Manual do usuário

AWS Health

AWS Health: Manual do usuário

Table of Contents

O que AWS Healthé

AWS Health fornece visibilidade contínua do desempenho de seus recursos e da disponibilidade de suas Serviços da AWS contas. Você pode usar AWS Health eventos para saber como as mudanças de serviços e recursos podem afetar seus aplicativos em execução AWS. AWS Health fornece informações relevantes e oportunas para ajudá-lo a gerenciar eventos em andamento. AWS Health também ajuda você a conhecer e a se preparar para as atividades planejadas. O serviço fornece alertas e notificações acionados por mudanças na integridade dos AWS recursos, para que você tenha visibilidade e orientação quase instantâneas do evento para ajudar a acelerar a solução de problemas.

Todos os clientes podem usar o AWS Health Dashboard AWS , desenvolvido pelo AWS Health API. O painel não requer configuração e está pronto para ser usado por AWS usuários autenticados. Para obter mais destaques do serviço, consulte a página de detalhes AWS Health do AWS Health painel Página .

AWS Health fornece um console, chamado AWS Health Dashboard, para todos os clientes. Você não precisa escrever código ou realizar qualquer ação para configurar o painel.

Para aprender o básico AWS Health e os termos que você encontrará ao usar o serviço, Para entender os conceitos básicos do see. AWS Health Conceitos para AWS Health

Observações

- O AWS Health painel está disponível para todos AWS os clientes sem custo adicional.
- Todos AWS os clientes podem receber AWS Health eventos pela Amazon sem EventBridge custo adicional.
- Se você tiver um plano Business, Enterprise On-Ramp ou Enterprise Support, você pode usar o AWS Health API para se integrar com sistemas internos e de terceiros. Para obter mais informações, consulte a AWS Health APIReferência.
- Para obter mais informações sobre AWS Support os planos disponíveis, consulte AWS Support.

Conceitos para AWS Health

Aprenda sobre AWS Health conceitos e entenda como você pode usar o serviço para manter a integridade de seus aplicativos, serviços e recursos em seu Conta da AWS.

Tópicos

AWS Health evento

AWS Health eventos, também conhecidos como eventos de Saúde, são notificações AWS Health enviadas em nome de outros AWS serviços. Você pode usar esses eventos para saber mais sobre mudanças futuras ou programadas que possam afetar sua conta. Por exemplo, AWS Health pode enviar um evento se o AWS Identity and Access Management (IAM) planeja descontinuar uma política gerenciada ou AWS Config planeja suspender o uso de uma regra gerenciada. AWS Health também envia eventos quando há problemas de disponibilidade de serviço em um Região da AWS. Você pode revisar a descrição do evento para entender o problema, identificar os recursos afetados e realizar as ações recomendadas.

Há dois tipos de eventos de integridade:

Sumário

Evento específico da conta

Os eventos específicos da conta são locais para você Conta da AWS ou para uma conta da sua AWS organização. Por exemplo, se houver um problema com um tipo de instância do Amazon Elastic Compute Cloud (Amazon EC2) em uma região que você usa AWS Health , fornece informações sobre o evento e o nome dos recursos afetados.

Você pode encontrar eventos específicos da conta no seu AWS Health painel, na AWS Health API ou usar o Amazon CloudWatch Events para receber notificações.

Evento de evento de

Eventos públicos são eventos de serviço relatados que não são específicos de uma conta. Por exemplo, se houver um problema de serviço para o Amazon Simple Storage Service (Amazon S3) na região Leste dos EUA (Ohio) AWS Health , forneça informações sobre o evento, mesmo que você não use esse serviço ou tenha buckets S3 nessa região. Recomendamos que você revise as notificações públicas antes de agir sobre elas.

Você pode encontrar eventos públicos em seu AWS Health Painel e no AWS Health Painel — Integridade do serviço.

Se você tiver uma conta, consulte Começando com seu AWS Health painel.

Se você não tiver uma conta, consulte AWS Health Painel de controle.

AWS Health Painel

Se você tiver um Conta da AWS, seu AWS Health painel mostra eventos públicos e eventos específicos da conta.

Recomendamos que você use seu AWS Health Painel para saber mais sobre eventos que fornecem informações gerais, como um problema futuro de manutenção de um serviço em uma região. Você também pode usar o AWS Health Painel para saber mais sobre eventos que podem afetá-lo diretamente, como um recurso obsoleto em sua conta.

Você pode fazer login no AWS Management Console para ver seu AWS Health painel em https://health.aws.amazon.com/health/home.

Para ter mais informações, consulte Começando com seu AWS Health painel.

AWS Health Painel — Integridade do serviço

Se você não tiver uma conta, você pode usar o AWS Health Dashboard — Service health em https://health.aws.amazon.com/health/status para ver eventos públicos. Eventos públicos são problemas de serviço relatados AWS que fornecem informações sobre a disponibilidade do serviço. Este site mostra apenas eventos públicos, que não são específicos de nenhuma conta. Não é necessário fazer login no painel de suporte.

Para ter mais informações, consulte AWS Health Painel de controle.

Nome de evento de evento de evento

Os códigos de tipo de evento mostrados em um evento de Saúde incluem o serviço afetado e o tipo de evento. Por exemplo, se você receber um evento de Saúde com o código do tipo de evento `AWS_EC2_SYSTEM_MAINTENANCE_EVENT`, isso significa que o serviço está agendando um evento de manutenção que pode afetar você. Use essas informações para planejar com antecedência ou realizar ações em sua conta.

Categorias de tipos de eventos

Todos os eventos de Health têm uma categoria de tipo de evento associada. Para alguns eventos, a categoria do tipo de evento pode aparecer no código do tipo de evento, como o código `AWS_RDS_MAINTENANCE_SCHEDULED`. Neste exemplo, a categoria está programada. Você pode usar essas informações para entender as categorias de eventos em um alto nível.

Recomendamos que você monitore todas as categorias de tipos de eventos. Observe que cada categoria aparece para diferentes tipos de eventos. Você também pode usar a operação da API DescribeEventTypes para encontrar a categoria do tipo de evento.

Notificação de contas

> Esses eventos fornecem informações sobre a administração ou a segurança de suas contas e serviços. Esses eventos podem ser informativos ou exigir uma ação urgente de sua parte. Recomendamos que você preste atenção a esses tipos de eventos e analise todas as ações recomendadas.
>
> Veja a seguir exemplos de códigos de tipo de evento para notificações de conta:

- AWS_S3_OPEN_ACCESS_BUCKET_NOTIFICATION: você tem um bucket Amazon S3 que pode permitir acesso público.
- AWS_BILLING_SUSPENSION_NOTICE: sua conta tem cobranças pendentes e foi suspensa, ou você desativou sua conta.
- AWS_WORKSPACES_OPERATIONAL_NOTIFICATION— Há um problema de serviço para a Amazon WorkSpaces.

Problema

Esses eventos são eventos inesperados que afetam AWS serviços ou recursos. Eventos comuns nessa categoria incluem comunicações sobre problemas operacionais que estão causando a degradação do serviço ou problemas localizados em nível de recursos, para sua conscientização.

Veja a seguir alguns exemplos de códigos de tipo de evento relativos a problemas.

- AWS_EC2_OPERATIONAL_ISSUE: um problema operacional de um serviço, como atrasos no uso do serviço.
- AWS_EC2_API_ISSUE: um problema operacional para a API de um serviço, como maior latência para uma operação de API.
- AWS_EBS_VOLUME_ATTACHMENT_ISSUE: um problema de nível de recurso localizado que poderia afetar os recursos do seu Amazon Elastic Block Store (Amazon EBS).
- AWS_ABUSE_PII_CONTENT_REMOVAL_REPORT: esse evento significa que sua conta poderá ser suspensa se você não agir.

Alteração programada

Eventos programados fornecem informações sobre futuras alterações nos seus serviços e recursos. Esses eventos incluem eventos planejados do ciclo de vida, como end-of-support notificações e atualizações automáticas para diferentes versões. Alguns eventos podem recomendar que você tome medidas para evitar interrupções no serviço, enquanto outros ocorrerão automaticamente sem nenhuma ação de sua parte. Seu recurso pode estar temporariamente indisponível durante a atividade de alteração programada. Todos os eventos nessa categoria são eventos específicos da conta.

Veja a seguir exemplos de códigos de tipo de evento para alterações programadas:

- AWS_EC2_INSTANCE_RETIREMENT_SCHEDULED: uma instância EC2 da Amazon exige uma reinicialização.
- AWS_SAGEMAKER_SCHEDULED_MAINTENANCE— SageMaker requer um evento de manutenção, como a correção de um problema de serviço.

- `AWS_RDS_PLANNED_LIFECYCLE_EVENT`— O Amazon RDS está programando um evento de ciclo de vida planejado, como um end-of-support evento para uma de suas versões, que exige a ação do cliente.

> **Tip**
>
> Se você usar a AWS Health API ou o AWS Command Line Interface (AWS CLI) para retornar detalhes do evento, o `Event` objeto conterá o `eventScopeCode` campo com o `ACCOUNT_SPECIFIC` valor. Para obter mais informações, consulte a AWS Health Referência da API do .

Status do evento

O status do evento informa se o evento de Saúde está aberto, fechado ou próximo. Você pode ver os eventos de Health no AWS Health Dashboard ou na AWS Health API por até 90 dias.

Entidades afetadas

As entidades afetadas são AWS recursos que podem ser afetados pelo evento. Por exemplo, se você receber um evento programado para manutenção do Amazon EC2 para um tipo específico de instância que você está usando em sua conta, você pode usar o evento Health para determinar a ID das instâncias afetadas. Use essas informações para resolver qualquer possível problema de serviço, como criar ou suspender o uso de recursos.

AWS Health eventos na Amazon EventBridge

Você pode configurar EventBridge as regras da Amazon para suas contas para automatizar ações após o AWS Health evento apropriado ser recebido por uma conta. Essas podem ser ações gerais, como enviar todas as mensagens de eventos do ciclo de vida planejado para uma interface de bate-papo. Ou podem ser ações específicas, como acionar um fluxo de trabalho em uma ferramenta de gerenciamento de serviços de TI.

Para ter mais informações, consulte Monitorando eventos AWS Health com a Amazon EventBridge.

AWS Health API

Você pode usar a AWS Health API para acessar programaticamente as informações que aparecem no AWS Health Painel, como as seguintes:

- Obtenha informações sobre eventos que podem afetar seus AWS serviços e recursos
- Ative ou desative o recurso de visualização organizacional para sua AWS organização
- Filtre seus eventos por serviços específicos, categorias de tipo de evento e códigos de tipo de evento

Para obter mais informações, consulte a AWS Health Referência da API do .

> **Note**
>
> Você deve ter um plano Business, Enterprise On-Ramp ou Enterprise Support da AWS Supportpara usar a AWS Health API. Se você chamar a AWS Health API de uma conta que não tem um plano Business, Enterprise On-Ramp ou Enterprise Support, você receberá uma `SubscriptionRequiredException` mensagem de erro.

Visualização organizacional

Você pode usar esse recurso para agregar todos os eventos de saúde das suas AWS contas AWS Organizations em uma única visualização no AWS Health Painel. Em seguida, você pode entrar na conta de gerenciamento da sua organização ou usar a AWS Health API para visualizar todos os eventos que possam afetar as diferentes contas e recursos. Você pode ativar esse recurso no AWS Health console ou na API. Para ter mais informações, consulte Agregando AWS Health eventos em todas as contas.

Começando com seu AWS Health painel

Você pode usar seu AWS Health painel para saber mais sobre AWS Health eventos. Esses eventos podem afetar seu Serviços da AWS ou Conta da AWS. Depois de entrar na sua conta, o AWS Health Painel mostra as informações das seguintes formas:

- Eventos da sua conta: esta página mostra eventos específicos da sua conta. Você pode ver as alterações abertas, recentes e programadas. Você também pode visualizar notificações e um log de eventos que mostra todos os eventos dos últimos 90 dias.
- Eventos da sua organização: Esta página mostra eventos específicos da sua organização em AWS Organizations. Você pode visualizar alterações abertas, recentes e programadas para sua organização. Você também pode visualizar notificações, bem como um log de eventos que mostra todos os eventos da organização nos últimos 90 dias.

> **Note**
>
> Se você não tiver um Conta da AWS, você pode usar o AWS Health Painel de controle para saber mais sobre a disponibilidade geral do serviço.
> Se você tiver uma conta, recomendamos que faça login no seu AWS Health Painel para obter informações mais detalhadas sobre eventos e mudanças futuras que possam afetar seus serviços e recursos.

Tópicos

- Configurando sua AWS conta
- Como visualizar os eventos da sua conta no AWS Health Dashboard
- Configurando a Amazon EventBridge

Configurando sua AWS conta

Antes de habilitar AWS Health, você deve ter um Conta da AWS. Se você não tiver uma AWS conta, conclua as etapas a seguir para criar uma.

Inscreva-se para um Conta da AWS

Se você não tiver um Conta da AWS, conclua as etapas a seguir para criar um.

Para se inscrever em um Conta da AWS

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

   Parte do procedimento de inscrição envolve receber uma chamada telefônica e inserir um código de verificação no teclado do telefone.

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

AWS envia um e-mail de confirmação após a conclusão do processo de inscrição. A qualquer momento, você pode visualizar a atividade atual da sua conta e gerenciar sua conta acessando https://aws.amazon.com/e escolhendo Minha conta.

Criar um usuário com acesso administrativo

Depois de se inscrever em um Conta da AWS, proteja seu Usuário raiz da conta da AWS AWS IAM Identity Center, habilite e crie um usuário administrativo para que você não use o usuário root nas tarefas diárias.

Proteja seu Usuário raiz da conta da AWS

1. Faça login AWS Management Consolecomo proprietário da conta escolhendo Usuário raiz e inserindo seu endereço de Conta da AWS e-mail. Na próxima página, insira sua senha.

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

   Para obter instruções, consulte Habilitar um MFA dispositivo virtual para seu usuário Conta da AWS root (console) no Guia IAM do usuário.

Criar um usuário com acesso administrativo

1. Ative o IAM Identity Center.

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

2. No IAM Identity Center, conceda acesso administrativo a um usuário.

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

Iniciar sessão como o usuário com acesso administrativo

- Para entrar com seu usuário do IAM Identity Center, use o login URL que foi enviado ao seu endereço de e-mail quando você criou o usuário do IAM Identity Center.

  Para obter ajuda para fazer login usando um usuário do IAM Identity Center, consulte Como fazer login no portal de AWS acesso no Guia Início de Sessão da AWS do usuário.

Atribuir acesso a usuários adicionais

1. No IAM Identity Center, crie um conjunto de permissões que siga as melhores práticas de aplicação de permissões com privilégios mínimos.

   Para obter instruções, consulte Create a permission set no Guia do usuário do AWS IAM Identity Center .

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

   Para obter instruções, consulte Add groups no Guia do usuário do AWS IAM Identity Center .

Como visualizar os eventos da sua conta no AWS Health Dashboard

Você pode entrar na sua conta para receber recomendações e eventos personalizados.

Para visualizar os eventos da conta em seu AWS Health painel

1. Abra seu AWS Health painel em https://health.aws.amazon.com/health/casa.
2. No painel de navegação, em A integridade da sua conta, você pode escolher as seguintes opções:
   a. Edições abertas e recentes: visualize eventos abertos e fechados recentemente.
   b. Mudanças programadas: veja os próximos eventos que podem afetar seus serviços e recursos.
   c. Outras notificações: veja todas as outras notificações e eventos em andamento dos últimos sete dias que possam afetar sua conta.
   d. Log de eventos: visualizar todos os eventos dos últimos 90 dias.

Questões abertas e recentes

Use a guia Problemas abertos e recentes para ver todos os eventos em andamento dos últimos sete dias que podem afetar a sua conta.

Ao selecionar um evento na lista do painel, o painel Detalhes é exibido com informações sobre o evento e os recursos afetados pelo evento. Para obter mais informações, consulte Detalhes do evento.

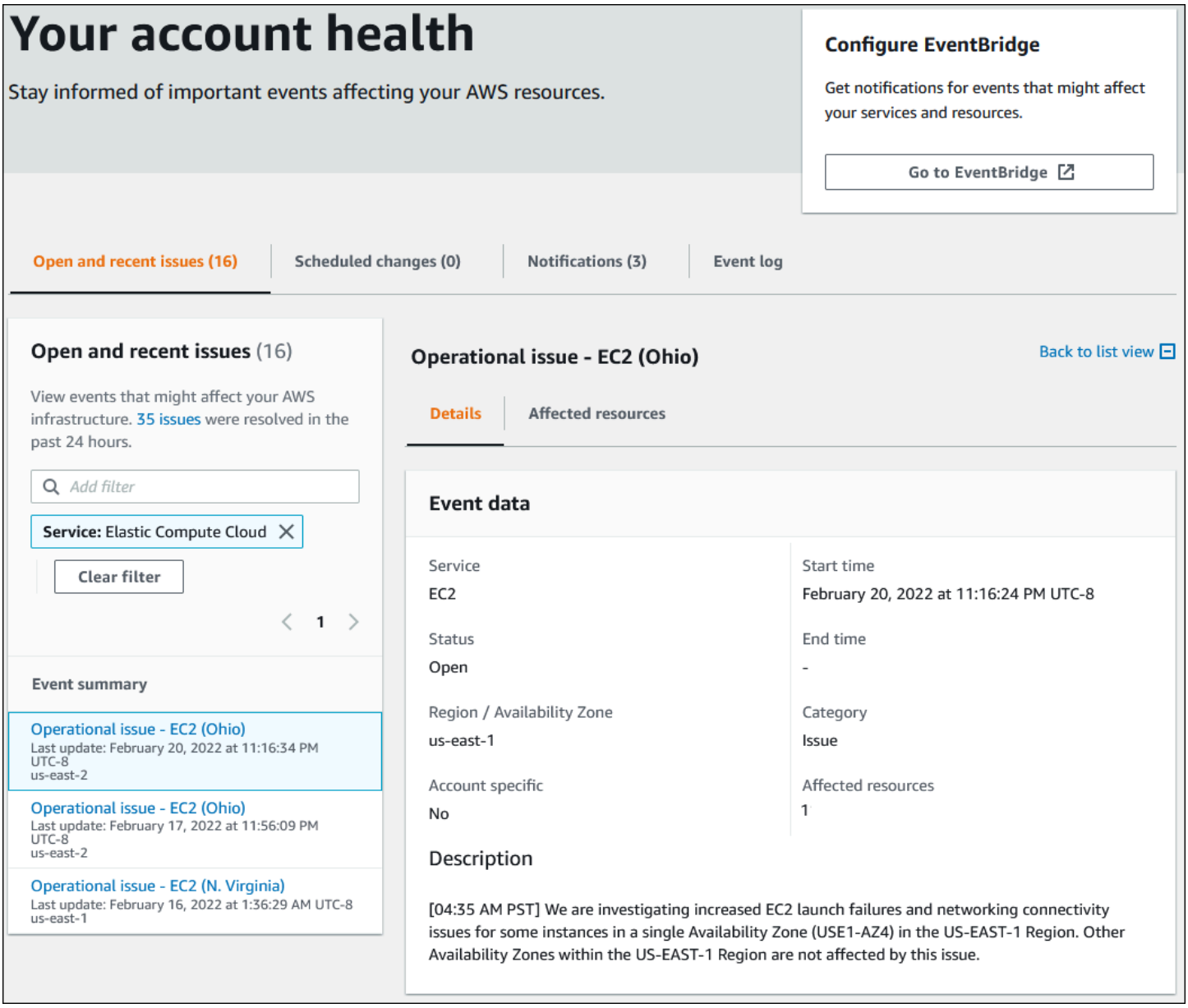
Você pode filtrar os eventos que aparecem em qualquer grupo, escolhendo opções da lista de filtros. Por exemplo, você pode restringir os resultados por zona de disponibilidade, região, horário de término do evento ou horário da última atualização AWS service (Serviço da AWS), etc.

Para ver todos os eventos, em vez dos recentes que aparecem no painel, escolha a guia Log de eventos.

> **Note**
>
> No momento, não é possível excluir notificações para eventos que aparecem no seu AWS Health Dashboard. . Depois que um evento é AWS service (Serviço da AWS) resolvido, a notificação é removida da visualização do painel.

Example : Evento sobre questões operacionais para o Amazon Elastic Compute Cloud (AmazonEC2)

A imagem a seguir mostra um evento de falhas de lançamento e problemas de conectividade para EC2 instâncias da Amazon.



Mudanças programadas

Use a guia Alterações programadas para ver os próximos eventos que podem afetar sua conta. Esses eventos podem incluir atividades de manutenção programadas para serviços e eventos planejados do ciclo de vida que exigem ação para serem resolvidos. Para ajudá-lo a planejar essas atividades, será fornecida uma visualização de calendário para que você possa mapear essas alterações programadas em um calendário mensal. Os filtros estão disponíveis Para obter mais

informações sobre eventos de ciclo de vida planejados, consulte Eventos de ciclo de vida planejados para AWS Health.

Outra notificação

Use a guia Notificações para ver todas as outras notificações e eventos em andamento dos últimos sete dias que possam afetar sua conta. Isso pode incluir eventos, como rotações de certificados, notificações de cobrança e vulnerabilidades de segurança.

Log de eventos

Use a guia Registro de eventos para ver todos os AWS Health eventos. A tabela de log inclui colunas adicionais para que você possa filtrar por Status e Hora de início.

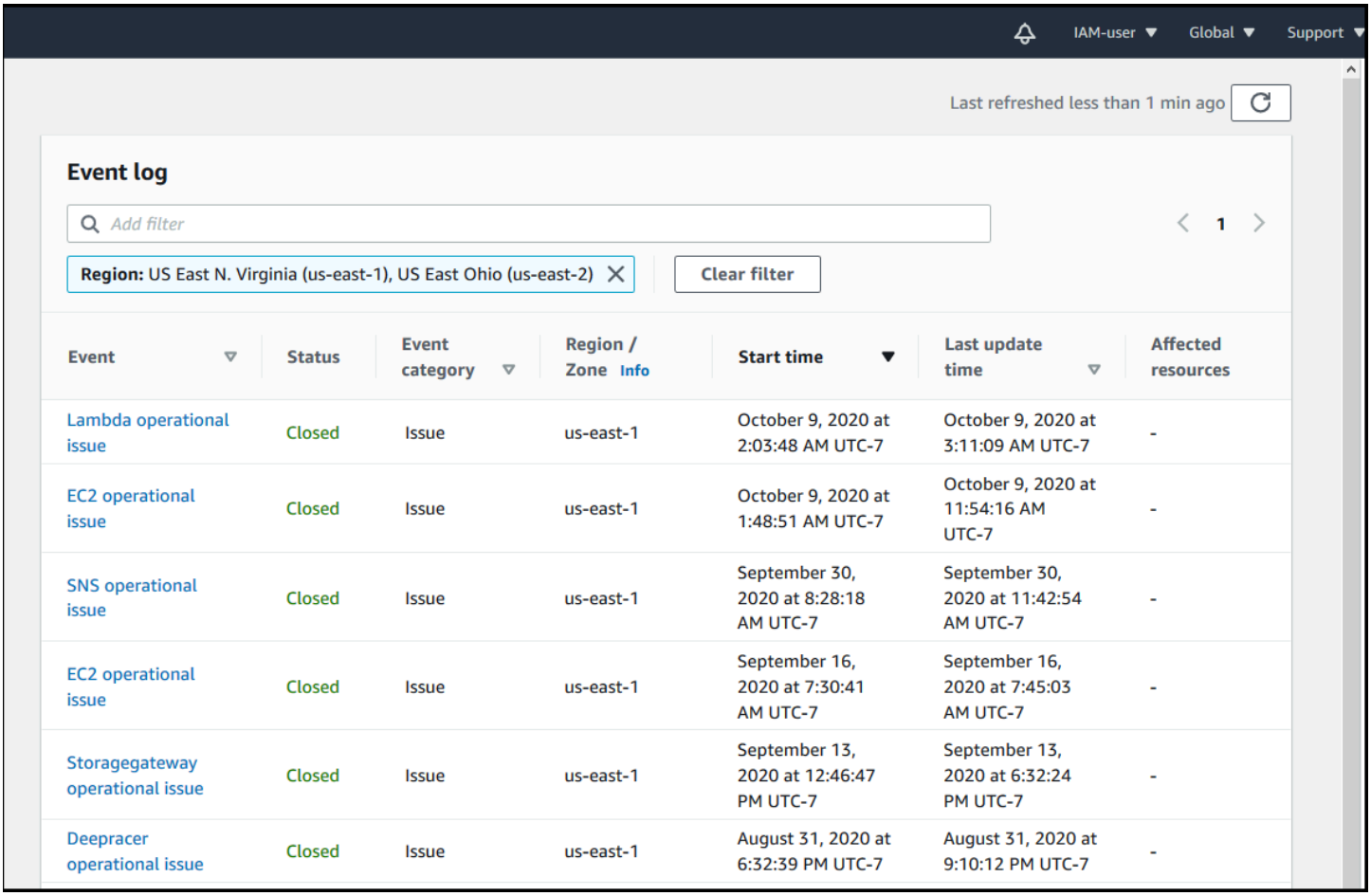
Ao selecionar um evento na tabela Log de eventos, o painel Detalhes do evento é exibido com informações sobre o evento e os recursos afetados pelo evento. Para obter mais informações, consulte Detalhes do evento.

Você pode escolher as seguintes opções de filtro para otimizar os seus resultados:

- Zona de disponibilidade
- Horário de término
- Evento
- Evento ARN
- Categoria de evento
- Hora da última atualização
- Região
- ID do recurso/ARN
- Serviço
- Horário de início
- Status

Example : Log de eventos

A imagem a seguir mostra eventos recentes para as regiões Leste dos EUA (Norte da Virgínia) e Leste dos EUA (Ohio).



Detalhes do evento

Quando você escolhe um evento, duas guias aparecem sobre o evento. A guia Detalhes fornece as seguintes informações:

- Serviço
- Status
- Zona de disponibilidade / região
- Se o evento é específico da conta ou não
- Horário de início e término
- Categoria
- Número de recursos afetados
- Descrição e um cronograma de atualizações sobre o evento

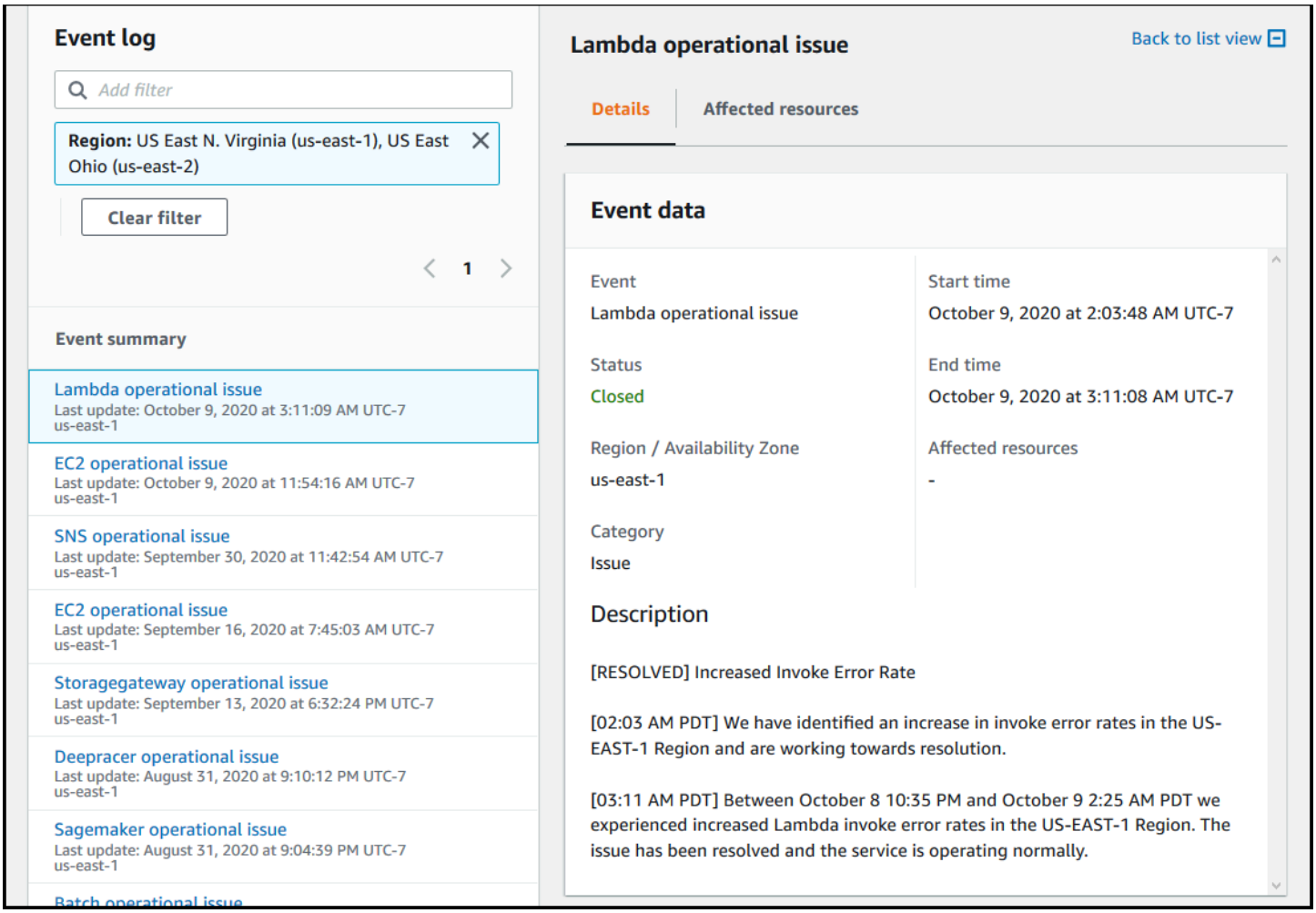
A guia Recursos afetados mostra as seguintes informações sobre todos os AWS recursos afetados pelo evento:

- O ID do recurso (por exemplo, um ID de EBS volume da Amazon, como`vol-a1b2c34f`) ou o Nome do recurso da Amazon (ARN), se disponível ou relevante.
- Para eventos de ciclo de vida planejados, essa lista de recursos afetados também contém o status mais recente dos recursos (Pendente, Desconhecido ou Resolvido). Essa lista geralmente é atualizada uma vez a cada 24 horas.

Você pode filtrar os itens que aparecem nos recursos. Você pode restringir seus resultados por ID de recurso ouARN.

Example : AWS Health evento para AWS Lambda

A captura de tela a seguir mostra um exemplo para Lambda.



Tipos de eventos

Há dois tipos de AWS Health eventos:

- Eventos públicos são eventos de serviço que não são específicos de uma conta da . Por exemplo, se houver um problema com a Amazon EC2 em um Região da AWS, AWS Health fornece informações sobre o evento, mesmo que você não use serviços ou recursos nessa região.
- Os eventos específicos da conta são específicos da sua conta da ou de uma conta na sua organização. Por exemplo, se houver um problema com uma EC2 instância da Amazon em uma região que você usa, AWS Health fornece informações sobre o evento e a lista de EC2 instâncias da Amazon afetadas.

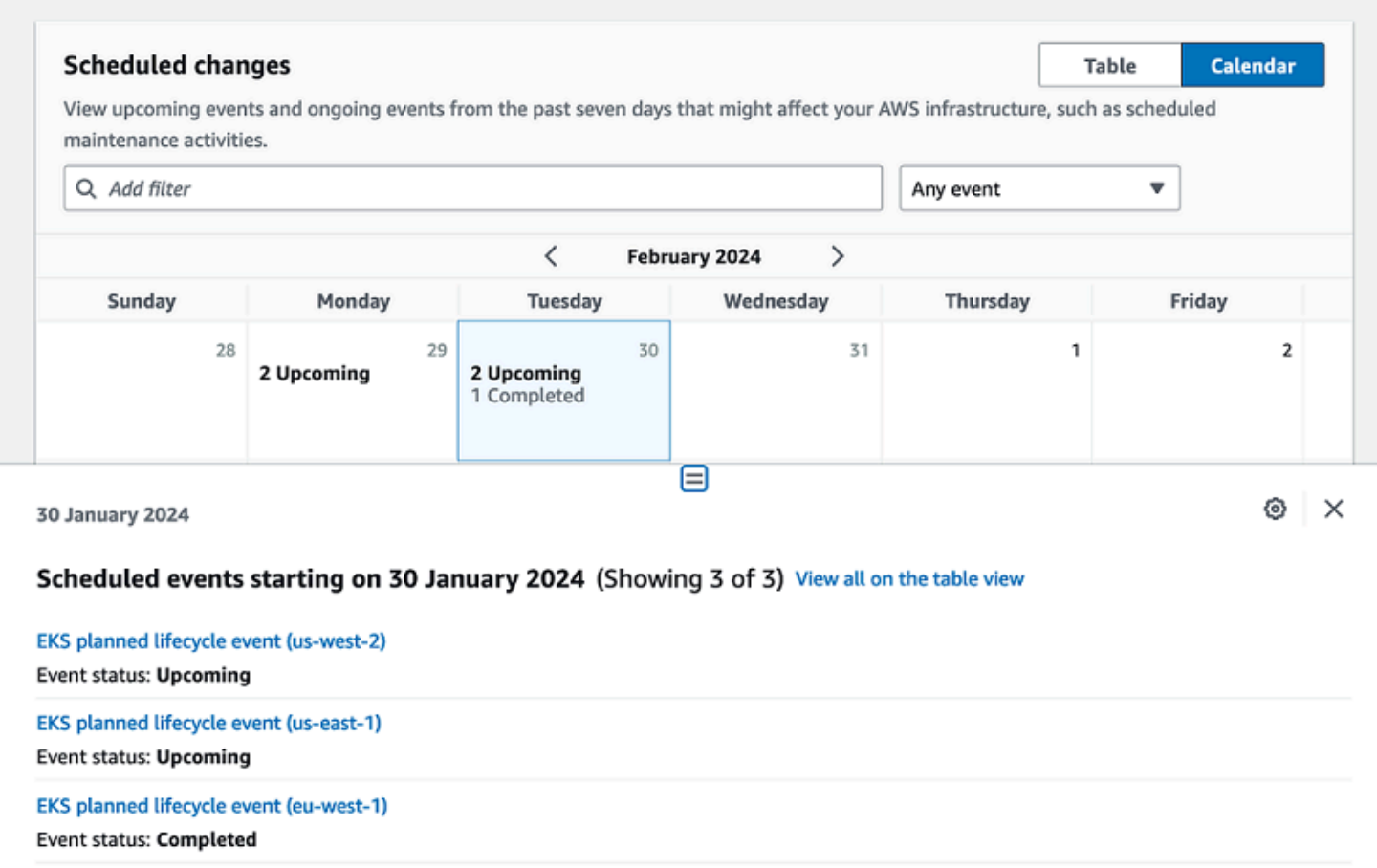
Você pode usar as seguintes opções para identificar se um evento é público ou específico da conta:

- No AWS Health Painel, escolha a guia Recursos afetados para um evento. Eventos com recursos são específicos para a conta. Eventos sem recursos são públicos e não são específicos da conta. Para obter mais informações, consulte Começando com seu AWS Health painel.
- Use o AWS Health API para retornar o `eventScopeCode` parâmetro. Os eventos podem ter o valor `PUBLIC`, `ACCOUNT_SPECIFIC` ou `NONE`. Para obter mais informações, consulte a DescribeEventDetailsoperação na AWS Health APIReferência.

Visualização do calendário

A visualização do calendário está disponível na guia Alterações agendadas para projetar AWS Health eventos em um calendário mensal. Essa visualização permite que você veja as alterações programadas até três meses no passado e um ano no futuro.

AWS Health os eventos são exibidos por data. Selecione uma data para exibir um painel lateral que contém mais detalhes sobre o AWS Health evento. Eventos futuros e em andamento são exibidos em preto. Os eventos concluídos são exibidos em cinza. Se houver mais de dois eventos em uma data, somente o número de eventos em preto e cinza será mostrado. Selecione uma data para exibir uma lista de AWS Health eventos no painel lateral. Você pode selecionar um evento no painel lateral para exibir informações sobre o evento. O painel lateral tem rastros para navegar até uma visualização anterior.



Visualizar os recursos afetados

AWS Health eventos podem especificar os recursos precisos que são afetados. Você pode ver os recursos afetados na guia Recursos afetados do AWS Health evento. Para ver o status, selecione o AWS Health evento. O status será exibido na guia de recursos afetados no painel lateral. Para eventos planejados do ciclo de vida, AWS Health os eventos fornecem atualizações diárias do status dos recursos afetados.

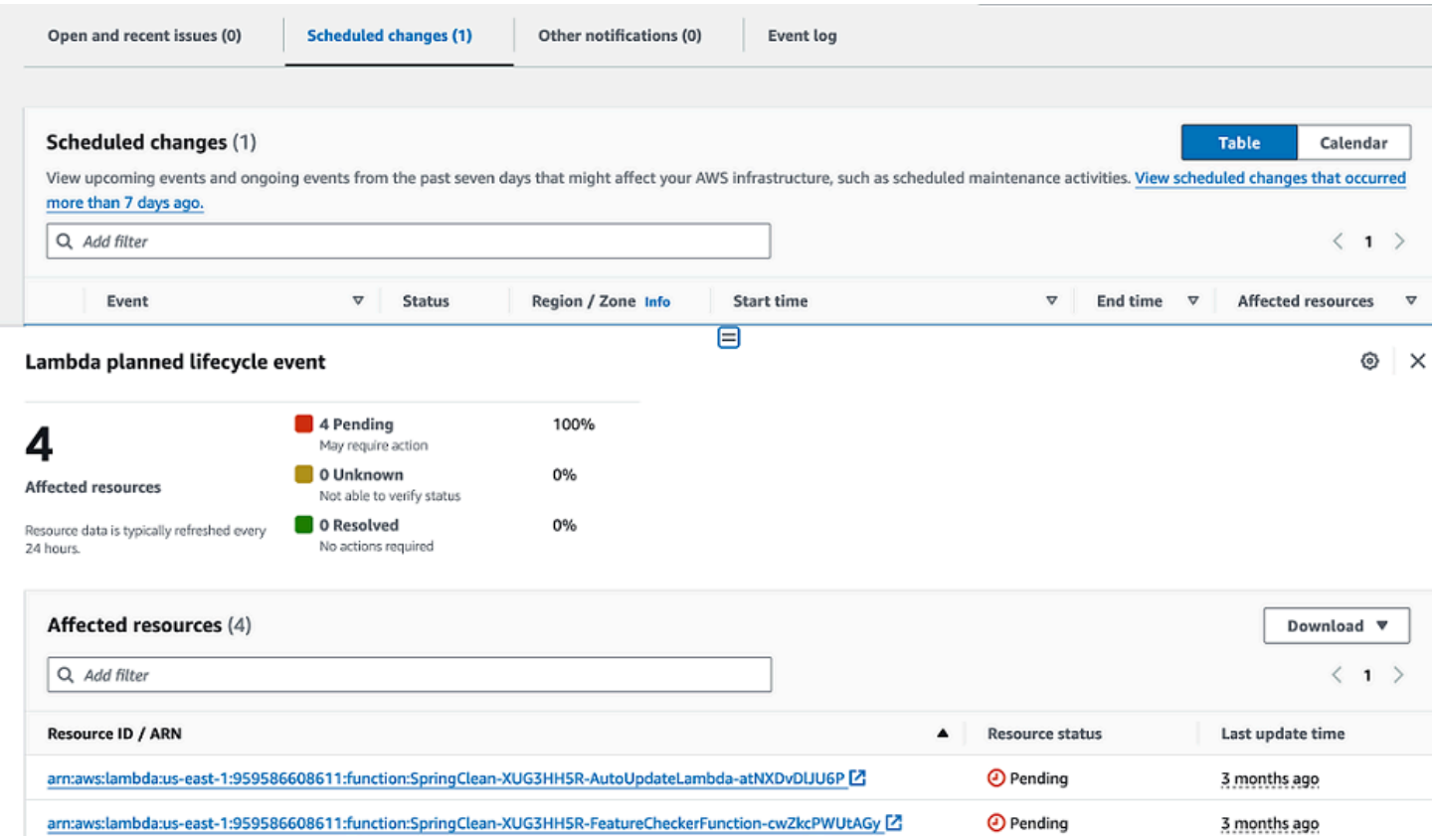
AWS Health Os eventos no nível da conta exibem um resumo dos status dos recursos afetados na parte superior da guia Recursos afetados. Uma lista dos recursos afetados é exibida em uma tabela junto com o status correspondente. Os eventos planejados do ciclo de vida são um exemplo de tipos de eventos que usam o campo de status do recurso. Para saber mais sobre eventos de ciclo de vida planejados, consulte. Eventos de ciclo de vida planejados para AWS Health

Quando você acessa a visualização da organização, AWS Health os eventos exibem um resumo do status de todos os recursos afetados para todas as contas incluídas. Depois do resumo, há uma lista das contas afetadas e o número de recursos pendentes dessa conta. Selecione o número da

conta ou o número de recursos pendentes para exibir o resumo da visualização da conta. O resumo da visualização da conta tem rastros para retornar à lista organizacional das contas afetadas. Um resumo dos status dos recursos afetados é exibido na parte superior do painel dividido.

Você pode baixar a lista de recursos afetados na guia Recursos afetados em CSV ou no JSON formato. Na visão organizacional, o arquivo baixado inclui todos os recursos nas contas listadas. Navegue até o nível da conta na exibição organizacional para incluir somente recursos dessa conta no arquivo baixado. Cada recurso afetado no arquivo baixado inclui o Conta da AWS ID, o eventoARN, o nome da entidade, a entidadeARN, o status e a hora da última atualização do recurso. Se os filtros estiverem ativados, o arquivo baixado incluirá somente os resultados filtrados.

Você pode baixar somente um arquivo por vez. Os arquivos são baixados automaticamente na pasta de download padrão do seu navegador e têm um nome de arquivo predefinido com base no Região da AWS, no título do evento, na data de início do evento e na data do download.



Configurações de fuso horário

Você pode ver os eventos no AWS Health Painel em seu fuso horário local ou emUTC. Se você alterar o fuso horário no seu AWS Health Painel, todos os carimbos de data/hora no painel e nos eventos públicos serão atualizados para o fuso horário especificado.

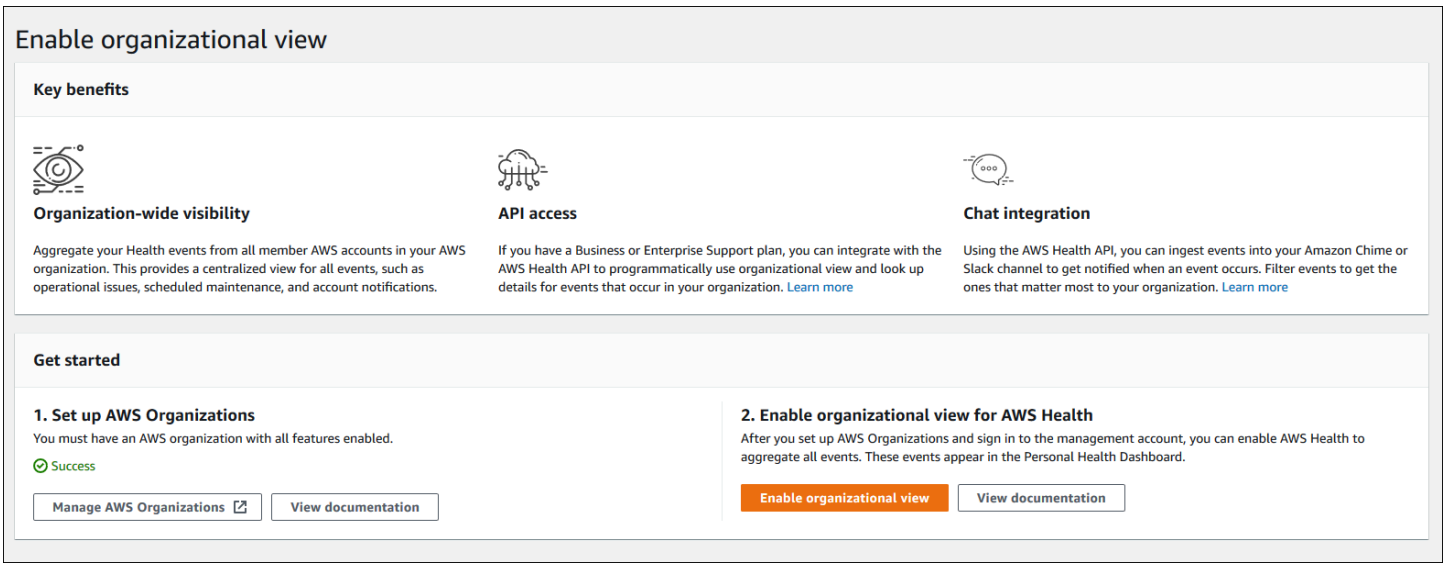
Para atualizar suas configurações de fuso horário

1. Abra seu AWS Health painel em https://health.aws.amazon.com/health/casa.
2. Na parte inferior da página, escolha Preferências de cookies.
3. Selecione Permitido para cookies funcionais. Escolha Salvar preferências.
4. No painel de navegação do seu AWS Health Painel, escolha Configurações de fuso horário.
5. Selecione um fuso horário para suas sessões AWS Health do Dashboard. Em seguida, escolha Salvar alterações.

A integridade da sua organização

AWS Health se integra AWS Organizations para que você possa visualizar os eventos de todas as contas que fazem parte da sua organização. Isso fornece uma exibição centralizada para eventos que aparecem em sua organização. Você pode usar esses eventos para monitorar alterações em seus recursos, serviços e aplicativos.

Para obter mais informações, consulte Agregando AWS Health eventos em todas as contas.



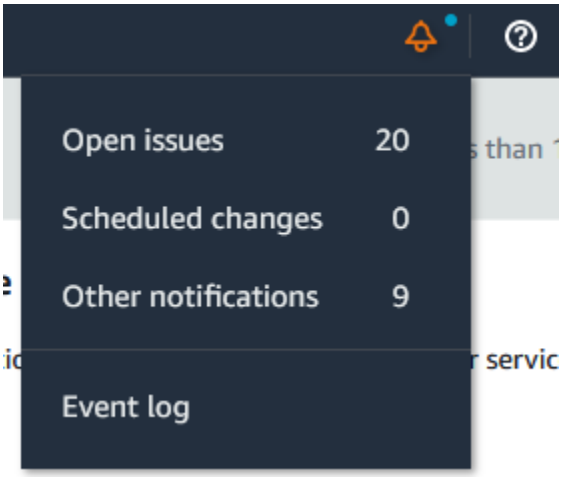
Alertas para AWS Health eventos

Seu AWS Health painel tem um ícone de sino na barra de navegação do console com um menu de alerta. Esse recurso exibe o número de AWS Health eventos recentes que aparecem no painel em cada categoria. Esse ícone de sino aparece em vários AWS consoles, como os da AmazonEC2, Amazon Relational Database Service (RDSAmazon) AWS Identity and Access Management , IAM () e. AWS Trusted Advisor

Escolha o ícone de sino para ver se os eventos recentes afetam a sua conta. Em seguida, você pode escolher um evento para navegar até seu AWS Health painel para obter mais informações.

Example : Eventos abertos

A imagem a seguir mostra eventos de abertura e notificação de uma conta.



Configurando a Amazon EventBridge

Use EventBridge para detectar e reagir às mudanças nos AWS Health eventos. Você pode monitorar AWS Health eventos específicos que ocorrem em sua conta e, em seguida, configurar regras para AWS Health notificá-lo ou agir quando os eventos mudarem.

Use EventBridge com AWS Health

1. Abra seu AWS Health painel em https://health.aws.amazon.com/health/casa.
2. Para navegar até o EventBridge console para criar uma regra, faça o seguinte:
   - No painel de navegação, em Health Integrations, escolha Amazon. EventBridge
   - Em Configurar EventBridge, escolha Ir para EventBridge.
3. Siga este procedimento para criar e monitorar eventos. Consulte Monitorando eventos AWS Health com a Amazon EventBridge.

AWS Health Painel de controle

Você pode usar o AWS Health Painel — Integridade do serviço para ver a integridade de todos Serviços da AWS. Esta página mostra eventos de serviço relatados para serviços em Regiões da AWS. Você não precisa fazer login ou acessar Conta da AWS a página AWS Health Dashboard — Service health.

> **Tip**
>
> Este site mostra apenas eventos públicos, que não são específicos para um Conta da AWS. Se você já tem uma conta, recomendamos que faça login para ver seu AWS Health painel e se manter informado sobre eventos que podem afetar sua conta e seus serviços. Para obter mais informações, consulte Começando com seu AWS Health painel.

Para visualizar o AWS Health painel — Integridade do serviço

1. Navegue até a página de https://health.aws.amazon.com/health/status.

   > **Note**
   >
   > Se você já estiver conectado à sua página Conta da AWS, você será redirecionado para a página AWS Health Painel — Saúde da sua conta.

2. Em Integridade do serviço, escolha Problemas abertos e recentes para ver os eventos relatados recentemente. Você pode visualizar as seguintes informações sobre o evento:

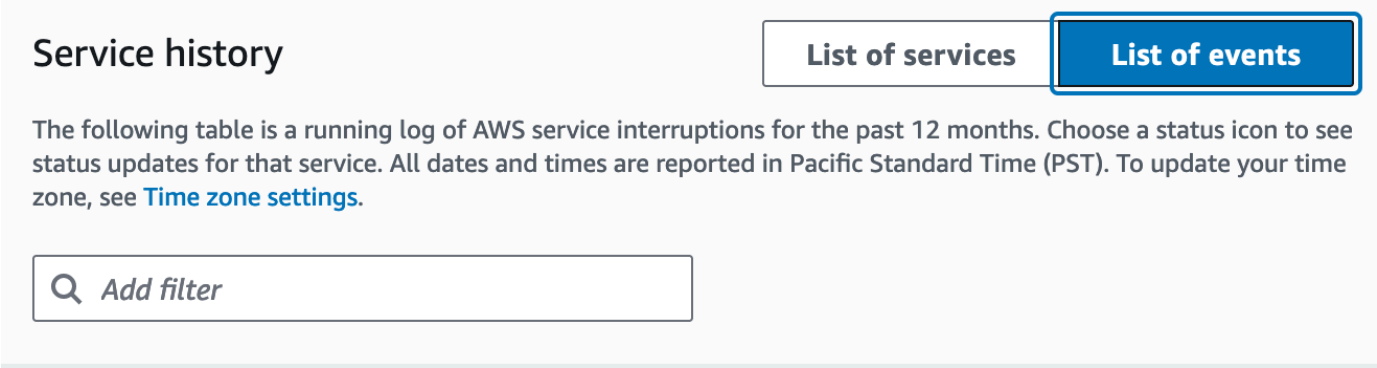
   - O nome do evento e a região afetada. Por exemplo, problema operacional: Amazon Elastic Compute Cloud (Norte da Virgínia)
   - O nome do serviço
   - A gravidade do evento, como informativa ou degradação
   - Um cronograma das atualizações recentes do evento
   - Uma lista das Serviços da AWS que também são afetadas por este evento

> **Note**
>
> Você pode ver os eventos em seu fuso horário local ou emUTC. Para obter mais informações, consulte Configurações de fuso horário.

3. (Opcional) Ao lado do evento, escolha RSSassinar um RSS feed desse evento. Você receberá notificações sobre esse serviço específico no especificado Região da AWS.
4. Escolha Histórico de serviços para ver a tabela de histórico de serviços. Esta tabela mostra todas as AWS service (Serviço da AWS) interrupções dos últimos 12 meses.

> **Tip**
>
> Você pode filtrar por serviço, Região da AWS, e data.

5. Ao lado de um evento de serviço em andamento, escolha o ícone de status ( ) para ver mais informações sobre o evento.
6. (Opcional) Para ver isso como uma lista de eventos históricos, escolha o botão Lista de eventos. Escolha qualquer evento na coluna de eventos para ver mais informações sobre esse evento específico no painel lateral pop-up.



> **Note**
>
> Selecionar qualquer evento público após setembro de 2023 preencherá o URL no navegador com um link para esse AWS Health evento público. Depois de selecionar esse link, você navega até a visualização da lista de eventos com o pop-up do evento.

7. (Opcional) Escolha RSSassinar um RSS feed. Você receberá notificações sobre esse serviço específico no especificado Região da AWS.
8. (Opcional) Você pode ver os eventos em seu fuso horário local ouUTC. Para obter mais informações, consulte Configurações de fuso horário.
9. (Opcional) Se você tiver uma conta, escolha Abrir a integridade da sua conta para fazer login. Depois de fazer login, você pode ver os eventos específicos da sua conta. Para obter mais informações, consulte Começando com seu AWS Health painel.

Eventos de ciclo de vida planejados para AWS Health

Saiba mais sobre eventos de ciclo de vida planejados para. AWS Health

Tópicos

O que são eventos de ciclo de vida planejados?

AWS Health comunica mudanças importantes que podem afetar a disponibilidade de seus aplicativos. No modelo de responsabilidade AWS compartilhada, AWS age para manter o hardware e a infraestrutura subjacentes que suportam seus recursos atualizados e seguros. No entanto, algumas mudanças exigem ação ou coordenação do cliente para evitar impacto em seus aplicativos. AWS Health notifica você com antecedência sobre mudanças importantes, como:

- Fim do suporte de software de código aberto - Alguns Serviços da AWS executam versões de software de código aberto. Se a comunidade de código aberto encerrar o suporte para versões de software, AWS informará quando você precisa tomar medidas para atualizar e evitar impactos em seus aplicativos.
  - Fim do suporte à versão do mecanismo Amazon RDS para MySQL
  - Fim do suporte à versão Amazon EKS Kubernetes
- Mudanças que afetam recursos AWS próprios que podem exigir sua ação.
  - Expiração dos certificados da Autoridade de Certificação do Amazon RDS.
  - O Amazon WorkDocs Companion está chegando ao fim da vida útil e não está mais disponível.

  > **Note**
  >
  > Todas as notificações que atenderem a esses critérios serão relatadas AWS Health como Eventos de Ciclo de Vida Planejado.
- Esgotamento dinâmico de recursos e metadados aprimorados: desde o momento em que você recebe a notificação durante a vida útil do AWS Health evento, seus recursos afetados

são associados ao AWS Health evento como entidades afetadas com um status de entidade específico. Os recursos afetados são especificados no formato ARN, quando aplicável. Se seus recursos afetados exigirem a ação do cliente, eles serão listados com o status “PENDENTE”. Se os recursos afetados tiveram a ação necessária executada ou os recursos foram excluídos, o status será atualizado como “RESOLVIDO”.

> **Note**
>
> - As atualizações do estado dos recursos são realizadas de forma assíncrona e periódica e podem ter um atraso de até 72 horas em raras ocasiões.
> - Nas exceções em que as atualizações dinâmicas não são fornecidas, em vez de os recursos terem o status “PENDENTE” ou “RESOLVIDO”, os recursos não receberão nenhum status.
> - As atualizações de status de recursos não são suportadas nas regiões da China AWS GovCloud (US) e da China.

O que devo esperar ao receber uma notificação de evento de ciclo de vida planejado?

A AWS Health experiência de eventos planejados do ciclo de vida ajuda suas equipes a aprender sobre as próximas mudanças no ciclo de vida e a monitorar a conclusão das ações.

Categoria de tipo: Alteração programada

Código do tipo de evento: AWS_{SERVICE}_PLANNED_LIFECYCLE_EVENT

Hora de início do evento: a hora de início do evento é mais cedo que seus recursos forem afetados pela alteração.

Hora de término do evento: a hora de término do evento é a data em que a alteração termina em todos os AWS recursos. Observe que a hora de término nem sempre é especificada. É importante tratar a hora de início como a data da alteração.

> **Note**
>
> As organizações podem esperar receber um único ARN de evento para cada evento de ciclo de vida planejado agrupado por região em que há recursos afetados. Mas eles podem

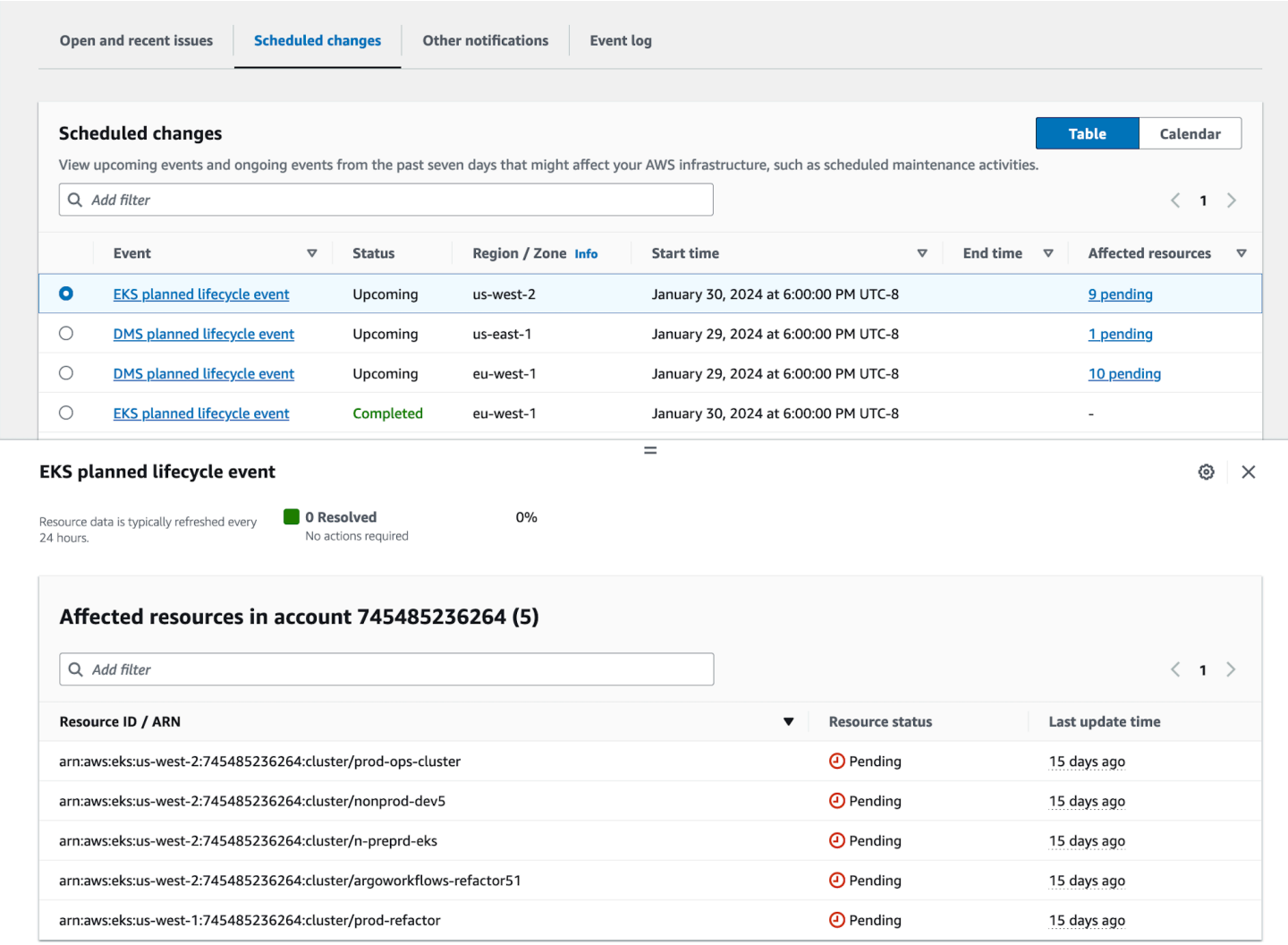
receber vários ARNs se a organização tiver um grande número de afetados Contas da AWS ou recursos.

Visibilidade antecipada dos eventos planejados do ciclo de vida: os eventos planejados do ciclo de vida foram projetados para ter um prazo mínimo de 180 dias para versões/alterações principais e 90 dias para versões/alterações menores, sempre que possível.

Esgotamento dinâmico de recursos e metadados aprimorados: desde o momento em que você recebe a notificação durante a vida útil do AWS Health evento, seus recursos afetados são associados ao AWS Health evento como entidades afetadas com um status de entidade específico. Os recursos afetados são especificados no formato ARN, quando aplicável. Se seus recursos afetados exigirem a ação do cliente, eles serão listados com o status “PENDENTE”. Se os recursos afetados tiveram a ação necessária executada ou os recursos foram excluídos, o status será atualizado como “RESOLVIDO”.

Note

- AWS Health as notificações fornecem atualizações de status ao longo do tempo, sempre que possível, exceto nas regiões da China AWS GovCloud (US) e da China.
- As atualizações do estado dos recursos são realizadas de forma assíncrona e periódica e podem ter um atraso de até 72 horas em raras ocasiões.

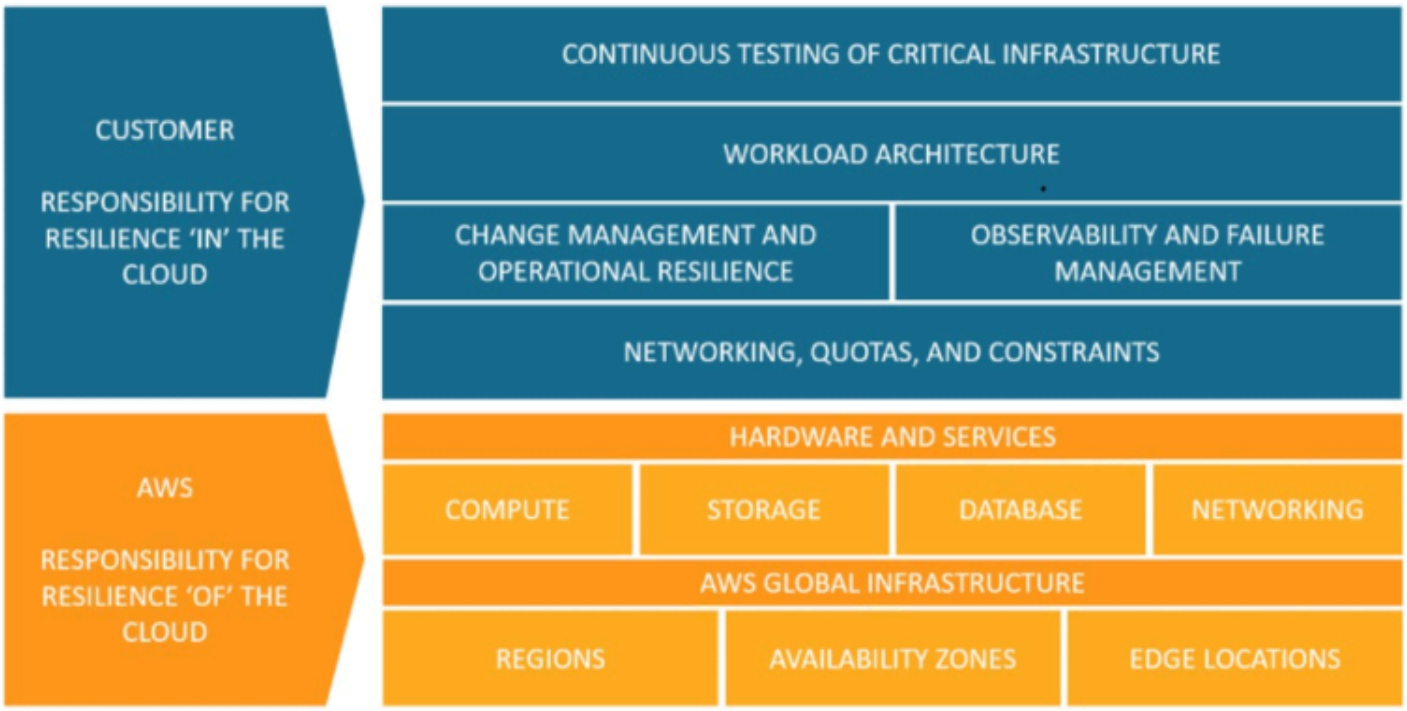


Depois que a data planejada do evento terminar:

1. Se aplicável, o serviço pode implementar a alteração descrita em seu recurso a qualquer momento após a data de início do evento.
2. Se você resolver todos os recursos antes da data de término do suporte, seu AWS Health evento mudará para o status “Encerrado”.
3. Se você tiver recursos pendentes após a data que não foram resolvidos, o AWS Health evento permanecerá aberto por 90 dias após a data de início ou término. Em seguida, o evento será excluído.

Modelo de responsabilidade compartilhada para resiliência

Segurança e conformidade são responsabilidades compartilhadas entre o cliente AWS e o cliente. Dependendo dos serviços implantados, esse modelo compartilhado pode ajudar a aliviar a carga operacional do cliente. Isso ocorre porque AWS opera, gerencia e controla os componentes do sistema operacional host e da camada de virtualização até a segurança física das instalações nas quais o serviço opera. O cliente assume a responsabilidade e o gerenciamento do sistema operacional convidado (incluindo atualizações e patches de segurança) e de outros softwares de aplicativos associados, além da configuração do firewall do grupo AWS de segurança fornecido. Para obter mais informações, consulte o Modelo de responsabilidade compartilhada.



Acessando eventos planejados do ciclo de vida

Os eventos planejados do ciclo de vida podem ser acessados e monitorados usando vários canais:

- Use a Amazon EventBridge
- Use o AWS Health painel
  - Visualização do calendário
  - Visualizar os recursos afetados
- Use a AWS Health API

Configurando notificações de AWS usuário para AWS Health

AWS Health fornece informações sobre operações de serviço, como problemas operacionais, manutenção planejada e eventos planejados do ciclo de vida do software. Para uma visibilidade abrangente dos detalhes do AWS Health evento, como o recurso afetadoIDs, o status atual (aberto ou fechado) e o status do recurso, é uma prática recomendada usar AWS Health endpoints, como a AWS Health API fonte aws.health na Amazon e o EventBridge Dashboard. AWS Health Esses endpoints fornecem as informações mais detalhadas e em tempo real sobre eventos e mudanças em andamento que podem afetar suas cargas de trabalho.

AWS O User Notifications notifica você por meio de canais adicionais de UX (e-mail, chat ou notificações push para o AWS Console Mobile Application). AWS Health as notificações de eventos não contêm tantos dados detalhados quanto os endpoints listados acima; no entanto, elas fornecem uma maneira simples e eficaz de notificar as partes interessadas sobre problemas e mudanças. Com base nas regras criadas, o User Notifications cria e envia uma notificação quando um evento corresponde aos valores especificados em uma regra. Você pode selecionar para quais canais de entrega de UX uma notificação é enviada e configurar a agregação para reduzir o número de notificações geradas para eventos específicos. As notificações também estão visíveis na Central de notificações do console. Por exemplo, você pode receber notificações por chat se tiver recursos em sua AWS conta programados para atualizações, como instâncias do Amazon Elastic Compute Cloud (AmazonEC2).

Para saber mais sobre como configurar as notificações AWS do usuário, consulte Introdução às notificações AWS do usuário.

Integração AWS Health com outros sistemas usando o AWS Health API

AWS Health é um serviço RESTful web usado HTTPS como transporte e JSON formato de serialização de mensagens. O código do seu aplicativo pode fazer solicitações diretamente para AWS Health API o. Ao usar o REST API diretamente, você deve escrever o código necessário para assinar e autenticar suas solicitações. Para obter mais informações sobre as AWS Health operações e os parâmetros, consulte a AWS Health APIReferência.

> **Note**
>
> Você deve ter um plano Business, Enterprise On-Ramp ou Enterprise Support da AWS Supportpara usar o. AWS Health API Se você ligar AWS Health API de uma AWS conta que não tem um plano Business, Enterprise On-Ramp ou Enterprise Support, você receberá uma `SubscriptionRequiredException` mensagem de erro.

Você pode usar o AWS SDKs para agrupar as AWS Health REST API chamadas, o que pode simplificar o desenvolvimento do seu aplicativo. Você especifica suas AWS credenciais, e essas bibliotecas cuidam da autenticação e solicitam a assinatura para você.

AWS Health também fornece um AWS Health painel no AWS Management Console que você pode usar para visualizar e pesquisar eventos e entidades afetadas. Consulte Começando com seu AWS Health painel.

Escolha de endpoints para solicitações AWS Health API

A AWS Health API seguir, uma arquitetura de aplicativo multirregional Arquitetura de e tem dois endpoints regionais em uma configuração ativa-passiva. Para suportar o DNS failover ativo-passivo, AWS Health fornece um endpoint único e global. Você pode realizar uma DNS pesquisa no endpoint global para determinar o endpoint ativo e a região de assinatura AWS correspondente. Isso ajuda você a saber qual endpoint usar em seu código, para que você possa obter as informações mais recentes. AWS Health

Ao fazer uma solicitação ao endpoint global, você deve especificar suas credenciais de AWS acesso ao endpoint regional de destino e configurar a assinatura para sua região. Caso contrário, sua

autenticação poderá falhar. Para obter mais informações, consulte AWS Health APISolicitações de assinatura.

A tabela a seguir representa a configuração padrão.

Descrição	Região de assinatura	Endpoint	Protocolo
Ativo	us-east-1	health.us-east-1.amazonaws.com	HTTPS
Passivo	us-east-2	health.us-east-2.amazonaws.com	HTTPS
Global	us-east-1 **Note** Essa é a região de assinatura do endpoint ativo atual.	global.health.amazonaws.com	HTTPS

Para determinar se um endpoint é o endpoint ativo, faça uma DNS pesquisa no endpoint global eCNAME, em seguida, extraia a AWS região do nome resolvido.

Example : DNS pesquisa no endpoint global

Em seguida, o comando retorna o endpoint Região us-east-1. Essa saída informa para qual endpoint você deve usar. AWS Health

```
dig global.health.amazonaws.com | grep CNAME
global.health.amazonaws.com. 10 IN CNAME health.us-east-1.amazonaws.com
```

Tip

Tanto os endpoints ativos quanto os passivos retornam AWS Health dados. No entanto, os dados AWS Health mais recentes só estão disponíveis no endpoint ativo. Os dados do

endpoint passivo acabarão sendo consistentes com o endpoint ativo. Recomendamos que você reinicie todos os fluxos de trabalho quando o endpoint ativo for alterado.

Experimente AWS Health demonstrações de endpoints

Nos exemplos de código a seguir, AWS Health usa uma DNS pesquisa no endpoint global para determinar o endpoint regional ativo e a região de assinatura. Em seguida, o código reinicia o fluxo de trabalho se o endpoint ativo for alterado.

Tópicos

- Experimente a demonstração do Java
- Experimente a demonstração do Python

Experimente a demonstração do Java

Pré-requisito

Você deve instalar o Gradle.

Para usar o exemplo Java

1. Baixe a demonstração do endpoint de AWS Health alta disponibilidade em. GitHub
2. Navegue até o diretório de projeto do `high-availability-endpoint/java`.
3. Em uma janela de linha de comando, digite o seguinte comando:

```
gradle build
```

4. Insira os comandos a seguir para especificar suas AWS credenciais.

```
export AWS_ACCESS_KEY_ID="AKIAIOSFODNN7EXAMPLE"
export AWS_SECRET_ACCESS_KEY="wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY"
export AWS_SESSION_TOKEN="your-aws-token"
```

5. Insira o comando a seguir para executar a ferramenta .

```
gradle run
```

Example : saída AWS Health do evento

O exemplo de código retorna o AWS Health evento recente dos últimos sete dias em sua AWS conta. No exemplo a seguir, a saída inclui um AWS Health evento para o AWS Config serviço.

```
> Task :run
[main] INFO aws.health.high.availability.endpoint.demo.HighAvailabilityV2Workflow
 - EventDetails(Event=Event(Arn=arn:aws:health:global::event/CONFIG/
AWS_CONFIG_OPERATIONAL_NOTIFICATION/AWS_CONFIG_OPERATIONAL_NOTIFICATION_88a43e8a-
e419-4ca7-9baa-56bcde4dba3,
Service=CONFIG, EventTypeCode=AWS_CONFIG_OPERATIONAL_NOTIFICATION,
 EventTypeCategory=accountNotification, Region=global,
 StartTime=2020-09-11T02:55:49.899Z, LastUpdatedTime=2020-09-11T03:46:31.764Z,
StatusCode=open, EventScopeCode=ACCOUNT_SPECIFIC),
 EventDescription=EventDescription(LatestDescription=As part of our ongoing efforts
 to optimize costs associated with recording changes related to certain ephemeral
 workloads,
AWS Config is scheduled to release an update to relationships modeled within
 ConfigurationItems (CI) for 7 EC2 resource types on August 1, 2021.
Examples of ephemeral workloads include changes to Amazon Elastic Compute Cloud
 (Amazon EC2) Spot Instances, Amazon Elastic MapReduce jobs, and Amazon EC2
 Autoscaling.
This update will optimize CI models for EC2 Instance, SecurityGroup, Network
 Interface, Subnet, VPC, VPN Gateway, and Customer Gateway resource types to record
 direct relationships and deprecate indirect relationships.

A direct relationship is defined as a one-way relationship (A->B) between a
 resource (A) and another resource (B), and is typically derived from the Describe
 API response of resource (A).
An indirect relationship, on the other hand, is a relationship that AWS Config
 infers (B->A), in order to create a bidirectional relationship.
For example, EC2 instance -> Security Group is a direct relationship, since
 security groups are returned as part of the describe API response for an EC2
 instance.
But Security Group -> EC2 instance is an indirect relationship, since EC2 instances
 are not returned when describing an EC2 Security group.

Until now, AWS Config has recorded both direct and indirect relationships. With
 the launch of Advanced queries in March 2019, indirect relationships can easily be
 answered by running Structured Query Language (SQL) queries such as:

SELECT
```

```
 resourceId,
 resourceType
WHERE
 resourceType ='AWS::EC2::Instance'
AND
 relationships.resourceId = 'sg-234213'

By deprecating indirect relationships, we can optimize the information contained
 within a
Configuration Item while reducing AWS Config costs related to relationship
 changes.
This is especially useful in case of ephemeral workloads where there is a high
 volume of configuration changes for EC2 resource types.

Which resource relationships are being removed?

Resource Type: Related Resource Type
1 AWS::EC2::CustomerGateway: AWS::VPN::Connection
2 AWS::EC2::Instance: AWS::EC2::EIP, AWS::EC2::RouteTable
3 AWS::EC2::NetworkInterface: AWS::EC2::EIP, AWS::EC2::RouteTable
4 AWS::EC2::SecurityGroup: AWS::EC2::Instance, AWS::EC2::NetworkInterface
5 AWS::EC2::Subnet: AWS::EC2::Instance, AWS::EC2::NetworkACL,
 AWS::EC2::NetworkInterface, AWS::EC2::RouteTable
6 AWS::EC2::VPC: AWS::EC2::Instance, AWS::EC2::InternetGateway,
 AWS::EC2::NetworkACL, AWS::EC2::NetworkInterface, AWS::EC2::RouteTable,
 AWS::EC2::Subnet, AWS::EC2::VPNGateway, AWS::EC2::SecurityGroup
7 AWS::EC2::VPNGateway: AWS::EC2::RouteTable, AWS::EC2::VPNConnection

Alternate mechanism to retrieve this relationship information:
The SelectResourceConfig API accepts a SQL SELECT command, performs the
 corresponding search, and returns resource configurations matching the properties.
 You can use this API to retrieve the same relationship information.
For example, to retrieve the list of all EC2 Instances related to a particular VPC
 vpc-1234abc, you can use the following query:

SELECT
 resourceId,
 resourceType
WHERE
 resourceType ='AWS::EC2::Instance'
AND
 relationships.resourceId = 'vpc-1234abc'
```

```
If you have any questions regarding this deprecation plan, please contact AWS
 Support [1]. Additional sample queries to retrieve the relationship information
 for the resources listed above is provided in [2].

[1] https://aws.amazon.com/support
[2] https://docs.aws.amazon.com/config/latest/developerguide/
examplerelationshipqueries.html),
EventMetadata={})
```

Recursos de Java

- Para obter mais informações, consulte a Interface HealthClient na AWS SDK for Java APIReferência e o código-fonte.
- Para obter mais informações sobre a biblioteca usada nesta demonstração para DNS pesquisas, consulte dnsjava em. GitHub

Experimente a demonstração do Python

Pré-requisito

Você deve instalar o Python 3.

Para usar o exemplo do Python

1. Baixe a demonstração do endpoint de AWS Health alta disponibilidade em. GitHub
2. Navegue até o diretório de projeto do `high-availability-endpoint/python`.
3. Em uma janela de linha de comando, digite o seguinte comando:

```
pip3 install virtualenv
virtualenv -p python3 v-aws-health-env
```

> **Note**
>
> Para Python 3.3 e mais recente, você pode usar o módulo `venv` integrado para criar um ambiente virtual, em vez de instalar o `virtualenv`. Para obter mais informações, consulte venv: criação de ambientes virtuais no site da Python.

```
python3 -m venv v-aws-health-env
```

4. Insira o seguinte comando para ativar o ambiente virtual:

```
source v-aws-health-env/bin/activate
```

5. Execute o seguinte comando para instalar as dependências.

```
pip install -r requirements.txt
```

6. Insira os comandos a seguir para especificar suas AWS credenciais.

```
export AWS_ACCESS_KEY_ID="AKIAIOSFODNN7EXAMPLE"
export AWS_SECRET_ACCESS_KEY="wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY"
export AWS_SESSION_TOKEN="your-aws-token"
```

7. Insira o comando a seguir para executar a ferramenta .

```
python3 main.py
```

Example : saída AWS Health do evento

O exemplo de código retorna o AWS Health evento recente dos últimos sete dias em sua AWS conta. A saída a seguir retorna um AWS Health evento para uma notificação AWS de segurança.

```
INFO:botocore.credentials:Found credentials in environment variables.
INFO:root:Details: {'arn': 'arn:aws:health:global::event/SECURITY/
AWS_SECURITY_NOTIFICATION/AWS_SECURITY_NOTIFICATION_0e35e47e-2247-47c4-
a9a5-876544042721',
'service': 'SECURITY', 'eventTypeCode': 'AWS_SECURITY_NOTIFICATION',
 'eventTypeCategory': 'accountNotification', 'region': 'global', 'startTime':
 datetime.datetime(2020, 8, 19, 23, 30, 42, 476000,
tzinfo=tzlocal()), 'lastUpdatedTime': datetime.datetime(2020, 8, 20, 20, 44, 9,
 547000, tzinfo=tzlocal()), 'statusCode': 'open', 'eventScopeCode': 'PUBLIC'},
 description:
{'latestDescription': 'This is the second notice regarding TLS requirements on FIPS
 endpoints.\n\nWe
are in the process of updating all AWS Federal Information Processing Standard
 (FIPS) endpoints across all AWS regions
```

```
to Transport Layer Security (TLS) version 1.2 by March 31, 2021 . In order to avoid
 an interruption in service, we encourage you to act now, by ensuring that you
 connect to AWS FIPS endpoints at a TLS version of 1.2.
If your client applications fail to support TLS 1.2 it will result in connection
 failures when TLS versions below 1.2 are no longer supported.\n\nBetween now and
 March 31, 2021 AWS will remove TLS 1.0 and TLS 1.1 support from each FIPS endpoint
 where no connections below TLS 1.2 are detected over a 30-day period.
After March 31, 2021 we may deploy this change to all AWS FIPS endpoints, even if
 there continue
to be customer connections detected at TLS versions below 1.2. \n\nWe will provide
 additional updates and reminders on the AWS Security Blog, with a 'TLS' tag [1].
 If you need further guidance or assistance, please contact AWS Support [2] or your
 Technical Account Manager (TAM).
Additional information is below.\n\nHow can I identify clients that are connecting
 with TLS
1.0/1.1?\nFor customers using S3 [3], Cloudfront [4] or Application Load Balancer
 [5] you can use
your access logs to view the TLS connection information for these services, and
 identify client
connections that are not at TLS 1.2. If you are using the AWS Developer Tools on
 your clients,
you can find information on how to properly configure your client's TLS versions
 by visiting Tools to Build on AWS [7] or our associated AWS Security Blog has a
 link for each unique code language [7].\n\nWhat is Transport Layer Security (TLS)?
\nTransport Layer Security (TLS Protocols) are cryptographic protocols designed to
 provide secure communication across a computer network
[6].\n\nWhat are AWS FIPS endpoints? \nAll AWS services offer Transport Layer
 Security (TLS) 1.2 encrypted endpoints that can be used for all API calls. Some
 AWS services also offer FIPS 140-2 endpoints [9] for customers that require use
 of FIPS validated cryptographic libraries. \n\n[1] https://aws.amazon.com/blogs/
security/tag/tls/\n[2] https://aws.amazon.com/support\n[3]
https://docs.aws.amazon.com/AmazonS3/latest/dev/LogFormat.html\n[4] https://
docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/AccessLogs.html\n[5]
 https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-
access-logs.html\n[6] https://aws.amazon.com/tools\n[7] https://aws.amazon.com/
blogs/security/tls-1-2-to-become-the-minimum-for-all-aws-fips-endpoints\n[8]
https://en.wikipedia.org/wiki/Transport_Layer_Security\n[9] https://aws.amazon.com/
compliance/fips'}
```

8. Ao terminar, insira o comando a seguir para desativar a máquina virtual.

```
deactivate
```

Recursos Python

- Para obter mais informações sobre o`Health. Client`, consulte a Referência AWS SDKpara Python (Boto3). API
- Para obter mais informações sobre a biblioteca usada nesta demonstração para DNS pesquisas, consulte o kit de ferramentas dnspython e o código-fonte em. GitHub

AWS Health APISolicitações de assinatura

Quando você usa o AWS SDKs ou o AWS Command Line Interface (AWS CLI) para fazer solicitações AWS, essas ferramentas assinam automaticamente as solicitações para você com a chave de acesso que você especifica ao configurar as ferramentas. Por exemplo, se você usar o AWS SDK for Java para a demonstração anterior de endpoint de alta disponibilidade, não precisará assinar as solicitações sozinho.

Exemplos de código Java

Para obter mais exemplos de como usar o AWS Health API com o AWS SDK for Java, consulte este código de exemplo.

Ao fazer solicitações, é altamente recomendável que você não use as credenciais AWS da sua conta raiz para AWS Health acesso regular a. Você pode usar as credenciais de um IAM usuário. Para obter mais informações, consulte Bloquear as chaves de acesso do usuário raiz da sua AWS conta no Guia IAM do usuário.

Se você não usa o AWS SDKs ou o AWS CLI, então você mesmo deve assinar suas solicitações. Recomendamos que você use o AWS Signature Version 4. Para obter mais informações, consulte Assinar AWS API solicitações no Referência geral da AWS.

Aprenda a usar o AWS Health API com exemplos de Java

Os exemplos de código Java a seguir demonstram como inicializar um AWS Health cliente e recuperar informações sobre eventos e entidades.

Etapa 1: Inicialize as credenciais

São necessárias credenciais válidas para se comunicar com o. AWS Health API Você pode usar o par de chaves de qualquer IAM usuário associado à AWS conta.

Crie e inicialize uma AWSCredentialsinstância:

```
AWSCredentials credentials = null;
try {
       credentials = new ProfileCredentialsProvider("default").getCredentials();
} catch (Exception e) {
throw new AmazonClientException(
   "Cannot load the credentials from the credential profiles file. "
   + "Please make sure that your credentials file is at the correct "
   + "location (/home/username/.aws/credentials), and is in valid format.", e);
}
```

Etapa 2: inicializar um cliente AWS Health API

Use o objeto de credenciais de inicialização da etapa anterior para criar um cliente do AWS Health :

```
import com.amazonaws.services.health.AWSHealthClient;

AWSHealth awsHealthClient = new AWSHealthClient(credentials);
```

Etapa 3: use AWS Health API as operações para obter informações sobre o evento

DescribeEvents

```
import com.amazonaws.services.health.model.DescribeEventsRequest;
import com.amazonaws.services.health.model.DescribeEventsResult;
import com.amazonaws.services.health.model.Event;
import com.amazonaws.services.health.model.EventFilter;

DescribeEventsRequest request = new DescribeEventsRequest();

EventFilter filter = new EventFilter();
// Filter on any field from the supported AWS Health EventFilter model.
// Here is an example for Region us-east-1 events from the EC2 service.
filter.setServices(singletonList("EC2"));
filter.setRegions(singletonList("us-east-1"));
request.setFilter(filter);

DescribeEventsResult response = awsHealthClient.describeEvents(request);
List<Event> resultEvents = response.getEvents();
```

```
Event currentEvent = null;
for (Event event : resultEvents) {
    // Display result event data; here is a subset.
    System.out.println(event.getArn());
    System.out.println(event.getService());
    System.out.println(event.getRegion());
    System.out.println(event.getAvailabilityZone());
    System.out.println(event.getStartTime());
    System.out.println(event.getEndTime());
 }
```

DescribeEventAggregates

```
import com.amazonaws.services.health.model.DescribeEventAggregatesRequest;
import com.amazonaws.services.health.model.DescribeEventAggregatesResult;
import com.amazonaws.services.health.model.EventAggregate;
import com.amazonaws.services.health.model.EventFilter;

DescribeEventAggregatesRequest request = new DescribeEventAggregatesRequest();
// set the aggregation field
request.setAggregateField("eventTypeCategory");

// filter more on result if needed
EventFilter filter = new EventFilter();
filter.setRegions(singleton("us-east-1"));
request.setFilter(filter);

DescribeEventAggregatesResult response =
 awsHealthClient.describeEventAggregates(request);

// print event count for each eventTypeCategory
for (EventAggregate aggregate: response.getEventAggregates()) {
    System.out.println("Event Category:" + aggregate.getAggregateValue());
    System.out.println("Event Count:" + aggregate.getCount());
 }
```

DescribeEventDetails

```
import com.amazonaws.services.health.model.DescribeEventDetailsRequest;
import com.amazonaws.services.health.model.DescribeEventDetailsResult;
import com.amazonaws.services.health.model.Event;
import com.amazonaws.services.health.model.EventDetails;
```

```
DescribeEventDetailsRequest describeEventDetailsRequest = new
 DescribeEventDetailsRequest();
// set event ARN and local value

describeEventDetailsRequest.setEventArns(singletonList("arn:aws:health:us-
east-1::event/service/eventTypeCode/eventId"));
describeEventDetailsRequest.setLocale("en-US");
filter.setEventArns
DescribeEventDetailsResult describeEventDetailsResult =
 awsHealthClient.describeEventDetails(request);
EventDetails eventDetail = describeEventDetailsResult.getSuccessfulSet().get(0);

// check event-related fields
Event event = eventDetail.getEvent();
System.out.println(event.getService());
System.out.println(event.getRegion());
System.out.println(event.getAvailabilityZone());
System.out.println(event.getStartTime());
System.out.println(event.getEndTime());

// print out event description
System.out.println(eventDetail.getEventDescription().getLatestDescription());
```

DescribeAffectedEntities

```
import com.amazonaws.services.health.model.AffectedEntity;
import com.amazonaws.services.health.model.DateTimeRange;
import com.amazonaws.services.health.model.DescribeAffectedEntitiesRequest;
import
 com.amdescribeEventDetailsRequestazonaws.services.health.model.DescribeAffectedEntitiesResult;

DescribeAffectedEntitiesRequest request = new DescribeAffectedEntitiesRequest();
EntityFilter filter = new EntityFilter();

filter.setEventArns(singletonList("arn:aws:health:us-
east-1::event/service/eventTypeCode/eventId"));

DescribeAffectedEntitiesResult response =
 awsHealthClient.describeAffectedEntities(request);

for (AffectedEntity affectedEntity: response.getEntities()) {
```

```
    System.out.println(affectedEntity.getEntityValue());
    System.out.println(affectedEntity.getAwsAccountId());
    System.out.println(affectedEntity.getEntityArn());
 }
```

DescribeEntityAggregates

```
import com.amazonaws.services.health.model.DescribeEntityAggregatesRequest;
import com.amazonaws.services.health.model.DescribeEntityAggregatesResult;
import com.amazonaws.services.health.model.EntityAggregate;

DescribeEntityAggregatesRequest request = new DescribeEntityAggregatesRequest();

request.setEventArns(singletonList("arn:aws:health:us-
east-1::event/service/eventTypeCode/eventId"));

DescribeEntityAggregatesResult response =
 awsHealthClient.describeEntityAggregates(request);

for (EntityAggregate entityAggregate : response.getEntityAggregates()) {
    System.out.println(entityAggregate.getEventArn());
    System.out.println(entityAggregate.getCount());
 }
```

Segurança em AWS Health

A segurança na nuvem AWS é a maior prioridade. Como AWS cliente, você se beneficia de data centers e arquiteturas de rede criados para atender aos requisitos das organizações mais sensíveis à segurança.

A segurança é uma responsabilidade compartilhada entre você AWS e você. O modelo de responsabilidade compartilhada descreve isso como segurança da nuvem e segurança na nuvem:

- Segurança da nuvem — AWS é responsável por proteger a infraestrutura que executa AWS os serviços na AWS nuvem. AWS também fornece serviços que você pode usar com segurança. Auditores terceirizados testam e verificam regularmente a eficácia de nossa segurança como parte dos Programas de Conformidade Programas de AWS de . Para saber mais sobre os programas de conformidade que se aplicam AWS Health, consulte AWS Serviços no escopo do programa de conformidade AWS .
- Segurança na nuvem — Sua responsabilidade é determinada pelo AWS serviço que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade dos dados, os requisitos da empresa e as leis e regulamentos aplicáveis.

Esta documentação ajuda você a entender como aplicar o modelo de responsabilidade compartilhada ao usar AWS Health. Os tópicos a seguir mostram como configurar para atender AWS Health aos seus objetivos de segurança e conformidade. Você também aprenderá a usar outros AWS serviços que ajudam a monitorar e proteger seus AWS Health recursos.

Tópicos

Proteção de dados em AWS Health

O modelo de responsabilidade AWS compartilhada modelo se aplica à proteção de dados em AWS Health. Conforme descrito neste modelo, AWS é responsável por proteger a infraestrutura global que executa todos os Nuvem AWS. Você é responsável por manter o controle sobre seu conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para obter mais informações sobre privacidade de dados, consulte Privacidade de dados FAQ. Para obter informações sobre proteção de dados na Europa, consulte o Modelo de Responsabilidade AWS Compartilhada e GDPR a postagem no blog AWS de segurança.

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 a autenticação multifator (MFA) com cada conta.
- UseSSL/TLSpara se comunicar com AWS os recursos. Exigimos TLS 1,2 e recomendamos TLS 1,3.
- Configure API e registre as 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 FIPS 140-3 módulos criptográficos validados ao acessar AWS por meio de uma interface de linha de comando ou umaAPI, use um endpoint. FIPS Para obter mais informações sobre os FIPS endpoints disponíveis, consulte Federal Information Processing Standard (FIPS) 140-3.

É altamente recomendável que nunca sejam colocadas informações de identificação confidenciais, como endereços de e-mail dos seus clientes, em marcações ou campos de formato livre, como um campo Nome. Isso inclui quando você trabalha com AWS Health ou Serviços da AWS usa o console,API, AWS CLI, ou AWS SDKs. Quaisquer dados inseridos em tags ou campos de texto de

formato livre usados para nomes podem ser usados para logs de faturamento ou de diagnóstico. Se você fornecer um URL para um servidor externo, é altamente recomendável que você não inclua informações de credenciais no URL para validar sua solicitação para esse servidor.

Criptografia de dados

Veja as informações a seguir sobre como AWS Health criptografa dados.

A criptografia de dados se refere à proteção de dados em trânsito (à medida que viajam do serviço para sua AWS conta) e em repouso (enquanto são armazenados nos AWS serviços). Você pode proteger dados em trânsito usando Transport Layer Security (TLS) ou em repouso usando criptografia do lado do cliente.

AWS Health não registra informações de identificação pessoal (PII), como endereços de e-mail ou nomes de clientes em eventos.

Criptografia em repouso

Todos os dados armazenados pelo AWS Health são criptografados em repouso.

Criptografia em trânsito

Todos os dados enviados de e para lá AWS Health são criptografados em trânsito.

Gerenciamento de chaves

AWS Health não oferece suporte a chaves de criptografia gerenciadas pelo cliente para dados criptografados na AWS nuvem.

Gerenciamento de identidade e acesso para o AWS Health

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. IAMos administradores controlam quem pode ser autenticado (conectado) e autorizado (tem permissões) a usar AWS Health os recursos. IAMé um AWS service (Serviço da AWS) que você pode usar sem custo adicional.

Tópicos

- Autenticando com identidades
- Gerenciando acesso usando políticas
- Como AWS Health funciona com IAM
- AWS Health exemplos de políticas baseadas em identidade
- Solução de problemas AWS Health de identidade e acesso
- Usar funções vinculadas ao serviço do AWS Health
- AWS políticas gerenciadas para AWS Health

Público

A forma como você usa AWS Identity and Access Management (IAM) difere, dependendo do trabalho que você faz AWS Health.

Usuário do serviço — Se você usar o AWS Health serviço para fazer seu trabalho, seu administrador fornecerá as credenciais e as permissões de que você precisa. À medida que você usa mais AWS Health 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 atributo no AWS Health, consulte Solução de problemas AWS Health de identidade e acesso.

Administrador de serviços — Se você é responsável pelos AWS Health recursos da sua empresa, provavelmente tem acesso total AWS Health a. É seu trabalho determinar quais AWS Health recursos e recursos seus usuários do serviço devem acessar. Em seguida, você deve enviar solicitações ao IAM administrador para alterar as permissões dos usuários do serviço. Revise as informações nesta página para entender os conceitos básicos doIAM. Para saber mais sobre como sua empresa pode usar IAM com AWS Health, consulteComo AWS Health funciona com IAM.

IAMadministrador — Se você for IAM administrador, talvez queira saber detalhes sobre como criar políticas para gerenciar o acesso AWS Health. Para ver exemplos de políticas AWS Health baseadas em identidade que você pode usar emIAM, consulte. AWS Health exemplos de políticas baseadas em identidade

Autenticando com identidades

A autenticação é a forma como você faz login AWS usando suas credenciais de identidade. Você deve estar autenticado (conectado AWS) como IAM usuário ou assumindo uma IAM função. Usuário raiz da conta da AWS

Você pode entrar AWS como uma identidade federada usando credenciais fornecidas por meio de uma fonte de identidade. AWS IAM Identity Center Os usuários (do 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 entra como uma identidade federada, seu administrador configurou previamente a federação de identidades usando IAM funções. 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 você mesmo assinar solicitações, consulte Assinar AWS API solicitações no Guia IAM do usuário.

Independente do método de autenticação usado, também pode ser exigido que você forneça informações adicionais de segurança. Por exemplo, AWS recomenda que você use a autenticação multifator (MFA) para aumentar a segurança da sua conta. Para saber mais, consulte Autenticação multifator no Guia AWS IAM Identity Center do usuário e Uso da autenticação multifator (MFA) AWS no Guia do IAMusuário.

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 ver a lista completa de tarefas que exigem que você faça login como usuário raiz, consulte Tarefas que exigem credenciais de usuário raiz no Guia do IAM usuário.

Grupos e usuários do IAM

Um IAMusuário é uma identidade dentro da sua Conta da AWS que tem permissões específicas para uma única pessoa ou aplicativo. Sempre que possível, recomendamos confiar em credenciais temporárias em vez de criar IAM usuários que tenham 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 IAM os usuários, recomendamos que você alterne as chaves de acesso. Para obter mais informações, consulte Alterne as chaves de acesso regularmente para casos de uso que exigem credenciais de longo prazo no Guia do IAMusuário.

Um IAMgrupo é uma identidade que especifica uma coleção de IAM usuários. 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 IAM recursos.

Usuários são diferentes de perfis. Um usuário é exclusivamente associado a uma pessoa ou a uma aplicação, mas um perfil pode ser assumido por qualquer pessoa que precisar dele. Os usuários têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte Quando criar um IAM usuário (em vez de uma função) no Guia do IAM usuário.

IAMfunções

Uma IAMfunção é uma identidade dentro da sua Conta da AWS que tem permissões específicas. É semelhante a um IAM usuário, mas não está associado a uma pessoa específica. Você pode assumir temporariamente uma IAM função no AWS Management Console trocando de funções. Você pode assumir uma função chamando uma AWS API operação AWS CLI or ou usando uma personalizadaURL. Para obter mais informações sobre métodos de uso de funções, consulte Métodos para assumir uma função no Guia IAM do usuário.

IAMfunções com credenciais temporárias são úteis nas seguintes situações:

- Acesso de usuário federado: para atribuir permissões a identidades federadas, você pode criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas pelo mesmo. Para obter informações sobre funções para federação, consulte Criação de uma função para um provedor de identidade terceirizado no Guia IAM do usuário. Se você usa o IAM Identity Center, configura um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o IAM Identity Center correlaciona o conjunto de permissões a uma função em. IAM Para obter informações sobre conjuntos de permissões, consulte Conjuntos de Permissões no Manual do Usuário do AWS IAM Identity Center .
- Permissões temporárias IAM de IAM usuário — Um usuário ou função pode assumir uma IAM função para assumir temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas — Você pode usar uma IAM função para permitir que alguém (um diretor confiável) em uma conta diferente acesse recursos em sua conta. Os perfis são a principal forma

de conceder acesso entre contas. No entanto, com alguns Serviços da AWS, você pode anexar uma política diretamente a um recurso (em vez de usar uma função como proxy). Para saber a diferença entre funções e políticas baseadas em recursos para acesso entre contas, consulte Acesso a recursos entre contas IAM no Guia do IAM usuário.

- 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 do principal de chamada, usando um perfil de serviço ou um perfil vinculado a serviço.
  - Sessões de acesso direto (FAS) — Quando você usa um IAM usuário ou uma função para realizar ações em AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. FASusa 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. FASas solicitações 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 FAS solicitações, consulte Encaminhar sessões de acesso.
  - Função de serviço — Uma função de serviço é uma IAMfunção que um serviço assume para realizar ações em seu nome. Um IAM administrador pode criar, modificar e excluir uma função de serviço internamenteIAM. Para obter mais informações, consulte Criação de uma função para delegar permissões a uma AWS service (Serviço da AWS) no Guia do IAM usuário.
  - 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 a função de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um IAM administrador pode visualizar, mas não editar, as permissões das funções vinculadas ao serviço.
- Aplicativos em execução na Amazon EC2 — Você pode usar uma IAM função para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma EC2 instância e fazendo AWS CLI AWS API solicitações. 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 os programas em execução na EC2 instância recebam credenciais temporárias. Para obter mais informações, consulte Como usar uma IAM função para conceder permissões a aplicativos executados em EC2 instâncias da Amazon no Guia IAM do usuário.

Para saber se usar IAM funções ou IAM usuários, consulte Quando criar uma IAM função (em vez de um usuário) no Guia do IAM usuário.

Gerenciando 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 JSON documentos. Para obter mais informações sobre a estrutura e o conteúdo dos documentos de JSON política, consulte Visão geral das JSON políticas no Guia IAM do usuário.

Os administradores podem usar AWS JSON políticas para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

Por padrão, usuários e funções não têm permissões. Para conceder permissão aos usuários para realizar ações nos recursos de que precisam, um IAM administrador pode criar IAM políticas. O administrador pode então adicionar as IAM políticas às funções e os usuários podem assumir as funções.

IAMas políticas definem permissões para uma ação, independentemente do método usado para realizar 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 do AWS Management Console AWS CLI, do ou do AWS API.

Políticas baseadas em identidade

Políticas baseadas em identidade são documentos de políticas de JSON permissões que você pode anexar a uma identidade, como um IAM usuário, grupo de usuários ou função. 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 Criação de IAM políticas no Guia do IAMusuário.

As políticas baseadas em identidade podem ser categorizadas ainda adicionalmente 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 Escolha entre políticas gerenciadas e políticas em linha no Guia do IAMusuário.

Políticas baseadas no recurso

Políticas baseadas em recursos são documentos JSON de política que você anexa a um recurso. Exemplos de políticas baseadas em recursos são políticas de confiança de IAM funções e políticas de bucket do Amazon S3. Em serviços que suportem políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações um principal especificado pode executar nesse recurso e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Políticas baseadas em recursos são políticas em linha localizadas nesse serviço. Você não pode usar políticas AWS gerenciadas de uma política baseada IAM em recursos.

AWS Health suporta condições baseadas em recursos. É possível especificar quais eventos do AWS Health os usuários podem visualizar. Por exemplo, você pode criar uma política que só permita que um IAM usuário acesse EC2 eventos específicos da Amazon no AWS Health Dashboard.

Para obter mais informações, consulte Recursos.

Listas de controle de acesso

As listas de controle de acesso (ACLs) controlam quais diretores (membros da conta, usuários ou funções) têm permissões para acessar um recurso. ACLssão semelhantes às políticas baseadas em recursos, embora não usem o formato de documento JSON de política.

Amazon S3, AWS WAF, e Amazon VPC são exemplos de serviços que oferecem suporte. ACLs Para saber maisACLs, consulte a visão geral da lista de controle de acesso (ACL) no Guia do desenvolvedor do Amazon Simple Storage Service.

AWS Health não suportaACLs.

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 as permissões máximas que uma política baseada em identidade pode conceder a uma IAM entidade (IAMusuário ou função). 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 IAM entidades no Guia IAM do usuário.
- Políticas de controle de serviço (SCPs) — SCPs são JSON políticas que especificam as permissões máximas para uma organização ou unidade organizacional (OU) em AWS Organizations. AWS Organizations é um serviço para agrupar e gerenciar centralmente vários Contas da AWS que sua empresa possui. Se você habilitar todos os recursos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as suas contas. Os SCP limites de permissões para entidades nas contas dos membros, incluindo cada uma Usuário raiz da conta da AWS. Para obter mais informações sobre Organizations eSCPs, consulte Políticas de controle de serviços 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 atributo. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, consulte Políticas de sessão no Guia IAM do usuário.

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 política estão envolvidos, consulte Lógica de avaliação de políticas no Guia IAM do usuário.

Como AWS Health funciona com IAM

Antes de usar IAM para gerenciar o acesso ao AWS Health, você deve entender quais IAM recursos estão disponíveis para uso AWS Health. Para obter uma visão geral de como AWS Health e outros

AWS serviços funcionam comIAM, consulte AWS Serviços que funcionam com IAM no Guia do IAM usuário.

Tópicos

- Políticas baseadas em identidade do AWS Health
- Políticas baseadas em recursos do AWS Health
- Autorização baseada em tags do AWS Health
- AWS Health IAMfunções

Políticas baseadas em identidade do AWS Health

Com políticas IAM baseadas em identidade, você pode especificar ações e recursos permitidos ou negados, bem como as condições sob as quais as ações são permitidas ou negadas. AWS Health oferece suporte a ações, recursos e chaves de condição específicos. Para saber mais sobre todos os elementos que você usa em uma JSON política, consulte Referência IAM JSON de elementos de política no Guia do IAM usuário.

Ações

Os administradores podem usar AWS JSON políticas para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O `Action` elemento de uma JSON política descreve as ações que você pode usar para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome da AWS API operação associada. Há algumas exceções, como ações somente de permissão que não têm uma operação correspondente. API 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 AWS Health usam o seguinte prefixo antes da ação:`health:`. Por exemplo, para conceder permissão a alguém para visualizar informações detalhadas sobre eventos específicos com a DescribeEventDetailsAPIoperação, você inclui a `heath:DescribeEventDetails` ação na política.

As declarações de política devem incluir um `NotAction` elemento `Action` ou. AWS Health define seu próprio conjunto de ações que descrevem as tarefas que você pode executar com esse serviço.

Para especificar várias ações em uma única declaração, separe-as com vírgulas, conforme a seguir.

```
"Action": [
      "health:action1",
      "health:action2"
```

Você também pode especificar várias ações utilizando caracteres curinga (*). Por exemplo, para especificar todas as ações que começam com a palavra `Describe`, inclua a ação a seguir:

```
"Action": "health:Describe*"
```

Para ver uma lista de AWS Health ações, consulte Ações definidas por AWS Health no Guia do IAM usuário.

Recursos

Os administradores podem usar AWS JSON políticas para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento `Resource` JSON de política especifica o objeto ou objetos aos quais a ação se aplica. As instruções devem incluir um elemento `Resource` ou `NotResource`. Como prática recomendada, especifique um recurso usando seu Amazon Resource Name (ARN). Isso pode ser feito para ações que oferecem compatibilidade com um tipo de recurso específico, conhecido como permissões em nível de recurso.

Para ações que não oferecem compatibilidade com permissões em nível de recurso, como operações de listagem, use um curinga (*) para indicar que a instrução se aplica a todos os recursos.

```
"Resource": "*"
```

Um AWS Health evento tem o seguinte formato Amazon Resource Name (ARN).

```
arn:${Partition}:health:*::event/service/event-type-code/event-ID
```

Por exemplo, para especificar o `EC2_INSTANCE_RETIREMENT_SCHEDULED_ABC123-DEF456` evento em sua declaração, use o seguinteARN.

```
"Resource": "arn:aws:health:*::event/EC2/EC2_INSTANCE_RETIREMENT_SCHEDULED/
EC2_INSTANCE_RETIREMENT_SCHEDULED_ABC123-DEF456"
```

Para especificar todos os AWS Health eventos da Amazon EC2 que pertencem a uma conta específica, use o caractere curinga (*).

```
"Resource": "arn:aws:health:*::event/EC2/*/*"
```

Para obter mais informações sobre o formato deARNs, consulte Amazon Resource Names (ARNs) e AWS Service Namespaces.

Algumas AWS Health ações não podem ser executadas em um recurso específico. Nesses casos, você deve utilizar o caractere curinga (*).

```
"Resource": "*"
```

AWS Health APIas operações podem envolver vários recursos. Por exemplo, a DescribeEventsoperação retorna informações sobre eventos que atendem a um critério de filtro especificado. Isso significa que um IAM usuário deve ter permissões para visualizar esse evento.

Para especificar vários recursos em uma única instrução, separe-os ARNs com vírgulas.

```
"Resource": [
      "resource1",
      "resource2"
```

AWS Health suporta somente permissões em nível de recurso para eventos de saúde e somente para as operações e. DescribeAffectedEntitiesDescribeEventDetailsAPI Para obter mais informações, consulte Condições baseadas em recursos e em ações.

Para ver uma lista dos tipos de AWS Health recursos e seusARNs, consulte Recursos definidos por AWS Health no Guia do IAM usuário. Para saber com quais ações você pode especificar cada recurso, consulte Ações definidas por AWS Health. ARN

Chaves de condição

Os administradores podem usar AWS JSON políticas para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento `Condition` (ou bloco `Condition`) permite que você especifique condições nas quais uma instrução estiver em vigor. O elemento `Condition` é opcional. É possível criar expressões

condicionais que usem agentes de condição, como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação.

Se você especificar vários elementos `Condition` em uma instrução ou várias chaves em um único `Condition` elemento, a AWS os avaliará usando uma operação lógica `AND`. Se você especificar vários valores para uma única chave de condição, AWS avalia a condição usando uma `OR` operação lógica. Todas as condições devem ser atendidas antes que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar condições. Por exemplo, você pode conceder permissão a um IAM usuário para acessar um recurso somente se ele estiver marcado com o nome de IAM usuário. Para obter mais informações, consulte elementos de IAM política: variáveis e tags no Guia IAM do usuário.

AWS suporta chaves de condição globais e chaves de condição específicas do serviço. Para ver todas as chaves de condição AWS globais, consulte as chaves de contexto de condição AWS global no Guia IAM do usuário.

AWS Health define seu próprio conjunto de chaves de condição e também oferece suporte ao uso de algumas chaves de condição globais. Para ver todas as chaves de condição AWS globais, consulte Chaves de contexto de condição AWS global no Guia IAM do usuário.

As DescribeEventDetailsAPIoperações DescribeAffectedEntitiese suportam as `health:eventTypeCode` chaves de `health:service` condição e.

Para ver uma lista de chaves de AWS Health condição, consulte Chaves de condição AWS Health no Guia IAM do usuário. Para saber com quais ações e recursos você pode usar uma chave de condição, consulte Ações definidas por AWS Health.

Exemplos

Para ver exemplos de políticas AWS Health baseadas em identidade, consulte. AWS Health exemplos de políticas baseadas em identidade

Políticas baseadas em recursos do AWS Health

Políticas baseadas em recursos são documentos JSON de política que especificam quais ações um determinado diretor pode realizar no AWS Health recurso e sob quais condições. AWS Health oferece suporte a políticas de permissões baseadas em recursos para eventos de saúde. As políticas

baseadas em recursos permitem conceder permissão de uso a outras contas especificada por recurso. Você também pode usar uma política baseada em recursos para permitir que um AWS serviço acesse seus AWS Health eventos.

Para habilitar o acesso entre contas, você pode especificar uma conta ou IAM entidades inteiras em outra conta como principal em uma política baseada em recursos. Adicionar uma entidade principal entre contas à política baseada em recurso é apenas metade da tarefa de estabelecimento da relação de confiança. Quando o principal e o recurso estão em AWS contas diferentes, você também deve conceder permissão à entidade principal para acessar o recurso. Conceda permissão anexando uma política baseada em identidade para a entidade. No entanto, se uma política baseada em recurso conceder acesso a uma entidade principal na mesma conta, nenhuma política baseada em identidade adicional será necessária. Para obter mais informações, consulte Como as IAM funções diferem das políticas baseadas em recursos no Guia do IAMusuário.

AWS Health suporta somente políticas baseadas em recursos para as operações DescribeAffectedEntitiese. DescribeEventDetailsAPI Você pode especificar essas ações em uma política para definir quais entidades principais (contas, usuários, funções e usuários federados) podem realizar ações no AWS Health evento.

Exemplos

Para ver exemplos de políticas AWS Health baseadas em recursos, consulte. Condições baseadas em recursos e em ações

Autorização baseada em tags do AWS Health

AWS Health não oferece suporte à marcação de recursos ou ao controle de acesso com base em tags.

AWS Health IAMfunções

Uma IAMfunção é uma entidade dentro da sua AWS conta que tem permissões específicas.

Usando credenciais temporárias com AWS Health

Você pode usar credenciais temporárias para entrar com a federação, assumir uma IAM função ou assumir uma função entre contas. Você obtém credenciais de segurança temporárias ligando para AWS STS API operações como AssumeRoleou GetFederationToken.

AWS Health suporta o uso de credenciais temporárias.

Funções vinculadas a serviço

As funções vinculadas ao serviço permitem que AWS os serviços acessem recursos em outros serviços para concluir uma ação em seu nome. As funções vinculadas ao serviço aparecem em sua IAM conta e são de propriedade do serviço. Um IAM administrador pode visualizar, mas não editar, as permissões para funções vinculadas ao serviço.

AWS Health oferece suporte a funções vinculadas a serviços para integração. AWS Organizations A função vinculada ao serviço é chamada de `AWSServiceRoleForHealth_Organizations`. Anexada à função está a política OrganizationsServiceRolePolicy AWS gerenciada Health_. A política AWS gerenciada AWS Health permite acessar eventos de saúde de outras AWS contas na organização.

Você pode usar a EnableHealthServiceAccessForOrganizationoperação para criar a função vinculada ao serviço na conta. No entanto, se você quiser desativar esse recurso, primeiro deverá chamar a DisableHealthServiceAccessForOrganizationoperação. Em seguida, você pode excluir a função por meio do IAM console ou AWS Command Line Interface (AWS CLI). IAM API Para obter mais informações, consulte Usando funções vinculadas a serviços no Guia do IAMusuário.

Para obter mais informações, consulte Agregando AWS Health eventos em todas as contas.

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. As funções de serviço aparecem na sua IAM conta e são de propriedade da conta. Isso significa que um IAM administrador pode alterar as permissões para essa função. Porém, fazer isso pode alterar a funcionalidade do serviço.

AWS Health não oferece suporte a funções de serviço.

AWS Health exemplos de políticas baseadas em identidade

Por padrão, IAM usuários e funções não têm permissão para criar ou modificar AWS Health recursos. Eles também não podem realizar tarefas usando o AWS Management Console, AWS CLI, ou AWS API. Um IAM administrador deve criar IAM políticas que concedam aos usuários e funções permissão para realizar API operações específicas nos recursos especificados de que precisam. O administrador deve então anexar essas políticas aos IAM usuários ou grupos que exigem essas permissões.

Para saber como criar uma política IAM baseada em identidade usando esses exemplos de documentos JSON de política, consulte Criação de políticas na JSON guia do IAMusuário.

Tópicos

Melhores práticas de política

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir AWS Health recursos em sua conta. Essas ações podem incorrer em custos para seus Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com as políticas AWS gerenciadas e passe para as permissões de privilégios mínimos — Para começar a conceder permissões aos seus usuários e cargas de trabalho, use as políticas AWS gerenciadas que concedem permissões para muitos casos de uso comuns. Eles estão disponíveis no seu Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo AWS cliente que sejam específicas para seus casos de uso. Para obter mais informações, consulte políticas AWS gerenciadas ou políticas AWS gerenciadas para funções de trabalho no Guia IAM do usuário.
- Aplique permissões com privilégios mínimos — Ao definir permissões com IAM políticas, conceda somente as permissões necessárias para realizar uma tarefa. Você faz isso definindo as ações que podem ser executadas em atributos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para obter mais informações sobre IAM como usar para aplicar permissões, consulte Políticas e permissões IAM no Guia IAM do usuário.
- Use condições nas IAM políticas para restringir ainda mais o acesso — Você pode adicionar uma condição às suas políticas para limitar o acesso a ações e recursos. Por exemplo, você pode escrever uma condição de política para especificar que todas as solicitações devem ser enviadas usandoSSL. Você também pode usar condições para conceder acesso às ações de serviço se elas forem usadas por meio de uma ação específica AWS service (Serviço da AWS), como AWS CloudFormation. Para obter mais informações, consulte Elementos IAM JSON da política: Condição no Guia IAM do usuário.

- Use o IAM Access Analyzer para validar suas IAM políticas e garantir permissões seguras e funcionais — o IAM Access Analyzer valida políticas novas e existentes para que as políticas sigam a linguagem da IAM política (JSON) e as melhores práticas. IAM IAMO Access Analyzer fornece mais de 100 verificações de políticas e recomendações práticas para ajudá-lo a criar políticas seguras e funcionais. Para obter mais informações, consulte Validação da política do IAM Access Analyzer no Guia do IAM Usuário.
- Exigir autenticação multifatorial (MFA) — Se você tiver um cenário que exija IAM usuários ou um usuário root Conta da AWS, ative MFA para obter segurança adicional. Para exigir MFA quando API as operações são chamadas, adicione MFA condições às suas políticas. Para obter mais informações, consulte Configurando o API acesso MFA protegido no Guia do IAMusuário.

Para obter mais informações sobre as melhores práticas emIAM, consulte as melhores práticas de segurança IAM no Guia IAM do usuário.

Usar o console do AWS Health

Para acessar o AWS Health console, você deve ter um conjunto mínimo de permissões. Essas permissões devem permitir que você liste e visualize detalhes sobre os AWS Health recursos em sua AWS conta. Se você criar uma política baseada em identidade que seja mais restritiva do que as permissões mínimas exigidas, o console não funcionará conforme planejado para entidades (IAMusuários ou funções) com essa política.

Para garantir que essas entidades ainda possam usar o AWS Health console, você pode anexar a seguinte política AWS gerenciada, AWSHealthFullAccess.

Essa política `AWSHealthFullAccess` concede a uma entidade acesso total ao seguinte:

- Ativar ou desativar o recurso de visualização AWS Health organizacional para todas as contas em uma AWS organização
- O AWS Health Dashboard no AWS Health console
- AWS Health APIoperações e notificações
- Exibir informações sobre contas que fazem parte da sua AWS organização
- Exibir as unidades organizacionais (OU) da conta de gerenciamento

Example : AWSHealthFullAccess

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:DisableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "organizations:ServicePrincipal": "health.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "health:*",
                "organizations:DescribeAccount",
                "organizations:ListAccounts",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListParents"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:AWSServiceName": "health.amazonaws.com"
                }
            }
        }
    ]
}
```

> **Note**
>
> Você também pode usar a política `Health_OrganizationsServiceRolePolicy` AWS gerenciada, para que AWS Health possa visualizar eventos de outras contas em sua

organização. Para obter mais informações, consulte Usar funções vinculadas ao serviço do AWS Health.

Você não precisa permitir permissões mínimas do console para usuários que estão fazendo chamadas somente para AWS CLI o. ou AWS API o. Em vez disso, permita o acesso somente às ações que correspondam à API operação que você está tentando realizar.

Para obter mais informações, consulte Adicionar permissões a um usuário no Guia do IAM usuário.

Permitir que usuários visualizem suas próprias permissões

Este exemplo mostra como você pode criar uma política que permita IAM aos usuários visualizar as políticas embutidas e gerenciadas que estão anexadas à identidade do usuário. Essa política inclui permissões para concluir essa ação no console ou programaticamente usando o AWS CLI ou. AWS API

```
{
    "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": "*"
        }
    ]
}
```

Acessando o AWS Health Dashboard e o AWS Health API

O AWS Health Dashboard está disponível para todas as AWS contas. O AWS Health API está disponível somente para contas com um plano Business, Enterprise On-Ramp ou Enterprise Support. Para obter mais informações, consulte AWS Support.

Você pode usar IAM para criar entidades (usuários, grupos ou funções) e, em seguida, conceder a essas entidades permissões para acessar o AWS Health Dashboard e AWS Health API o.

Por padrão, IAM os usuários não têm acesso ao AWS Health Dashboard ou ao AWS Health API. Você dá aos usuários acesso às AWS Health informações da sua conta anexando IAM políticas a um único usuário, grupo de usuários ou função. Para obter mais informações, consulte Identidades (usuários, grupos e funções) e Visão geral das IAM políticas.

Depois de criar IAM usuários, você pode atribuir senhas individuais a esses usuários. Em seguida, eles podem entrar na sua conta e visualizar AWS Health as informações usando uma página de login específica da conta. Para obter mais informações, consulte Como usuários fazem login na conta.

> **Note**
>
> Um IAM usuário com permissões de visualização AWS Health Dashboard tem acesso somente para leitura às informações de saúde em todos os AWS serviços da conta, o que pode incluir, mas não está limitado a, AWS recursos IDs como EC2 instância da AmazonIDs, endereços IP de EC2 instâncias e notificações gerais de segurança.
> Por exemplo, se uma IAM política conceder acesso somente ao AWS Health Dashboard e ao AWS Health API, o usuário ou a função à qual a política se aplica poderá acessar todas as informações publicadas sobre AWS serviços e recursos relacionados, mesmo que outras IAM políticas não permitam esse acesso.

Você pode usar dois grupos de APIs for AWS Health.

- Contas individuais — Você pode usar operações como DescribeEventse DescribeEventDetailspara obter informações sobre AWS Health eventos para sua conta.
- Conta organizacional — Você pode usar operações como DescribeEventsForOrganizatione DescribeEventDetailsForOrganizationpara obter informações sobre AWS Health eventos de contas que fazem parte da sua organização.

Para obter mais informações sobre as API operações disponíveis, consulte a AWS Health APIReferência.

Ações individuais

Você pode definir o `Action` elemento de uma IAM política com`health:Describe*`. Isso permite o acesso ao AWS Health Dashboard AWS Health e. AWS Health suporta controle de acesso a eventos com base no serviço `eventTypeCode` e.

Descrever o acesso

Esta declaração de política concede acesso AWS Health Dashboard a qualquer uma das `Describe*` AWS Health API operações. Por exemplo, um IAM usuário com essa política pode acessar o AWS Health Dashboard AWS Management Console e chamar a AWS Health `DescribeEvents` API operação.

Example : Descrever o acesso

```
{
  "Version": "2012-10-17",
  "Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "health:Describe*"
    ],
    "Resource": "*"
  }]
}
```

Negar acesso

Esta declaração de política nega o acesso ao AWS Health Dashboard e o. AWS Health API Um IAM usuário com essa política não pode visualizar AWS Management Console e não pode chamar nenhuma das AWS Health API operações. AWS Health Dashboard

Example : Negar acesso

```
{
  "Version": "2012-10-17",
  "Statement": [
  {
    "Effect": "Deny",
    "Action": [
      "health:*"
    ],
    "Resource": "*"
  }]
}
```

Visualização organizacional

Se quiser ativar a visualização organizacional para AWS Health, você deve permitir o acesso às AWS Organizations ações AWS Health e.

O `Action` elemento de uma IAM política deve incluir as seguintes permissões:

- `iam:CreateServiceLinkedRole`
- `organizations:EnableAWSServiceAccess`
- `organizations:DescribeAccount`
- `organizations:DisableAWSServiceAccess`
- `organizations:ListAccounts`
- `organizations:ListDelegatedAdministrators`
- `organizations:ListParents`

Para entender as permissões exatas necessárias para cada umaAPIs, consulte Ações definidas por AWS Health APIs e notificações no Guia IAM do usuário.

> **Note**
>
> Você deve usar as credenciais da conta de gerenciamento de uma organização para acessar o formulário AWS Health APIs. AWS Organizations Para obter mais informações, consulte Agregando AWS Health eventos em todas as contas.

Acesso total à AWS Health visualização organizacional

Esta declaração de política concede acesso a todas AWS Health as AWS Organizations ações necessárias para o recurso de visualização organizacional.

Example : Permitir acesso à visualização AWS Health organizacional

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:DisableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "organizations:ServicePrincipal": "health.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "health:*",
                "organizations:DescribeAccount",
                "organizations:ListAccounts",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListParents"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/health.amazonaws.com/
AWSServiceRoleForHealth*"
        }
    ]
}
```

Negar acesso à AWS Health visualização organizacional

Esta declaração de política nega o acesso às AWS Organizations ações, mas permite o acesso às AWS Health ações de uma conta individual.

Example : negar acesso à visualização AWS Health organizacional

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "health:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:DisableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "organizations:ServicePrincipal": "health.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Deny",
            "Action": [
                "organizations:DescribeAccount",
                "organizations:ListAccounts",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListParents"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": "iam:CreateServiceLinkedRole",
```

```
            "Resource": "arn:aws:iam::*:role/aws-service-role/health.amazonaws.com/
AWSServiceRoleForHealth*"
        }
    ]
}
```

> **Note**
>
> Se o usuário ou grupo ao qual você deseja conceder permissões já tiver uma IAM política, você poderá adicionar a declaração AWS Health de política específica a essa política.

Condições baseadas em recursos e em ações

AWS Health suporta IAMas condições para as DescribeEventDetailsAPIoperações DescribeAffectedEntitiese. Você pode usar condições baseadas em recursos e ações para restringir os eventos que eles AWS Health API enviam para um usuário, grupo ou função.

Para fazer isso, atualize o `Condition` bloco da IAM política ou defina o `Resource` elemento. Você pode usar String Conditions para restringir o acesso com base em determinados campos de AWS Health eventos.

Você pode usar os seguintes campos ao especificar um AWS Health evento em sua política:

- `eventTypeCode`
- `service`

> **Observações**
>
> - As DescribeEventDetailsAPIoperações DescribeAffectedEntitiese oferecem suporte a permissões em nível de recurso. Por exemplo, você pode criar uma política para permitir ou negar eventos do AWS Health específicos.
> - As DescribeEventDetailsForOrganizationAPIoperações DescribeAffectedEntitiesForOrganizatione não oferecem suporte a permissões em nível de recurso.
> - Para obter mais informações, consulte Ações, recursos e chaves de condição AWS Health APIs e Notificações na Referência de Autorização de Serviço.

Example : Condição baseada em ação

Esta declaração de política concede acesso AWS Health Dashboard e às AWS Health `Describe*` API operações, mas nega acesso a quaisquer AWS Health eventos relacionados à AmazonEC2.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "health:Describe*",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "health:DescribeAffectedEntities",
                "health:DescribeEventDetails"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "health:service": "EC2"
                }
            }
        }
    ]
}
```

Example : Condição baseada em recursos

A política a seguir tem o mesmo efeito, mas faz uso do elemento `Resource`.

```
{
  "Version": "2012-10-17",
  "Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "health:Describe*"
    ],
    "Resource": "*"
  },
```

```
  {
    "Effect": "Deny",
    "Action": [
      "health:DescribeEventDetails",
      "health:DescribeAffectedEntities"
    ],
    "Resource": "arn:aws:health:*::event/EC2/*/*"
  }]
}
```

Example : eventTypeCode condição

Esta declaração de política concede acesso AWS Health Dashboard e às AWS Health `Describe*` API operações, mas nega acesso a quaisquer AWS Health eventos com `eventTypeCode` as correspondentes`AWS_EC2_*`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "health:Describe*",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "health:DescribeAffectedEntities",
                "health:DescribeEventDetails"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "health:eventTypeCode": "AWS_EC2_*"
                }
            }
        }
    ]
}
```

> **Important**
>
> Se você chamar as DescribeEventDetailsoperações DescribeAffectedEntitiese e não tiver permissão para acessar o AWS Health evento, o `AccessDeniedException` erro será exibido. Para obter mais informações, consulte Solução de problemas AWS Health de identidade e acesso.

Solução de problemas AWS Health de identidade e acesso

Use as informações a seguir para diagnosticar e corrigir problemas comuns que você pode encontrar ao trabalhar com AWS Health e. IAM

Tópicos

- Não estou autorizado a realizar uma ação em AWS Health
- Não estou autorizado a realizar iam: PassRole
- Quero visualizar minhas chaves de acesso
- Sou administrador e quero permitir que outras pessoas acessem AWS Health
- Quero permitir que pessoas fora da minha AWS conta acessem meus AWS Health recursos

Não estou autorizado a realizar uma ação em AWS Health

Se isso AWS Management Console indicar que você não está autorizado a realizar uma ação, entre em contato com o administrador para obter ajuda. O administrador é a pessoa que forneceu o seu nome de usuário e senha.

O `AccessDeniedException` erro aparece quando um usuário não tem permissão para usar AWS Health Dashboard as AWS Health API operações.

Nesse caso, o administrador do usuário precisa atualizar a política para permitir o acesso do usuário.

AWS Health APIIsso requer um plano Business, Enterprise On-Ramp ou Enterprise Support da. AWS Support Se você ligar AWS Health API de uma conta que não tem um plano Business, Enterprise On-Ramp ou Enterprise Support, o seguinte código de erro será retornado:. `SubscriptionRequiredException`

Não estou autorizado a realizar iam: PassRole

Se você receber uma mensagem de erro informando que não está autorizado a executar a ação `iam:PassRole`, as suas políticas devem ser atualizadas para permitir que você passe uma função para o AWS Health.

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 fazer isso, é preciso ter permissões para passar o perfil para o serviço.

O exemplo de erro a seguir ocorre quando um IAM usuário chamado `marymajor` tenta usar o console para realizar uma ação no AWS Health. 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 IAM usuário, você pode ver sua ID de 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, deverá adicionar novas chaves de acesso ao seu IAM usuário. 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 ver as instruções, consulte Gerenciamento de chaves de acesso no Guia IAM do usuário.

Sou administrador e quero permitir que outras pessoas acessem AWS Health

Para permitir que outras pessoas acessem AWS Health, você deve conceder permissão às pessoas ou aplicativos que precisam de acesso. Se você estiver usando AWS IAM Identity Center para gerenciar pessoas e aplicativos, você atribui conjuntos de permissões a usuários ou grupos para definir seu nível de acesso. Os conjuntos de permissões criam e atribuem IAM políticas automaticamente às IAM funções associadas à pessoa ou ao aplicativo. Para obter mais informações, consulte Conjuntos de permissões no Guia AWS IAM Identity Center do usuário.

Se você não estiver usando o IAM Identity Center, deverá criar IAM entidades (usuários ou funções) para as pessoas ou aplicativos que precisam de acesso. Você deve anexar uma política à entidade que concede a eles as permissões corretas no AWS Health. Depois que as permissões forem concedidas, forneça as credenciais ao usuário ou desenvolvedor do aplicativo. Eles usarão essas credenciais para acessar AWS. Para saber mais sobre a criação de IAM usuários, grupos, políticas e permissões, consulte IAMIdentidades, políticas e permissões IAM no Guia do IAM usuário.

Quero permitir que pessoas fora da minha AWS conta acessem meus AWS Health recursos

Você pode criar um perfil que os usuários de outras contas ou pessoas fora da sua organização podem usar para acessar seus recursos. Você pode especificar quem é confiável para assumir o perfil. Para serviços que oferecem suporte a políticas baseadas em recursos ou listas de controle de acesso (ACLs), você pode usar essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte:

- Para saber se é AWS Health compatível com esses recursos, consulteComo AWS Health funciona com IAM.
- Para saber como fornecer acesso aos seus recursos em todos os Contas da AWS que você possui, consulte Fornecer acesso a um IAM usuário em outro Conta da AWS de sua propriedade no Guia do IAM usuário.
- Para saber como fornecer acesso aos seus recursos a terceiros Contas da AWS, consulte Fornecer Contas da AWS acesso a terceiros no Guia do IAM usuário.
- Para saber como fornecer acesso por meio da federação de identidades, consulte Fornecendo acesso a usuários autenticados externamente (federação de identidades) no Guia do IAMusuário.
- Para saber a diferença entre usar funções e políticas baseadas em recursos para acesso entre contas, consulte Acesso a recursos entre contas IAM no Guia do IAM usuário.

Usar funções vinculadas ao serviço do AWS Health

AWS Health usa AWS Identity and Access Management (IAM) funções vinculadas ao serviço. Uma função vinculada ao serviço é um tipo exclusivo de IAM função vinculada diretamente a. AWS Health As funções vinculadas a serviços são predefinidas pelo AWS Health e incluem todas as permissões que o serviço requer para chamar outros Serviços da AWS para você.

Você pode usar uma função vinculada ao serviço para configurar para evitar AWS Health a adição manual das permissões necessárias. AWS Health define as permissões de suas funções vinculadas ao serviço e, a menos que seja definido de outra forma, só AWS Health pode assumir suas funções. As permissões definidas incluem a política de confiança e a política de permissões, e essa política de permissões não pode ser anexada a nenhuma outra IAM entidade.

Permissões de função vinculada ao serviço AWS Health

AWS Health tem duas funções vinculadas ao serviço:

- AWSServiceRoleForHealth_Organizations— Essa função confia no AWS Health (`health.amazonaws.com`) para assumir a função de acesso Serviços da AWS para você. A política `Health_OrganizationsServiceRolePolicy` AWS gerenciada está anexada a essa função.
- AWSServiceRoleForHealth_EventProcessor— Essa função confia no diretor AWS Health de serviço (`event-processor.health.amazonaws.com`) para assumir a função por você. A política `AWSHealth_EventProcessorServiceRolePolicy` AWS gerenciada está anexada a essa função. O responsável pelo serviço usa a função para criar uma regra EventBridge

gerenciada pela Amazon para detecção e resposta a AWS incidentes. Essa regra é a infraestrutura necessária Conta da AWS para fornecer informações de alteração do estado de alarme de sua conta para AWS Health.

Para obter mais informações sobre as políticas AWS gerenciadas, consulteAWS políticas gerenciadas para AWS Health.

Crie uma função vinculada ao serviço para o AWS Health

Você não precisa criar o AWSServiceRoleForHealth_Organizations função vinculada ao serviço. Quando você chama a EnableHealthServiceAccessForOrganizationoperação, AWS Health cria essa função vinculada ao serviço na conta para você.

Você deve criar manualmente o AWSServiceRoleForHealth_EventProcessor função vinculada ao serviço em sua conta. Para obter mais informações, consulte Criação de uma função vinculada ao serviço no Guia do IAMusuário.

Editar uma função vinculada ao serviço para o AWS Health

AWS Health não permite que você edite a função vinculada ao serviço. Depois que você criar um perfil vinculado ao serviço, não poderá alterar o nome do perfil, pois várias entidades podem fazer referência ao perfil. No entanto, você pode editar a descrição da função usandoIAM. Para obter mais informações, consulte Edição de uma função vinculada ao serviço no Guia do IAMusuário.

Excluir uma função vinculada ao serviço para o AWS Health

Para excluir o AWSServiceRoleForHealth_Organizations função, você deve primeiro chamar a DisableHealthServiceAccessForOrganizationoperação. Em seguida, você pode excluir a função por meio do IAM console ou AWS Command Line Interface (AWS CLI). IAM API

Para excluir o AWSServiceRoleForHealth_EventProcessor função, entre em contato AWS Support e peça que eles retirem suas cargas de trabalho da Detecção e Resposta a AWS Incidentes. Depois que esse processo for concluído, você poderá excluir qualquer função por meio do IAM console ou AWS CLI. IAM API

Informações relacionadas

Para obter mais informações, consulte Usando funções vinculadas a serviços no Guia do IAMusuário.

AWS políticas gerenciadas para AWS Health

Uma política AWS gerenciada é uma política autônoma criada e administrada por AWS. AWS as políticas gerenciadas são projetadas para fornecer permissões para muitos casos de uso comuns, para que você possa começar a atribuir permissões a usuários, grupos e funções.

Lembre-se de que as políticas AWS gerenciadas podem não conceder permissões de privilégio mínimo para seus casos de uso específicos porque elas estão disponíveis para uso de todos os AWS clientes. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo cliente da 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 API operações são disponibilizadas para os serviços existentes.

Para obter mais informações, consulte as políticas AWS gerenciadas no Guia IAM do usuário.

AWS Health tem as seguintes políticas gerenciadas.

Sumário

AWS política gerenciada: AWSHealth_EventProcessorServiceRolePolicy

AWS Health usa o AWSHealth_EventProcessorServiceRolePolicy AWS política gerenciada. Essa política gerenciada é anexada à função vinculada ao serviço do `AWSServiceRoleForHealth_EventProcessor`. A política permite que a função vinculada ao serviço realize ações em seu nome. Você não pode anexar essa política às suas IAM entidades. Para obter mais informações, consulte Usar funções vinculadas ao serviço do AWS Health.

A política gerenciada tem as seguintes permissões para permitir o acesso AWS Health à EventBridge regra da Amazon para detecção e resposta a AWS incidentes.

Detalhes das permissões

Esta política inclui as seguintes permissões:

- `events`— Descreve e exclui EventBridge regras e descreve e atualiza as metas dessas regras.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Condition": {
                "StringEquals": {"events:ManagedBy": "event-
processor.health.amazonaws.com"}
            },
            "Action": [
                "events:DeleteRule",
                "events:RemoveTargets",
                "events:PutTargets",
                "events:PutRule"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "events:ListTargetsByRule",
                "events:DescribeRule"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

Para obter uma lista de alterações na política, consulte AWS Health atualizações nas políticas AWS gerenciadas.

AWS política gerenciada: Health_OrganizationsServiceRolePolicy

AWS Health usa o Health_OrganizationsServiceRolePolicy AWS política gerenciada. Essa política gerenciada é anexada à função vinculada ao serviço do `AWSServiceRoleForHealth_Organizations`. A política permite que a função vinculada ao serviço realize ações em seu nome. Você não pode anexar essa política às suas IAM entidades. Para obter mais informações, consulte Usar funções vinculadas ao serviço do AWS Health.

Essa política concede permissões que permitem AWS Health acessar AWS Organizations os detalhes necessários para a visualização Health Organizational.

Detalhes das permissões

Esta política inclui as seguintes permissões:

- `organizations`— Descreve as contas em AWS Organizations e as Serviços da AWS que podem ser usadas com Organizations.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccounts",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListDelegatedAdministrators",
                "organizations:DescribeOrganization",
                "organizations:DescribeAccount"
            ],
            "Resource": "*"
        }
    ]
}
```

Para obter uma lista de alterações na política, consulte AWS Health atualizações nas políticas AWS gerenciadas.

AWS política gerenciada: AWSHealthFullAccess

AWS Health usa o AWSHealthFullAccess AWS política gerenciada. A política concede às entidades (IAMusuários ou funções) acesso ao AWS Health console. Para obter mais informações, consulte Usar o console do AWS Health.

Detalhes das permissões

Esta política inclui as seguintes permissões:

- `organizations`— Ative ou desative o recurso de visualização AWS Health organizacional para todas as contas em uma AWS organização e visualize as unidades organizacionais (OU) da conta de gerenciamento
- `health`— Acesso às AWS Health API operações e notificações
- `iam`— Cria uma IAM função vinculada ao AWS Health serviço

```
{
    "Version": "2012-10-17",
        "Statement": [
            {
                "Sid": "OrganizationWriteAccess",
                "Effect": "Allow",
                "Action": [
                    "organizations:EnableAWSServiceAccess",
                    "organizations:DisableAWSServiceAccess"
                ],
                "Resource": "*",
                "Condition": {
                    "StringEquals": {
                        "organizations:ServicePrincipal": "health.amazonaws.com"
                    }
                }
            },
            {
                "Sid": "HealthFullAccess",
                "Effect": "Allow",
                "Action": [
                    "health:*",
                    "organizations:DescribeAccount",
```

```
                    "organizations:ListAccounts",
                    "organizations:ListDelegatedAdministrators",
                    "organizations:ListParents"
                ],
                "Resource": "*"
            },
            {
                "Sid": "ServiceLinkAccess",
                "Effect": "Allow",
                "Action": "iam:CreateServiceLinkedRole",
                "Resource": "*",
                "Condition": {
                    "StringEquals": {
                        "iam:AWSServiceName": "health.amazonaws.com"
                    }
                }
            }
        ]
}
```

Para obter uma lista de alterações na política, consulte AWS Health atualizações nas políticas AWS gerenciadas.

AWS Health atualizações nas políticas AWS gerenciadas

Veja detalhes sobre as atualizações das políticas AWS gerenciadas AWS Health desde que esse serviço começou a rastrear essas alterações. Para receber alertas automáticos sobre alterações nessa página, assine o RSS feed na Histórico do documento para AWS Health página.

A tabela a seguir descreve atualizações importantes nas políticas AWS Health gerenciadas desde 13 de janeiro de 2022.

AWS Health

Alteração	Descrição	Data
AWS política gerenciada: AWSHealthFullAccess -	AWS Health expandiu a AWSHealthFullAccess política	16 de outubro de 2023

Alteração	Descrição	Data
Atualização em uma política existente	para AWS GovCloud (US) Regions as regiões da China.	
AWS política gerenciada: Health_OrganizationsServiceRolePolicy - Atualização em uma política existente	AWS Health adicionou novas AWS Organizations ações para permitir que a função vinculada ao serviço descreva as contas e os AWS serviços com os quais você pode usar. AWS Organizations	19 de julho de 2023
Publicação do log de alterações	Registro de alterações das políticas AWS Health gerenciadas.	13 de janeiro de 2023

Registro e monitoramento em AWS Health

O monitoramento é uma parte importante da manutenção da confiabilidade, disponibilidade e desempenho de AWS Health suas outras AWS soluções. AWS fornece as seguintes ferramentas de monitoramento para observar AWS Health, relatar quando algo está errado e tomar medidas quando apropriado:

- A Amazon CloudWatch monitora seus AWS recursos e os aplicativos nos quais você executa AWS em tempo real. É possível coletar e rastrear métricas, criar painéis personalizados e definir alarmes que o notificam ou que realizam ações quando uma métrica especificada atinge um limite definido. Por exemplo, você pode CloudWatch monitorar o CPU uso ou outras métricas de suas instâncias do Amazon Elastic Compute Cloud (AmazonEC2) e iniciar automaticamente novas instâncias quando necessário. Para obter mais informações, consulte o Guia CloudWatch do usuário da Amazon.
- A Amazon EventBridge fornece um near-real-time fluxo de eventos do sistema que descrevem mudanças nos AWS recursos. EventBridge permite a computação automatizada orientada por eventos. Você pode criar regras que observem determinados eventos e acionem ações automatizadas em outros AWS serviços quando esses eventos acontecem. Para obter mais informações, consulte Monitorando eventos AWS Health com a Amazon EventBridge.

- AWS CloudTrailcaptura API chamadas 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 AWS Health.

Validação de conformidade para AWS Health

Para saber se um AWS service (Serviço da AWS) está dentro do escopo de programas de conformidade específicos, consulte Serviços da AWS Escopo por Programa de Conformidade Serviços da AWS e escolha o programa de conformidade em que você está interessado. Para obter informações gerais, consulte Programas de AWS conformidade Programas AWS de .

Você pode baixar relatórios de auditoria de terceiros usando AWS Artifact. Para obter mais informações, consulte Baixar relatórios em AWS Artifact .

Sua responsabilidade de conformidade ao usar Serviços da AWS é determinada pela confidencialidade de seus dados, pelos objetivos de conformidade de sua empresa e pelas leis e regulamentações aplicáveis. AWS fornece os seguintes recursos para ajudar na conformidade:

- Guias de início rápido sobre segurança e conformidade — Esses guias de implantação discutem considerações arquitetônicas e fornecem etapas para a implantação de ambientes básicos AWS focados em segurança e conformidade.
- Arquitetura para HIPAA segurança e conformidade na Amazon Web Services — Este whitepaper descreve como as empresas podem usar AWS para criar HIPAA aplicativos qualificados.

> **Note**
>
> Nem todos Serviços da AWS são HIPAA elegíveis. Para obter mais informações, consulte a Referência de serviços HIPAA elegíveis.

- 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, por exemplo PCIDSS, 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 Health

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 aplicativos 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 datacenters tradicionais.

AWS Health os eventos são armazenados e replicados em várias zonas de disponibilidade. Essa abordagem garante que você possa acessá-los a partir das operações AWS Health Dashboard ou das AWS Health API operações. Você pode ver AWS Health eventos de até 90 dias a partir da data em que eles ocorrerem.

Para obter mais informações sobre AWS regiões e zonas de disponibilidade, consulte Infraestrutura AWS global.

Segurança da infraestrutura no AWS Health

Como serviço gerenciado, AWS Health é protegido pelos procedimentos AWS globais de segurança de rede descritos no whitepaper Amazon Web Services: Visão geral dos processos de segurança.

Você usa API chamadas AWS publicadas para acessar AWS Health pela rede. Os clientes devem oferecer suporte ao Transport Layer Security (TLS) 1.0 ou posterior. Recomendamos TLS 1.2 ou posterior. Os clientes também devem oferecer suporte a pacotes de criptografia com sigilo direto perfeito (), como Ephemeral Diffie-Hellman (PFS) ou Elliptic Curve Ephemeral Diffie-Hellman (). DHE ECDHE A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

Além disso, as solicitações devem ser assinadas usando uma ID de chave de acesso e uma chave de acesso secreta associada a um IAM principal. Ou você pode usar o AWS Security Token Service (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

Análise de configuração e vulnerabilidade em AWS Health

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.

Melhores práticas de segurança do AWS Health

Veja as seguintes melhores práticas para trabalhar com AWS Health.

Conceda AWS Health aos usuários o mínimo de permissões possíveis

Siga o princípio de privilégio mínimo usando o conjunto mínimo de permissões de políticas de acesso para os usuários e grupos do . Por exemplo, você pode permitir que um usuário AWS Identity and Access Management (IAM) acesse AWS Health Dashboard o. No entanto, não é possível permitir que esse mesmo usuário habilite ou desabilite o acesso ao AWS Organizations.

Para obter mais informações, consulte AWS Health exemplos de políticas baseadas em identidade.

Veja o AWS Health Dashboard

Verifique AWS Health Dashboard com frequência para identificar eventos que possam afetar sua conta ou seus aplicativos. Por exemplo, você pode receber uma notificação de evento sobre seus

recursos, como uma instância do Amazon Elastic Compute Cloud (AmazonEC2) que precisa ser atualizada.

Para obter mais informações, consulte Começando com seu AWS Health painel.

Integre AWS Health com Amazon Chime ou Slack

Você pode se integrar AWS Health às suas ferramentas de bate-papo. Essa integração permite que você e sua equipe sejam notificados sobre AWS Health eventos em tempo real. Para obter mais informações, consulte as AWS Health Ferramentas em GitHub.

Monitor de AWS Health eventos

Você pode se integrar AWS Health com o Amazon CloudWatch Events para criar regras para eventos específicos. Quando o CloudWatch Events detecta um evento que corresponde à sua regra, você é notificado e pode então agir. CloudWatch Os eventos de eventos são específicos da região, portanto, você deve configurar esse serviço na região em que seu aplicativo ou infraestrutura reside.

Em alguns casos, a região do AWS Health evento não pode ser determinada. Se ocorrer essa situação, o evento será exibido na região Leste dos EUA (Norte da Virgínia) por padrão. Você pode configurar CloudWatch eventos nesta região para garantir o monitoramento desses eventos.

Para obter mais informações, consulte Monitorando eventos AWS Health com a Amazon EventBridge.

Agregando AWS Health eventos em todas as contas

Por padrão, você pode usar AWS Health para visualizar os AWS Health eventos de uma única AWS conta. Se você usa AWS Organizations, você também pode visualizar AWS Health eventos de forma centralizada em toda a sua organização. Esse atributo fornece acesso às mesmas informações que as operações de uma única conta. Você pode usar filtros para visualizar eventos em AWS regiões, contas e serviços específicos.

É possível agregar eventos para identificar contas da organização afetadas por um evento operacional ou para ser notificado sobre vulnerabilidades de segurança. Também é possível usar essas informações para gerenciar e automatizar proativamente os eventos de manutenção de recursos em toda a sua organização. Use esse recurso para se manter informado sobre mudanças futuras nos AWS serviços que podem exigir atualizações ou alterações no código.

É uma prática recomendada usar o recurso Administrador Delegado para delegar acesso à visualização AWS Health Organizacional a uma conta de membro. Isso facilita o acesso das equipes operacionais aos AWS Health eventos em sua organização. O recurso Administrador Delegado permite que você mantenha sua conta de gerenciamento restrita, ao mesmo tempo em que fornece às equipes a visibilidade de que precisam para agir em AWS Health eventos.

Important

- AWS Health não registra eventos que ocorreram em sua organização antes de você ativar a visualização organizacional. Por exemplo, se uma conta membro (111122223333) em sua organização recebeu um evento para o Amazon Elastic Compute Cloud (AmazonEC2) antes de você ativar esse recurso, esse evento não aparecerá na sua visão organizacional.
- AWS Health os eventos que foram enviados para contas em sua organização aparecerão na exibição organizacional enquanto o evento estiver disponível, por até 90 dias, mesmo que uma ou mais dessas contas deixem sua organização.
- Os eventos organizacionais ficam disponíveis por 90 dias antes de serem excluídos. Essa cota não pode ser aumentada.

Pré-requisitos

Antes da visualização organizacional, é necessário:

- Fazer parte de uma organização com todos os atributos habilitados.
- Faça login na conta de gerenciamento como usuário AWS Identity and Access Management (IAM) ou assuma uma IAM função.

  Você também pode fazer login como usuário raiz (não recomendado) na conta de gerenciamento da sua organização. Para obter mais informações, consulte Bloquear as chaves de acesso do usuário root da sua AWS conta no Guia IAM do usuário.
- Se você entrar como IAM usuário, use uma IAM política que conceda acesso às ações AWS Health e da Organizations, como a AWSHealthFullAccesspolítica. Para obter mais informações, consulte AWS Health exemplos de políticas baseadas em identidade.

Tópicos

Habilitar a visualização organizacional

Você pode usar o AWS Health console para obter uma visão centralizada dos eventos de saúde em sua AWS organização.

A visão organizacional está disponível no AWS Health console para todos os AWS Support planos sem custo adicional.

> **Note**
>
> Se você quiser permitir que os usuários acessem esse recurso na conta de gerenciamento, eles devem ter permissões como a AWSHealthFullAccesspolítica. Para obter mais informações, consulte AWS Health exemplos de políticas baseadas em identidade.

Enabling organizational view (Console)

Você pode ativar a visualização organizacional no AWS Health console. Você deve entrar na conta de gerenciamento da sua AWS organização.

Para visualizar o AWS Health painel de controle da sua organização

1. Abra seu AWS Health painel em https://health.aws.amazon.com/health/casa.
2. No painel de navegação, em Integridade da sua organização, escolha Configurações.
3. Em Habilitar visualização organizacionalHabilitar o modo de visualização organizacional.
4. (Opcional) Se você quiser fazer alterações em suas AWS organizações, como criar unidades organizacionais (OUs), escolha Gerenciar AWS Organizations.

   Para obter mais informações, consulte Conceitos básicos do AWS Organizations no Manual do usuário do AWS Organizations .

> **Observações**
>
> - A habilitação desse recurso é um processo assíncrono e leva um tempo para ser concluída. Dependendo do número de contas na sua organização, poderá levar vários minutos para o carregamento das contas. Você pode sair e verificar o console de AWS Health mais tarde.
> - Se você tiver um plano Business, Enterprise On-Ramp ou Enterprise Support, poderá chamar a DescribeHealthServiceStatusForOrganizationAPIoperação para verificar o status do processo.
> - Quando você habilita esse recurso, a função `AWSServiceRoleForHealth_Organizations` vinculada ao serviço com a política `Health_OrganizationsServiceRolePolicy` AWS gerenciada é aplicada à conta de gerenciamento na organização. Para obter mais informações, consulte Usar funções vinculadas ao serviço do AWS Health.

Enabling organizational view (CLI)

Você pode ativar a visualização organizacional usando a EnableHealthServiceAccessForOrganizationAPIoperação.

Você pode usar o AWS Command Line Interface (AWS CLI) ou seu próprio código para chamar essa operação.

> **Note**
>
> - Você deve ter um plano Business, Enterprise On-Ramp ou Enterprise Support para ligar para o. AWS Health API
> - Você deve usar o endpoint da região Leste dos EUA (Norte da Virgínia).

Example

O AWS CLI comando a seguir ativa esse recurso em sua AWS conta. É possível usar esse comando na conta de gerenciamento ou em uma conta que possa assumir a função com as permissões necessárias.

```
aws health enable-health-service-access-for-organization --region us-east-1
```

Os exemplos de código a seguir chamam a EnableHealthServiceAccessForOrganizationAPIoperação.

Python

```
import boto3

client = boto3.client('health')

response = client.enable_health_service_access_for_organization()

print(response)
```

Java

Você pode usar a AWS SDK versão Java 2.0 para o exemplo a seguir.

```
import software.amazon.awssdk.services.health.HealthClient;
import software.amazon.awssdk.services.health.HealthClientBuilder;

import software.amazon.awssdk.services.health.model.ConcurrentModificationException;
```

```
import
 software.amazon.awssdk.services.health.model.EnableHealthServiceAccessForOrganizationReques
import
 software.amazon.awssdk.services.health.model.EnableHealthServiceAccessForOrganizationRespon
import
 software.amazon.awssdk.services.health.model.DescribeHealthServiceStatusForOrganizationRequ
import
 software.amazon.awssdk.services.health.model.DescribeHealthServiceStatusForOrganizationResp

import software.amazon.awssdk.auth.credentials.DefaultCredentialsProvider;

import software.amazon.awssdk.regions.Region;

public class EnableHealthServiceAccessDemo {
    public static void main(String[] args) {
        HealthClient client = HealthClient.builder()
            .region(Region.US_EAST_1)
            .credentialsProvider(
                DefaultCredentialsProvider.builder().build()
            )
            .build();

        try {
            DescribeHealthServiceStatusForOrganizationResponse statusResponse =
 client.describeHealthServiceStatusForOrganization(
                DescribeHealthServiceStatusForOrganizationRequest.builder().build()
            );

            String status =
 statusResponse.healthServiceAccessStatusForOrganization();
            if ("ENABLED".equals(status)) {
                System.out.println("EnableHealthServiceAccessForOrganization already
 enabled!");
                return;
            }

            client.enableHealthServiceAccessForOrganization(
                EnableHealthServiceAccessForOrganizationRequest.builder().build()
            );

            System.out.println("EnableHealthServiceAccessForOrganization is in
 progress");
        } catch (ConcurrentModificationException cme) {
```

```
            System.out.println("EnableHealthServiceAccessForOrganization is already
 in progress. Wait for the action to complete before trying again.");
        } catch (Exception e) {
            System.out.println("EnableHealthServiceAccessForOrganization FAILED: " +
 e);
        }
    }
}
```

Para obter mais informações, consulte o AWS SDKGuia do desenvolvedor do Java 2.0.

Quando você habilita esse recurso, a função `AWSServiceRoleForHealth_Organizations` vinculada ao serviço com a política `Health_OrganizationsServiceRolePolicy` AWS gerenciada é aplicada à conta de gerenciamento na organização.

> **Note**
>
> A habilitação desse recurso é um processo assíncrono e leva um tempo para ser concluída. Você pode chamar a DescribeHealthServiceStatusForOrganizationoperação para verificar o status do processo.

Visualizando a visão organizacional

Você pode usar o AWS Health console para obter uma visão centralizada dos eventos de saúde em sua AWS organização.

A visão organizacional está disponível no AWS Health console para todos os AWS Support planos sem custo adicional.

> **Note**
>
> Se você quiser permitir que os usuários acessem esse recurso na conta de gerenciamento, eles devem ter permissões como a AWSHealthFullAccesspolítica. Para obter mais informações, consulte AWS Health exemplos de políticas baseadas em identidade.

Viewing organizational view events (Console)

Depois de habilitar a visualização organizacional, AWS Health exibe eventos de saúde para todas as contas em sua organização.

Quando uma conta se junta à sua organização, ela é adicionada AWS Health automaticamente à visualização organizacional. Quando uma conta sai da organização, novos eventos dessa conta não são mais registrados em log na visualização organizacional. No entanto, os eventos existentes permanecem e você ainda pode consultá-los por até 90 dias.

AWS retém os dados da política da conta por 90 dias a partir da data efetiva do encerramento da conta do administrador. Ao final do período de 90 dias, exclui AWS permanentemente todos os dados da política da conta.

- Para reter as descobertas por mais de 90 dias, você pode arquivar as políticas. Você também pode usar uma ação personalizada com uma EventBridge regra para armazenar as descobertas em um bucket do S3.
- Desde que AWS retenha os dados da política, ao reabrir a conta fechada, AWS reatribui a conta como administradora do serviço e recupera os dados da política de serviço da conta.
- Para obter mais informações, consulte Encerrar uma conta.

Important

Para clientes nas AWS GovCloud (US) regiões:

- Antes de fechar sua conta, faça backup e, em seguida, exclua os dados da política e outros recursos da conta. Você não terá mais acesso a eles depois de fechar a conta.

Note

Quando você ativa esse recurso, o AWS Health console pode exibir eventos públicos do AWS Health Painel — Integridade do serviço nos últimos 7 dias. Esses eventos públicos não são específicos para contas na sua organização. Eventos do AWS Health Painel — A integridade do serviço fornece informações públicas sobre a disponibilidade regional dos AWS serviços.

Você pode visualizar eventos de visualização organizacional nas seguintes páginas:

Problemas abertos e recentes

Você pode usar a guia Problemas abertos e recentes para visualizar eventos que podem afetar sua AWS infraestrutura, como alterações Serviços da AWS e recursos que afetam sua organização.

Para visualizar eventos de visualização organizacional

1. Abra seu AWS Health painel em https://health.aws.amazon.com/health/casa.
2. No painel de navegação, em Status da sua organização, escolha Problemas abertos e recentes para visualizar eventos relatados recentemente.
3. Escolha um evento. Na guia Detalhes, você pode revisar as seguintes informações sobre o evento:

   - Nome do evento
   - Status
   - Zona de disponibilidade / região
   - IDs da conta afetada
   - Horário de início
   - End Time
   - Categoria
   - Descrição

Mudanças programadas

Use a guia Alterações agendadas para ver os próximos eventos que podem afetar sua organização. Esses eventos podem incluir atividades de manutenção programadas para serviços.

Outras notificações

Use a guia Notificações para ver todas as outras notificações e eventos em andamento dos últimos sete dias que possam afetar sua organização. Isso pode incluir eventos, como rotações de certificados, notificações de cobrança e vulnerabilidades de segurança.

Log de eventos

Você também pode usar a guia Registro de eventos para visualizar AWS Health eventos para visualização organizacional. O layout e o comportamento da coluna são semelhantes aos da guia Problemas abertos e recentes, exceto que a guia Log de eventos inclui colunas adicionais e opções de filtro, como Categoria do evento, Status e Horário de início.

Para exibir eventos de visualização organizacional na guia Log de eventos

1. Abra seu AWS Health painel em https://health.aws.amazon.com/health/casa.
2. No painel de navegação, em Integridade da sua organização, escolha Log de eventos.
3. Em Log de eventos, escolha o nome do evento. Você pode ver as seguintes informações sobre o evento:

   - Nome do evento
   - Status
   - Zona de disponibilidade / região
   - IDs da conta afetada
   - Horário de início
   - End Time
   - Categoria
   - Descrição

Viewing affected accounts and resources (Console)

Em Integridade da sua organização, você pode ver as contas em sua organização que são afetadas pelo evento e quaisquer recursos relacionados. Por exemplo, se houver um evento futuro para a manutenção de instâncias do Amazon Elastic Compute Cloud (AmazonEC2), as contas em sua organização que têm EC2 instâncias da Amazon podem aparecer na guia Detalhes. Você pode identificar os recursos específicos e entrar em contato com o responsável pela conta.

Para visualizar contas e recursos afetados

1. Abra seu AWS Health painel em https://health.aws.amazon.com/health/casa.
2. No painel de navegação, em Integridade da sua organização, selecione uma das guias.
3. Escolha um evento que tenha um valor para as Contas afetadas.
4. Escolha a guia Contas afetadas.

5. Escolha Mostrar detalhes da conta para ver as seguintes informações sobre as contas:
   - ID da conta
   - Nome da conta
   - E-mail principal
   - Unidade organizacional (UO)
6. Expandir a conta para visualizar os recursos afetados.
7. Se houver mais de 10 recursos, escolha Visualizar todos os recursos para visualizá-los.
8. Para filtrar por ID da conta para esse evento específico, faça o seguinte:
   a. Na guia Contas afetadas, escolha Adicionar filtro, escolha ID da conta e, então, insira a ID da conta. Você só pode inserir um ID de conta por vez.
   b. Escolha Aplicar. A conta que você inseriu aparecerá na lista.

Viewing organizational view events (CLI)

Depois de habilitar esse recurso, AWS Health começa a registrar eventos que afetam as contas na organização. Quando uma conta ingressa na organização, o AWS Health a adiciona automaticamente à visualização organizacional.

> **Note**
>
> AWS Health não registra eventos que ocorreram em sua organização antes de você ativar a visualização organizacional.

Quando uma conta sai da organização, novos eventos dessa conta não são mais registrados em log na visualização organizacional. No entanto, os eventos existentes permanecem e você ainda pode consultá-los por até 90 dias.

AWS retém os dados da política da conta por 90 dias a partir da data efetiva do encerramento da conta do administrador. Ao final do período de 90 dias, exclui AWS permanentemente todos os dados da política da conta.

- Para reter as descobertas por mais de 90 dias, você pode arquivar as políticas. Você também pode usar uma ação personalizada com uma EventBridge regra para armazenar as descobertas em um bucket do S3.

- Desde que AWS retenha os dados da política, ao reabrir a conta fechada, AWS reatribui a conta como administradora do serviço e recupera os dados da política de serviço da conta.
- Para obter mais informações, consulte Encerrar uma conta.

> **Important**
>
> Para clientes nas AWS GovCloud (US) regiões:
>
> - Antes de fechar sua conta, faça backup e, em seguida, exclua os dados da política e outros recursos da conta. Você não terá mais acesso a eles depois de fechar a conta.

Você pode usar as AWS Health API operações para retornar eventos da visão organizacional.

Example : Descrever eventos da visualização organizacional

O AWS CLI comando a seguir retorna eventos de saúde para AWS contas em sua organização.

```
aws health describe-events-for-organization --region us-east-1
```

Desabilitar a visualização organizacional

Se você não quiser agregar eventos para sua organização, desative esse recurso na conta de gerenciamento ou desative a exibição organizacional usando a DisableHealthServiceAccessForOrganizationAPIoperação.

Disabling organizational view events (Console)

AWS Health interrompe a agregação de eventos para todas as outras contas em sua organização. Você pode continuar visualizando eventos anteriores da sua organização até que eles sejam excluídos.

Para desabilitar a visualização organizacional

1. Abra seu AWS Health painel em https://health.aws.amazon.com/health/casa.
2. No painel de navegação, em Integridade da sua organização, escolha Configurações.
3. Na página Habilitar visualização organizacional, escolha Desativar visualização organizacional.

Depois de desativar esse recurso, AWS Health não agrega mais eventos da sua organização. No entanto, a função vinculada ao serviço permanece na conta de gerenciamento até que você a exclua por meio do console AWS Identity and Access Management (IAM) ou AWS Command Line Interface (AWS CLI). IAM API Para obter mais informações, consulte Excluindo uma função vinculada ao serviço no Guia do IAM usuário.

Disabling organizational view events (CLI)

Example

O AWS CLI comando a seguir desativa esse recurso da sua conta.

```
aws health disable-health-service-access-for-organization --region us-east-1
```

> **Note**
>
> Você também pode desativar o recurso organizacional usando a API operação Organizations D isableAWSService Access. Depois que você chama essa operação, o AWS Health para de agregar eventos de todas as outras contas em sua organização. Se você chamar as AWS Health API operações para visualização organizacional, AWS Health retornará um erro. AWS Health continua agregando eventos de saúde para sua AWS conta.

Depois de desativar esse recurso, AWS Health não agrega mais eventos da sua organização. No entanto, a função vinculada ao serviço permanece na conta de gerenciamento até que você a exclua por meio do console AWS Identity and Access Management (IAM) ou. IAM API AWS CLIPara obter mais informações, consulte Excluindo uma função vinculada ao serviço no Guia do IAM usuário.

Visão organizacional do administrador delegado

Com AWS Health, você pode aproveitar o recurso de administrador delegado de AWS Organizations que permite que uma conta diferente da conta de gerenciamento visualize eventos agregados AWS Health no AWS Health Dashboard ou programaticamente por meio da API do AWS Health. O recurso de administrador delegado oferece flexibilidade para diferentes equipes visualizarem e gerenciarem eventos de saúde em toda a organização. É uma prática recomendada de segurança AWS delegar responsabilidades fora da conta de gerenciamento, sempre que possível.

Sumário

Registre um administrador delegado para sua visualização organizacional

Depois de habilitar a visualização organizacional para sua organização, você pode registrar até cinco contas de membros em sua organização como administrador delegado. Para fazer isso, contacte a operação da API RegisterDelegatedAdministrator. Depois de registrar as contas dos membros, elas recebem contas administrativas delegadas e podem acessar a visualização organizacional do AWS Health no AWS Health Dashboard. Se a conta tiver um plano de suporte Business, Enterprise On-Ramp ou Enterprise https://aws.amazon.com/premiumsupport/plans/business/https://aws.amazon.com/premiumsupport/plans/enterprise-onramphttps://aws.amazon.com/premiumsupport/plans/enterprise, os administradores delegados poderão usar a AWS Health API para acessar AWS Health a visão organizacional.

Para estabelecer um administrador delegado, na conta de gerenciamento da sua organização, chame o comando a seguir AWS Command Line Interface (AWS CLI). É possível usar esse comando na conta de gerenciamento ou em uma conta que possa assumir a função com as permissões AWS Identity and Access Management necessárias. No exemplo de comando a seguir, substitua ACCOUNT_ID pelo ID da conta do membro que você deseja registrar junto com o responsável pelo serviço principal AWS Health “health.amazonaws.com”.

```
aws organizations register-delegated-administrator --account-id ACCOUNT_ID --service-
principal  health.amazonaws.com
```

Depois que um administrador delegado for registrado, você tem visibilidade de todos os eventos de AWS Health que afetam as contas em sua organização. Você pode visualizar eventos históricos dos últimos 90 dias ou desde que o recurso de visualização organizacional foi ativado pela primeira vez, o que for mais recente. Observe que habilitar o recurso de administrador delegado é um processo assíncrono e leva até um minuto para ser concluído.

Remova um administrador delegado da sua visualização organizacional

Para remover o acesso de um administrador delegado, chame a operação da API DeregisterDelegatedAdministrator.

Na conta de gerenciamento da sua organização, chame o AWS CLI comando a seguir para remover uma conta de membro como administrador delegado. No exemplo de comando a seguir, substitua ACCOUNT_ID pelo ID da conta do membro que você deseja remover.

```
aws organizations deregister-delegated-administrator --account-id ACCOUNT_ID --service-
principal  health.amazonaws.com
```

Monitorando eventos AWS Health com a Amazon EventBridge

Você pode usar EventBridge a Amazon para detectar e reagir a AWS Health eventos. 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 tipo de evento, capture informações, tome medidas corretivas, inicie eventos ou realize outras ações. Por exemplo, você pode usar AWS Health para receber notificações por e-mail se tiver AWS recursos programados para atualizações, como instâncias do Amazon Elastic Compute Cloud (AmazonEC2). Conta da AWS

Observações

- AWS Health realiza eventos com base no melhor esforço. Nem sempre é garantido que os eventos sejam entregues EventBridge a.
- Todas EventBridge as regras que você criar só podem receber notificações para você Conta da AWS. Para receber eventos organizacionais para outras contas dentro da sua AWS Organizations, consulte Agregação de AWS Health eventos usando visualização organizacional e acesso de administrador delegado.

Você pode escolher entre vários tipos de alvo EventBridge como parte do seu AWS Health fluxo de trabalho, incluindo:

- AWS Lambda funções
- Amazon Kinesis Data Streams
- Filas do Amazon Simple Queue Service (AmazonSQS)
- Alvos integrados (como ações CloudWatch de alarme)
- Tópicos do Amazon Simple Notification Service (AmazonSNS)

Por exemplo, é possível usar uma função do Lambda para enviar uma notificação a um canal do Slack quando ocorrer um evento do . Ou você pode usar o Lambda e EventBridge enviar mensagens de texto ou SMS notificações personalizadas com a Amazon SNS quando ocorrer um AWS Health evento.

Para exemplos de automação e alertas personalizados que você pode criar em resposta a AWS Health eventos, consulte as AWS Health Ferramentas em GitHub.

Tópicos

Criação de EventBridge regras para Região da AWS cobertura

Você deve criar uma EventBridge regra para cada região para a qual deseja receber AWS Health eventos. Se você não criar uma regra, não receberá eventos. Por exemplo, para receber eventos da região Oeste dos EUA (Oregon), você deverá criar uma regra para esta região.

Configurar uma regra adicional em uma região de backup adiciona uma camada extra de resiliência aos seus fluxos de trabalho, caso sua regra principal seja afetada por um evento contínuo. Os eventos públicos de AWS Health são enviados simultaneamente para a região afetada e para uma região de backup. Consulte Sobre eventos públicos da AWS Health para obter mais informações. Para todas as regiões na AWS partição padrão, você pode configurar uma regra no Oeste dos EUA (Oregon) como backup para continuar recebendo eventos, mesmo que sua região principal seja afetada por um problema contínuo. A região de backup para a região Oeste dos EUA (Oregon) é a região Leste dos EUA (N. da Virgínia).

Por exemplo, se você estiver monitorando eventos na região da Europa (Frankfurt) e essa região estiver temporariamente indisponível, também AWS Health entregará esse evento para a região

Oeste dos EUA (Oregon). Em seguida, sua EventBridge regra de backup envia o evento para os destinos que você especificou. Para criar uma regra de backup, siga o procedimento abaixo para Configurando uma EventBridge regra para enviar notificações sobre eventos no AWS Health e use a região do Oeste dos EUA (Oregon).

Alguns AWS Health eventos não são específicos da região. Eventos que não são específicos de uma região são chamados de eventos globais. Isso inclui eventos enviados para AWS Identity and Access Management (IAM). Para receber eventos globais, você deve criar uma regra para a região do Leste dos EUA (Norte da Virgínia) como região primária e o Oeste dos EUA (Oregon) como região de backup.

Para receber eventos globais no AWS GovCloud (US), você deve criar uma regra na região AWS GovCloud (Oeste dos EUA).

Monitoramento de eventos públicos e específicos da conta para AWS Health

Quando você cria uma EventBridge regra para monitorar eventos AWS Health, a regra fornece eventos específicos da conta e eventos públicos:

- Eventos específicos da conta afetam sua conta e seus recursos, como um evento que informa sobre uma atualização necessária em uma EC2 instância da Amazon ou outros eventos de alteração programados.
- Os eventos públicos aparecem noAWS Health Dashboard: integridade do serviço. Os eventos públicos não são específicos de Contas da AWS e fornecem informações públicas sobre a disponibilidade regional de um serviço.

> **Important**
>
> Para receber os dois tipos de eventos, sua regra deve usar o valor de `"source": [ "aws.health"]`. Wildcards, como `"source": [ "aws.health*"]` não corresponderão ao padrão de monitoramento de nenhum evento.

Se você estiver monitorando eventos públicos a partir de um Região da AWS, recomendamos que você crie uma regra de backup. Os eventos públicos de AWS Health são enviados simultaneamente para a região afetada e para uma região de backup. É recomendável que você elimine a duplicação

de AWS Health eventos usando eventARN, communicationId pois eles permanecem consistentes para AWS Health mensagens enviadas para a região de backup.

Você pode identificar se um evento é público ou específico da conta em EventBridge, usando o eventScopeCode parâmetro. Os eventos podem ter o `PUBLIC` ou`ACCOUNT_SPECIFIC`. Você também filtrar a sua regra neste parâmetro.

Por exemplo, eventos públicos para o Amazon Elastic Compute Cloud .

O evento a seguir mostra um problema operacional da Amazon EC2 na região Leste dos EUA (Norte da Virgínia).

```
{
    "version": "0",
    "id": "fd9d4512-1eb0-50f6-0491-d016ae56aef0",
    "detail-type": "AWS Health Event",
    "source": "aws.health",
    "account": "123456789012",
    "time": "2023-02-15T10:07:10Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "eventArn": "arn:aws:health:us-east-1::event/EC2/AWS_EC2_OPERATIONAL_ISSUE",
        "service": "EC2",
        "eventTypeCode": "AWS_EC2_OPERATIONAL_ISSUE",
        "eventTypeCategory": "issue",
        "eventScopeCode": "PUBLIC",
        "communicationId": "01b0993207d81a09dcd552ebd1e633e36cf1f09a-1",
        "startTime": "Wed, 15 Feb 2023 22:07:07 GMT",
        "lastUpdatedTime": "Wed, 15 Feb 2023 22:07:07 GMT",
        "statusCode": "open",
        "eventRegion": "us-east-1",
        "eventDescription": [{
            "latestDescription": "We are investigating increased API Error rates and
 Latencies for Amazon Elastic Compute Cloud in the US-EAST-1 Region.",
            "language": "en_US"
        }],
        "page": "1",
        "totalPages": "1",
        "affectedAccount": "123456789012"

    }
```

```
}
```

Instalando uma função vinculada ao serviço para usar a Detecção e Resposta a AWS Incidentes

Se você usar a Detecção e Resposta a AWS Incidentes em sua conta, deverá instalar a função `AWSServiceRoleForHealth_EventProcessor` vinculada ao serviço em sua conta.

Essa função vinculada a serviço `event-processor.health.amazonaws.com` confia no principal para assumir a função. A política `AWSHealth_EventProcessorServiceRolePolicy` AWS gerenciada está anexada a essa função. Essa política lista as permissões que a função pode executar, como chamar outra pessoa Serviços da AWS para você.

Essa função então cria uma regra EventBridge gerenciada pela Amazon em sua conta. A regra é chamada `AWSHealthEventProcessor-DO-NOT-DELETE`. Essa regra é a infraestrutura necessária para que sua conta EventBridge possa fornecer informações de alteração do estado de alarme de sua conta para AWS Health.

Informações relacionadas

Para saber mais, consulte os tópicos a seguir:

- Usar funções vinculadas ao serviço do AWS Health
- AWS política gerenciada: AWSHealth_EventProcessorServiceRolePolicy

AWS HealthAmazon EventBridge Esquema de eventos

A seguir está o esquema para AWS Health eventos. Alterações ou adições à versão anterior do esquema são destacadas como “Novas”. Um exemplo de payload é fornecido após o esquema.

AWS Health Esquema do evento

AWS Health Esquema do evento

Parâmetro	Descrição	Obrigatório
version	EventBridge Versão,	Sim

Parâmetro	Descrição	Obrigatório
	atualmente “0"	
id	O uniqueEventBridge identificador do evento	Sim
detalhe-tipo	Descreve o tipo de detalhe. Para AWS Health eventos, isso será &AWS Health Event ou AWS Health Abuse Event	Sim
source	A fonte do barramento de eventos. Para AWS Health eventos, isso será aws.health	Sim

Parâmetro	Descrição	Obrigatório
conta	O accountId para o qual o AWS Health evento foi enviado. **Note** Para a visão organizacional, isso será diferente de affectedAccount se for recebido na conta de gerenciamento ou de administrador delegado.	Sim

Parâmetro	Descrição	Obrigatório
time	Horário para o qual a notificação foi enviada EventBridge. Formato: .`yyyy mm-d ddThh:mm:s sZ` .	Sim

Parâmetro	Descrição	Obrigatório
região	Identifica a pessoa para Região da AWS a qual a notificação foi entregue. **Note** Esse campo não indica a região afetada por esse AWS Health evento. Isso é fornecido por “detalhe” . eventRegion”.	Sim

Parâmetro	Descrição	Obrigatório
recursos	Descreve a lista de recursos afetados em uma conta, se houver recursos afetados. **Note** Esse campo pode ficar vazio se não houver nenhum recurso referenciado.	Não
detalhe	Esta seção contém todos os detalhes do AWS Health evento, conforme listado abaixo.	Sim

Parâmetro		Descrição	Obrigatório
	eventArn	Identificador exclusivo do AWS Health evento para a região específica, incluindo a região e o ID do evento. **Note** Um eventArn não é exclusivo de uma conta de cliente específica ou de uma região.	Sim

Parâmetro		Descrição	Obrigatório
	serviço	Os AWS service (Serviço da AWS) afetados pelo AWS Health evento. Por exemplo, AmazonEC2, Amazon Simple Storage Service, Amazon Redshift ou Amazon Relational Database Service.	Sim

Parâmetro		Descrição	Obrigatório
	eventTypeCode	O identificador exclusivo do tipo de evento. Por exemplo: `AWS_EC2_INSTANCE_NETWORK_MAINTENANCE_SCHEDULED` e `AWS_EC2_INSTANCE_REBOOT_MAINTENANCE_SCHEDULED`. Os eventos que incluem geralmente `MAINTENANCE_SCHEDULED` são realizados aproximadamente duas semanas antes dostartTime. **Note** Todos os	Sim

Parâmetro		Descrição	Obrigatório
		novos eventos de ciclo de vida planejados têm o tipo de evento `AWS_{SERVICE}_PLANNED_LIFECYCLE_EVENT`.	
	eventTypeCategory	O código de categoria do evento. Os valores possíveis são `issue`, `accountNotification`, `investigation` e `scheduledChange`.	Sim

Parâmetro		Descrição	Obrigatório
	eventScopeCode	Indica se o AWS Health evento é público ou específico da conta. Os valores possíveis são `ACCOUNT_SPECIFIC` ou `PUBLIC`.	Sim

Parâmetro		Descrição	Obrigatório
	communicationId (Novo)	Um identificador exclusivo para essa comunicação para o AWS Health evento. Mensagens com o mesmo communicationId são possíveis mensagens de backup ou páginas de um único AWS Health evento. Esse identificador pode ser usado com o accountId para ajudar a eliminar a duplicação de mensagens. **Note** Com o lançamen	Sim

Parâmetro	Descrição	Obrigatório
	o do recurso de paginação, communicationId inclui o número da página para manter o communicationId exclusivo em todas as páginas, por exemplo, 1234567810-1. Para obter mais informações, consulte Paginação de eventos	

Parâmetro		Descrição	Obrigatório
		em AWS Health EventBridge.	
	startTime	A hora de início do AWS Health evento no formato:`DoW, DD, MMM, YYYY, HH:MM:SS TZ`. **Note** O horário de início dos eventos programados pode ser no futuro.	Sim

Parâmetro		Descrição	Obrigatório
	endTime	A hora de término do AWS Health evento no formato:`DoW, DD MMM YYYY HH:MM:SS TZ`. **Note** endTime pode não ser fornecido para eventos que serão definidos no futuro.	Não

Parâmetro		Descrição	Obrigatório
	lastUpdatedTime	O horário da última atualização do AWS Health evento no formato:`DoW, DD MMM YYYY HH:MM:SS TZ`.	Sim
	statusCode	Status do AWS Health evento. Os valores possíveis são `open`, `closed` ou `upcoming`.	Sim
	eventRegion	A região impactada descrita por este AWS Health evento.	Sim

Parâmetro			Descrição	Obrigatório
	eventDescription		Uma seção que descreve o AWS Health evento. Isso inclui campos de idioma e texto para descrever o evento.	Sim
		idioma	Idioma usado no AWS Health evento. Isso normalmente é determinado pela região na qual o evento é publicado. Para a região us-east-1, normalmente seria “en_US”.	Sim

Parâmetro			Descrição	Obrigatório
		latestDescription	Descreve o AWS Health evento conforme ele é renderizado a partir do AWS Health API e normalmente aparece no AWS Health painel. **Note** Para eventos públicos, ele contém somente a atualização mais recente e não todo o histórico do evento.	Sim

Parâmetro		Descrição	Obrigatório
	eventMetadata	Metadados adicionais do evento que podem ser fornecidos para o evento de AWS Health .	Não

Parâmetro			Descrição	Obrigatório
		<metadata key 1>	chave de metadados, cadeias de valores “keystring1": “keyvalue1" **Note** Os pares de valores-chave para metadado do evento são determinados pelo serviço que enviou o evento. AWS Health	Não

Parâmetro			Descrição	Obrigatório
	affectedEntities		Uma matriz que descreve o valor do recurso e o status dos recursos afetados nesse AWS Health evento.	Não
		entityValue	O ID do recurso/entidade	Não
		lastUpdatedtime (Novo)	A hora em que o status desse recurso/entidade foi atualizado pela última vez no formato: `DoW, DD MMM YYYY HH:MM:SS TZ`	Não

Parâmetro			Descrição	Obrigatório
		status (novo)	O status do recurso/ entidade afetado. Os valores possíveis incluem `IMPAIRED`, `UNIMPAIRED` , `PENDING`, `RESOLVED`, `UNKNOWN`.	Não

Parâmetro		Descrição	Obrigatório
	página (Nova)	A página que essa mensagem represent a. Para obter mais informaçõ es, consulte Paginação de eventos em AWS Health EventBridge. Note A paginaçã ocorre somente em recursos. Outras causas da violação do limite de tamanho de 256 KB farão com que a	Sim

Parâmetro		Descrição	Obrigatório
		comunicação falhe.	

Parâmetro		Descrição	Obrigatório
	totalPages (Novo)	O número total de instâncias desse tipo de recurso. Para obter mais informaçõ es, consulte Paginação de eventos em AWS Health EventBridge. **Note** Você pode usar isso para determina r se recebeu todas as páginas de uma comunica ão de várias páginas de	Sim

Parâmetro	Descrição	Obrigatório
	uma conta.	

Parâmetro		Descrição	Obrigatório
	affectedAccount (Novo)	Essa é accountId a conta afetada. **Note** Isso pode ser diferente do campo “conta” se esse evento de saúde for enviado para uma conta que faz parte de uma AWS Organizations e é recebido na	Sim

Parâmetro		Descrição	Obrigatório
		conta de gerenciamento ou de administrador delegado.	

Evento de Saúde Pública — Problema EC2 operacional da Amazon


```
{
    "version": "0",
    "id": "7bf73129-1428-4cd3-a780-95db273d1602",
    "detail-type": "AWS Health Event",
    "source": "aws.health",
    "account": "123456789012",
    "time": "2023-01-27T09:01:22Z",
    "region": "af-south-1",
    "resources": [],
    "detail": {
        "eventArn": "arn:aws:health:af-south-1::event/EC2/AWS_EC2_OPERATIONAL_ISSUE/
AWS_EC2_OPERATIONAL_ISSUE_7f35c8ae-af1f-54e6-a526-d0179ed6d68f",
        "service": "EC2",
        "eventTypeCode": "AWS_EC2_OPERATIONAL_ISSUE",
        "eventTypeCategory": "issue",
        "eventScopeCode": "PUBLIC",
        "communicationId": "01b0993207d81a09dcd552ebd1e633e36cf1f09a-1",
        "startTime": "Fri, 27 Jan 2023 06:02:51 GMT",
        "endTime": "Fri, 27 Jan 2023 09:01:22 GMT",
        "lastUpdatedTime": "Fri, 27 Jan 2023 09:01:22 GMT",
        "statusCode": "open",
        "eventRegion": "af-south-1",
        "eventDescription": [{
            "language": "en_US",
            "latestDescription": "Current severity level: Operating normally\n
\n[RESOLVED] \n\n [03:15 PM PST] We continue see recovery \n\nThe following AWS
```

```
 services were previously impacted but are now operating normally: APPSYNC, BACKUP,
 EVENTS."
        }],
        "affectedEntities": [],
        "page": "1",
        "totalPages": "1",
        "affectedAccount": "123456789012"
    }
}
```

AWS Health Evento específico da conta - Problema no Elastic Load Balancing API

```
{
    "version": "0",
    "id": "121345678-1234-1234-1234-123456789012",
    "detail-type": "AWS Health Event",
    "source": "aws.health",
    "account": "123456789012",
    "time": "2022-06-10T06:27:57Z",
    "region": "ap-southeast-2",
    "resources": [],
    "detail": {
        "eventArn": "arn:aws:health:ap-southeast-2::event/
AWS_ELASTICLOADBALANCING_API_ISSUE_90353408594353980",
        "service": "ELASTICLOADBALANCING",
        "eventTypeCode": "AWS_ELASTICLOADBALANCING_API_ISSUE",
        "eventTypeCategory": "issue",
        "eventScopeCode": "ACCOUNT_SPECIFIC",
        "communicationId": "01b0993207d81a09dcd552ebd1e633e36cf1f09a-1",
        "startTime": "Fri, 10 Jun 2022 05:01:10 GMT",
        "endTime": "Fri, 10 Jun 2022 05:30:57 GMT",
        "statusCode": "open",
        "eventRegion": "ap-southeast-2",
        "eventDescription": [{
            "language": "en_US",
            "latestDescription": "A description of the event will be provided here"
        }],
        "page": "1",
        "totalPages": "1",
        "affectedAccount": "123456789012"
    }
```

```
}
```

AWS Health Evento específico da conta - Amazon EC2 Instance Store Drive Performance Degraded

```
{
    "version": "0",
    "id": "121345678-1234-1234-1234-123456789012",
    "detail-type": "AWS Health Event",
    "source": "aws.health",
    "account": "123456789012",
    "time": "2022-06-03T06:27:57Z",
    "region": "us-west-2",
    "resources": [
        "i-abcd1111"
    ],
    "detail": {
        "eventArn": "arn:aws:health:us-west-2::event/
AWS_EC2_INSTANCE_STORE_DRIVE_PERFORMANCE_DEGRADED_90353408594353980",
        "service": "EC2",
        "eventTypeCode": "AWS_EC2_INSTANCE_STORE_DRIVE_PERFORMANCE_DEGRADED",
        "eventTypeCategory": "issue",
        "eventScopeCode": "ACCOUNT_SPECIFIC",
        "communicationId": "01b0993207d81a09dcd552ebd1e633e36cf1f09a-1",
        "startTime": "Fri, 3 Jun 2022 05:01:10 GMT",
        "endTime": "Fri, 3 Jun 2022 05:30:57 GMT",
        "statusCode": "open",
        "eventRegion": "us-west-2",
        "eventDescription": [{
            "language": "en_US",
            "latestDescription": "A description of the event will be provided here"
        }],
        "affectedEntities": [{
            "entityValue": "i-abcd1111"
        }],
        "page": "1",
        "totalPages": "1",
        "affectedAccount": "123456789012"
    }
}
```

Paginação de eventos em AWS Health EventBridge

AWS Health oferece suporte à paginação de AWS Health eventos quando a lista de “recursos” ou “affectedEntities” faz com que o tamanho da mensagem EventBridge exceda o limite de 256 KB. Anteriormente, AWS Health não comunicava a lista completa de recursos com eventos quando excedia esse limite.

AWS Health agora inclui todos os “recursos” e “detalhes”. affectedEntities” na mensagem. Se esta lista de “recursos” e “detalhes”. affectedEntities” excede 256 KB e, em seguida, AWS Health divide o evento de saúde em várias páginas e publica essas páginas como mensagens individuais em. EventBridge Cada página mantém o mesmo evento ARN e ajuda communicationId a recombinar a lista de “recursos” ou “detalhes”. affectedEntities” depois que todas as páginas forem recebidas.

Essas mensagens adicionais podem causar mensagens desnecessárias, por exemplo, quando a EventBridge regra é direcionada para uma interface legível por humanos, como e-mail ou bate-papo. Clientes com notificações legíveis por humanos podem adicionar um filtro no campo “detail.page” para processar somente a primeira página, o que elimina as mensagens desnecessárias criadas nas páginas subsequentes.

Várias mudanças de esquema estão incluídas para apoiar o lançamento da paginação. communicationIdAgora, cada uma inclui o número da página hifenizada após acommunicationId, mesmo quando há apenas uma página. Há também dois novos campos, detail.page e detail. totalPages, que descrevem o número da página atual e o número total de páginas do AWS Health evento. As informações contidas em cada mensagem paginada são as mesmas, exceto pela lista de “detalhes”. affectedEntities” ou “recursos”. Essas listas podem ser reconstruídas após o recebimento de todas as páginas. As páginas dos recursos e entidades afetados são independentes de ordem.

Agregando AWS Health eventos usando a visão organizacional e o acesso de administrador delegado

AWS Health oferece suporte à visão organizacional e ao acesso delegado do administrador para AWS Health eventos publicados na Amazon EventBridge. Quando a visualização organizacional é ativada AWS Health, a conta de gerenciamento ou uma conta de administrador delegado recebe um único feed de AWS Health eventos de todas as contas da sua organização em AWS Organizations.

Esse recurso foi projetado para fornecer uma visão centralizada para ajudar a gerenciar AWS Health eventos em toda a sua organização. Configurar a visualização organizacional e uma EventBridge

regra na conta de gerenciamento não desativa EventBridge as regras para outras contas em sua organização.

Para obter mais informações sobre como habilitar a visualização organizacional e o acesso de administrador delegado em AWS Health, consulte Agregando eventos AWS Health.

Integrando monitoramento e notificações de AWS Health eventos com JIRA e ServiceNow

Você pode integrar AWS Health eventos com JIRA e ServiceNow receber informações operacionais e de conta, preparar-se para mudanças programadas e gerenciar eventos de saúde usando o Service Management Connector (SMC). A SMC integração com AWS Health pode usar eventos de saúde enviados EventBridge para criar, mapear e atualizar automaticamente JIRA tíquetes e ServiceNow incidentes.

Você pode usar a visão organizacional e o acesso delegado de administrador para gerenciar facilmente os eventos de Saúde em toda a organização JIRA e ServiceNow incorporar AWS Health informações diretamente no fluxo de trabalho da sua equipe.

Para obter mais informações sobre ServiceNow integração usando oSMC, consulte Integrando AWS Health em ServiceNow.

Para obter mais informações sobre a integração do JIRA Management Cloud usando oSMC, consulte AWS Health em JIRA.

Configurando uma EventBridge regra para enviar notificações sobre eventos no AWS Health

Você pode criar uma EventBridge regra para ser notificado sobre AWS Health eventos em sua conta. Antes de criar regras de eventos para AWS Health, 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 e no novo EventBridge — Acompanhe e responda às mudanças em seus AWS recursos.
- Crie os destinos para usar em suas regras de evento.

Para criar uma EventBridge regra para AWS Health

1. Abra o EventBridge console da Amazon em https://console.aws.amazon.com/events/.
2. Para alterar o Região da AWS, use o seletor de região no canto superior direito da página. Selecione uma região na qual você deseja rastrear eventos do AWS Health .
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 e eventos de EventBridge parceiros.
8. Em Origem do evento, para Padrão do evento selecione Serviços da AWS.
9. Em Padrão de evento, para AWS service (Serviço da AWS), escolha Saúde.
10. Em Tipo de evento, selecione uma das seguintes opções:
    - Eventos específicos de abuso de saúde: Crie uma regra para eventos AWS Health que tenham a palavra `Abuse` no nome do tipo de evento.
    - Eventos específicos de saúde — Crie uma regra para eventos específicos AWS service (Serviço da AWS), como a AmazonEC2.
11. Você pode escolher Qualquer serviço ou Serviços específicos. Se você escolher um serviço específico, escolha uma das seguintes opções:
    - Selecione Qualquer categoria de tipo de evento para criar uma regra que se aplica a todas as categorias de tipo de evento.
    - Escolha categorias específicas do tipo de evento e, em seguida, escolha um valor na lista, como problema accountNotification, ou scheduledChange.

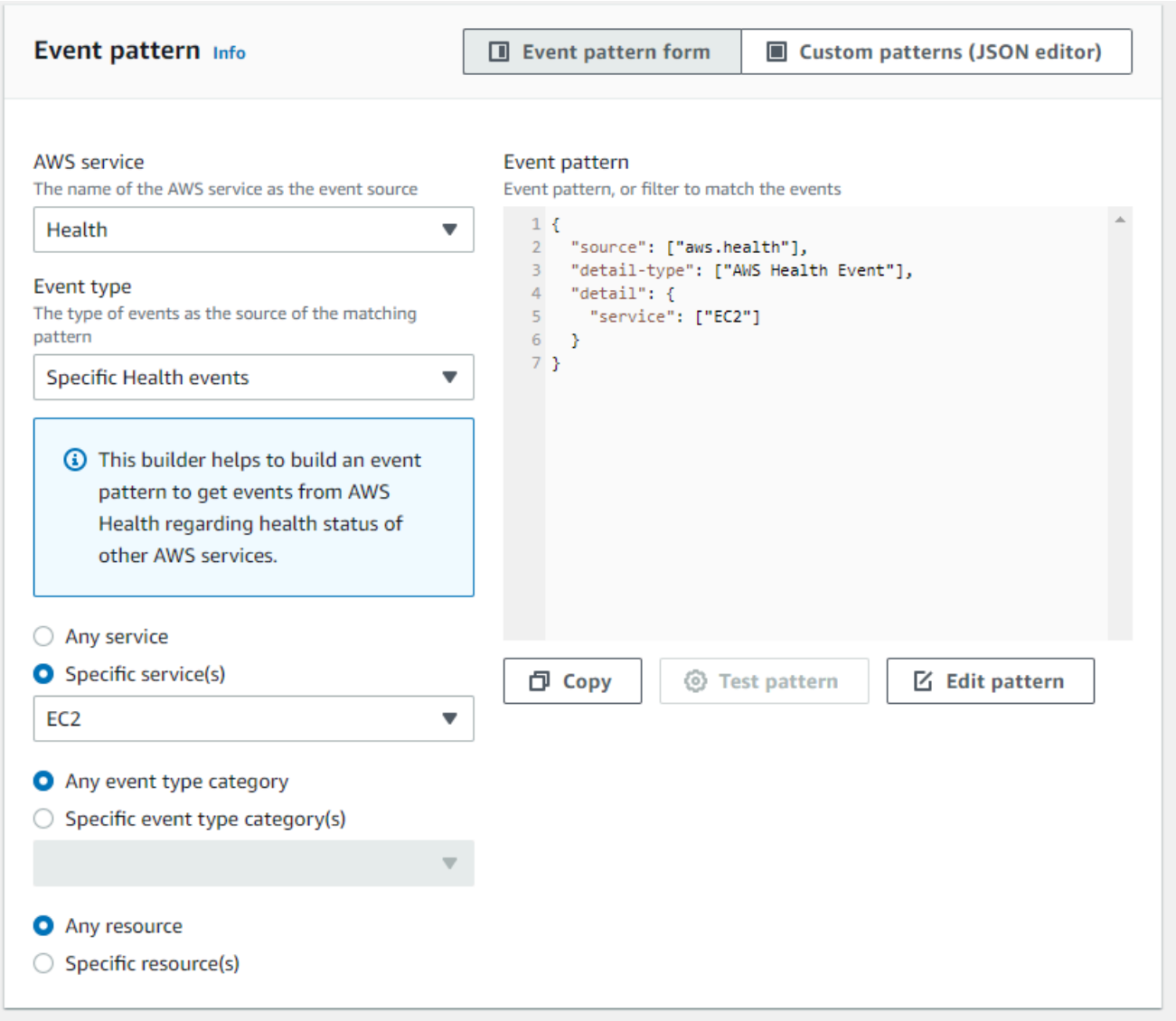
> **Tip**
>
> - Para monitorar todos os AWS Health eventos de um serviço específico, recomendamos que você escolha Qualquer categoria de tipo de evento e Qualquer recurso. Isso garante que sua regra monitore todos os eventos do AWS Health , incluindo novos códigos de tipo de evento, para o serviço especificado. Para ver um exemplo de regra, veja todos os EC2 eventos da Amazon.

- Você pode criar uma regra para monitorar mais de uma categoria de serviço ou de tipo de evento. Para fazer isso, você deve atualizar manualmente o padrão de eventos da regra. Para obter mais informações, consulte Criação de uma regra para vários serviços e categorias.

12. Se você escolheu uma categoria específica de serviço e tipo de evento, escolha uma das seguintes opções para códigos de tipo de evento.
    - Selecione Qualquer código de tipo de evento para criar uma regra que se aplica a todos os códigos de tipos de evento.
    - Selecione códigos específicos de tipo de evento e, em seguida, escolha um ou mais valores da lista. Isso cria uma regra que se aplica somente a códigos de tipo de evento específicos. Por exemplo, se você escolher **`AWS_EC2_INSTANCE_STOP_SCHEDULED`**e **`AWS_EC2_INSTANCE_RETIREMENT_SCHEDULED`**, sua regra se aplicará somente a esses eventos quando eles ocorrerem em sua conta.
13. Escolha uma das seguintes opções para os recursos afetados.
    - Escolha Qualquer ID do recurso para criar uma regra que se aplica a todos os recursos.
    - Escolha o (s) recurso (s) específico (s) e insira um ou mais recursos. IDs Por exemplo, você pode especificar um ID de EC2 instância da Amazon, como *`i-EXAMPLEa1b2c3de4`*, para monitorar eventos que afetam somente esse recurso.
14. Analise a configuração da regra para garantir que ela atenda aos requisitos de monitoramento de eventos.
15. Escolha Próximo.
16. Na página Selecionar destinos, escolha o tipo de destino criado para essa regra e, em seguida, configure quaisquer opções adicionais necessárias para esse tipo. Por exemplo, você pode enviar o evento para uma SQS fila da Amazon ou para um SNS tópico da Amazon.
17. Escolha Próximo.
18. (Opcional) Na página Configurar tags, adicione tags e escolha Próximo.
    - Observação: no momento, as tags não são enviadas pela fonte aws.health em. EventBridge
19. Na página Analisar e criar, analise a configuração da regra garantindo que ela atenda aos requisitos de monitoramento de eventos.
20. Escolha Criar regra.

Example : Regra para todos os EC2 eventos da Amazon

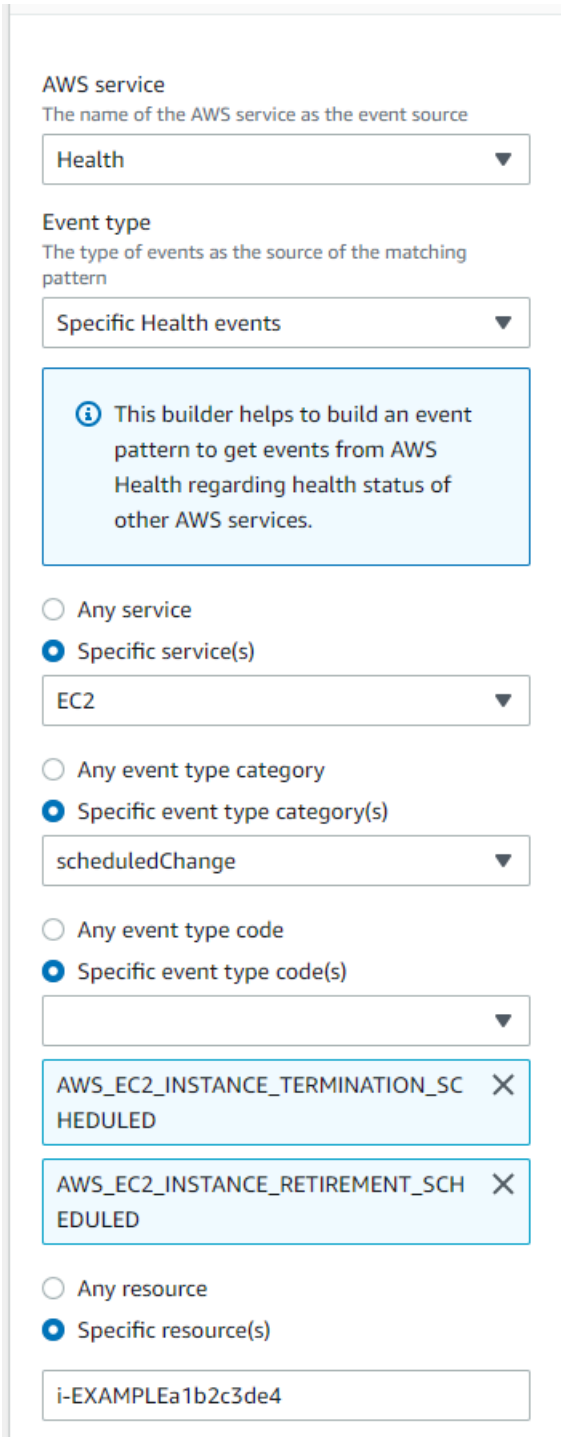
O exemplo a seguir cria uma regra para EventBridge monitorar todos os EC2 eventos da Amazon, incluindo categorias de tipos de eventos, códigos de eventos e recursos.



Example : Regra para EC2 eventos específicos da Amazon

O exemplo a seguir cria uma regra para EventBridge monitorar o seguinte:

- O EC2 serviço da Amazon
- A categoria scheduledChangedo tipo de evento
- Os códigos de tipo de evento para `AWS_EC2_INSTANCE_TERMINATION_SCHEDULED` e `AWS_EC2_INSTANCE_RETIREMENT_SCHEDULED`
- A instância com o ID `i-EXAMPLEa1b2c3de4`



Criação de uma regra para vários serviços e categorias

Os exemplos do procedimento anterior mostram como criar uma regra para uma única categoria de serviço e tipo de evento. Você também pode criar uma regra para vários serviços e categorias de tipos de eventos. Isso significa que você não precisa criar uma regra separada para cada serviço e categoria que você deseja monitorar. Para isso, você deve criar uma lista de funções.

Você pode usar uma das opções a seguir:

Para adicionar serviços e categorias a uma regra existente

1. No EventBridge console, na página Regras, escolha o nome da regra.
2. No canto superior direito, escolha Editar.
3. Escolha Próximo.
4. Em Padrão de evento, escolha Editar padrão e, em seguida, insira suas alterações no campo de texto.
5. Escolha Avançar até chegar à página Revisar e atualizar.
6. Escolha Atualizar regra para salvar suas alterações.

Para adicionar serviços e categorias a uma nova regra

1. Para fazer isso, siga o procedimento em Configurando uma EventBridge regra para enviar notificações sobre eventos no AWS Health para a etapa 9.
2. Em vez de escolher um único serviço ou categoria nas listas, em Padrão de evento, escolha Editar padrão.
3. Insira suas alterações no campo de texto. Consulte o exemplo de padrão a seguir como modelo para criar seu próprio padrão de evento.
4. Revise seu padrão de eventos e siga o restante do procedimento Configurando uma EventBridge regra para enviar notificações sobre eventos no AWS Health para criar sua regra.

Use o API ou AWS Command Line Interface (AWS CLI)

Para uma regra nova ou existente, use a PutRuleAPIoperação ou o `aws events put-rule` comando para atualizar o padrão do evento. Para ver um exemplo de AWS CLI comando, consulte put-rule na Referência de AWS CLI Comandos.

Example Exemplo: vários serviços e categorias de tipos de eventos

O padrão de evento a seguir cria uma regra para monitorar eventos para as categorias `issue`e `accountNotification`, e tipo de `scheduledChange` evento para três AWS serviços: AmazonEC2, Amazon EC2 Auto Scaling e Amazon. VPC

```
{
  "detail": {
```

```
    "eventTypeCategory": [
      "issue",
      "accountNotification",
      "scheduledChange"
    ],
    "service": [
      "AUTOSCALING",
      "VPC",
      "EC2"
    ]
  },
  "detail-type": [
    "AWS Health Event"
  ],
  "source": [
    "aws.health"
  ]
}
```

Configurando AWS Chatbot para enviar notificações sobre eventos em AWS Health

Você pode receber AWS Health eventos diretamente em seus clientes de bate-papo, como Slack e Amazon Chime. Você pode usar esse evento para identificar problemas AWS de serviço recentes que possam afetar seus AWS aplicativos e sua infraestrutura. Em seguida, você pode entrar no seu AWS Health Dashboard para saber mais sobre a atualização. Por exemplo, se você estiver monitorando o tipo de `AWS_EC2_INSTANCE_STOP_SCHEDULED` evento em sua AWS conta, o AWS Health evento poderá aparecer diretamente no seu canal do Slack.

Pré-requisitos

Antes de começar, você precisa fazer o seguinte:

- Um cliente de bate-papo configurado com AWS Chatbot. Você pode configurar o Amazon Chime e Slack. Para obter mais informações, consulte Conceitos básico com AWS Chatbot no Guia de administração do AWS Chatbot .
- Um SNS tópico da Amazon que você criou e no qual está inscrito. Se você já tem um SNS tópico, pode usar um já existente. Para obter mais informações, consulte Introdução à Amazon SNS no Guia do desenvolvedor do Amazon Simple Notification Service.

Para receber AWS Health eventos com AWS Chatbot

1. Siga o procedimento no Configurando uma EventBridge regra para enviar notificações sobre eventos no AWS Health até a etapa 13.

   a. Ao terminar de configurar o padrão de eventos na etapa 13, adicione uma vírgula na última linha do padrão e adicione a linha a seguir para remover mensagens de bate-papo desnecessárias dos eventos AWS Health paginados. Consulte Paginação de eventos em AWS Health EventBridge.

      ```
      "detail.page": ["1"]
      ```

   b. Ao escolher o alvo na etapa 14, escolha um SNS tópico. Você usará esse mesmo SNS tópico no AWS Chatbot console.

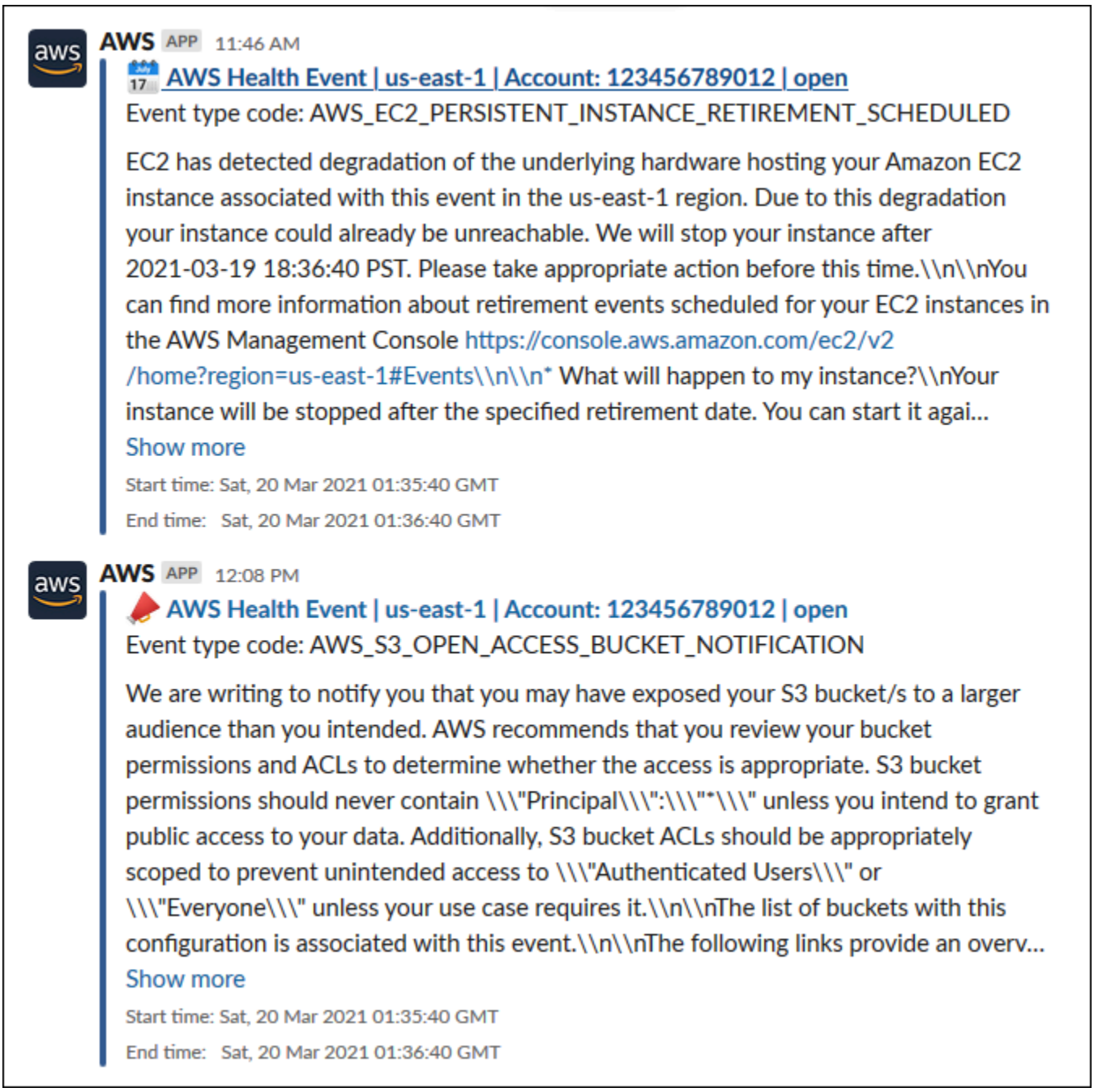
   c. Conclua o restante do procedimento para criar a regra.

2. Navegue até o console do AWS Chatbot.
3. Escolha seu cliente de bate-papo, como o nome do canal do Slack, e escolha Editar.
4. Na seção Notificações - opcional, em Tópicos, escolha o mesmo SNS tópico que você especificou na etapa 1.
5. Escolha Salvar.

   Quando AWS Health enviar um evento para EventBridge que corresponda à sua regra, o AWS Health evento aparecerá no seu cliente de chat.
6. Escolha o nome do evento para ver mais informações em seu AWS Health painel.

Example : AWS Health eventos enviados para o Slack

Veja a seguir um exemplo de dois AWS Health eventos para a Amazon EC2 e o Amazon Simple Storage Service (Amazon S3) na região Leste dos EUA (Norte da Virgínia) que aparecem no canal do Slack.



Executando operações em EC2 instâncias automaticamente em resposta a eventos em AWS Health

Você pode automatizar ações que respondem a eventos programados para suas EC2 instâncias da Amazon. Ao AWS Health enviar um evento para sua AWS conta, sua EventBridge regra pode então invocar alvos, como documentos de AWS Systems Manager automação, para automatizar ações em seu nome.

Por exemplo, quando um evento de desativação de EC2 instância da Amazon é agendado para uma EC2 instância apoiada pela Amazon Elastic Block Store (AmazonEBS), AWS Health enviará o tipo de `AWS_EC2_PERSISTENT_INSTANCE_RETIREMENT_SCHEDULED` evento para o seu AWS Health painel. Quando sua regra detecta esse tipo de evento, você pode automatizar a parada e o início da instância. Assim, você não precisa realizar essas ações manualmente.

> **Note**
>
> Para automatizar ações para suas EC2 instâncias da Amazon, as instâncias devem ser gerenciadas pelo Systems Manager.

Para obter mais informações, consulte Automatizar a Amazon EC2 com EventBridge o Guia EC2do usuário da Amazon.

Pré-requisitos

Você deve criar uma política AWS Identity and Access Management (IAM), criar uma IAM função e atualizar a política de confiança da função antes de criar uma regra.

Crie uma IAM política

Siga esse procedimento para criar uma política gerenciada pelo cliente para seu perfil. Essa política concede permissão ao perfil para realizar ações para você. Esse procedimento usa o editor JSON de políticas no IAM console.

Para criar uma política do IAM

1. Faça login no AWS Management Console e abra o IAM console em https://console.aws.amazon.com/iam/.
2. No painel de navegação, escolha Policies.
3. Escolha Criar política.
4. Escolha a JSONguia.
5. Copie o seguinte JSON e, em seguida, substitua o padrão JSON no editor.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```
      "Effect": "Allow",
      "Action": [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:DescribeInstanceStatus"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ssm:*"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "sns:Publish"
      ],
      "Resource": [
        "arn:aws:sns:*:*:Automation*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:PassRole"
      ],
      "Resource": "arn:aws:iam::123456789012:role/AutomationEVRole"
    }
  ]
}
```

a. No `Resource` parâmetro, para o Amazon Resource Name (ARN), insira o ID AWS da sua conta.

b. Você também pode substituir o nome da função ou usar o padrão. Este exemplo usa *`AutomationEVRole`*.

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 Revisar política, insira um Nome, como *AutomationEVRolePolicy* e uma Descrição opcional.
10. Revise a página Resumo para ver as permissões que a política permite e, em seguida, escolha Criar política. Quando estiver satisfeito com a política, escolha Criar política.

Essa política define as ações que o perfil pode realizar. Para obter mais informações, consulte Criação de IAM políticas (console) no Guia IAM do usuário.

Crie uma IAM função

Depois de criar a política, você deve criar uma IAM função e, em seguida, anexar a política a essa função.

Para criar uma função para um AWS serviço

1. Faça login no AWS Management Console e abra o IAM console em https://console.aws.amazon.com/iam/.
2. No painel de navegação, escolha Funções e Criar função.
3. Em Selecionar tipo de entidade confiável, selecione AWS serviço .
4. Escolha EC2o serviço que você deseja permitir que assuma essa função.
5. Selecione Next: Permissions (Próximo: permissões).
6. Insira o nome da política que você criou, como *AutomationEVRolePolicy*e, em seguida, marque a caixa de seleção ao lado da política.
7. Escolha Próximo: tags.
8. (Opcional) Para adicionar metadados ao perfil, use tags como pares de chave-valor.
9. Escolha Próximo: revisar.
10. Em Nome da função, insira *AutomationEVRole*. Esse nome deve ser o mesmo nome que aparece na ARN IAM política que você criou.
11. (Opcional) Em Descrição da função, digite uma descrição para a função.
12. Revise a função e escolha Criar função.

Para obter mais informações, consulte Criação de uma função para um AWS serviço no Guia IAM do usuário.

Atualize a política de confiança.

Por último, você pode atualizar a política de confiança para a função que você criou. Você deve concluir esse procedimento para poder escolher essa função no EventBridge console.

Para atualizar a política de confiança de uma função

1. Faça login no AWS Management Console e abra o IAM console em https://console.aws.amazon.com/iam/.
2. No painel de navegação, escolha Perfis.
3. Na lista de funções em sua AWS conta, escolha o nome da função que você criou, como *AutomationEVRole*.
4. Escolha a guia Relacionamentos de confiança e, em seguida, selecione Editar relacionamento de confiança.
5. Para Documento de política, copie o seguinteJSON, remova a política padrão e cole a cópia JSON em seu lugar.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "ssm.amazonaws.com",
                    "events.amazonaws.com"
                ]
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

6. Escolha Update Trust Policy.

Para obter mais informações, consulte Modificar a política de confiança de uma função (console) no Guia do IAM usuário.

Crie uma regra para EventBridge

Siga este procedimento para criar uma regra no EventBridge console para que você possa automatizar a parada e o início das EC2 instâncias que estão programadas para serem desativadas.

Para criar uma regra EventBridge para ações automatizadas do Systems Manager

1. Abra o EventBridge console da Amazon em https://console.aws.amazon.com/events/.
2. No painel de navegação, em Eventos, escolha Regras.
3. Na página Criar regra, insira um Nome e Descrição para sua regra.
4. Em Definir padrão, escolha Padrão de evento e escolha Padrão predefinido por serviço.
5. Para Provedor de serviços, escolha AWS.
6. Em Nome do serviço, selecione Integridade.
7. Para Tipo de evento, escolha Eventos de integridade específicos.
8. Escolha serviços específicos e, em seguida, escolha EC2.
9. Escolha categorias específicas do tipo de evento e, em seguida, escolha scheduledChange.
10. Escolha os códigos de tipos de eventos específicos e, em seguida, escolha o código do tipo de evento.

    Por exemplo, para instâncias EC2 EBS apoiadas pela Amazon, escolha**AWS_EC2_PERSISTENT_INSTANCE_RETIREMENT_SCHEDULED**.
    Para EC2 instâncias com armazenamento de instâncias da Amazon, escolha. **AWS_EC2_INSTANCE_RETIREMENT_SCHEDULED**
11. Escolha Qualquer recurso.

    O Padrão de evento terá aparência semelhante ao exemplo a seguir.

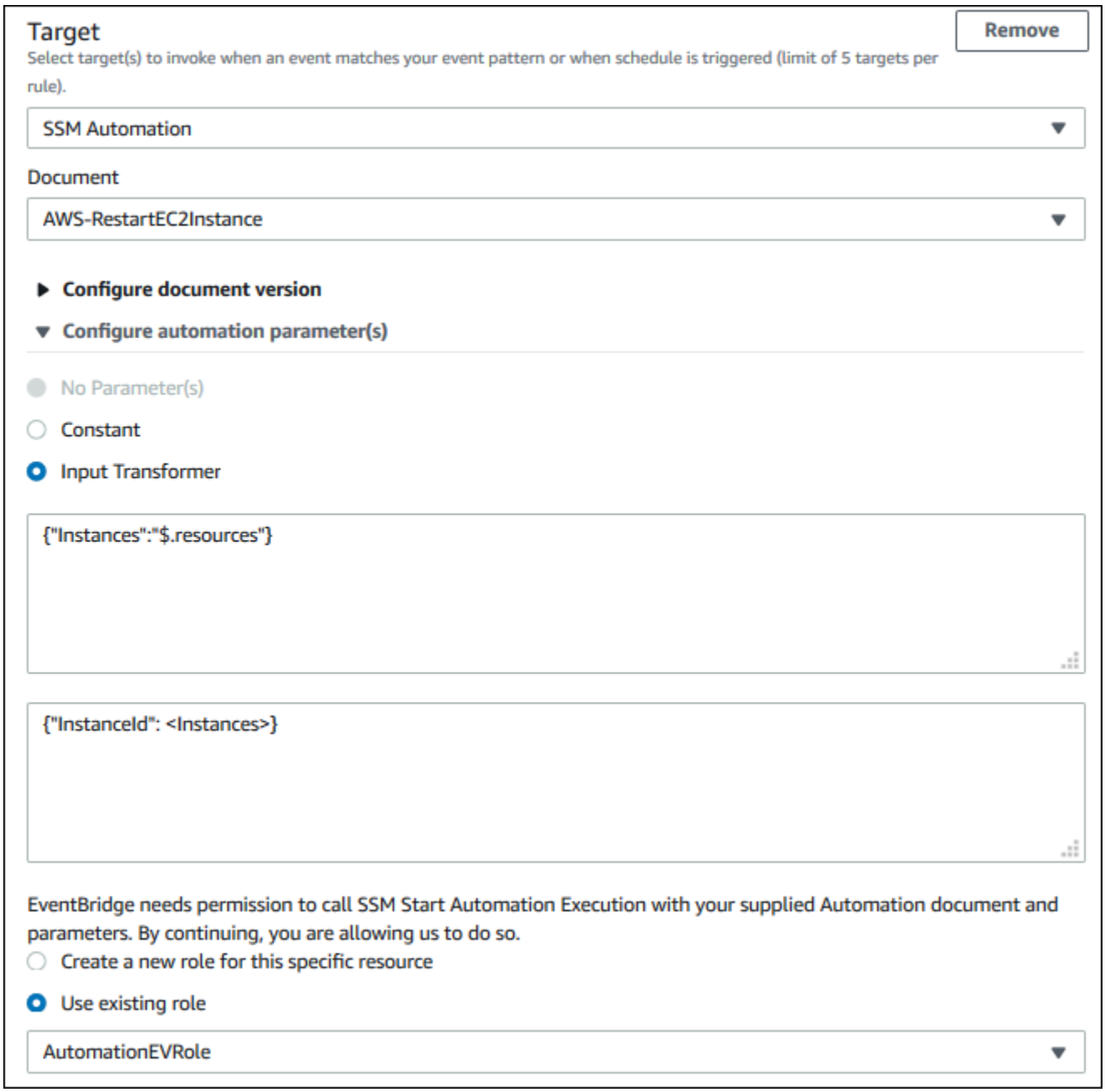
    Example

```
{
  "source": [
    "aws.health"
  ],
  "detail-type": [
    "AWS Health Event"
  ],
  "detail": {
    "service": [
```

```
      "EC2"
    ],
    "eventTypeCategory": [
      "scheduledChange"
    ],
    "eventTypeCode": [
      "AWS_EC2_PERSISTENT_INSTANCE_RETIREMENT_SCHEDULED"
    ]
  }
}
```

12. Adicione o destino do documento de automação do gerenciador de sistema. Em Selecionar alvos, em Alvo, escolha SSMAutomação.
13. Para Documento, escolha `AWS-RestartEC2Instance`.
14. Expanda Configurar parâmetros de automação e selecione Transformador de entrada.
15. Para o campo Caminho de entrada, insira **`{"Instances":"$.resources"}`**.
16. Para o segundo campo, insira **`{"InstanceId": <Instances>}`**.
17. Escolha Usar função existente e, em seguida, escolha a IAM função que você criou, como *`AutomationEVRole`*.

    O destino deve ser como o exemplo a seguir.



> **Note**
>
> Se você não tiver uma IAM função existente com as permissões necessárias EC2 e o relacionamento confiável do Systems Manager, sua função não aparecerá na lista. Para obter mais informações, consulte Pré-requisitos.

18. Escolha Criar.

Se ocorrer um evento em sua conta que corresponda à sua regra, EventBridge enviará o evento para o alvo especificado.

Monitoramento AWS Health

O monitoramento é uma parte importante da manutenção da confiabilidade, disponibilidade e desempenho de AWS Health suas outras AWS soluções. AWS fornece as seguintes ferramentas de monitoramento para observar AWS Health, relatar quando algo está errado e tomar medidas quando apropriado:

- A Amazon CloudWatch monitora seus AWS recursos e os aplicativos em que você executa AWS em tempo real. É possível coletar e rastrear métricas, criar painéis personalizados e definir alarmes que o notificam ou que realizam ações quando uma métrica especificada atinge um limite definido. Para obter mais informações, consulte o Guia CloudWatch do usuário da Amazon.

  Você pode usar a Amazon EventBridge para ser notificado sobre AWS Health eventos que possam afetar seus serviços e recursos. Por exemplo, se AWS Health publicar um evento sobre suas EC2 instâncias da Amazon, você pode usar essas notificações para agir e atualizar ou substituir seus recursos conforme necessário. Para obter mais informações, consulte Monitorando eventos AWS Health com a Amazon EventBridge.
- AWS CloudTrail captura API chamadas 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

Registrando AWS Health API chamadas com AWS CloudTrail

AWS Health é integrado com AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, função ou AWS serviço em AWS Health. CloudTrail captura API chamadas AWS Health como eventos. As chamadas capturadas incluem chamadas do AWS Health console e chamadas de código para as AWS Health API operações. Se você criar uma trilha, poderá habilitar a entrega contínua de CloudTrail eventos para um bucket do Amazon S3, incluindo eventos para. AWS Health 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 Health, 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 Health informações em CloudTrail

CloudTrail é ativado em sua AWS conta quando você cria a conta. Quando uma atividade de evento suportada ocorre em AWS Health, 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 Health, 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, a trilha se aplica a todas as AWS regiões. A trilha loga eventos de todas as Regiões na partição da AWS e entrega os arquivos de log para o bucket do Amazon S3 especificado por você. Além disso, você pode configurar outros AWS serviços para analisar e agir com base nos dados de eventos coletados nos CloudTrail registros. Para obter mais informações, consulte as informações a seguir.

- Visão Geral para Criar uma Trilha
- CloudTrail Serviços e integrações compatíveis
- Configurando as SNS notificações da Amazon para CloudTrail
- Recebendo arquivos de CloudTrail log de várias regiões e recebendo arquivos de CloudTrail log de várias contas

Todas AWS Health API as operações são registradas CloudTrail e documentadas na AWS Health APIReferência. Por exemplo, chamadas para as `DescribeAffectedEntities` operações `DescribeEventsDescribeEventDetails`, e geram entradas nos arquivos de CloudTrail log.

AWS Health suporta o registro das seguintes ações como eventos em arquivos de CloudTrail log:

- Se a solicitação foi feita com root ou IAM credenciais
- Se a solicitação foi feita com credenciais de segurança temporárias de um perfil ou de um usuário federado
- Se a solicitação foi feita por outro AWS serviço

Para obter mais informações, consulte o CloudTrail userIdentityElemento.

Você pode armazenar seus arquivos de log no seu bucket do Amazon S3 pelo tempo que quiser. Você também pode definir as regras de ciclo de vida do Amazon S3 para arquivar ou excluir os arquivos de log automaticamente. Por padrão, seus arquivos de log são criptografados com a criptografia do lado do servidor Amazon S3 (). SSE

Para ser notificado sobre a entrega do arquivo de log, você pode configurar CloudTrail para publicar SNS notificações da Amazon quando novos arquivos de log forem entregues. Para obter mais informações, consulte Configurando as SNS notificações da Amazon para CloudTrail.

Você também pode agregar arquivos de AWS Health log de várias AWS regiões e várias AWS contas em um único bucket do Amazon S3.

Para obter mais informações, consulte Recebendo arquivos de CloudTrail log de várias regiões e Recebendo arquivos de CloudTrail log de várias contas.

Exemplo: entradas do arquivo de AWS Health 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 API chamadas públicas, portanto, eles não aparecem em nenhuma ordem específica.

O exemplo a seguir mostra uma entrada de CloudTrail registro que demonstra a DescribeEntityAggregatesoperação.


```
{
   "Records": [
   {
   "eventVersion": "1.05",
   "userIdentity": {
      "type": "IAMUser",
      "principalId": "AIDACKCEVSQ6C2EXAMPLE",
      "arn": "arn:aws:iam::123456789012:user/JaneDoe",
      "accountId": "123456789012",
      "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
      "userName": "JaneDoe",
      "sessionContext": {"attributes": {
```

```
         "mfaAuthenticated": "false",
         "creationDate": "2016-11-21T07:06:15Z"
      }},
      "invokedBy": "AWS Internal"
    },
   "eventTime": "2016-11-21T07:06:28Z",
   "eventSource": "health.amazonaws.com",
   "eventName": "DescribeEntityAggregates",
   "awsRegion": "us-east-1",
   "sourceIPAddress": "203.0.113.0",
   "userAgent": "AWS Internal",
   "requestParameters": {"eventArns": ["arn:aws:health:us-east-1::event/EBS/
EBS_LOST_VOLUME/EBS_LOST_VOLUME_123"]},
   "responseElements": null,
   "requestID": "05b299bc-afb9-11e6-8ef4-c34387f40bd4",
   "eventID": "e4deb9dc-dbc2-4bdb-8515-73e8abcbc29b",
   "eventType": "AwsApiCall",
   "recipientAccountId": "123456789012"
   }
   ],
   ...
}
```

Histórico do documento para AWS Health

A tabela a seguir descreve a documentação desta versão do AWS Health.

- APIversão: 2016-08-04

A tabela a seguir descreve atualizações importantes na AWS Health documentação, a partir de 28 de agosto de 2020. Você pode se inscrever no RSS feed para receber notificações sobre as atualizações.

Alteração	Descrição	Data
Corrigido JSON em Monitoramento de AWS Health eventos com a Amazon EventBridge	Para obter mais informações, consulte Monitoramento de AWS Health eventos com a Amazon EventBridge.	3 de setembro de 2024
Informações atualizadas sobre o download dos recursos afetados	Para obter mais informações, consulte a visualização Recursos afetados.	27 de julho de 2024
Removida a privacidade do tráfego entre redes da documentação da seção AWS Health Segurança	Para obter mais informações, consulte Segurança em AWS Health.	27 de março de 2024
Atualizou o AWS Health painel — Eventos de integridade do serviço e ciclo de vida planejado para AWS Health documentação.	Para obter mais informações, consulte AWS Health Painel — Eventos de integridade do serviço e ciclo de vida planejado para. AWS Health	15 de fevereiro de 2024
Um marcador duplicado foi removido em Criação EventBridge de uma regra para AWS Health	Um marcador duplicado foi removido em Criação de EventBridge uma regra para. AWS Health	4 de dezembro de 2023

Documentação acrescentada para eventos planejados de ciclo de vida	Para obter mais informações, consulte Eventos de ciclo de vida do AWS Health.	31 de outubro de 2023
Documentação atualizada para `AWSHealthFullAccess`	Agora você pode usar a `AWSHealthFullAccess` política gerenciada em AWS GovCloud (US) Regions. Consulte as políticas AWS gerenciadas para AWS Health.	16 de outubro de 2023
Documentação adicionada para configurar as notificações AWS do usuário no AWS Health.	Agora você pode configurar as notificações AWS do usuário em AWS Health. Para obter mais informações, consulte Configurar notificações de AWS usuário para AWS Health.	30 de agosto de 2023
A documentação do recurso de administrador delegado foi adicionada à seção Agregação de AWS Health eventos.	Para obter mais informações, consulte Administrador delegado de organização.	27 de julho de 2023
SLRatualização da política	Atualização da política AWS gerenciada: Health_OrganizationsServiceRolePolicy. Para obter mais informações, consulte AWS Políticas gerenciadas para o AWS Health.	19 de julho de 2023

AWS Health o esquema agora oferece suporte a metadados de eventos	Agora você pode receber metadados de AWS Health eventos. Para obter mais informações, consulte Monitoramento de AWS Health eventos com a Amazon EventBridge.	20 de junho de 2023
Documentação atualizada para a Amazon EventBridge	Agora você pode usar uma EventBridge regra da Amazon para monitorar eventos públicos e específicos da conta. Para obter mais informações, consulte Monitoramento de AWS Health eventos com a Amazon EventBridge.	2 de maio de 2023
Documentação adicionada para políticas AWS gerenciadas	Documentação acrescentada para as políticas gerenciadas AWS para AWS Health e o Uso de funções vinculadas a serviços para AWS Health.	18 de janeiro de 2023
Documentação de configuração de fuso horário adicionada	Use o novo recurso de fuso horário para visualizar o AWS Health Painel em seu fuso horário local ou emUTC. Para obter mais informações, consulte Introdução ao seu AWS Health Painel — Saúde da sua conta e AWS Health Painel — Integridade do serviço.	21 de setembro de 2022

Documentação atualizada	Documentação adicionada para o AWS Health Aware. Para obter mais informações, consulte AWS Health redis.	25 de maio de 2022
Documentação atualizada	O Service Health Dashboard e o AWS Personal Health Dashboard foram renomeados para o Dashboard. AWS Health Para obter mais informações, consulte Introdução ao seu AWS Health Painel — Saúde da sua conta e AWS Health Painel — Integridade do serviço.	28 de fevereiro de 2022
Documentação atualizada para a Amazon EventBridge	Novo tópico AWS Health para usar a Amazon EventBridge para monitorar eventos de Saúde. Para obter mais informações, consulte Monitoramento de AWS Health eventos com a Amazon EventBridge.	3 de fevereiro de 2022
Documentação atualizada	Se você tiver um plano Enterprise On-Ramp Support, você pode usar o. AWS Health API	24 de novembro de 2021
Documentação acrescentada	Novo tópico para AWS Health conceitos. Para obter mais informações, consulte Conceitos do AWS Health.	29 de julho de 2021

Documentação atualizada para CloudWatch eventos	Foi adicionada uma seção sobre como criar uma regra para vários serviços e categorias de tipos de eventos. Para obter mais informações, consulte Criação de uma regra para vários serviços e categorias.	7 de maio de 2021
Documentação atualizada para CloudWatch eventos	A seção foi atualizada para automatizar AWS Systems Manager as ações das regras do Amazon CloudWatch Events. Para obter mais informações, consulte Automação de ações para instâncias da Amazon EC2.	28 de abril de 2021
Documentação atualizada para CloudWatch eventos	Foi adicionada uma seção para receber AWS Health eventos em seu cliente de bate-papo. Para obter mais informações, consulte Recebendo AWS Health eventos com AWS Chatbot.	16 de março de 2021

Documentação atualizada	Os tópicos a seguir foram atualizados: • Atualizado o tópico Agregação de eventos de AWS Health • Reorganizou e atualizou o tópico Monitor de AWS Health eventos com Amazon CloudWatch Events • Atualizou a seção de condições baseadas em recursos e ações	29 de janeiro de 2021
Adicionado o AWS Health painel para visualização organizacional no AWS Health console	Você pode usar o AWS Health console para ativar o recurso de visualização organizac ional. Em seguida, você pode visualizar os eventos de saúde das contas dos membros em sua organização AWS .	14 de dezembro de 2020
Demonstração de endpoint de alta disponibilidade	Você pode usar o código de exemplo para determinar o endpoint regional ativo e a AWS região de assinatura para AWS Health.	22 de outubro de 2020
Atualizações no Guia do usuário AWS Health	A organização atualizou e adicionou um RSS feed para que você possa se inscrever para receber as atualizações mais recentes da AWS Health documentação.	28 de agosto de 2020

Atualizações anteriores

Alteração	Descrição	Data
Atualizado o tópico de visualização organizacional para incluir exemplos.	Consulte Agregando AWS Health eventos em todas as contas.	3 de junho de 2020
Segurança e AWS Health	Adição de informações sobre considerações de segurança no uso do AWS Health. Consulte Segurança em AWS Health.	5 de maio de 2020
Adição de uma nova seção para explicar como usar a visualização organizacional para eventos agregados em todas as contas no AWS Organizations.	Consulte Agregando AWS Health eventos em todas as contas.	18 de dezembro de 2019
Foi adicionada uma nova seção “Condições baseadas em recursos e ações” para explicar as restrições de eventos oferecidas pela. AWS Health API	Consulte Gerenciamento de identidade e acesso para o AWS Health.	2 de agosto de 2018
Foi adicionada uma nota sobre a visibilidade das AWS Health informações.	Consulte Gerenciamento de identidade e acesso para o AWS Health.	16 de agosto de 2017
Liberação de serviços.	AWS Health lançado.	1° de dezembro de 2016

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.