa ação em contexto no seguinte exemplo de código:

- [Conheça os conceitos básicos](#)

.NET

SDK para .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 [ResolveCase](#) na Referência AWS SDK para .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 [ResolveCase](#) na 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 [ResolveCase](#) 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 [ResolveCase](#) Referência AWS SDK para JavaScript da API.

Kotlin

SDK para 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 [ResolveCase](#) referência da API AWS SDK for Kotlin.

PowerShell

Ferramentas para PowerShell V4

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 [ResolveCase](#) em Referência de Ferramentas da AWS para PowerShell cmdlet (V4).

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 [ResolveCase](#)Referência da API AWS SDK for Python (Boto3).

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulte [Usando AWS Support com um AWS SDK](#). Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Monitoramento e registro para AWS Support

O monitoramento é uma parte importante da manutenção da confiabilidade, disponibilidade e desempenho de Suporte suas outras AWS soluções. AWS fornece as seguintes ferramentas de monitoramento para observar Suporte, relatar quando algo está errado e realizar ações automáticas quando apropriado:

- 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 CloudTrail captura 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 S3 que você especificar. 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 obter mais informações, consulte o [Guia do usuário do AWS CloudTrail](#).

Tópicos

- [Monitorando AWS Support casos com a Amazon EventBridge](#)
- [Registrando chamadas de AWS Support API com AWS CloudTrail](#)
- [Registrando AWS Support o aplicativo em chamadas de API do Slack usando 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

AWS Support realiza eventos com base no melhor esforço. Não é garantido que os eventos sejam sempre entregues ao EventBridge.

Criação de uma EventBridge regra para AWS Support casos

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 AWS Support caso, 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

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 AWS eventos 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 Suporte e, em seguida, enviará o evento para o destino que você especificou.

Observações

- Ao receber um evento, você pode usar o `origin` parâmetro para determinar se você ou um AWS Support agente 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. Essa regra monitorará AWS CloudTrail os registros de chamadas de AWS Support API em sua conta.

Exemplos de AWS Support eventos

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 ao AWS Support responder 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 com AWS Support, consulte os seguintes recursos:

- [Como automatizar a AWS Support API com a Amazon EventBridge](#)
- [AWS Support notificador de atividade de caso](#) em GitHub

Registrando chamadas de AWS Support API com AWS CloudTrail

AWS Support é integrado com AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, função ou AWS serviço em AWS Support. CloudTrail captura chamadas de API AWS Support como eventos. As chamadas capturadas incluem chamadas do AWS Support console e chamadas de código para as operações AWS Support da API.

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 AWS Support. 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 feita AWS Support, 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](#).

AWS Support informações em CloudTrail

CloudTrail é ativado em sua AWS conta quando você cria a conta. Quando uma atividade de evento suportada ocorre em AWS Support, 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 AWS conta. Para obter mais informações, consulte [Visualização de eventos com histórico de CloudTrail eventos](#).

Para um registro contínuo dos eventos em sua AWS conta, incluindo eventos para AWS Support, crie uma trilha. Uma trilha permite CloudTrail entregar arquivos de log para um bucket do Amazon S3. Por padrão, quando uma trilha é criada no console, a mesma é aplicada a todas as regiões da AWS. A trilha registra eventos de todas as regiões na AWS partição e entrega os arquivos de log ao bucket do Amazon S3 que você especificar. Além disso, você pode configurar outros AWS serviços para analisar e agir com base nos dados de eventos coletados nos CloudTrail registros. Para obter mais informações, consulte:

- [Visão geral da criação de uma trilha](#)
- [CloudTrail serviços e integrações suportados](#)
- [Configurando notificações do Amazon SNS para CloudTrail](#)
- [Receber arquivos de log do CloudTrail de várias regiões](#) e [Receber arquivos de log do CloudTrail de várias contas](#)

Todas as operações AWS Support da API são registradas CloudTrail e documentadas na [Referência da AWS Support API](#).

Por exemplo, chamadas para as ResolveCase operações CreateCase, DescribeCases e geram entradas nos arquivos de CloudTrail log.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar o seguinte:

- Se a solicitação foi feita com credenciais de usuário root ou 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 serviço.

Para obter mais informações, consulte [Elemento userIdentity do CloudTrail](#).

Você também pode agregar arquivos de AWS Support log de várias AWS regiões e várias AWS contas em um único bucket do Amazon S3.

AWS Trusted Advisor informações no CloudTrail registro

Trusted Advisor é um AWS Support serviço que você pode usar para verificar sua AWS conta em busca de formas de economizar custos, melhorar a segurança e otimizar sua conta.

Todas as operações Trusted Advisor da API são registradas CloudTrail e documentadas na [Referência da AWS Support API](#).

Por exemplo, chamadas para as `RefreshTrustedAdvisorCheck`, `operacoesDescribeTrustedAdvisorCheckRefreshStatuses`, `DescribeTrustedAdvisorCheckResult` e geram entradas nos arquivos de CloudTrail log.

Note

CloudTrail também registra as ações Trusted Advisor do console. Consulte [Registrando ações AWS Trusted Advisor do console com AWS CloudTrail](#).

Entendendo as entradas do arquivo de AWS Support log

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 solicitação única de qualquer fonte. Ele inclui informações sobre a operação solicitada, a data e a hora da operação, 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 `CreateCase`

O exemplo a seguir mostra uma entrada de CloudTrail registro para a [CreateCase](#) operação.

```
{
  "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 registro para RefreshTrustedAdvisorCheck

O exemplo a seguir mostra uma entrada de CloudTrail registro para a [RefreshTrustedAdvisorCheck](#) operação.

```
{
  "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"
}
```

Registrando AWS Support o aplicativo em chamadas de API do Slack usando AWS CloudTrail

O AWS Support aplicativo no Slack é integrado ao AWS CloudTrail. CloudTrail fornece um registro das ações realizadas por um usuário, função ou AWS service (Serviço da AWS) no AWS Support aplicativo. Para criar esse registro, CloudTrail captura todas as chamadas públicas de API para o AWS Support aplicativo como eventos. Essas chamadas capturadas incluem chamadas do console do AWS Support aplicativo e chamadas de código para as operações públicas da API do AWS Support aplicativo. Se você criar uma trilha, poderá habilitar a entrega contínua de CloudTrail eventos para um bucket do Amazon S3. Isso inclui eventos para o AWS Support App. Se você não configurar uma trilha, ainda poderá ver os eventos mais recentes no CloudTrail console no Histórico de eventos. Você pode usar as informações CloudTrail coletadas para determinar a solicitação que

foi feita ao AWS Support App. 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 CloudTrail, consulte o [Guia AWS CloudTrail do usuário](#).

AWS Support Informações do aplicativo em CloudTrail

Quando você cria o seu Conta da AWS, isso é ativado CloudTrail na conta. Quando a atividade pública da API ocorre no AWS Support aplicativo, 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 no seu Conta da AWS. Para obter mais informações, consulte [Visualização de eventos com histórico de CloudTrail eventos](#).

Para um registro contínuo dos eventos em seu Conta da AWS, incluindo eventos para o AWS Support aplicativo, crie uma trilha. Por padrão, quando você cria uma trilha no console, ela é aplicada a todas as Regiões da AWS. A trilha registra eventos de todas as regiões na partição da AWS e entrega os arquivos de log no bucket do Amazon S3 que você especifica. Além disso, você pode configurar outros Serviços da AWS para analisar mais detalhadamente os dados de eventos coletados nos CloudTrail registros e agir com base nos dados. Para obter mais informações, consulte:

- [Visão geral da criação de uma trilha](#)
- [CloudTrail serviços e integrações suportados](#)
- [Configurando notificações do Amazon SNS para CloudTrail](#)
- [Recebendo arquivos de CloudTrail log de várias regiões](#) e [Recebendo arquivos de CloudTrail log de várias contas](#)

CloudTrail registra todas as ações públicas AWS Support do aplicativo. Essas ações estão também documentadas em [AWS Support App in Slack API Reference](#). Por exemplo, chamadas para o `CreateSlackChannelConfiguration` `GetAccountAlias` e `UpdateSlackChannelConfiguration` as ações geram entradas nos arquivos de CloudTrail log.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar o seguinte:

- Se a solicitação foi feita com credenciais de usuário root ou 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](#).

Entendendo as entradas do arquivo de log do AWS Support aplicativo

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. 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 CloudTrail registro para a [CreateSlackChannelConfiguration](#) operação.

```
{
  "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 CloudTrail registro para a [ListSlackChannelConfigurations](#) operação.

```

{
  "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 CloudTrail registro para a [GetAccountAlias](#) operação.

```

{
  "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"
}
```

Monitoramento e registro de AWS Support planos

O monitoramento é uma parte importante da manutenção da confiabilidade, disponibilidade e desempenho dos Support Plans e de suas outras AWS soluções. AWS fornece as seguintes ferramentas de monitoramento para monitorar os Support Plans, relatar quando algo está errado e realizar ações automáticas quando apropriado:

- AWS CloudTrail captura 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 S3 que você especificar. 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 obter mais informações, consulte o [Guia do usuário do AWS CloudTrail](#).

Tópicos

- [Chamadas da API Logging AWS Support Plans com AWS CloudTrail](#)

Chamadas da API Logging AWS Support Plans com AWS CloudTrail

AWS Support O Plans é integrado com AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, função ou um AWS service (Serviço da AWS). CloudTrail captura chamadas de API para AWS Support planos como eventos. As chamadas capturadas incluem chamadas do console AWS Support Plans e chamadas de código para as operações da API AWS Support Plans.

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 Planos. AWS Support 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 feita aos AWS Support Planos, 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](#).

AWS Support Informações sobre planos em CloudTrail

CloudTrail é ativado no seu Conta da AWS quando você cria a conta. Quando uma atividade de evento suportada ocorre nos AWS Support Planos, essa atividade é registrada em um CloudTrail evento junto com outros AWS service (Serviço da AWS) eventos no histórico de eventos. É possível visualizar, pesquisar e baixar eventos recentes em sua conta. Para obter mais informações, consulte [Visualização de eventos com histórico de CloudTrail eventos](#).

Para um registro contínuo de eventos em sua conta, incluindo eventos para AWS Support Planos, 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 eventos de todas as regiões na AWS partição e entrega os arquivos de log ao bucket do Amazon S3 que você especificar. Além disso, você pode configurar outros Serviços da AWS para analisar e agir com base nos dados do evento coletados nos CloudTrail registros. Para obter mais informações, consulte:

- [Visão geral da criação de uma trilha](#)
- [CloudTrail serviços e integrações suportados](#)
- [Configurando notificações do Amazon SNS para CloudTrail](#)
- [Receber arquivos de log do CloudTrail de várias regiões](#) e [Receber arquivos de log do CloudTrail de várias contas](#)

Todas as operações da API AWS Support Plans são registradas por CloudTrail. Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar o seguinte:

- Se a solicitação foi feita com credenciais de usuário root ou 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 de AWS Support planos de várias Regiões da AWS e várias contas em um único bucket do Amazon S3.

Entendendo as entradas do arquivo de log de AWS Support planos

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 solicitação única de qualquer fonte. Ele inclui informações sobre a operação solicitada, a data e a hora da operação, 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 log para **GetSupportPlan**

O exemplo a seguir mostra uma entrada de CloudTrail registro para a GetSupportPlan operação.

```
{
  "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 CloudTrail registro para a GetSupportPlanUpdateStatus operação.

```
{  
  "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 CloudTrail registro para a StartSupportPlanUpdate operação.

```

{
  "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 CloudTrail registro para a **CreateSupportPlanSchedule** operação.

```

{
  "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"  
}
```

Example : entrada de log para **ListSupportPlanModifiers**

O exemplo a seguir mostra uma entrada de CloudTrail registro para a ListSupportPlanModifiers operação.

```
{  
  "eventVersion": "1.09",  
  "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:sts::111122223333:user/janedoe",  
        "accountId": "111122223333",  
        "userName": "Admin"  
      },  
      "attributes": {  
        "creationDate": "2024-08-15T15:44:43Z",  
        "mfaAuthenticated": "false"  
      }  
    },  
  },  
  "eventTime": "2024-08-15T16:29:59Z",  
  "eventSource": "supportplans.amazonaws.com",  
  "eventName": "ListSupportPlanModifiers",  
  "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"  
}
```

Registrando alterações em seu Suporte plano

Important

A partir de 3 de agosto de 2022, as operações a seguir foram descontinuadas e não aparecerão nos seus novos registros. CloudTrail Para ver uma lista das operações compatíveis, consulte [Entendendo as entradas do arquivo de log de AWS Support planos](#).

- `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 escolhe Opt-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 registro para `DescribeSupportLevelSummary`

O exemplo a seguir mostra uma entrada de CloudTrail registro para a `DescribeSupportLevelSummary` ação.

```
{
```

```

"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 registro para UpdateProbationAutoCancellation

O exemplo a seguir mostra uma entrada de CloudTrail registro para a UpdateProbationAutoCancellation ação.

```

{
  "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 registro para UpdateSupportLevel

O exemplo a seguir mostra uma entrada de CloudTrail registro da UpdateSupportLevel ação a ser alterada para Developer Support.

```

{
  "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"  
}
```

Monitoramento e registro para AWS Trusted Advisor

O monitoramento é uma parte importante da manutenção da confiabilidade, disponibilidade e desempenho de Trusted Advisor suas outras AWS soluções. AWS fornece as seguintes ferramentas de monitoramento para observar Trusted Advisor, relatar quando algo está errado e realizar ações automáticas quando apropriado:

- 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.

Por exemplo, Trusted Advisor fornece a verificação de permissões de bucket do Amazon S3. Essa verificação identifica se você tem buckets que têm permissões de acesso aberto ou permitem acesso a qualquer usuário AWS autenticado. Se a permissão de um bucket for alterada, o status da Trusted Advisor verificação será alterado. EventBridge detecta esse evento e, em seguida, envia uma notificação para que você possa agir. Para obter mais informações, consulte o [Guia EventBridge do usuário da Amazon](#).

- AWS Trusted Advisor as verificações identificam maneiras de reduzir custos, aumentar o desempenho e melhorar a segurança AWS da sua conta. Você pode usar EventBridge para monitorar o status das Trusted Advisor verificações. Em seguida, você pode usar CloudWatch a Amazon para criar alarmes sobre Trusted Advisor métricas. Esses alarmes notificam você quando o status de uma Trusted Advisor verificação muda, como um recurso atualizado ou uma cota de serviço atingida.
- AWS CloudTrail captura 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 S3 que você especificar. 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 obter mais informações, consulte o [Guia do usuário do AWS CloudTrail](#).

Tópicos

- [Monitorando resultados de AWS Trusted Advisor cheques com a Amazon EventBridge](#)
- [Criação de CloudWatch alarmes da Amazon para monitorar métricas AWS Trusted Advisor](#)
- [Registrando ações AWS Trusted Advisor do console 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 que você especifica 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 AWS Lambda função para passar uma notificação para um canal do 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 respostas Trusted Advisor, consulte Trusted Advisor ferramentas em.](#) GitHub

Observações

- Trusted Advisor realiza eventos com base no melhor esforço. Não é garantido que os eventos sejam sempre entregues ao EventBridge.
- Você deve ter um AWS Support plano Business, Enterprise On-Ramp ou Enterprise para criar uma regra para Trusted Advisor verificações. 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 para Trusted 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 AWS eventos 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.
 - ERRO — Trusted Advisor recomenda uma ação para a verificação.
 - INFORMAÇÕES — não é Trusted Advisor possível determinar o status do cheque.
 - OK — Trusted Advisor não detecta um problema na verificação.
 - AVISO — Trusted Advisor detecta um possível problema na verificação e recomenda uma 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 de AWS recursos:
 - Escolha Any resource ID (Qualquer ID do recurso) para criar uma regra que monitora todos os recursos.
 - Escolha IDs de recursos específicos por ARN e, em seguida, insira os nomes de recursos da Amazon que você deseja. ARNs
 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 as Trusted Advisor verificações e, em seguida, enviará o evento para o destino que você especificou.

Criação de CloudWatch alarmes da Amazon para monitorar métricas AWS Trusted Advisor

Ao AWS Trusted Advisor atualizar seus cheques, Trusted Advisor publica métricas sobre os resultados de seus cheques em CloudWatch. Você pode visualizar as métricas no CloudWatch. Você também pode criar alarmes para detectar alterações de status em Trusted Advisor verificações e alterações de status de recursos e uso da cota de serviço (anteriormente chamado de limites).

Siga este procedimento para criar um CloudWatch alarme para uma Trusted Advisor métrica específica.

Tópicos

- [Pré-requisitos](#)
- [CloudWatch métricas para Trusted Advisor](#)

- [Trusted Advisor métricas e dimensões](#)

Pré-requisitos

Antes de criar CloudWatch alarmes para Trusted Advisor métricas, revise as seguintes informações:

- Entenda como CloudWatch usa métricas e alarmes. Para obter mais informações, consulte [Como CloudWatch funciona](#) no Guia do CloudWatch usuário da Amazon.
- Use o Trusted Advisor console ou a AWS Support API para atualizar suas verificações e obter os resultados mais recentes. Para obter mais informações, consulte [Atualizar resultados da verificação](#).

Para criar um CloudWatch alarme para Trusted Advisor métricas

1. Abra o CloudWatch console em <https://console.aws.amazon.com/cloudwatch/>.
2. Use o seletor de região e escolha a AWS região 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, você pode inserir o nome da métrica ServiceLimitUsage ou a dimensão, como o nome do Trusted Advisor cheque.

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 [Trusted Advisor métricas e dimensões](#).

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 e o nome da métrica é YellowResources.

N. Virginia ▾		All > TrustedAdvisor > Check Metrics	Trusted ✕	Advisor ✕	IAM ✕	Access ✕	Key ✕
☐	CheckName (2)					Metric Name	
☐	IAM Access Key Rotation					RedResources	
☒	IAM Access Key Rotation					YellowResources	

8. Escolha Seleccionar métrica.
9. Na página Especificar métricas e condições, verifique se o nome da métrica e o 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 $\geq$ threshold (Maior/Igual $\geq$ 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 YellowResources métricas GreenChecksRedChecks, YellowChecks, RedResources, e, você pode especificar um limite que seja qualquer número inteiro maior ou igual a zero.
- Trusted Advisor não envia métricas para GreenResources, que são recursos para os quais Trusted Advisor não detectou nenhum problema.

12. Escolha 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.

Notification

Alarm state trigger
Define the alarm state that will trigger this action.

☒ **In alarm**
The metric or expression is outside of the defined threshold.

☐ **OK**
The metric or expression is within the defined threshold.

☐ **Insufficient data**
The alarm has just started or not enough data is available.

Remove

Select an SNS topic
Define the SNS (Simple Notification Service) topic that will receive the notification.

☒ **Select an existing SNS topic**

☐ Create new topic

☐ Use topic ARN

Send a notification to...

Q Default_CloudWatch_Alarms_Topic X

Only email lists for this account are available.

Email (endpoints)
janedoe@example.com - [View in SNS Console](#)

Add notification

15. Escolha Próximo.
16. Em Name e Description (Nome e Descrição), insira um nome e uma descrição para o seu alarme.
17. Escolha 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 CloudWatch alarme

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 "IAMAccessKeyRotationCheckAlarm" 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=IAMAccessKeyRotationCheckAlarm>

Alarm Details:

- Name: IAMAccessKeyRotationCheckAlarm
- 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:IAMAccessKeyRotationCheckAlarm

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:

CloudWatch métricas para Trusted Advisor

Você pode usar o CloudWatch console ou o AWS Command Line Interface (AWS CLI) para encontrar as métricas disponíveis para Trusted Advisor.

Para obter uma lista dos namespaces, métricas e dimensões de todos os serviços que publicam métricas, consulte [AWS serviços que publicam CloudWatch métricas no Guia CloudWatch](#) do usuário da Amazon.

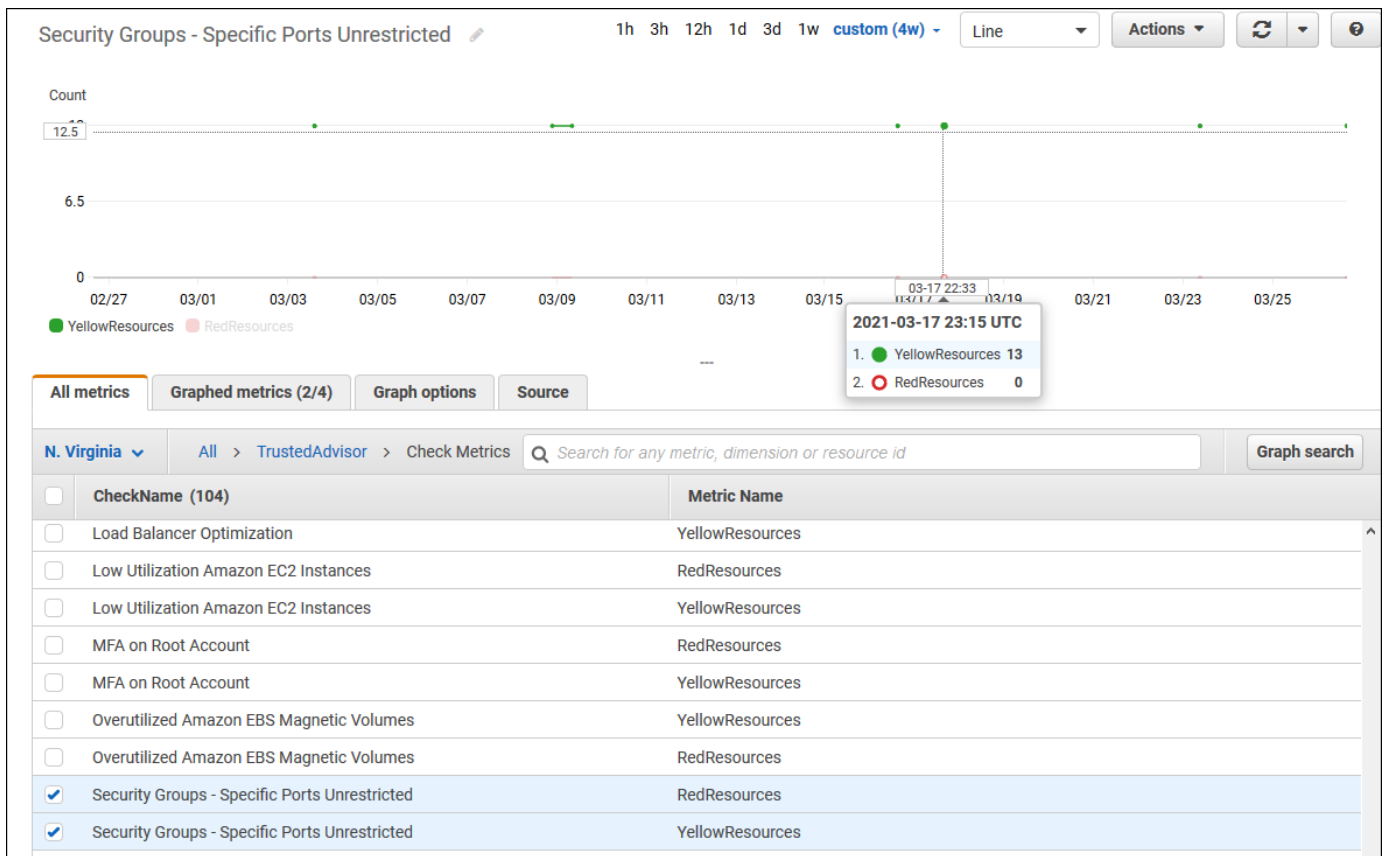
Exibir Trusted Advisor métricas (console)

Você pode entrar no CloudWatch console e ver as métricas disponíveis para Trusted Advisor.

Para visualizar Trusted Advisor as métricas disponíveis (console)

1. Abra o CloudWatch console em <https://console.aws.amazon.com/cloudwatch/>.
2. Use o seletor de região e escolha a AWS região Leste dos EUA (Norte da Virgínia).
3. No painel de navegação, selecione 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 identifica 13 recursos que são amarelos. Trusted Advisor recomenda que você investigue cheques amarelos.



7. (Opcional) Para adicionar esse gráfico a um CloudWatch painel, escolha Ações e, em seguida, escolha Adicionar ao painel.

Para obter mais informações sobre a criação de um gráfico para visualizar suas métricas, consulte [Representação gráfica de uma métrica](#) no Guia do CloudWatch usuário da Amazon.

Exibir Trusted Advisor métricas (CLI)

Você pode usar o AWS CLI comando [list-metrics](#) para visualizar as métricas disponíveis para Trusted Advisor

Example : Listar todas as métricas para Trusted Advisor

O exemplo a seguir especifica o AWS/TrustedAdvisor namespace para o qual visualizar todas as métricas. 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"
  },
  ...
]
```

Trusted Advisor métricas e dimensões

Consulte as tabelas a seguir para ver as Trusted Advisor métricas e dimensões que você pode usar para seus CloudWatch alarmes e gráficos.

Trusted Advisor métricas em nível de verificação

Você pode usar as seguintes métricas para Trusted Advisor verificações.

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 (investigação recomendada).

Trusted Advisor métricas de nível de cota de serviço

Você pode usar as seguintes métricas para AWS service (Serviço da AWS) cotas.

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

Você pode usar a seguinte dimensão para Trusted Advisor verificações.

Dimensão	Descrição
CheckName	O nome do Trusted Advisor cheque. É possível encontrar todos os nomes de verificações na seção Console do Trusted Advisor ou em AWS Trusted Advisor verifique a referência .

Dimensões para métricas de cota de serviço

Você pode usar as seguintes dimensões para métricas Trusted Advisor de cota de serviço.

Dimensão	Descrição
Region	O Região da AWS para uma cota de serviço.
ServiceName	O nome da AWS service (Serviço da AWS).
ServiceLimit	O nome do cota de serviço. Para obter mais informações sobre cotas de serviço, consulte AWS service (Serviço da AWS) quotas , na Referência geral da AWS.

Registrando ações AWS Trusted Advisor do console com AWS CloudTrail

Trusted Advisor é integrado com AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, função ou AWS serviço em Trusted Advisor. CloudTrail captura ações para eventos Trusted Advisor como. As chamadas capturadas incluem chamadas do Trusted Advisor console. 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 feita Trusted 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 Advisor informações 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 AWS conta. Para obter mais informações, consulte [Visualização de eventos com histórico de CloudTrail eventos](#).

Para um registro contínuo dos eventos em sua AWS conta, incluindo eventos para Trusted Advisor, crie uma trilha. Uma trilha permite CloudTrail entregar arquivos de log para um bucket do Amazon S3. Por padrão, quando uma trilha é criada no console, a mesma é aplicada a todas as regiões da AWS. A trilha registra eventos de todas as regiões na AWS partição e entrega os arquivos de log ao bucket do Amazon S3 que você especificar. Além disso, você pode configurar outros AWS serviços para analisar e agir com base nos dados de eventos coletados nos CloudTrail registros. Para obter 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 Advisor suporta o registro de um subconjunto das ações do Trusted Advisor console como eventos em arquivos de CloudTrail log. CloudTrail registra as seguintes ações:

- [BatchUpdateRecommendationResourceExclusion](#)
- 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 das ações do Trusted Advisor console, 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 [Registrando chamadas de AWS Support API com AWS CloudTrail](#).

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar o seguinte:

- Se a solicitação foi feita com credenciais de usuário root ou 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 serviço.

Para obter mais informações, consulte o elemento [CloudTrail UserIdentity](#).

Exemplo: entradas do arquivo de Trusted Advisor log

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 do bucket (ID) do Amazon S3. 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, a Amazon EC2 oferece o EC2 Rescue, que os clientes podem usar para examinar suas instâncias do Windows para ajudar a identificar problemas comuns, coletar arquivos de log e ajudar Suporte a solucionar seus problemas. Você também pode usar o EC2 Rescue para analisar volumes de inicialização de instâncias não funcionais. Para obter mais informações, consulte [Como posso usar o EC2 Rescue para solucionar e corrigir problemas comuns na minha instância EC2 do Windows?](#)

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 HTTP APIs
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
Nuvem de computação elástica da Amazon (Amazon EC2)	Solução de problemas de instâncias Solução de problemas de instâncias do Windows Solução de problemas do VM Import/Export Solução de problemas de erros de solicitação de API
Amazon Elastic Container Service (Amazon ECS)	Solução de problemas do Amazon ECS

Serviço	Link
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 (Memcached)	Solução de problemas de aplicativos
Amazon ElastiCache (Redis OSS)	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
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

Serviço	Link
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
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
SageMaker Inteligência Artificial da Amazon	Solucionar erros Solução de problemas do Amazon SageMaker AI Studio
Amazon Silk	Solução de problemas
Amazon Simple Email Service (Amazon SES)	Solução de problemas do Amazon SES

Serviço	Link
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
A introdução do AWS Trusted Advisor capítulo foi atualizada para mostrar que os planos Basic e Developer Support não oferecem suporte à atualização automática de cheques. Você deve atualizar manualmente as verificações de segurança para ver o status da verificação mais recente.	Para obter detalhes, consulte AWS Trusted Advisor .	11 de junho de 2025
Verificação atualizada: o uso AWS STS global de endpoints agora Regiões da AWS está disponível em todos os níveis do AWS Support plano.	Para obter detalhes, consulte o Registro de alterações para AWS Trusted Advisor verificar as verificações .	9 de junho de 2025
Nova verificação: recomendações de otimização de custos do Amazon Aurora para	Para obter detalhes, consulte o Registro de alterações para AWS Trusted Advisor verificar as verificações .	9 de junho de 2025

armazenamento em cluster de banco de dados

Nova verificação: uso AWS STS global de endpoints em Regiões da AWS

Para obter detalhes, consulte o [Registro de alterações para AWS Trusted Advisor verificar as verificações](#).

2 de junho de 2025

15 novos Hub de Otimização de Custos da AWS cheques adicionados ao Trusted Advisor

Para obter detalhes, consulte o [Registro de alterações para AWS Trusted Advisor verificar as verificações](#).

30 de maio de 2025

Três Trusted Advisor verificações atualizadas

Para obter detalhes, consulte o [Registro de alterações para AWS Trusted Advisor verificar as verificações](#).

21 de maio de 2025

Novo recurso: Atualizar a gravidade do caso de suporte

Para obter detalhes, consulte a seção Alteração do nível de gravidade de um caso de [suporte Criação de casos de suporte e gerenciamento de casos](#).

21 de maio de 2025

Horário atualizado em que você pode ver os detalhes do AWS Support caso.

Para obter detalhes, consulte [Segurança para seus AWS Support casos](#).

29 de abril de 2025

Duas Trusted Advisor verificações atualizadas

Para obter detalhes, consulte o [Registro de alterações para AWS Trusted Advisor verificar as verificações](#).

2 de abril de 2025

Descrição adicionada para a Suporte API

Foi adicionada a descrição das ações de AWS Suporte API em [Gerenciar acesso ao AWS Support Centro](#).

07 de março de 2025

[6 verificações obsoletas AWS Security Hub](#)

Para obter detalhes, consulte o [Registro de alterações para AWS Trusted Advisor verificar as verificações](#).

05 de março de 2025

[Referências removidas às métricas em nível de categoria para Trusted Advisor](#)

As métricas em nível de categoria para Trusted Advisor estão obsoletas. As referências às métricas em nível de categoria foram removidas de Criar [CloudWatch alarmes da Amazon](#) para monitorar métricas. AWS Trusted Advisor

27 de janeiro de 2025

[Documentação atualizada para Trusted Advisor](#)

Foram adicionadas duas novas verificações: AWS CloudTrail Management Events Logging e Amazon RDS Continuous Backups Not Enabled. Para obter mais informações, consulte [Registro de alterações para AWS Trusted Advisor verificações](#).

23 de dezembro de 2024

[Documentação atualizada para Trusted Advisor](#)

Recursos atualizados do Auto Scaling Group. Para obter mais informações, consulte [Registro de alterações para AWS Trusted Advisor verificações](#).

23 de dezembro de 2024

Documentação atualizada para Trusted Advisor	Verificação de acesso externo do IAM Access Analyzer atualizada. Para obter mais informações, consulte Registro de alterações para AWS Trusted Advisor verificações .	23 de dezembro 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 .	25 de novembro de 2024
Documentação atualizada para Trusted Advisor	Adicionado 1 novo Trusted Advisor cheque. Para obter mais informações, consulte Registro de alterações para AWS Trusted Advisor verificações .	22 de novembro de 2024
Documentação adicionada para políticas AWS gerenciadas do AWS Partner-Led Support	Documentação adicionada para uma nova política AWS gerenciadaAWSPartnerLedSupportReadOnlyAccess . Para obter mais informações, consulte as políticas AWS gerenciadas do AWS Partner-Led Support .	22 de novembro de 2024

Documentação atualizada para Trusted Advisor	3 Trusted Advisor verificações atualizadas. Para obter mais informações, consulte Registro de alterações para AWS Trusted Advisor verificações .	7 de novembro de 2024
Documentação atualizada para AWS Support planos	Foi adicionado um novo exemplo de registro da ListSupportPlanModifiers operação às chamadas da API Logging Suporte Plans com a AWS CloudTrail página.	6 de novembro de 2024
Documentação atualizada para AWSTrustedAdvisorServiceRolePolicy	Foram adicionadas novas ações do IAM elasticloadbalancing:DescribeListeners e elasticloadbalancing:DescribeRules , para integrar uma nova verificação de segurança. Para obter mais informações, consulte Políticas gerenciadas pela AWS : AWSTrustedAdvisorServiceRolePolicy .	30 de outubro de 2024
Documentação atualizada para Trusted Advisor	Foram adicionados 4 novos Trusted Advisor cheques. Para obter mais informações, consulte Registro de alterações para AWS Trusted Advisor verificações .	11 de outubro 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](#).

8 de outubro de 2024

[Documentação atualizada para Trusted Advisor](#)

1 verificação de otimização de custos foi movida para o pilar Tolerância a falhas. 1 verificação de segurança e 1 verificação de tolerância a falhas atualizadas. Para obter mais informações, consulte [Registro de alterações para AWS Trusted Advisor verificações](#).

2 de outubro de 2024

[Seção AWS Trusted Advisor Engage atualizada](#)

A seção AWS Trusted Advisor Engage foi atualizada para fazer referência ao AWS Countdown. Para obter mais informações, consulte [Introdução ao AWS Trusted Advisor Engage \(versão prévia\)](#).

16 de setembro de 2024

[Documentação atualizada para AWS Support planos](#)

Foram adicionadas uma nova permissão e CloudTrail documentação para visualizar uma lista de modificadores do plano 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](#).

9 de setembro de 2024

[Documentação atualizada para Trusted Advisor](#)

Trusted Advisor adicionou 9 novos cheques em 23 de agosto. Para obter mais informações, consulte [Registro de alterações para AWS Trusted Advisor verificações](#).

23 de agosto de 2024

[Documentação atualizada para Trusted Advisor](#)

Atualizou 1 verificação de excelência Trusted Advisor operacional e adicionou 1 nova verificação Trusted Advisor de segurança. Para obter mais informações, consulte [Registro de alterações para AWS Trusted Advisor verificações](#).

22 de agosto de 2024

[Documentação atualizada para Trusted Advisor](#)

6 verificações Trusted Advisor de segurança atualizadas. Para obter mais informações, consulte [Registro de alterações para AWS Trusted Advisor verificações](#).

20 de agosto de 2024

[Documentação atualizada
para Trusted Advisor](#)

2 Trusted Advisor cheques atualizados. Para obter mais informações, consulte [Registro de alterações para AWS Trusted Advisor verificações](#).

12 de agosto 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](#).

5 de agosto de 2024

[Documentação atualizada
para Trusted Advisor](#)

9 Trusted Advisor cheques atualizados. Para obter mais informações, consulte [Registro de alterações para AWS Trusted Advisor verificações](#).

21 de julho de 2024

[Documentação atualizada
para AWSTrustedAdvisorS
erviceRolePolicy](#)

11 de junho de 2024

Foram adicionadas novas ações do IAM access-analyzer:ListAnalyzers cloudwatch:ListMetrics dax:DescribeCluster ,ec2:DescribeNatGateways ,ec2:DescribeRouteTables ,ec2:DescribeVpcEndpoints ,ec2:GetManagedPrefixListEntries ,elasticloadbalancing:DescribeTargetHealth ,iam:ListSAMLProviders , kafka:DescribeClusterV2 network-firewall:ListFirewalls network-firewall:DescribeFirewall e sqs:GetQueueAttributes para integrar novas verificações. Para obter mais informações, consulte [Políticas gerenciadas pela AWS : AWSTrustedAdvisorServiceRolePolicy](#).

[Foram removidas 5 AWS Trusted Advisor verificações da documentação](#)

Foram removidas 5 AWS Trusted Advisor verificações que agora estão obsoletas. Para obter mais informações, consulte [Registro de alterações para AWS Trusted Advisor verificações](#).

15 de maio de 2024

[Adicionou 1 nova verificação AWS Trusted Advisor de segurança à documentação](#)

Foi adicionada 1 nova verificação AWS Trusted Advisor de segurança à documentação. Para obter mais informações, consulte [Registro de alterações para AWS Trusted Advisor verificações](#).

15 de maio de 2024

[Três verificações de tolerância a falhas foram removidas da documentação](#)

Foram removidas 3 verificações de tolerância a falhas que agora estão obsoletas. Para obter mais informações, consulte [Registro de alterações para AWS Trusted Advisor verificações](#).

25 de abril de 2024

[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 Suporte plano](#)

Atualizações nos recursos dos Suporte planos. Para obter mais informações, consulte [Suporte os planos](#).

11 de março 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](#).

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 AWSTrustedAdvisorS
erviceRolePolicy](#)

Foram adicionadas novas ações do IAM `cloudtrail:GetTrail` `cloudtrail:ListTrails` `cloudtrail:GetEventSelectors` `outposts:GetOutposts` `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 atualizadas para incluir a declaração `AWSTruste dAdvisorPriorityReadOnlyAccess` e gerenciadas para incluir a declaração `AWSTruste dAdvisorPriorityFullAccess`. Para obter mais informações, consulte [Políticas gerenciadas pela AWS para 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 informações, consulte o [Registro de alterações para AWS Trusted Advisor verificações](#).

12 de outubro de 2023

[Documentação atualizada
para AWSTrustedAdvisorServiceRolePolicy](#)

Foram adicionadas novas ações route53resolver:ListResolveEndpoints , route53resolver:ListResolveEndpointIpAddresses , ec2:DescribeSubnets , kafka:ListClustersV2 e kafka:ListNodes do IAM para integrar as novas verificações de resiliência. Para obter mais informações, consulte [Políticas gerenciadas pela AWS : AWSTrustedAdvisorServiceRolePolicy](#).

14 de setembro 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](#).

28 de agosto de 2023

[Documentação atualizada para Trusted Advisor](#)

Foram adicionadas 1 novas verificações de limites de serviço para AWS Lambda. Para obter mais informações, 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 informações, 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 interações. Página adicionada com [exemplos de políticas de controle de serviço para AWS Trusted Advisor](#).

27 de julho 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](#).

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 Resiliência e 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:

16 de fevereiro de 2023

- 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 recomendações.

Para obter mais informações, consulte [Introdução ao Trusted Advisor Priority](#).

[Exemplos de código atualizados para Suporte](#)

Foram adicionados exemplos de código.NET, Java e Kotlin que mostram como usar Suporte com um kit de desenvolvimento de AWS software (SDK). Para obter mais informações, consulte [Exemplos de código para Suporte uso AWS SDKs](#).

16 de janeiro 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](#).

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:

14 de dezembro de 2022

- Casos de suporte para conta e faturamento.
- Suporte em japonês para casos de suporte técnico.
- Para obter mais informações, consulte [Como criar casos de suporte em um canal do Slack](#).

[Documentação atualizada para AWS Support](#)

Foi adicionada documentação sobre novos endpoints para a Suporte 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 CloudFormation 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 Resiliência 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 sua 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.

29 de setembro de 2022

- [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](#)

[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](#)

Foi adicionada uma nova verificação de segurança para a Amazon EC2. Para obter mais informações, consulte o [Registro de alterações para AWS Trusted Advisor verificações](#).

1.º de setembro de 2022

[Documentação atualizada do
AWS Support aplicativo no
Slack](#)

Consulte os seguintes tópicos: 24 de agosto de 2022

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 informações, 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](#).

[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 agosto de 2022

[Documentação adicionada para Trusted Advisor Priority](#)

Trusted Advisor O Priority adiciona suporte aos seguintes recursos:

17 de agosto de 2022

- Administradores delegados
- Notificações diárias e semanais por e-mail para resumos de recomendações
- Reabrir recomendações resolvidas ou rejeitadas
- AWS políticas gerenciadas

Para obter mais informações, consulte [Introdução ao Trusted Advisor Priority](#).

[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:

7 de julho de 2022

- 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](#).

[Documentação atualizada
para AWS Support](#)

Adição de documentação que explica como gerenciar casos de suporte.

28 de junho de 2022

- [Updating an existing support case](#) (Atualizar um caso de suporte existente)
- [Solução de problemas](#)

[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 que são 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 informações, consulte [Introdução ao Trusted Advisor Priority](#).

28 de fevereiro de 2022

[Documentação atualizada para usar a Amazon EventBridge para Trusted Advisor](#)

Você pode criar uma EventBridge regra para monitorar as alterações em seus Trusted Advisor cheques. Para obter mais informações, 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 notificações sobre seus casos de suporte. Para obter mais informações, consulte [Monitoramento de Suporte com EventBridge](#).

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 EC2 instâncias da Amazon que estão executando o Microsoft SQL Server.

20 de dezembro de 2021

- Consolidação de EC2 instâncias da Amazon para Microsoft SQL Server
- EC2 Instâncias da Amazon provisionadas em excesso para o Microsoft SQL Server
- Fim do suporte às EC2 instâncias da Amazon com Microsoft SQL Server

Para obter mais informações, consulte [Referência da verificação do AWS Trusted Advisor.](#)

[Documentação atualizada
para Trusted Advisor](#)

Trusted Advisor adicionou
quatro novas verificações para
AWS Well-Architected

20 de dezembro de 2021

- 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](#).

[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 informações, 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 Support](#) [AWS 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 Suporte 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:

12 de maio de 2021

- 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](#)

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 informações, 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 atualizadas para o Amazon Elastic Block Store	Cinco AWS Trusted Advisor verificações atualizadas para o Amazon EBS no Registro 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 Registrando alterações em seu Suporte plano .	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 Registrando ações AWS Trusted Advisor do console 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 no Registro 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 AWS Trusted Advisor informações no CloudTrail registro .	22 de outubro de 2020
AWS Support Cotas adicionadas	Adicionadas informações sobre as cotas e restrições do Suporte. Consulte Suporte 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 Visão organizacional para AWS Trusted Advisor .	17 de julho de 2020

Alteração	Descrição	Data
Segurança e AWS Support	Atualização de informações sobre considerações 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 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.	1º 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 AWS terminologia mais recente, consulte o [AWS glossário](#) na Glossário da AWS Referência.

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.