Manual do usuário

AWS CloudTrail

Versão 1.0

AWS CloudTrail: Manual do usuário

Table of Contents

O que é AWS CloudTrail?

AWS CloudTrail é um AWS service (Serviço da AWS) que ajuda você a possibilitar a auditoria operacional e de risco, a governança e a conformidade do seu Conta da AWS. As ações realizadas por um usuário, função ou AWS serviço são registradas como eventos em CloudTrail. Os eventos incluem ações realizadas no AWS Management Console, AWS Command Line Interface, e AWS SDKs e APIs.

CloudTrail está ativo no seu Conta da AWS quando você o cria. Quando ocorre uma atividade em seu Conta da AWS, essa atividade é registrada em um CloudTrail evento.

CloudTrail fornece três maneiras de registrar eventos:

- Histórico de eventos: o Histórico de eventos fornece um registro visualizável, pesquisável, baixável e imutável dos últimos 90 dias de eventos de gerenciamento em uma Região da AWS. É possível pesquisar eventos filtrando-os por um único atributo. Você recebe acesso automático ao Histórico de eventos ao criar sua conta. Para ter mais informações, consulte Trabalhando com o histórico de CloudTrail eventos.

  Não há CloudTrail cobrança pela visualização do histórico de eventos.
- CloudTrail Lake — AWS CloudTrail Lake é um data lake gerenciado para capturar, armazenar, acessar e analisar a atividade do usuário e da API AWS para fins de auditoria e segurança. CloudTrail O Lake converte eventos existentes no formato JSON baseado em linhas para o formato Apache ORC. O ORC é um formato colunar de armazenamento otimizado para recuperação rápida de dados. Os eventos são agregados em armazenamentos de dados de eventos, que são coleções imutáveis de eventos com base nos critérios que você seleciona aplicando seletores de eventos avançados. Você pode manter os dados do evento em um armazenamento de dados de eventos por até 3.653 dias (cerca de 10 anos) se escolher a opção de preço de retenção extensível de um ano ou até 2.557 dias (cerca de 7 anos) se escolher a opção de preço de retenção por sete anos. Você pode criar um armazenamento de dados de eventos para um único Conta da AWS ou para vários Contas da AWS usando AWS Organizations. Você pode importar todos CloudTrail os registros existentes de seus buckets do S3 para um armazenamento de dados de eventos novo ou existente. Você também pode visualizar as principais tendências de CloudTrail eventos com os painéis do Lake. Para ter mais informações, consulte Trabalhando com AWS CloudTrail Lake.

  CloudTrail Os armazenamentos e consultas de dados de eventos em Lake incorrem em cobranças. Ao criar um armazenamento de dados de eventos, você escolhe a opção de

preço que deseja usar para ele. A opção de preço determina o custo para a ingestão e para o armazenamento de eventos, e o período de retenção padrão e máximo para o armazenamento de dados de eventos. Ao executar consultas no Lake, você paga de acordo com a quantidade de dados examinados. Para obter informações sobre CloudTrail preços e gerenciamento de custos do Lake, consulte AWS CloudTrail Preços Gerenciando os custos CloudTrail do Lake e.

- Trilhas — As trilhas capturam um registro das AWS atividades, entregando e armazenando esses eventos em um bucket do Amazon S3, com entrega opcional para a CloudWatch Logs e a Amazon. EventBridge Você pode inserir esses eventos em suas soluções de monitoramento de segurança. Você também pode usar suas próprias soluções de terceiros ou soluções como o Amazon Athena para pesquisar e analisar seus CloudTrail registros. Você pode criar trilhas para uma Conta da AWS ou várias Contas da AWS usando AWS Organizations. Você pode registrar eventos do Insights para analisar seus eventos de gerenciamento em busca de comportamento anômalo nos volumes de chamadas a APIs e em suas taxas de erros. Para ter mais informações, consulte Criando uma trilha para o seu Conta da AWS.

  Você pode entregar uma cópia dos seus eventos de gerenciamento contínuos para o bucket do S3 sem nenhum custo CloudTrail criando uma trilha. No entanto, há cobranças de armazenamento do Amazon S3. Para obter mais informações sobre CloudTrail preços, consulte AWS CloudTrail Preços. Para receber informações sobre a definição de preço do Amazon S3, consulte Definição de preço do Amazon S3.

A visibilidade AWS da atividade da sua conta é um aspecto fundamental das melhores práticas operacionais e de segurança. Você pode usar CloudTrail para visualizar, pesquisar, baixar, arquivar, analisar e responder à atividade da conta em toda a sua AWS infraestrutura. Você pode identificar quem ou o que tomou qual ação, quais recursos foram utilizados, quando o evento ocorreu e outros detalhes para ajudá-lo a analisar e responder às atividades em sua AWS conta.

Você pode se CloudTrail integrar aos aplicativos usando a API, automatizar a criação de repositórios de dados de trilhas ou eventos para sua organização, verificar o status dos armazenamentos de dados de eventos e das trilhas que você cria e controlar como os usuários visualizam os CloudTrail eventos.

Acessando CloudTrail

Você pode trabalhar com CloudTrail qualquer uma das seguintes formas.

Tópicos

- CloudTrail console
- AWS CLI
- CloudTrail APIs
- AWS SDKs

CloudTrail console

Faça login no AWS Management Console e abra o CloudTrail console em https://console.aws.amazon.com/cloudtrail/.

O CloudTrail console fornece uma interface de usuário para realizar várias CloudTrail tarefas, como:

- Visualizando eventos recentes e histórico de eventos da sua AWS conta.
- Baixar um arquivo filtrado ou completo dos últimos 90 dias de eventos de gerenciamento do histórico de eventos.
- Criação e edição de CloudTrail trilhas.
- Criação e edição de armazenamentos de dados de eventos do CloudTrail Lake.
- Execução de consultas em armazenamentos de dados de eventos.
- Configuração de CloudTrail trilhas, incluindo:
  - Seleção de um bucket do Amazon S3 para trilhas.
  - Definir um prefixo.
  - Configurando a entrega para o CloudWatch Logs.
  - Usando AWS KMS chaves para criptografia de dados de trilhas.
  - Habilitação de notificações do Amazon SNS para entrega de arquivos de log em trilhas.
  - Adicione e gerencie as tags de suas trilhas.
- Configurando armazenamentos de dados de eventos do CloudTrail Lake, incluindo:
  - Integrando armazenamentos de dados de eventos com CloudTrail parceiros ou com seus próprios aplicativos, para registrar eventos de fontes externas. AWS
  - Federando armazenamentos de dados de eventos para executar consultas do Amazon Athena.
  - Usando AWS KMS chaves para criptografia de dados do armazenamento de dados de eventos.
  - Adição e gerenciamento de tags para seus armazenamentos de dados de eventos.

Para obter mais informações sobre o AWS Management Console, consulte AWS Management Console.

AWS CLI

AWS Command Line Interface É uma ferramenta unificada que você pode usar para interagir na linha CloudTrail de comando. Para mais informações, consulte o Guia do usuário do AWS Command Line Interface. Para ver uma lista completa dos comandos da CloudTrail CLI, consulte cloudtrail e cloudtrail-data na Referência de comandos.AWS CLI

CloudTrail APIs

Além do console e da CLI, você também pode usar as APIs CloudTrail RESTful para programar diretamente. CloudTrail Para obter mais informações, consulte a Referência AWS CloudTrail da API e a Referência da API CloudTrail -Data.

AWS SDKs

Como alternativa ao uso da CloudTrail API, você pode usar um dos AWS SDKs. Cada SDK consiste em bibliotecas e código de exemplo para várias plataformas e linguagens de programação. Os SDKs fornecem uma maneira conveniente de criar acesso programático a. CloudTrail Por exemplo, você pode usar os SDKs para assinar solicitações de maneira criptográfica, gerenciar erros e realizar automaticamente novas tentativas de solicitações. Para obter mais informações, consulte a AWS página Ferramentas para criar.

Como CloudTrail funciona

Você tem acesso automático ao histórico de CloudTrail eventos ao criar seu Conta da AWS. O Histórico de eventos fornece um registro visualizável, pesquisável, baixável e imutável dos últimos 90 dias de eventos de gerenciamento gravados em uma Região da AWS.

Para um registro contínuo dos eventos dos Conta da AWS últimos 90 dias, crie uma trilha ou um armazenamento de dados de eventos do CloudTrail Lake.

Tópicos

- CloudTrail Histórico do evento
- CloudTrail Armazenamentos de dados de lagos e eventos
- CloudTrail trilhas

- CloudTrail Eventos do Insights
- CloudTrail canais

CloudTrail Histórico do evento

Você pode visualizar facilmente os últimos 90 dias de eventos de gerenciamento no CloudTrail console acessando a página Histórico de eventos. Você também pode visualizar o histórico de eventos executando o comando aws cloudtrail lookup-events ou a operação da API `LookupEvents`. É possível pesquisar eventos no Histórico de eventos filtrando eventos em um único atributo. Para ter mais informações, consulte Trabalhando com o histórico de CloudTrail eventos.

O Histórico de eventos não está conectado a nenhuma trilha ou armazenamento de dados de eventos existente em sua conta e não é afetado por alterações de configuração feitas em suas trilhas e seus armazenamentos de dados de eventos.

Não há CloudTrail cobrança pela visualização da página do histórico de eventos ou pela execução do `lookup-events` comando.

CloudTrail Armazenamentos de dados de lagos e eventos

Você pode criar um armazenamento de dados de eventos para registrar CloudTrail eventos (eventos de gerenciamento, eventos de dados), eventos do CloudTrail Insights, AWS Audit Manager evidências, itens de AWS Config configuração ou eventos externos AWS.

Os armazenamentos de dados de eventos podem registrar eventos da conta atual Região da AWS ou de todos os Regiões da AWS eventos da sua AWS conta. Os armazenamentos de dados de eventos que você está usando para registrar eventos de integração externos AWS devem ser somente para uma única região; eles não podem ser armazenamentos de dados de eventos de várias regiões.

Se você criou uma organização em AWS Organizations, você pode criar um armazenamento de dados de eventos da organização que registra todos os eventos de todas as AWS contas dessa organização. Os armazenamentos de dados de eventos da organização podem ser aplicados a todas as regiões da AWS , ou à região atual. Os armazenamentos de dados de eventos da organização devem ser criados com a conta de gerenciamento ou conta de administrador delegado e, quando especificados como aplicáveis a uma organização, são aplicados automaticamente a todas as contas-membro da respectiva organização. As contas de membro não podem ver o armazenamento de dados de eventos da organização, nem podem modificá-lo ou excluí-lo. Os armazenamentos de dados de eventos da organização não podem ser usados para coletar eventos

de fora da AWS. Para ter mais informações, consulte Armazenamentos de dados de eventos da organização.

Por padrão, todos os eventos em um armazenamento de dados de eventos são criptografados por CloudTrail. Ao configurar um armazenamento de dados de eventos, você pode optar por usar o seu próprio AWS KMS key. Usar sua própria chave KMS gera AWS KMS custos de criptografia e descriptografia. Após associar um armazenamento de dados de eventos a uma chave do KMS, não será possível remover ou alterar a chave do KMS. Para ter mais informações, consulte Criptografando arquivos de CloudTrail log com AWS KMS chaves (SSE-KMS).

A tabela a seguir fornece informações sobre tarefas que você pode realizar em armazenamentos de dados de eventos.

Tarefa	Descrição
Veja os painéis do Lake	Você pode usar os painéis do CloudTrail Lake para visualizar os eventos em armazenamentos de dados de eventos que coletam eventos de gerenciamento, eventos de dados do S3 ou eventos do Insights.
Eventos de gerenciamento de registros	Configure seu armazenamento de dados de eventos para registrar somente eventos de leitura, somente gravação ou todos os eventos de gerenciamento. Por padrão, os dados de eventos armazenam eventos de gerenciamento de registros.
Registrar eventos de dados	Configure seu armazenamento de dados de eventos para registrar eventos de dados. Você pode usar seletores de eventos avançados para filtrar os `resources.ARN` campos `eventName` `readOnly`, e e para registrar somente os eventos de interesse.
Eventos do Log Insights	Configure os armazenamentos de dados de eventos para registrar eventos do Insights a fim de ajudar a identificar e responder a atividades incomuns associadas a chamadas de APIs de gerenciamento. Para ter mais informações, consulte Registrar eventos do Insights. Cobranças adicionais são aplicáveis aos eventos do Insights. Você será cobrado separadamente se ativar o Insights tanto

Tarefa	Descrição
	para trilhas quanto para armazenamentos de dados de eventos. Para obter mais informações, consulte Preços do AWS CloudTrail.
Copiar eventos da trilha	Você pode copiar eventos da trilha para um armazenamento de dados de eventos novo ou existente para criar um point-in-time instantâneo dos eventos registrados na trilha.
Habilitar a federação em um armazenamento de dados de eventos	Você pode federar um armazenamento de dados de eventos para ver os metadados associados ao armazenamento de dados de eventos no catálogo de AWS Glue dados e executar consultas SQL nos dados do evento usando o Amazon Athena. Os metadados da tabela armazenados no Catálogo de AWS Glue Dados permitem que o mecanismo de consulta do Athena saiba como encontrar, ler e processar os dados que você deseja consultar.
Interromper ou iniciar a ingestão de eventos em um armazenamento de dados de eventos	Você pode interromper e iniciar a ingestão de eventos em armazenamentos de dados de eventos que coletam eventos CloudTrail de gerenciamento e dados ou itens de AWS Config configuração.
Crie uma integração com uma fonte de eventos fora do AWS	Você pode usar as integrações do CloudTrail Lake para registrar e armazenar dados de atividades do usuário de fora de AWS; de qualquer fonte em seus ambientes híbridos, como aplicativos internos ou SaaS hospedados no local ou na nuvem, máquinas virtuais ou contêineres. Para obter informações sobre os parceiros de integração disponíveis, consulte AWS CloudTrail Lake Integrations.
Veja exemplos de consultas do Lake no console CloudTrail	O CloudTrail console fornece vários exemplos de consultas que podem ajudar você a começar a escrever suas próprias consultas.

Tarefa	Descrição
Criar ou editar uma consulta	As consultas em CloudTrail são criadas em SQL. Você pode criar uma consulta na guia CloudTrail Lake Editor escrevendo a consulta em SQL do zero ou abrindo uma consulta salva ou de amostra e editando-a.
Salvar os resultados da consulta em um bucket do S3	Ao executar uma consulta, você pode salvar os resultados de consulta em um bucket do S3.
Baixe os resultados da consulta salvos	Você pode baixar um arquivo CSV contendo os resultados da consulta do CloudTrail Lake salvos.
Validar os resultados da consulta salvos	Você pode usar a validação de integridade dos resultados da CloudTrail consulta para determinar se os resultados da consulta foram modificados, excluídos ou inalterados após a CloudTrail entrega dos resultados da consulta ao bucket do S3.

Para obter mais informações sobre CloudTrail Lake, consulteTrabalhando com AWS CloudTrail Lake.

CloudTrail Os armazenamentos e consultas de dados de eventos em Lake incorrem em cobranças. Ao criar um armazenamento de dados de eventos, você escolhe a opção de preço que deseja usar para ele. A opção de preço determina o custo para a ingestão e para o armazenamento de eventos, e o período de retenção padrão e máximo para o armazenamento de dados de eventos. Ao executar consultas no Lake, você paga de acordo com a quantidade de dados examinados. Para obter informações sobre CloudTrail preços e gerenciamento de custos do Lake, consulte AWS CloudTrail Preços Gerenciando os custos CloudTrail do Lake e.

CloudTrail trilhas

Uma trilha é uma configuração que permite a entrega de eventos a um bucket do Amazon S3 especificado. Você também pode entregar e analisar eventos em uma trilha com o Amazon CloudWatch Logs e a Amazon EventBridge.

As trilhas podem registrar eventos CloudTrail de gerenciamento, eventos de dados e eventos do Insights.

Você pode criar dois tipos de trilhas para uma Conta da AWS: trilhas multirregionais e trilhas de região única.

Trilhas multirregionais

Quando você cria uma trilha multirregional, CloudTrail registra todos os eventos Regiões da AWS na AWS partição em que você está trabalhando e entrega os arquivos de log de CloudTrail eventos em um bucket do S3 que você especificar. Se uma Região da AWS for adicionada após a criação de uma trilha multirregional, essa nova região será incluída automaticamente e os eventos dessa região serão registrados. Criar uma trilha de várias regiões é uma prática recomendada, pois você captura atividades em todas as regiões da conta. Todas as trilhas que você cria usando o CloudTrail console são multirregionais. Você pode converter uma trilha de região única em uma trilha de várias regiões usando o. AWS CLI Para obter mais informações, consulte Criar uma trilha no console e Converter uma trilha que se aplica a uma região para que ela se aplique a todas as regiões.

Trilhas de uma única região

Quando você cria uma trilha de região única, CloudTrail registra os eventos somente nessa região. Em seguida, ele entrega os arquivos de log de CloudTrail eventos para um bucket do Amazon S3 que você especificar. Só é possível criar uma trilha de região única usando a AWS CLI. Se você criar trilhas únicas adicionais, poderá fazer com que essas trilhas entreguem arquivos de log de CloudTrail eventos para o mesmo bucket do S3 ou para buckets separados. Essa é a opção padrão quando você cria uma trilha usando a AWS CLI ou a CloudTrail API. Para ter mais informações, consulte Criando, atualizando e gerenciando trilhas com o AWS CLI.

> **Note**
>
> Para os dois tipos de trilhas, é possível especificar um bucket do Amazon S3 de qualquer região.

Se você criou uma organização em AWS Organizations, você pode criar uma trilha da organização que registra todos os eventos de todas as AWS contas dessa organização. As trilhas da organização podem ser aplicadas a todas as AWS regiões ou à região atual. As trilhas da organização devem ser criadas com a conta de gerenciamento ou conta de administrador delegado e, quando especificadas como aplicáveis a uma organização, são aplicadas automaticamente a todas as contas-membro da respectiva organização. As contas dos membros podem ver a trilha da organização, mas não podem modificá-la ou excluí-la. Por padrão, as contas de membro não têm acesso aos arquivos de log de uma trilha da organização no bucket do Amazon S3.

Por padrão, quando você cria uma trilha no CloudTrail console, seus arquivos de registro de eventos são criptografados com uma chave KMS. Se você optar por não ativar a criptografia SSE-KMS, seus registros de eventos serão criptografados usando a criptografia do lado do servidor (SSE) do Amazon S3. Você pode armazenar seus arquivos de log no seu bucket do 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. Se você deseja receber notificações sobre a entrega e a validação dos arquivos de log, configure as notificações do Amazon SNS.

CloudTrail publica arquivos de log várias vezes por hora, aproximadamente a cada 5 minutos. Esses arquivos de log contêm chamadas de API de serviços na conta que oferecem suporte CloudTrail. Para ter mais informações, consulte CloudTrail serviços e integrações suportados.

> **Note**
>
> CloudTrail normalmente entrega registros em uma média de cerca de 5 minutos após uma chamada de API. Desta vez não há garantias. Consulte o Acordo de Nível de Serviço do AWS CloudTrail para obter mais informações.
> Se você configurar incorretamente sua trilha (por exemplo, o bucket do S3 está inacessível), CloudTrail tentará reenviar os arquivos de log para o bucket do S3 por 30 dias, e esses attempted-to-deliver eventos estarão sujeitos às cobranças padrão. CloudTrail Para evitar cobranças em uma trilha mal configurada, você precisa excluir a trilha.
> CloudTrail captura ações feitas diretamente pelo usuário ou em nome do usuário por um AWS serviço. Por exemplo, uma AWS CloudFormation `CreateStack` chamada pode resultar em chamadas de API adicionais para Amazon EC2, Amazon RDS, Amazon EBS ou outros serviços, conforme exigido pelo modelo. AWS CloudFormation Esse comportamento é normal e esperado. Você pode identificar se a ação foi realizada por um AWS serviço com o `invokedby` campo no CloudTrail evento.

A tabela a seguir fornece informações sobre tarefas que você pode realizar em trilhas.

Tarefa	Descrição
Registrando eventos de gerenciamento	Configure suas trilhas para registrar somente eventos de leitura, somente gravação ou todos os eventos de gerenciamento.

Tarefa	Descrição
Registrar eventos de dados	Você pode usar seletores de eventos avançados para criar seletores refinados para registrar somente os eventos de dados de interesse. Ao usar seletores de eventos avançados, você pode filtrar no `eventName` campo para incluir ou excluir o registro de chamadas de API específicas, o que pode ajudar a controlar os custos.
Eventos do Log Insights	Configure as trilhas para registrar eventos de Insights a fim de ajudar a identificar e responder a atividade incomum associada às chamadas de API de gerenciamento de . Cobranças adicionais são aplicáveis aos eventos do Insights. Você será cobrado separadamente se ativar o Insights tanto para trilhas quanto para armazenamentos de dados de eventos. Para obter mais informações, consulte Preços do AWS CloudTrail.
Veja os eventos do Insights	Depois de habilitar o CloudTrail Insights em uma trilha, você pode visualizar até 90 dias de eventos do Insights usando o CloudTrail console ou AWS CLI o.
Baixe os eventos do Insights	Depois de habilitar o CloudTrail Insights em uma trilha, você pode baixar um arquivo CSV ou JSON contendo até os últimos 90 dias de eventos do Insights para sua trilha.
Copie os eventos da trilha para o CloudTrail Lago	Você pode copiar eventos de trilha existentes para um armazenamento de dados de eventos do CloudTrail Lake para criar um point-in-time instantâneo dos eventos registrados na trilha.

Tarefa	Descrição
Crie e assine um tópico do Amazon SNS	Inscreva-se em um tópico para receber notificações sobre o fornecimento de arquivos de log ao seu bucket. O Amazon SNS pode notificar você de várias maneiras, inclusive de modo programático com o Amazon Simple Queue Service. **Note** Se você deseja receber notificações do SNS sobre a entrega de arquivos de log de todas as regiões, especifiq ue apenas um tópico do SNS para a sua trilha. Se você deseja processar programaticamente todos os eventos, consulte Usando a Biblioteca CloudTrai l de Processamento.
Visualize seus arquivos de log	Encontre e baixe seus arquivos de log do bucket do S3.

Tarefa	Descrição
Monitore eventos com CloudWatch registros	Você pode configurar sua trilha para enviar eventos para o CloudWatch Logs. Em seguida, você pode usar o CloudWatch Logs para monitorar sua conta em busca de chamadas e eventos específicos da API. **Note** Se você configurar uma trilha que se aplique a todas as regiões para enviar eventos a um grupo de CloudWatc h registros de registros, CloudTrail enviará eventos de todas as regiões para um único grupo de registros.
Ativar criptografia de log	A criptografia de arquivos de log fornece uma camada extra de segurança para os seus arquivos de log.
Habilitar a integridade do arquivo de log	A validação da integridade do arquivo de log ajuda você a verificar se os arquivos de log permaneceram inalterados desde que foram CloudTrail entregues.
Compartilhe arquivos de log com outros Contas da AWS	Você pode compartilhar arquivos de log entre contas.
Registros agregados de várias contas	Você pode agregar arquivos de log de várias contas em um único bucket.

Tarefa	Descrição
Trabalhe com soluções de parceiros	Analise sua CloudTrail produção com uma solução de parceiro que se integra a. CloudTrail As soluções de parceiros oferecem um amplo conjunto de recursos, como rastreamento de alterações, solução de problemas e análise de segurança.

Você pode entregar uma cópia dos seus eventos de gerenciamento contínuos para o bucket do S3 sem nenhum custo CloudTrail criando uma trilha. No entanto, há cobranças de armazenamento do Amazon S3. Para obter mais informações sobre CloudTrail preços, consulte AWS CloudTrail Preços. Para receber informações sobre a definição de preço do Amazon S3, consulte Definição de preço do Amazon S3.

CloudTrail Eventos do Insights

AWS CloudTrail O Insights ajuda AWS os usuários a identificar e responder a atividades incomuns associadas a chamadas de API e taxas de erro de API, analisando continuamente os eventos CloudTrail de gerenciamento. CloudTrail O Insights analisa seus padrões normais de volume de chamadas de API e taxas de erro de API, também chamados de linha de base, e gera eventos do Insights quando o volume de chamadas ou as taxas de erro estão fora dos padrões normais. Eventos de insights no volume de chamadas de API são gerados para `write` APIs de gerenciamento e eventos do Insights na taxa de erros da API são gerados para ambos`read` e `write` APIs de gerenciamento.

Por padrão, CloudTrail trilhas e armazenamentos de dados de eventos não registram eventos do Insights. Você deve configurar seu armazenamento de dados de trilhas ou eventos para registrar eventos do Insights. Para obter mais informações, consulte Registrando eventos do Insights com o AWS Management Console e Registrando eventos do Insights com o AWS Command Line Interface.

Cobranças adicionais são aplicáveis aos eventos do Insights. Você será cobrado separadamente se ativar o Insights tanto para trilhas quanto para armazenamentos de dados de eventos. Para obter mais informações, consulte Preços do AWS CloudTrail.

Visualizando eventos do Insights para trilhas e armazenamentos de dados de eventos

CloudTrail suporta eventos do Insights para trilhas e armazenamentos de dados de eventos, no entanto, existem algumas diferenças na forma como você visualiza e acessa os eventos do Insights.

Visualizar eventos do Insights para trilhas

Se você tiver eventos do Insights ativados em uma trilha e CloudTrail detectar atividades incomuns, os eventos do Insights serão registrados em uma pasta ou prefixo diferente no bucket do S3 de destino da sua trilha. Você também pode ver o tipo de insight e o período do incidente ao visualizar os eventos do Insights no CloudTrail console. Para ter mais informações, consulte Visualizando eventos do CloudTrail Insights para trilhas no CloudTrail console.

Depois de ativar o CloudTrail Insights pela primeira vez em uma trilha, pode levar até 36 horas CloudTrail para entregar o primeiro evento do Insights, se uma atividade incomum for detectada.

Visualizar eventos do Insights para armazenamentos de dados de eventos

Para registrar eventos do Insights no CloudTrail Lake, você precisa de um armazenamento de dados de eventos de destino que registre eventos do Insights e um armazenamento de dados de eventos de origem que permita o Insights e eventos de gerenciamento de registros. Para ter mais informações, consulte Crie um armazenamento de dados de eventos para eventos do CloudTrail Insights com o console.

Depois de ativar o CloudTrail Insights pela primeira vez no armazenamento de dados do evento de origem, pode levar até 7 dias CloudTrail para entregar o primeiro evento do Insights ao armazenamento de dados do evento de destino, se uma atividade incomum for detectada.

Se você tiver o CloudTrail Insights ativado em um armazenamento de dados de eventos de origem e CloudTrail detectar atividades incomuns, CloudTrail entrega os eventos do Insights ao seu armazenamento de dados de eventos de destino. Em seguida, você pode consultar seu armazenamento de dados de eventos de destino para obter informações sobre seus eventos do Insights e, opcionalmente, salvar os resultados da consulta em um bucket do S3. Para obter mais informações, consulte Criar ou editar uma consulta e Veja exemplos de consultas no console CloudTrail .

Você pode visualizar o painel de Eventos do Insights para visualizar os eventos do Insights em seu armazenamento de dados de eventos de destino. Para obter mais informações sobre painéis do Lake, consulte Veja os painéis CloudTrail do Lake.

CloudTrail canais

CloudTrail suporta dois tipos de canais:

Canais para integrações do CloudTrail Lake com fontes de eventos fora do AWS

CloudTrail O Lake usa canais para trazer eventos de fora AWS para o CloudTrail Lake de parceiros externos que trabalham com CloudTrail ou de suas próprias fontes. Ao criar um canal, você escolhe um ou mais armazenamentos de dados de eventos para armazenar eventos que cheguem da fonte do canal. É possível alterar os armazenamentos de dados de eventos de destino de um canal conforme necessário, desde que os armazenamentos de dados de eventos de destino estejam configurados para registrar em log eventos de atividades. Ao criar um canal para eventos de um parceiro externo, você fornece um ARN de canal para o parceiro ou aplicação da fonte. A política de recursos anexada ao canal permite que a fonte transmita eventos pelo canal. Para obter mais informações, consulte Crie uma integração com uma fonte de eventos fora do AWS e `CreateChannel` na Referência da API do AWS CloudTrail .

Canais vinculados ao serviço

AWS os serviços podem criar um canal vinculado ao serviço para receber CloudTrail eventos em seu nome. O AWS serviço que cria o canal vinculado ao serviço configura seletores de eventos avançados para o canal e especifica se o canal se aplica a todas as regiões ou à região atual.

Você pode usar o CloudTrail console ou AWS CLIvisualizar informações sobre qualquer canal CloudTrail vinculado ao serviço criado por. Serviços da AWS

CloudTrail conceitos

Esta seção resume os conceitos básicos relacionados a. CloudTrail

Conceitos:

- CloudTrail eventos
- Histórico de eventos
- Trilhas
- Trilhas organizacionais
- CloudTrail Armazenamentos de dados de lagos e eventos
- CloudTrail Percepções

- Tags
- AWS Security Token Service e CloudTrail
- Eventos de serviços globais

CloudTrail eventos

Um evento em CloudTrail é o registro de uma atividade em uma AWS conta. Essa atividade pode ser uma ação realizada por uma identidade do IAM ou um serviço que pode ser monitorado por CloudTrail. CloudTrailos eventos fornecem um histórico das atividades de contas de API e não API feitas por meio de AWS SDKs AWS Management Console, ferramentas de linha de comando e outros AWS serviços.

CloudTrail os arquivos de log não são um rastreamento de pilha ordenado das chamadas públicas de API, portanto, os eventos não aparecem em nenhuma ordem específica.

CloudTrail registra três tipos de eventos:

- Eventos de gerenciamento
- Eventos de dados
- Eventos do Insights

Todos os tipos de eventos usam um formato de log CloudTrail JSON.

Por padrão, as trilhas e os armazenamentos de dados de eventos registram eventos de gerenciamento, mas não eventos de dados ou do Insights.

Para obter informações sobre como Serviços da AWS integrar com CloudTrail, consulteAWS tópicos de serviço para CloudTrail.

Eventos de gerenciamento

Os eventos de gerenciamento fornecem informações sobre as operações de gerenciamento que são realizadas nos recursos AWS da sua conta. Elas também são conhecidas como operações de plano de controle.

Exemplos de eventos de gerenciamento incluem:

- Configurando a segurança (por exemplo, operações de AWS Identity and Access Management `AttachRolePolicy` API).

- Registro de dispositivos (por exemplo, operações de API `CreateDefaultVpc` do Amazon EC2).
- Configuração de regras para roteamento de dados (por exemplo, operações de API `CreateSubnet` do Amazon EC2).
- Configurar o registro (por exemplo, operações de AWS CloudTrail `CreateTrail` API).

Os eventos de gerenciamento também podem incluir eventos que não são de API que ocorrem na sua conta. Por exemplo, quando um usuário faz login na sua conta, CloudTrail registra o `ConsoleLogin` evento. Para ter mais informações, consulte Eventos não relacionados à API capturados por CloudTrail.

Por padrão, os dados de CloudTrail trilhas e eventos do CloudTrail Lake armazenam eventos de gerenciamento de registros. Para obter mais informações sobre eventos de gerenciamento de registros, consulteLog de eventos de gerenciamento.

Eventos de dados

Os eventos de dados fornecem informações sobre as operações do recurso executadas em um recurso ou dentro de um recurso. Elas também são conhecidas como operações de plano de dados. Eventos de dados geralmente são atividades de alto volume.

Exemplos de eventos de dados incluem:

- Atividade de API em nível de objeto do Amazon S3 (por exemplo,, `GetObject` `DeleteObject`, e operações de `PutObject` API) em objetos em buckets do S3.
- AWS Lambda atividade de execução da função (a `Invoke` API).
- CloudTrail `PutAuditEvents`atividade em um canal do CloudTrail Lake que é usada para registrar eventos externos AWS.
- Operações da API `Publish` e `PublishBatch` do Amazon SNS em tópicos.

A tabela a seguir mostra os tipos de eventos de dados disponíveis para trilhas e armazenamentos de dados de eventos. A coluna Tipo de evento de dados (console) mostra a seleção apropriada no console. A coluna de valor resources.type mostra o `resources.type` valor que você especificaria para incluir eventos de dados desse tipo em seu armazenamento de dados de trilhas ou eventos usando as AWS CLI APIs ou. CloudTrail

Para trilhas, você pode usar seletores de eventos básicos ou avançados para registrar eventos de dados para objetos do Amazon S3, funções do Lambda e tabelas do DynamoDB (mostradas nas três

primeiras linhas da tabela). É possível usar somente seletores de eventos avançados para registrar em log os tipos de eventos de dados mostrados nas linhas restantes.

Para armazenamentos de dados de eventos, é possível usar somente seletores de eventos avançados para incluir eventos de dados.

AWS service (Serviço da AWS)	Descrição	Tipo de evento de dados (console)	valor resources.type
Amazon DynamoDB	Atividade de API em nível de item do Amazon DynamoDB em tabelas (por exemplo `PutItem`, `Delete`, e operações de API). `UpdateItem` **Note** Para tabelas com fluxos habilitados, o campo `resources` no evento de dados contém `AWS::DynamoDB::Stream` e `AWS::DynamoDB::Table`. Se você especificar `AWS::DynamoDB::Tab`	DynamoDB	`AWS::DynamoDB::Table`

AWS service (Serviço da AWS)	Descrição	Tipo de evento de dados (console)	valor resources.type
	`le` como `resources.type`, ele registrará os eventos da tabela do DynamoDB e dos fluxos do DynamoDB por padrão. Para excluir eventos de streams, adicione um filtro no `eventName` campo.		
AWS Lambda	AWS Lambda atividade de execução da função (a `Invoke` API).	Lambda	`AWS::Lambda::Function`

AWS service (Serviço da AWS)	Descrição	Tipo de evento de dados (console)	valor resources.type
Amazon S3	Atividade de API em nível de objeto do Amazon S3 (por exemplo,, `GetObject` `DeleteObject` , e operações de `PutObject` API) em objetos em buckets do S3.	S3	`AWS::S3::Object`
AWS AppConfig	AWS AppConfig Atividade de API para operações de configuração, como chamadas para `StartConfiguration` `Session` `GetLatestConfiguration` e.	AWS AppConfig	`AWS::AppConfig::Configuration`
AWS Intercâmbio de dados B2B	Atividade da API B2B Data Interchange para operações do Transformer, como chamadas para `GetTransformerJob` e `StartTransformerJob` .	B2B Data Interchange	`AWS::B2BI::Transformer`

AWS service (Serviço da AWS)	Descrição	Tipo de evento de dados (console)	valor resources.type
Amazon Bedrock	Atividade da API do Amazon Bedrock em um alias de agente.	Alias de agente do Bedrock	`AWS::Bedrock::AgentAlias`
	Atividade da API do Amazon Bedrock em uma base de conhecimento.	Base de conhecimento do Bedrock	`AWS::Bedrock::KnowledgeBase`
Amazon CloudFront	CloudFront Atividade de API em um KeyValueStore.	CloudFront KeyValueStore	`AWS::CloudFront::KeyValueStore`
AWS Cloud Map	AWS Cloud Map Atividade de API em um namespace.	AWS Cloud Map namespace	`AWS::ServiceDiscovery::Namespace`
	AWS Cloud Map Atividade de API em um serviço.	AWS Cloud Map serviço	`AWS::ServiceDiscovery::Service`
AWS CloudTrail	CloudTrail `PutAuditEvents` atividade em um canal do CloudTrail Lake que é usada para registrar eventos externos AWS.	CloudTrail canal	`AWS::CloudTrail::Channel`

AWS service (Serviço da AWS)	Descrição	Tipo de evento de dados (console)	valor resources.type
Amazon CodeWhisperer	Atividade de CodeWhisperer API da Amazon em uma personalização.	CodeWhisperer personalização	`AWS::CodeWhisperer::Customization`
	Atividade CodeWhisperer da API da Amazon em um perfil.	CodeWhisperer	`AWS::CodeWhisperer::Profile`
Amazon Cognito	Atividade da API do Amazon Cognito em bancos de identidades do Amazon Cognito.	Bancos de identidades do Cognito	`AWS::Cognito::IdentityPool`
Amazon DynamoDB	Atividade de API do Amazon DynamoDB em fluxos.	DynamoDB Streams	`AWS::DynamoDB::Stream`
Amazon Elastic Block Store	APIs diretas do Amazon Elastic Block Store (EBS), como `PutSnapshotBlock`, `GetSnapshotBlock` e `ListChangedBlocks` nos snapshots do Amazon EBS.	APIs diretas do Amazon EBS	`AWS::EC2::Snapshot`

AWS service (Serviço da AWS)	Descrição	Tipo de evento de dados (console)	valor resources.type
Amazon EMR	Atividade da API do Amazon EMR em um espaço de trabalho de log de gravação antecipada.	Espaço de trabalho de log de gravação antecipada do EMR	`AWS::EMRWAL::Workspace`
Amazon FinSpace	Atividade de API do Amazon FinSpace em ambientes.	FinSpace	`AWS::FinSpace::Environment`

AWS service (Serviço da AWS)	Descrição	Tipo de evento de dados (console)	valor resources.type
AWS Glue	AWS Glue Atividade de API em tabelas criadas pelo Lake Formation. **Note** AWS Glue Atualmente, os eventos de dados para tabelas são suportados somente nas seguintes regiões: • Leste dos EUA (Norte da Virgínia) • Leste dos EUA (Ohio) • Oeste dos EUA (Oregon) • Europa (Irlanda) • Região Ásia-	Lake Formation	`AWS::Glue::Table`

AWS service (Serviço da AWS)	Descrição	Tipo de evento de dados (console)	valor resources.type
	Pacífico (Tóquio)		
Amazon GuardDuty	Atividade de GuardDuty API da Amazon para um detector.	GuardDuty detector	`AWS::GuardDuty::Detector`
AWS HealthImaging	AWS HealthImaging Atividade de API em armazenamentos de dados.	Armazenamento de dados de imagens médicas	`AWS::MedicalImaging::Datastore`
AWS IoT	AWS IoT Atividade de API em certificados.	Certificado de IoT	`AWS::IoT::Certificate`
	AWS IoT Atividade de API em coisas.	Coisa de IoT	`AWS::IoT::Thing`

AWS service (Serviço da AWS)	Descrição	Tipo de evento de dados (console)	valor resources.type
AWS IoT Greengrass Version 2	Atividade da API do Greengrass de um dispositivo principal do Greengrass em uma versão de componente. **Note** O Greengrass não registra eventos de acesso negado.	Versão do componente IoT Greengrass	`AWS::GreengrassV2::ComponentVersion`
	Atividade da API do Greengrass de um dispositivo principal do Greengrass em uma implantação. **Note** O Greengrass não registra eventos de acesso negado.	Implantação do IoT Greengrass	`AWS::GreengrassV2::Deployment`
AWS IoT SiteWise	Atividade da SiteWise API de IoT em ativos.	Ativo de IoT SiteWise	`AWS::IoTSiteWise::Asset`

AWS service (Serviço da AWS)	Descrição	Tipo de evento de dados (console)	valor resources.type
	Atividade da SiteWise API de IoT em séries temporais.	Série temporal de IoT SiteWise	`AWS::IoTSiteWise::TimeSeries`
AWS IoT TwinMaker	Atividade da TwinMaker API de IoT em uma entidade.	Entidade de IoT TwinMaker	`AWS::IoTTwinMaker::Entity`
	Atividade da TwinMaker API de IoT em um espaço de trabalho.	Espaço de trabalho de IoT TwinMaker	`AWS::IoTTwinMaker::Workspace`
Amazon Kendra Intelligent Ranking	Atividade da API do Amazon Kendra Intelligent Ranking em planos de execução de reclassificação.	Kendra Ranking	`AWS::KendraRanking::ExecutionPlan`
Amazon Keyspaces (para Apache Cassandra)	Atividade da API Amazon Keyspaces em uma tabela.	Mesa Cassandra	`AWS::Cassandra::Table`
Amazon Kinesis Data Streams	Atividade da API Kinesis Data Streams em streams.	Stream do Kinesis	`AWS::Kinesis::Stream`
	Atividade da API Kinesis Data Streams em consumidores de streams.	Consumidor de streaming do Kinesis	`AWS::Kinesis::StreamConsumer`

AWS service (Serviço da AWS)	Descrição	Tipo de evento de dados (console)	valor resources.type
Amazon Kinesis Video Streams	Atividade da API Kinesis Video Streams em streams de vídeo, como chamadas para e. `GetMedia` `PutMedia`	Fluxo de vídeo do Kinesis	`AWS::KinesisVideo::Stream`
Amazon Managed Blockchain	Atividade da API do Amazon Managed Blockchain em uma rede.	Rede do Managed Blockchain	`AWS::ManagedBlockchain::Network`
	Chamadas de JSON-RPC do Amazon Managed Blockchain em nós Ethereum, como `eth_getBalance` ou `eth_getBlockByNumber` .	Managed Blockchain	`AWS::ManagedBlockchain::Node`
Gráfico do Amazon Neptune	Atividades da API de dados, por exemplo, consultas, algoritmos ou pesquisa vetorial, em um gráfico do Neptune.	Gráfico do Neptune	`AWS::NeptuneGraph::Graph`
AWS Private CA	AWS Private CA Conector para atividade da API do Active Directory.	AWS Private CA Conector para Active Directory	`AWS::PCAConnectorAD::Connector`

AWS service (Serviço da AWS)	Descrição	Tipo de evento de dados (console)	valor resources.type
Aplicativos Amazon Q	Atividade da API de dados no Amazon Q Apps.	Aplicativos Amazon Q	`AWS::QApps:QApp`
Amazon Q Business	Atividade da API do Amazon Q Business em uma aplicação.	Aplicação do Amazon Q Business	`AWS::QBusiness::Application`
	Atividade da API do Amazon Q Business em uma fonte de dados.	Fonte de dados do Amazon Q Business	`AWS::QBusiness::DataSource`
	Atividade da API do Amazon Q Business em um índice.	Índice do Amazon Q Business	`AWS::QBusiness::Index`
	Atividade da API do Amazon Q Business em uma experiência na web.	Experiência na web do Amazon Q Business	`AWS::QBusiness::WebExperience`
Amazon RDS	Atividade da API do Amazon RDS em um cluster de banco de dados.	API de dados do RDS - cluster de banco de dados	`AWS::RDS::DBCluster`
Amazon S3	Atividade da API Amazon S3 em pontos de acesso.	Ponto de acesso do S3	`AWS::S3::AccessPoint`

AWS service (Serviço da AWS)	Descrição	Tipo de evento de dados (console)	valor resources.type
	Atividade da API de pontos de acesso do Amazon S3 Object Lambda, como chamadas para e. `CompleteMultipartUpload` `GetObject`	S3 Object Lambda	`AWS::S3ObjectLambda::AccessPoint`
Amazon S3 on Outposts	Atividade da API em nível de objeto do Amazon S3 on Outposts.	S3 Outposts	`AWS::S3Outposts::Object`
Amazon SageMaker	SageMaker `InvokeEndpointWithResponseStream` Atividade da Amazon em endpoints .	SageMaker ponto final	`AWS::SageMaker::Endpoint`
	Atividade da SageMaker API da Amazon em lojas de recursos.	SageMaker feature store	`AWS::SageMaker::FeatureGroup`
	Atividade da SageMaker API da Amazon em componentes de testes experimentais.	SageMaker componente experimental de métricas	`AWS::SageMaker::ExperimentTrialComponent`

AWS service (Serviço da AWS)	Descrição	Tipo de evento de dados (console)	valor resources.type
Amazon SNS	Operações da API `Publish` do Amazon SNS em endpoints da plataforma.	Endpoint da plataforma SNS	`AWS::SNS::PlatformEndpoint`
	Operações da API `Publish` e `PublishBatch` do Amazon SNS em tópicos.	Tópico do SNS	`AWS::SNS::Topic`
Amazon SQS	Atividade da API do Amazon SQS em mensagens.	SQS	`AWS::SQS::Queue`
AWS Step Functions	Atividade da API Step Functions em uma máquina de estado.	Máquina de estado do Step Functions	`AWS::StepFunctions::StateMachine`
Cadeia de Suprimentos AWS	Cadeia de Suprimentos AWS Atividade de API em uma instância .	Cadeia de suprimentos	`AWS::SCN::Instance`
Amazon SWF	Atividade da API Amazon SWF em domínios.	Domínio SWF	`AWS::SWF::Domain`
AWS Systems Manager	Atividade da API Systems Manager nos canais de controle.	Systems Manager (Gerenciador de sistemas)	`AWS::SSMMessages::ControlChannel`

AWS service (Serviço da AWS)	Descrição	Tipo de evento de dados (console)	valor resources.type
	Atividade da API Systems Manager em nós gerenciados.	Nó gerenciado pelo Systems Manager	`AWS::SSM::ManagedNode`
Amazon Timestream	Atividade da API `Query` do Amazon Timestream em bancos de dados.	Banco de dados do Timestream	`AWS::Timestream::Database`
	Atividade da API `Query` do Amazon Timestream em tabelas.	Tabela do Timestream	`AWS::Timestream::Table`
Amazon Verified Permissions	Atividade da API do Amazon Verified Permissions em um repositório de políticas.	Amazon Verified Permissions	`AWS::VerifiedPermissions::PolicyStore`
Amazon WorkSpaces Thin Client	WorkSpaces Atividade da API Thin Client em um dispositivo.	Dispositivo Thin Client	`AWS::ThinClient::Device`
	WorkSpaces Atividade da API Thin Client em um ambiente.	Ambiente Thin Client	`AWS::ThinClient::Environment`

AWS service (Serviço da AWS)	Descrição	Tipo de evento de dados (console)	valor resources.type
AWS X-Ray	Atividade da API X-Ray em rastreamentos.	Traço de raio-X	`AWS::XRay::Trace`

Eventos de dados não são registrados em log por padrão quando você cria uma trilha ou um armazenamento de dados de eventos. Para registrar eventos de CloudTrail dados, você deve adicionar explicitamente os recursos suportados ou os tipos de recursos para os quais deseja coletar atividades. Para obter mais informações sobre log de eventos de dados, consulte Eventos de dados de log.

Há cobranças adicionais para o registro de eventos de dados. Para CloudTrail saber os preços, consulte AWS CloudTrail Preços.

Eventos do Insights

CloudTrail Os eventos do Insights capturam atividades incomuns de taxa de chamadas de API ou taxa de erro em sua AWS conta analisando a atividade CloudTrail de gerenciamento. Os eventos do Insights fornecem informações relevantes, como a API associada, a hora do incidente e estatísticas, que ajudam a entender e agir com relação à atividade incomum. Ao contrário de outros tipos de eventos capturados em um armazenamento de dados de CloudTrail trilhas ou eventos, os eventos do Insights são registrados somente quando CloudTrail detectam alterações no uso da API ou no registro da taxa de erro da sua conta que diferem significativamente dos padrões de uso típicos da conta.

Exemplos de atividades que podem gerar eventos do Insights incluem:

- Sua conta geralmente registra em log no máximo 20 chamadas de API do `DeleteBucket` Amazon S3 por minuto, mas sua conta começa a registrar em log uma média de 100 chamadas de API `DeleteBucket` por minuto. Um evento do Insights é registrado em log no início da atividade incomum e outro evento do Insights é registrado em log para marcar o fim da atividade incomum.
- Sua conta geralmente registra em log 20 chamadas por minutos para a API do `AuthorizeSecurityGroupIngress` Amazon EC2, mas sua conta começa a registrar em log zero chamada para `AuthorizeSecurityGroupIngress`. Um evento do Insights é registrado

em log no início da atividade incomum, e dez minutos depois, quando a atividade incomum termina, outro evento do Insights é registrado em log para marcar o fim da atividade incomum.

- Sua conta normalmente registra menos de um `AccessDeniedException` erro em um período de sete dias no AWS Identity and Access Management API, `DeleteInstanceProfile`. Sua conta começa a registrar uma média de 12 `AccessDeniedException` erros por minuto na `DeleteInstanceProfile` chamada de API. Um evento do Insights é registrado no início da atividade incomum e outro evento do Insights é registrado para marcar o fim da atividade incomum.

Esses exemplos são fornecidos somente para fins ilustrativos. Seus resultados podem variar dependendo do seu caso de uso.

Para registrar eventos do CloudTrail Insights, você deve habilitar explicitamente os eventos do Insights em um armazenamento de dados de trilhas ou eventos novo ou existente. Para obter mais informações sobre registrar eventos do Insights, consulte Registrar eventos do Insights.

Cobranças adicionais são aplicáveis aos eventos do Insights. Você será cobrado separadamente se ativar o Insights tanto para trilhas quanto para armazenamentos de dados de eventos. Para obter mais informações, consulte Preços do AWS CloudTrail.

Visualizando eventos do Insights para trilhas e armazenamentos de dados de eventos

CloudTrail suporta eventos do Insights para trilhas e armazenamentos de dados de eventos, no entanto, existem algumas diferenças na forma como você visualiza e acessa os eventos do Insights.

Visualizar eventos do Insights para trilhas

Se você tiver eventos do Insights ativados em uma trilha e CloudTrail detectar atividades incomuns, os eventos do Insights serão registrados em uma pasta ou prefixo diferente no bucket do S3 de destino da sua trilha. Você também pode ver o tipo de insight e o período do incidente ao visualizar os eventos do Insights no CloudTrail console. Para ter mais informações, consulte Visualizando eventos do CloudTrail Insights para trilhas no CloudTrail console.

Visualizar eventos do Insights para armazenamentos de dados de eventos

Para registrar eventos do Insights no CloudTrail Lake, você precisa de um armazenamento de dados de eventos de destino que registre eventos do Insights e um armazenamento de dados de eventos de origem que permita o Insights e eventos de gerenciamento de registros. Para ter mais informações, consulte Crie um armazenamento de dados de eventos para eventos do CloudTrail Insights com o console.

Se você tiver o CloudTrail Insights ativado em um armazenamento de dados de eventos de origem e CloudTrail detectar atividades incomuns, CloudTrail entrega os eventos do Insights ao seu armazenamento de dados de eventos de destino. Em seguida, você pode consultar seu armazenamento de dados de eventos de destino para obter informações sobre seus eventos do Insights e, opcionalmente, salvar os resultados da consulta em um bucket do S3. Para obter mais informações, consulte Criar ou editar uma consulta e Veja exemplos de consultas no console CloudTrail .

Você pode visualizar o painel de Eventos do Insights para visualizar os eventos do Insights em seu armazenamento de dados de eventos de destino. Para ter mais informações, consulte Veja os painéis CloudTrail do Lake.

Histórico de eventos

CloudTrail o histórico de eventos fornece um registro visível, pesquisável, baixável e imutável dos últimos 90 dias de eventos de gerenciamento em um CloudTrail . Região da AWS Você pode usar esse histórico para obter visibilidade das ações realizadas em sua AWS conta nos AWS SDKs AWS Management Console, ferramentas de linha de comando e outros AWS serviços. Você pode personalizar sua visualização do histórico de eventos no CloudTrail console selecionando quais colunas serão exibidas. Para ter mais informações, consulte Trabalhando com o histórico de CloudTrail eventos.

Trilhas

Uma trilha é uma configuração que permite a entrega de CloudTrail eventos para um bucket do S3, com entrega opcional para a CloudWatch Logs e a Amazon EventBridge. Você pode usar uma trilha para escolher os CloudTrail eventos que deseja entregar, criptografar seus arquivos de log de CloudTrail eventos com uma AWS KMS chave e configurar as notificações do Amazon SNS para entrega de arquivos de log. Para obter mais informações sobre como criar e gerenciar uma trilha, consulte Criando uma trilha para o seu Conta da AWS.

Trilhas multirregionais e de região única

Você pode criar dois tipos de trilhas para uma Conta da AWS: trilhas multirregionais e trilhas de região única.

Trilhas multirregionais

Quando você cria uma trilha multirregional, CloudTrail registra todos os eventos Regiões da AWS na AWS partição em que você está trabalhando e entrega os arquivos de log de CloudTrail

eventos em um bucket do S3 que você especificar. Se uma Região da AWS for adicionada após a criação de uma trilha multirregional, essa nova região será incluída automaticamente e os eventos dessa região serão registrados. Criar uma trilha de várias regiões é uma prática recomendada, pois você captura atividades em todas as regiões da conta. Todas as trilhas que você cria usando o CloudTrail console são multirregionais. Você pode converter uma trilha de região única em uma trilha de várias regiões usando o. AWS CLI Para obter mais informações, consulte Criar uma trilha no console e Converter uma trilha que se aplica a uma região para que ela se aplique a todas as regiões.

Trilhas de uma única região

Quando você cria uma trilha de região única, CloudTrail registra os eventos somente nessa região. Em seguida, ele entrega os arquivos de log de CloudTrail eventos para um bucket do Amazon S3 que você especificar. Só é possível criar uma trilha de região única usando a AWS CLI. Se você criar trilhas únicas adicionais, poderá fazer com que essas trilhas entreguem arquivos de log de CloudTrail eventos para o mesmo bucket do S3 ou para buckets separados. Essa é a opção padrão quando você cria uma trilha usando a AWS CLI ou a CloudTrail API. Para ter mais informações, consulte Criando, atualizando e gerenciando trilhas com o AWS CLI.

> **Note**
>
> Para os dois tipos de trilhas, é possível especificar um bucket do Amazon S3 de qualquer região.

Uma trilha multirregional tem as seguintes vantagens:

- As configurações da trilha se aplicam de forma consistente a todos Regiões da AWS.
- Você recebe CloudTrail eventos de todos Regiões da AWS em um único bucket do Amazon S3 e, opcionalmente, em um grupo de CloudWatch logs de registros.
- Você gerencia a configuração de trilhas para todas Regiões da AWS em um único local.

Quando você aplica uma trilha a todas as AWS regiões, CloudTrail usa a trilha que você cria em uma região específica para criar trilhas com configurações idênticas em todas as outras regiões na AWS partição em que você está trabalhando.

Isso causa os seguintes efeitos:

- CloudTrail entrega arquivos de log da atividade da conta de todas as AWS regiões para o único bucket do Amazon S3 que você especificar e, opcionalmente, para um grupo de registros de CloudWatch registros.
- Se você configurou um tópico do Amazon SNS para a trilha, as notificações do SNS sobre entregas de arquivos de log em todas as AWS regiões serão enviadas para esse único tópico do SNS.

Independentemente de a trilha ser multirregional ou única, os eventos enviados para a Amazon EventBridge são recebidos no ônibus de eventos de cada região, em vez de em um único ônibus de eventos.

Várias trilhas por região

Se você tiver grupos de usuários diferentes, porém relacionados, como desenvolvedores, equipe de segurança e auditores de TI, poderá criar várias trilhas por região. Isso permite que cada grupo receba sua própria cópia dos arquivos de log.

CloudTrail suporta cinco trilhas por região. Uma trilha multirregional conta como uma trilha por região.

Veja a seguir um exemplo de uma região com cinco trilhas:

- Você duas trilhas na região Oeste dos EUA (Norte da Califórnia) que se aplicam somente a essa região.
- Você cria mais duas trilhas multirregionais na região Oeste dos EUA (Norte da Califórnia).
- Você cria outra trilha multirregional na região Ásia-Pacífico (Sydney). Esta trilha também existe como uma trilha na região Oeste dos EUA (Norte da Califórnia).

Você pode ver uma lista de trilhas Região da AWS na página Trilhas do CloudTrail console. Para ter mais informações, consulte Atualizar uma trilha. Para CloudTrail saber os preços, consulte AWS CloudTrail Preços.

Trilhas organizacionais

Uma trilha organizacional é uma configuração que permite a entrega de CloudTrail eventos na conta de gerenciamento e em todas as contas membros de uma AWS Organizations organização para o mesmo bucket do Amazon S3, CloudWatch Logs e Amazon. EventBridge Criar uma trilha

da organização ajuda você a definir uma estratégia de registro de eventos uniforme para sua organização.

Todas as trilhas da organização criadas usando o console são trilhas da organização em várias regiões que registram eventos da conta habilitada Regiões da AWS em cada membro da organização. Para registrar eventos em todas as AWS partições da sua organização, crie uma trilha organizacional multirregional em cada partição. Você pode criar uma trilha organizacional de uma única região ou de várias regiões usando o. AWS CLI Se você criar uma trilha de região única, registrará atividades somente na trilha Região da AWS (também conhecida como Região de origem).

Embora a maioria Regiões da AWS esteja ativada por padrão para você Conta da AWS, você deve ativar manualmente determinadas regiões (também chamadas de regiões opcionais). Para obter informações sobre quais regiões estão habilitadas por padrão, consulte Considerações antes de ativar e desativar regiões no Guia de AWS Account Management referência. Para ver a lista de regiões CloudTrail compatíveis, consulteCloudTrail Regiões suportadas.

Quando você cria uma trilha da organização, uma cópia da trilha com o nome que você dá a ela é criada nas contas dos membros que pertencem à sua organização.

- Se a trilha da organização for para uma única região e a região de origem da trilha não for uma região OPT, uma cópia da trilha será criada na região de origem da trilha da organização na conta de cada membro.
- Se a trilha da organização for para uma única região e a região de origem da trilha for uma região OPT, uma cópia da trilha será criada na região de origem da trilha da organização nas contas dos membros que habilitaram essa região.
- Se a trilha da organização for multirregional e a região de origem da trilha não for uma região opcional, uma cópia da trilha será criada em cada uma habilitada Região da AWS na conta de cada membro. Quando uma conta de membro ativa uma região de adesão, uma cópia da trilha multirregional é criada na região recém-selecionada para a conta membro após a conclusão da ativação dessa região.
- Se a trilha da organização for multirregional e a região de origem for uma região opcional, as contas dos membros não enviarão atividades para a trilha da organização, a menos que optem pela trilha multirregional em Região da AWS que a trilha multirregional foi criada. Por exemplo, se você criar uma trilha multirregional e escolher a região da Europa (Espanha) como a região de origem da trilha, somente as contas dos membros que habilitaram a região da Europa (Espanha) para sua conta enviarão a atividade da conta para a trilha da organização.

> **Note**
>
> CloudTrail cria trilhas organizacionais nas contas dos membros, mesmo que a validação de um recurso falhe. Exemplos de falhas de validação incluem:
>
> - uma política incorreta de bucket do Amazon S3
> - uma política de tópicos incorreta do Amazon SNS
> - incapacidade de entregar para um grupo de CloudWatch registros de registros
> - permissão insuficiente para criptografar usando uma chave KMS
>
> Uma conta membro com CloudTrail permissões pode ver qualquer falha de validação de uma trilha da organização visualizando a página de detalhes da trilha no CloudTrail console ou executando o AWS CLI get-trail-statuscomando.

Os usuários com CloudTrail permissões nas contas dos membros poderão ver as trilhas da organização (incluindo o ARN da trilha) ao entrarem no AWS CloudTrail console a partir de suas AWS contas ou ao executarem AWS CLI comandos como `describe-trails` (embora as contas dos membros devam usar o ARN para a trilha da organização, e não o nome, ao usar a). AWS CLI No entanto, os usuários nas contas dos membros não terão permissões suficientes para excluir trilhas da organização, ativar ou desativar o login, alterar os tipos de eventos registrados ou alterar as trilhas da organização de qualquer forma. Para obter mais informações sobre o AWS Organizations, consulte Terminologia e conceitos da organização. Para obter mais informações sobre como criar e trabalhar com trilhas da organização, consulte Criar uma trilha para uma organização.

CloudTrail Armazenamentos de dados de lagos e eventos

CloudTrail O Lake permite que você execute consultas detalhadas baseadas em SQL em seus eventos e registre eventos de fontes externas AWS, inclusive de seus próprios aplicativos e de parceiros integrados com o. CloudTrail Você não precisa ter uma trilha configurada em sua conta para usar o CloudTrail Lake.

Os eventos são agregados em armazenamentos de dados de eventos, que são coleções imutáveis de eventos com base nos critérios que você seleciona aplicando seletores de eventos avançados. Você pode manter os dados do evento em um armazenamento de dados de eventos por até 3.653 dias (cerca de 10 anos) se escolher a opção de preço de retenção extensível de um ano ou até

2.557 dias (cerca de 7 anos) se escolher a opção de preço de retenção por sete anos. Você pode salvar consultas do Lake para uso futuro e visualizar resultados de consultas por até sete dias. Você também pode salvar os resultados da consulta em um bucket do S3. CloudTrail O Lake também pode armazenar eventos de uma organização AWS Organizations em um armazenamento de dados de eventos ou eventos de várias regiões e contas. CloudTrail O Lake faz parte de uma solução de auditoria que ajuda você a realizar investigações de segurança e solucionar problemas. Para obter mais informações, consulte Trabalhando com AWS CloudTrail Lake e CloudTrail Conceitos e terminologia do lago.

CloudTrail Percepções

CloudTrail O Insights ajuda AWS os usuários a identificar e responder a volumes incomuns de chamadas de API ou erros registrados nas chamadas de API, analisando continuamente os eventos CloudTrail de gerenciamento. Um evento do Insights é um registro de níveis incomuns de `write` atividade da API de gerenciamento ou níveis incomuns de erros retornados na atividade da API de gerenciamento. Por padrão, trilhas e armazenamentos de dados de eventos não registram eventos do CloudTrail Insights. No console, é possível optar por registrar em log eventos do Insights ao criar ou atualizar uma trilha ou um armazenamento de dados de eventos. Ao usar a CloudTrail API, você pode registrar eventos do Insights editando as configurações de uma trilha existente ou armazenamento de dados de eventos com a `PutInsightSelectors`API. Cobranças adicionais se aplicam ao registro de eventos do CloudTrail Insights. Você será cobrado separadamente se ativar o Insights tanto para trilhas quanto para armazenamentos de dados de eventos. Para obter mais informações, consulte Registrar eventos do Insights e Definição de preço do AWS CloudTrail.

Tags

Uma tag é uma chave definida pelo cliente e um valor opcional que pode ser atribuído a AWS recursos, como CloudTrail trilhas, armazenamentos de dados de eventos e canais, buckets do S3 usados para armazenar arquivos de CloudTrail log, AWS Organizations organizações e unidades organizacionais e muito mais. Ao adicionar as mesmas tags às trilhas e aos buckets do S3 que você usa para armazenar arquivos de log das trilhas, você pode facilitar o gerenciamento, a pesquisa e a filtragem desses recursos. AWS Resource Groups Você pode implementar estratégias de marcação para ajudá-lo a encontrar e gerenciar seus recursos de forma consistente, efetiva e fácil. Para obter mais informações, consulte Melhores práticas para marcar AWS recursos.

AWS Security Token Service e CloudTrail

AWS Security Token Service (AWS STS) é um serviço que tem um endpoint global e também oferece suporte a endpoints específicos da região. Endpoint é um URL que é o ponto de entrada para solicitações de web service. Por exemplo, `https://cloudtrail.us-west-2.amazonaws.com` é o ponto de entrada regional do Oeste dos EUA (Oregon) para o AWS CloudTrail serviço. Os endpoints regionais ajudam a reduzir a latência em suas aplicações.

Quando você usa um AWS STS endpoint específico da região, a trilha nessa região fornece somente os AWS STS eventos que ocorrem nessa região. Por exemplo, se você estiver usando o endpoint `sts.us-west-2.amazonaws.com`, a trilha em us-west-2 fornece apenas os eventos AWS STS originados em us-west-2. Para obter mais informações sobre endpoints AWS STS regionais, consulte Ativação e desativação AWS STS em uma AWS região no Guia do usuário do IAM.

Para obter uma lista completa de endpoints AWS regionais, consulte AWS Regiões e endpoints no. Referência geral da AWS Para ver detalhes sobre os eventos do endpoint global AWS STS , consulte Eventos de serviços globais.

Eventos de serviços globais

> **Important**
>
> Em 22 de novembro de 2021, AWS CloudTrail mudou a forma como as trilhas capturam eventos de serviços globais. Agora, os eventos criados pela Amazon CloudFront AWS Identity and Access Management, e AWS STS são registrados na região em que foram criados, a região Leste dos EUA (Norte da Virgínia), us-east-1. Isso faz com que a forma como CloudTrail trata esses serviços seja consistente com a de outros serviços AWS globais. Para continuar recebendo eventos de serviços globais fora do Leste dos EUA (Norte da Virgínia), certifique-se de converter as trilhas de região única que usam eventos de serviços globais fora do Leste dos EUA (Norte da Virgínia) para trilhas de várias regiões. Para obter mais informações sobre como capturar eventos de serviços globais, consulte Como habilitar e desabilitar o registro de eventos de serviços globais que aparece adiante nesta seção. Por outro lado, o histórico de eventos no CloudTrail console e o aws cloudtrail lookup-events comando mostrarão esses eventos no Região da AWS local em que eles ocorreram.

Para a maioria dos serviços, os eventos são registrados na região em que a ação ocorreu. Para serviços globais como AWS Identity and Access Management (IAM) e Amazon AWS STS CloudFront, os eventos são entregues em qualquer trilha que inclua serviços globais.

Para a maioria dos serviços globais, os eventos são registrados como ocorridos em uma região Leste dos EUA (Norte da Virgínia), mas alguns eventos de serviço globais são registrados como ocorridos em outras regiões, como a região Leste dos EUA (Ohio) ou a região Oeste dos EUA (Oregon).

Para evitar o recebimento de eventos de serviços globais duplicados, lembre-se do seguinte:

- Os eventos de serviço global são entregues por padrão às trilhas criadas usando o CloudTrail console. Os eventos resumo são fornecidos ao bucket da trilha.
- Se você tiver várias trilhas de região única, considere a possibilidade de configurar suas trilhas para que os eventos de serviços globais sejam fornecidos somente em uma das trilhas. Para ter mais informações, consulte Como habilitar e desabilitar o registro de eventos de serviços globais.
- Quando você altera a configuração de uma trilha de registrar todas as regiões para registrar uma única região, o registro em log de eventos de serviços globais é desativado automaticamente para essa trilha. Do mesmo modo, quando você altera a configuração de uma trilha de registrar uma região única para registrar todas as regiões, o registro em log de eventos de serviços globais é ativado automaticamente para essa trilha.

  Para obter mais informações sobre como alterar o registro de eventos de serviços globais de uma trilha, consulte Como habilitar e desabilitar o registro de eventos de serviços globais.

Exemplo:

1. Você cria uma trilha no CloudTrail console. Por padrão, essa trilha registra eventos de serviços globais.
2. Você tem várias trilhas de região única.
3. Não é necessário incluir serviços globais para as trilhas de região única. Os eventos de serviços globais são fornecidos à primeira trilha. Para ter mais informações, consulte Criando, atualizando e gerenciando trilhas com o AWS CLI.

> **Note**
>
> Ao criar ou atualizar uma trilha com AWS SDKs ou CloudTrail API, você pode especificar se deseja incluir ou excluir eventos de serviço global para trilhas. AWS CLI Você não pode configurar o registro global de eventos do serviço a partir do CloudTrail console.

CloudTrail Regiões suportadas

> **Note**
>
> Para obter informações sobre regiões suportadas pelo CloudTrail Lake, consulteCloudTrail Regiões suportadas por lagos.
> Para obter informações sobre os pontos finais do plano de dados, consulte Pontos finais do plano de dados no. Referência geral da AWS

Nome da região	Região	Ponto final do plano de controle	Protocolo	Data do suporte
Leste dos EUA (Norte da Virgínia)	us-east-1	cloudtrail.us-east-1.amazonaws.com	HTTPS	13/11/2013
Leste dos EUA (Ohio)	us-east-2	cloudtrail.us-east-2.amazonaws.com	HTTPS	17/10/2016
Oeste dos EUA (Norte da Califórnia)	us-west-1	cloudtrail.us-west-1.amazonaws.com	HTTPS	13/05/2014
Oeste dos EUA (Oregon)	us-west-2	cloudtrail.us-west-2.amazonaws.com	HTTPS	13/11/2013

Nome da região	Região	Ponto final do plano de controle	Protocolo	Data do suporte
África (Cidade do Cabo)	af-south-1	cloudtrail.af-south-1.amazonaws.com	HTTPS	22/04/2020
Ásia-Pacífico (Hong Kong)	ap-east-1	cloudtrail.ap-east-1.amazonaws.com	HTTPS	24/04/2019
Ásia-Pacífico (Hyderabad)	ap-south-2	cloudtrail.ap-south-2.amazonaws.com	HTTPS	22/11/2022
Ásia-Pacífico (Jacarta)	ap-southeast-3	cloudtrail.ap-southeast-3.amazonaws.com	HTTPS	13/12/2021
Ásia-Pacífico (Melbourne)	ap-southeast-4	cloudtrail.ap-southeast-4.amazonaws.com	HTTPS	23/01/2023
Ásia-Pacífico (Mumbai)	ap-south-1	cloudtrail.ap-south-1.amazonaws.com	HTTPS	27/06/2016
Asia Pacific (Osaka)	ap-northeast-3	cloudtrail.ap-northeast-3.amazonaws.com	HTTPS	12/02/2018
Ásia-Pacífico (Seul)	ap-northeast-2	cloudtrail.ap-northeast-2.amazonaws.com	HTTPS	06/01/2016
Ásia-Pacífico (Singapura)	ap-southeast-1	cloudtrail.ap-southeast-1.amazonaws.com	HTTPS	30/06/2014

Nome da região	Região	Ponto final do plano de controle	Protocolo	Data do suporte
Ásia-Pacífico (Sydney)	ap-southeast-2	cloudtrail.ap-southeast-2.amazonaws.com	HTTPS	13/05/2014
Ásia-Pacífico (Tóquio)	ap-northeast-1	cloudtrail.ap-northeast-1.amazonaws.com	HTTPS	30/06/2014
Canadá (Central)	ca-central-1	cloudtrail.ca-central-1.amazonaws.com	HTTPS	08/12/2016
Oeste do Canadá (Calgary)	ca-west-1	cloudtrail.ca-west-1.amazonaws.com	HTTPS	20/12/2023
China (Pequim)	cn-north-1	cloudtrail.cn-north-1.amazonaws.com.cn	HTTPS	01/03/2014
China (Ningxia)	cn-northwest-1	cloudtrail.cn-northwest-1.amazonaws.com.cn	HTTPS	11/12/2017
Europa (Frankfurt)	eu-central-1	cloudtrail.eu-central-1.amazonaws.com	HTTPS	23/10/2014
Europa (Irlanda)	eu-west-1	cloudtrail.eu-west-1.amazonaws.com	HTTPS	13/05/2014
Europa (Londres)	eu-west-2	cloudtrail.eu-west-2.amazonaws.com	HTTPS	13/12/2016
Europa (Milão)	eu-south-1	cloudtrail.eu-south-1.amazonaws.com	HTTPS	27/04/2020
Europa (Paris)	eu-west-3	cloudtrail.eu-west-3.amazonaws.com	HTTPS	18/12/2017

Nome da região	Região	Ponto final do plano de controle	Protocolo	Data do suporte
Europa (Espanha)	eu-south-2	cloudtrail.eu-south-2.amazonaws.com	HTTPS	16/11/2022
Europa (Estocolmo)	eu-north-1	cloudtrail.eu-north-1.amazonaws.com	HTTPS	11/12/2018
Europa (Zurique)	eu-central-2	cloudtrail.eu-central-2.amazonaws.com	HTTPS	11/09/2022
Israel (Tel Aviv)	il-central-1	cloudtrail.il-central-1.amazonaws.com	HTTPS	31/07/2023
Oriente Médio (Barém)	me-south-1	cloudtrail.me-south-1.amazonaws.com	HTTPS	29/jul/2019
Oriente Médio (Emirados Árabes Unidos)	me-central-1	cloudtrail.me-central-1.amazonaws.com	HTTPS	30/08/2022
América do Sul (São Paulo)	sa-east-1	cloudtrail.sa-east-1.amazonaws.com	HTTPS	30/06/2014
AWS GovCloud (Leste dos EUA)	us-gov-east-1	cloudtrail.us-gov-east-1.amazonaws.com	HTTPS	12/11/2018
AWS GovCloud (Oeste dos EUA)	us-gov-west-1	cloudtrail.us-gov-west-1.amazonaws.com	HTTPS	16/08/2011

Para obter mais informações sobre o uso CloudTrail no AWS GovCloud (US) Regions, consulte Service Endpoints no Guia do AWS GovCloud (US) usuário.

Para obter mais informações sobre o uso CloudTrail na região da China (Pequim), consulte Endpoints e ARNs para AWS na China no. Referência geral da Amazon Web Services

CloudTrail serviços e integrações suportados

CloudTrail suporta eventos de registro para muitos Serviços da AWS. Você pode encontrar informações específicas para cada serviço compatível no guia do serviço. Para obter uma lista de tópicos específicos do serviço, consulte. AWS tópicos de serviço para CloudTrail Além disso, alguns Serviços da AWS podem ser usados para analisar e agir com base nos dados coletados nos CloudTrail registros.

> **Note**
>
> Para ver a lista de regiões com suporte para cada serviço, consulte Endpoints e cotas de serviços no Referência geral da Amazon Web Services.

Tópicos

- AWS integrações de serviços com registros CloudTrail
- CloudTrail integração com a Amazon EventBridge
- CloudTrail integração com AWS Organizations
- AWS tópicos de serviço para CloudTrail
- CloudTrail serviços não suportados

AWS integrações de serviços com registros CloudTrail

> **Note**
>
> Você também pode usar o CloudTrail Lake para consultar e analisar seus eventos. CloudTrail As consultas do Lake oferecem uma visão mais profunda e personalizável dos eventos do que pesquisas simples de chaves e valores no histórico de eventos ou em execução. `LookupEvents` CloudTrail Os usuários do Lake podem executar consultas complexas de linguagem de consulta padrão (SQL) em vários campos em um CloudTrail evento. Para obter

mais informações, consulte Trabalhando com AWS CloudTrail Lake e Copiando eventos da trilha para o CloudTrail lago.
CloudTrail Os armazenamentos e consultas de dados de eventos em Lake incorrem CloudTrail em cobranças. Para obter mais informações sobre os preços do CloudTrail Lake, consulte AWS CloudTrail Preços.

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 os tópicos a seguir.

AWS Serviço	Tópico	Descrição
Amazon Athena	Consultando registros AWS CloudTrail	Usar o Athena com CloudTrail registros é uma forma poderosa de aprimorar sua análise da atividade do AWS serviço. Por exemplo, é possível usar consultas para identificar tendências e isolar ainda mais a atividade por atributos, como endereço IP de origem ou usuário. Você pode criar tabelas automaticamente para consultar registros diretamente do CloudTrail console e usar essas tabelas para executar consultas no Athena. Para obter mais informações, consulte Criação de uma tabela para CloudTrail registros no CloudTrail console no Guia do usuário do Amazon Athena.

AWS Serviço	Tópico	Descrição
		Note Executar consultas no Amazon Athena implica custos adicionais. Para obter mais informações, consulte Preços do Amazon Athena.
CloudWatch Registros da Amazon	Monitoramento CloudTrail de arquivos de log com o Amazon CloudWatch Logs	Você pode configurar CloudTrail com o CloudWatch Logs para monitorar seus registros de trilhas e ser notificado quando ocorrer uma atividade específica. Por exemplo, você pode definir filtros métricos de CloudWatch registros que acionarão CloudWatch alarmes e enviarão notificações para você quando esses alarmes forem acionados. **Note** Aplica-se o preço padrão para Amazon CloudWatch e Amazon CloudWatch Logs. Para obter mais informações, consulte Definição de preço do Amazon CloudWatch .

CloudTrail integração com a Amazon EventBridge

EventBridge A Amazon é um AWS serviço que fornece um fluxo quase em tempo real de eventos do sistema que descrevem mudanças nos AWS recursos. Em EventBridge, você pode criar regras que respondam aos eventos registrados por CloudTrail. Para obter mais informações, consulte Criar uma regra na Amazon EventBridge.

Você pode oferecer eventos nos quais está inscrito EventBridge criando uma regra com o EventBridge console.

Do EventBridge console:

- Escolha o `AWS API Call via CloudTrail` tipo de detalhe para fornecer CloudTrail dados e eventos de gerenciamento com um `eventType` de. `AwsApiCall` Para registrar eventos com um valor de tipo detalhado de`AWS API Call via CloudTrail`, você deve ter uma trilha que esteja registrando eventos de gerenciamento ou de dados no momento.
- Escolha o `AWS Console Sign In via CloudTrail` tipo de detalhe para oferecer eventos de AWS Management Console login. Para registrar eventos com um tipo detalhado de`AWS Console Sign In via CloudTrail`, você deve ter uma trilha que esteja registrando eventos de gerenciamento no momento.
- Escolha o `AWS Insight via CloudTrail` tipo de detalhe para oferecer eventos do Insights. Para registrar eventos com um valor do tipo de detalhe de`AWS Insight via CloudTrail`, você deve ter uma trilha que esteja registrando eventos do Insights no momento. Para obter mais informações sobre registro em log de eventos do Insights, consulte Registrar eventos do Insights.

Para obter mais informações sobre como criar uma trilha, consulte Criar uma trilha.

CloudTrail integração com AWS Organizations

A conta de gerenciamento de uma AWS Organizations organização pode adicionar um administrador delegado para gerenciar os CloudTrail recursos da organização. É possível criar uma trilha ou um armazenamento de dados de eventos na conta de gerenciamento ou conta de administrador delegado de uma organização que colete todos os dados de eventos de todas as contas da AWS em uma organização no AWS Organizations. Criar uma trilha da organização ajuda você a definir uma estratégia de registro de eventos uniforme para sua organização.

Uma trilha organizacional é aplicada automaticamente a cada AWS conta em sua organização. Os usuários de contas-membro podem ver essas trilhas, mas não podem modificá-las e, por padrão,

não podem ver os arquivos de log criados para a trilha da organização. Para ter mais informações, consulte Criar uma trilha para uma organização.

AWS tópicos de serviço para CloudTrail

Você pode aprender mais sobre como os eventos de AWS serviços individuais são registrados em CloudTrail registros, incluindo exemplos de eventos desse serviço em arquivos de log. Para obter mais informações sobre como AWS serviços específicos se integram CloudTrail, consulte o tópico sobre integração no guia individual desse serviço.

Serviços que ainda estão em versão prévia, que ainda não foram lançados para disponibilidade geral (GA) ou que não têm APIs públicas, não são considerados compatíveis. CloudTrail atualmente não registra eventos específicos da política de endpoints do Amazon VPC.

> **Note**
>
> Para ver a lista de regiões com suporte para cada serviço, consulte Endpoints e cotas de serviços no Referência geral da Amazon Web Services.
> Para obter mais informações sobre quais serviços registram em log de eventos de dados, consulte Eventos de dados.

AWS Serviço	CloudTrail Tópicos	O suporte começou
Amazon API Gateway	Registre chamadas de gerenciamento de API para o Amazon API Gateway usando AWS CloudTrail	09/07/2015
Amazon AppFlow	Registrando chamadas de AppFlow API da Amazon com AWS CloudTrail	22/04/2020
Amazon AppStream 2.0	Registrando chamadas de API da Amazon AppStream 2.0 com AWS CloudTrail	25/04/2019

AWS Serviço	CloudTrail Tópicos	O suporte começou
Amazon Athena	Registro de chamadas de API do Amazon Athena com AWS CloudTrail	19/05/2017
Amazon Aurora	Monitoramento de chamadas de API do Amazon Aurora em AWS CloudTrail	31/08/2018
Amazon Bedrock	Registre chamadas da API Amazon Bedrock usando AWS CloudTrail	23/10/2023
Amazon Braket	Registro da API Amazon Braket com CloudTrail	08/12/2020
Amazon Chime	Registre chamadas de administração do Amazon Chime usando AWS CloudTrail	27/09/2017
Amazon Cloud Directory	Registrando chamadas de API do Cloud Directory usando AWS CloudTrail	26/01/2017
Amazon CloudFront	Usando AWS CloudTrail para capturar solicitações enviadas para a CloudFront API	28/05/2014
Amazon CloudSearch	Registrando chamadas CloudSearch do Amazon Configuration Service usando AWS CloudTrail	16/10/2014
Amazon CloudWatch	Registro de chamadas CloudWatch de API da Amazon AWS CloudTrail	30/04/2014

AWS Serviço	CloudTrail Tópicos	O suporte começou
CloudWatch Registros da Amazon	Registro de chamadas CloudWatch de API do Amazon Logs em AWS CloudTrail	10/03/2016
Amazon CodeCatalyst	Registro de chamadas de CodeCatalyst API em Connected Contas da AWS usando AWS CloudTrail	12/01/2022
CodeGuru Revisor da Amazon	Registro de chamadas de API do Amazon CodeGuru Reviewer com AWS CloudTrail	02/12/2019
Amazon CodeWhisperer	AWS CloudTrail e CodeWhisperer APIs	13/04/2023
Amazon Cognito	Registro de chamadas de API do Amazon Cognito com AWS CloudTrail	18/02/2016
Amazon Comprehend	Registro de chamadas de API do Amazon Comprehend com AWS CloudTrail	17/01/2018
Amazon Comprehend Medical	Log de chamadas de API do Amazon Comprehend Medical usando o AWS CloudTrail	27/11/2018
Amazon Connect	Log de chamadas de API do Amazon Connect com o AWS CloudTrail	11/12/2019
Amazon Data Firehose	Monitorando chamadas de API do Amazon Data Firehose com AWS CloudTrail	17/03/2016

AWS Serviço	CloudTrail Tópicos	O suporte começou
Amazon Data Lifecycle Manager	Registro de chamadas de API do Amazon Data Lifecycle Manager usando AWS CloudTrail	24/07/2018
Amazon Detective	Log de chamadas de API do Amazon Detective com o AWS CloudTrail	31/03/2020
DevOpsGuru da Amazon	Registrando chamadas de API do Amazon DevOps Guru com AWS CloudTrail	05/04/2021
Amazon DocumentDB (compatível com MongoDB)	Log de chamadas de API do Amazon DocumentDB com o AWS CloudTrail	09/01/2019
Amazon DynamoDB	Registrando operações do DynamoDB usando AWS CloudTrail	28/05/2015
Amazon EC2	Registre chamadas de API do Amazon EC2 usando AWS CloudTrail	13/11/2013
Amazon EC2 Auto Scaling	Registrando chamadas da API Auto Scaling usando CloudTrail	16/07/2014
Blocos de capacidade do Amazon EC2	Registrando chamadas de API de blocos de capacidade com AWS CloudTrail	31/10/2023
Amazon EC2 Image Builder	Registrando chamadas da API do EC2 Image Builder usando CloudTrail	02/12/2019

AWS Serviço	CloudTrail Tópicos	O suporte começou
Amazon Elastic Block Store (Amazon EBS) APIs diretas do EBS	Registrando chamadas de API usando AWS CloudTrail Registrar chamadas de API para as APIs diretas do EBS com AWS CloudTrail	Amazon EBS: 13/11/2013 APIs diretas do EBS: 30/06/2020
Amazon Elastic Container Registry (Amazon ECR)	Registrando chamadas de API do Amazon ECR usando AWS CloudTrail	21/12/2015
Amazon Elastic Container Service (Amazon ECS)	Registrando chamadas de API do Amazon ECS usando AWS CloudTrail	09/04/2015
Amazon Elastic File System (Amazon EFS)	Registro de chamadas de API do Amazon EFS com AWS CloudTrail	28/06/2016
Amazon Elastic Kubernetes Service (Amazon EKS)	Registro de chamadas de API do Amazon EKS com AWS CloudTrail	05/06/2018
Amazon Elastic Transcoder	Registro de chamadas de API do Amazon Elastic Transcoder com AWS CloudTrail	27/10/2014
Amazon ElastiCache	Registrando chamadas de ElastiCache API da Amazon usando AWS CloudTrail	15/09/2014
Amazon EMR	Registro de chamadas de API do Amazon EMR em AWS CloudTrail	04/04/2014

AWS Serviço	CloudTrail Tópicos	O suporte começou
Amazon EMR no EKS	Log de chamadas de API do Amazon EMR no EKS usando o AWS CloudTrail	12/09/2020
Amazon EventBridge	Registrando chamadas de EventBridge API da Amazon usando AWS CloudTrail	11/07/2019
Amazon FinSpace	Consultando registros AWS CloudTrail	18/10/2022
Amazon Forecast	Registrando chamadas da API Amazon Forecast com AWS CloudTrail	28/11/2018
Amazon Fraud Detector	Log de chamadas de API do Amazon Fraud Detector com o AWS CloudTrail	01/09/2020
Amazon FSx for Lustre	Registro de chamadas de API do Amazon FSx for Lustre com AWS CloudTrail	11/01/2019
Amazon FSx for Windows File Server	Monitoramento com AWS CloudTrail	28/11/2018
Amazon GameLift	Registrando chamadas de GameLift API da Amazon com AWS CloudTrail	27/01/2016
Amazon GuardDuty	Registrando chamadas de GuardDuty API da Amazon com AWS CloudTrail	12/02/2018
Amazon Inspector	Registrando chamadas de API do Amazon Inspector usando AWS CloudTrail	29/11/2021

AWS Serviço	CloudTrail Tópicos	O suporte começou
Amazon Inspector Classic	Registro de chamadas de API do Amazon Inspector Classic com AWS CloudTrail	20/04/2016
Verificação do Amazon Inspector	Amazon Inspector Digitalize informações em CloudTrail	27/11/2023
Amazon Interactive Video Service	Log de chamadas de API do Amazon IVS com o AWS CloudTrail	15/07/2020
Amazon Kendra	Registro de chamadas da API Amazon Kendra AWS CloudTrail com e registro de chamadas da API Amazon Kendra Intelligent Ranking com registros AWS CloudTrail	11/05/2020
Amazon Keyspaces (para Apache Cassandra)	Log de chamadas de API do Amazon Keyspaces com o AWS CloudTrail	13/01/2020
Amazon Managed Service for Apache Flink	Registro de chamadas de serviço gerenciado para a API Apache Flink com AWS CloudTrail	22/03/2019
Amazon Kinesis Data Streams	Registro de chamadas de API do Amazon Kinesis Data Streams usando AWS CloudTrail	25/04/2014
Amazon Kinesis Video Streams	Registro de chamadas de API do Kinesis Video Streams com AWS CloudTrail	24/05/2018

AWS Serviço	CloudTrail Tópicos	O suporte começou
Amazon Lex	Registro de chamadas de API do Amazon Lex com CloudTrail	15/08/2017
Amazon Lightsail	Registro de chamadas da API Lightsail com AWS CloudTrail	23/12/2016
Amazon Location Service	Registro e monitoramento com o AWS CloudTrail	15/12/2020
Amazon Lookout for Equipment	Monitorando o Amazon Lookout for Equipment	12/01/2020
Amazon Lookout for Metrics	Visualizando a atividade da API Amazon Lookout for Metrics em AWS CloudTrail	12/08/2020
Amazon Lookout for Vision	Log de chamadas do Amazon Lookout for Vision com o AWS CloudTrail	12/01/2020
Amazon Machine Learning	Registrando chamadas de API do Amazon ML usando AWS CloudTrail	10/12/2015
Amazon Macie	Registre chamadas de API do Amazon Macie usando o AWS CloudTrail	13/05/2020
Amazon Managed Blockchain	Log de chamadas de API do Amazon Managed Blockchain usando o AWS CloudTrail Log de chamadas de API do Ethereum para Managed Blockchain usando AWS CloudTrail (previsualização)	04/01/2019

AWS Serviço	CloudTrail Tópicos	O suporte começou
Amazon Managed Grafana	Log de chamadas de API do Amazon Managed Grafana usando o AWS CloudTrail	15/12/2020
Amazon Managed Service para Prometheus	Log de chamadas de API do Amazon Managed Service for Prometheus usando o AWS CloudTrail	15/12/2020
Amazon Managed Streaming for Apache Kafka	Registrando chamadas de API com AWS CloudTrail	11/12/2018
Amazon Managed Workflows for Apache Airflow	Visualizando registros de auditoria em AWS CloudTrail	24/11/2020
Amazon MemoryDB para Redis	Registro de chamadas de API do Amazon MemoryDB para Redis com AWS CloudTrail	19/08/2021
Amazon MQ	Registrando chamadas de API do Amazon MQ usando AWS CloudTrail	19/07/2018
Amazon Neptune	Registro de chamadas de API do Amazon Neptune usando AWS CloudTrail	30/05/2018
Amazon Nimble Studio	Registrando chamadas do Nimble Studio usando AWS CloudTrail	19/06/2023
Amazon One Enterprise	Registro de chamadas de API do Amazon One Enterprise usando AWS CloudTrail	27/11/2023

AWS Serviço	CloudTrail Tópicos	O suporte começou
OpenSearch Serviço Amazon	Monitorando chamadas OpenSearch de API do Amazon Service com AWS CloudTrail	01/10/2015
Amazon Personalize	Registro de chamadas de API do Amazon Personalize com AWS CloudTrail	28/11/2018
Amazon Pinpoint	Registro de chamadas de API do Amazon Pinpoint com AWS CloudTrail	06/02/2018
SMS do Amazon Pinpoint API de voz	Registro de chamadas de API do Amazon Pinpoint com AWS CloudTrail	16/11/2018
Amazon Polly	Registro de chamadas de API do Amazon Polly com AWS CloudTrail	30/11/2016
Amazon Q (para uso empresarial)	Registrando chamadas da API Amazon Q usando AWS CloudTrail	28/11/2023
Amazon Q (para uso do AWS Builder)	Registrando chamadas da API Amazon Q usando AWS CloudTrail	28/11/2023
Amazon Quantum Ledger Database (Amazon QLDB)	Registro de chamadas de API do Amazon QLDB com o AWS CloudTrail	10/09/2019
Amazon QuickSight	Operações de registro com CloudTrail	28/04/2017

AWS Serviço	CloudTrail Tópicos	O suporte começou
Amazon Relational Database Service (Amazon RDS)	Registrando chamadas de API do Amazon RDS usando AWS CloudTrail	13/11/2013
Insights de Performance do Amazon RDS	Registrando chamadas de API do Amazon RDS usando AWS CloudTrail A API Performance Insights do Amazon RDS é um subconjunto da API do Amazon RDS.	21/06/2018
Amazon Redshift	Registro de chamadas de API do Amazon Redshift com AWS CloudTrail	10/06/2014
Amazon Rekognition	Registro de chamadas da API Amazon Rekognition usando AWS CloudTrail	06/04/2018
Amazon Route 53	Uso do AWS CloudTrail para capturar solicitações enviadas à API do Route 53	11/02/2015
Controlador de recuperação de aplicação do Amazon Route 53	Registro de chamadas de API do Amazon Route 53 Application Recovery Controller usando AWS CloudTrail	27/07/2021
Amazon S3	Registrando chamadas de API do Amazon S3 usando AWS CloudTrail	Eventos de gerenciamento: 01/09/2015 Eventos de dados: 21/11/2016
Amazon S3 Glacier	Registrando chamadas de API do S3 Glacier usando AWS CloudTrail	11/12/2014

AWS Serviço	CloudTrail Tópicos	O suporte começou
Amazon SageMaker	Registrando chamadas de SageMaker API da Amazon com AWS CloudTrail	11/01/2018
Amazon Security Lake	Registro de chamadas de API do Amazon Security Lake usando CloudTrail	30/05/2023
Amazon Simple Email Service (Amazon SES)	Registrando chamadas de API do Amazon SES usando AWS CloudTrail	07/05/2015
Amazon Simple Notification Service (Amazon SNS)	Registro de chamadas de API do Amazon SNS usando AWS CloudTrail	09/10/2014
Amazon Simple Queue Service (Amazon SQS)	Registrando ações da API do Amazon SQS usando AWS CloudTrail	16/07/2014
Amazon Simple Workflow Service (Amazon SWF)	Gravando chamadas de API com AWS CloudTrail	Eventos de gestão: 13/05/2014 Eventos de dados: 14/02/2024
Amazon Textract	Registro de chamadas da API Amazon Textract com AWS CloudTrail	05/29/2019
Amazon Timestream	Registrando chamadas da API Timestream com AWS CloudTrail	30/09/2020
Amazon Transcribe	Registro de chamadas da API Amazon Transcribe com AWS CloudTrail	28/06/2018

AWS Serviço	CloudTrail Tópicos	O suporte começou
Amazon Translate	Log de chamadas de API do Amazon Translate com o AWS CloudTrail	04/04/2018
Amazon Verified Permissions	Registro de chamadas da API de permissões verificadas da Amazon usando AWS CloudTrail	13/06/2023
Amazon Virtual Private Cloud (Amazon VPC)	Registrando chamadas de API usando AWS CloudTrail A API do Amazon VPC é um subconjunto da API do Amazon EC2.	13/11/2013
Amazon VPC Lattice	CloudTrail troncos	31/03/2023
Amazon VPC Reachability Analyzer	Registrando chamadas da API Reachability Analyzer usando AWS CloudTrail	27/11/2023
Amazon WorkDocs	Registrando chamadas de WorkDocs API da Amazon usando AWS CloudTrail	27/08/2014
Amazon WorkMail	Registrando chamadas de WorkMail API da Amazon usando AWS CloudTrail	12/12/2017
Amazon WorkSpaces	Registrando chamadas de WorkSpaces API da Amazon usando CloudTrail	09/04/2015
Amazon WorkSpaces Thin Client	Registro de chamadas de API do Amazon WorkSpaces Thin Client usando AWS CloudTrail	26/11/2023

AWS Serviço	CloudTrail Tópicos	O suporte começou
Amazon WorkSpaces Web	Registro de chamadas WorkSpaces da Amazon Web API usando AWS CloudTrail	30/11/2021
Application Auto Scaling	Registro de chamadas da API Application Auto Scaling com AWS CloudTrail	31/10/2016
AWS Amplify	Log de chamadas de API do Amplify usando o AWS CloudTrail	30/11/2020
AWS App Mesh	Registrar chamadas à API do App Mesh com o AWS CloudTrail	AWS App Mesh 30/10/2019 App Mesh Envoy Management Service 18/03/2022
AWS App Runner	Registrando chamadas da API App Runner com AWS CloudTrail	18/05/2021
AWS AppConfig	Registrando chamadas de AWS AppConfig API usando AWS CloudTrail	Eventos de gestão: 31/07/2020 Eventos de dados: 01/04/2024
AWS AppFabric	Registrando chamadas de AWS AppFabric API usando AWS CloudTrail	27/06/2023
AWS Perfil de custos de aplicativos	AWS Referência da API Application Cost Profiler	13/05/2021
AWS Application Discovery Service	Log de chamadas de API do Application Discovery Service com o AWS CloudTrail	12/05/2016

AWS Serviço	CloudTrail Tópicos	O suporte começou
AWS Serviço de transformação de aplicativos	(Serviço de back-end usado por AWS ferramentas, como o AWS Microservice Extractor para .NET)	26/08/2023
AWS AppSync	Registrando chamadas de AWS AppSync API com AWS CloudTrail	13/02/2018
AWS Artifact	Registrando chamadas de AWS Artifact API com AWS CloudTrail	27/01/2023
AWS Audit Manager	Registrando chamadas de AWS Audit Manager API com AWS CloudTrail	12/07/2020
AWS Auto Scaling	Registrando chamadas de AWS Auto Scaling API usando CloudTrail	15/08/2018
AWS Intercâmbio de dados B2B	Registrando AWS chamadas da API B2B Data Interchange usando AWS CloudTrail	12/01/2023
AWS Backup	Registrando chamadas de AWS Backup API com AWS CloudTrail	04/02/2019
AWS Batch	Registrando chamadas de AWS Batch API com AWS CloudTrail	10/01/2018
AWS Billing and Cost Management	Registrando chamadas de AWS Billing and Cost Management API com AWS CloudTrail	07/06/2018

AWS Serviço	CloudTrail Tópicos	O suporte começou
AWS Billing Conductor	Registrando chamadas de AWS Billing Conductor API usando AWS CloudTrail	03/12/2024
AWS BugBust	Registrando chamadas de BugBust API usando CloudTrail	24/06/2021
AWS Certificate Manager	Como usar o AWS CloudTrail	25/03/2016
AWS Clean Rooms	Registrando chamadas de AWS Clean Rooms API usando AWS CloudTrail	21/03/2023
AWS Cloud Map	Registrando chamadas de AWS Cloud Map API com AWS CloudTrail	28/11/2018
AWS Cloud9	Registrando chamadas de AWS Cloud9 API com AWS CloudTrail	21/01/2019
AWS CloudFormation	Registrando chamadas de AWS CloudFormation API em AWS CloudTrail	02/04/2014
AWS CloudHSM	Registrando chamadas de AWS CloudHSM API usando AWS CloudTrail	08/01/2015
AWS CloudShell	Registro e monitoramento em AWS CloudShell	15/12/2020
AWS CloudTrail	AWS CloudTrail Referência de API (todas as chamadas de CloudTrail API são registradas por CloudTrail.)	13/11/2013

AWS Serviço	CloudTrail Tópicos	O suporte começou
AWS CodeArtifact	Registrando chamadas de CodeArtifact API com AWS CloudTrail	06/10/2020
AWS CodeBuild	Registrando chamadas de AWS CodeBuild API com AWS CloudTrail	01/12/2016
AWS CodeCommit	Registrando chamadas de AWS CodeCommit API com AWS CloudTrail	11/01/2017
AWS CodeDeploy	Monitorando implantações com AWS CloudTrail	16/12/2014
AWS CodePipeline	Registrando chamadas de CodePipeline API com AWS CloudTrail	09/07/2015
AWS CodeStar	Registrando chamadas de AWS CodeStar API com AWS CloudTrail	14/06/2017
AWS CodeStar Notificações	Registrando chamadas da API de AWS CodeStar notificações com AWS CloudTrail	05/11/2019
AWS Config	Registrando chamadas de AWS Config API por meio de AWS CloudTrail	10/02/2015
AWS Catálogo de controle	Chamadas de API AWS do Logging Control Catalog usando AWS CloudTrail	04/08/2024

AWS Serviço	CloudTrail Tópicos	O suporte começou
AWS Control Tower	Registrando AWS Control Tower ações com AWS CloudTrail	12/ago/2019
AWS Data Pipeline	Registrando chamadas de AWS Data Pipeline API usando AWS CloudTrail	02/12/2014
AWS Database Migration Service (AWS DMS)	Registrando chamadas de AWS Database Migration Service API usando AWS CloudTrail	04/02/2016
AWS DataSync	Registrando chamadas de AWS DataSync API com AWS CloudTrail	26/11/2018
AWS Nuvem de prazos	Registrando chamadas com CloudTrail	04/02/2024
AWS Device Farm	Registrando chamadas de AWS Device Farm API usando AWS CloudTrail	13/07/2015
AWS Direct Connect	Registrando chamadas de AWS Direct Connect API em AWS CloudTrail	08/03/2014
AWS Directory Service	Registrando chamadas de AWS Directory Service API usando CloudTrail	14/05/2015
AWS Elastic Beanstalk (Elastic Beanstalk)	Usando chamadas de API do Elastic Beanstalk com AWS CloudTrail	31/03/2014

AWS Serviço	CloudTrail Tópicos	O suporte começou
AWS Elastic Disaster Recovery	Registrando chamadas de AWS Elastic Disaster Recovery API usando AWS CloudTrail	17/11/2021
AWS Elemental MediaConnect	Registrando chamadas de AWS Elemental MediaConnect API com AWS CloudTrail	27/11/2018
AWS Elemental MediaConvert	Registrando chamadas de AWS Elemental MediaConvert API com CloudTrail	27/11/2017
AWS Elemental MediaLive	Registrando chamadas de MediaLive API com AWS CloudTrail	19/01/2019
AWS Elemental MediaPackage	Registrando chamadas de AWS Elemental MediaPackage API com AWS CloudTrail	21/12/2018
AWS Elemental MediaStore	Registrando chamadas de AWS Elemental MediaStore API com CloudTrail	27/11/2017
AWS Elemental MediaTailor	Registrando chamadas de AWS Elemental MediaTailor API com AWS CloudTrail	11/02/2019
AWS Resolução de entidades	Registrando chamadas da API de resolução de AWS entidades usando A AWS CloudTrail	26/07/2023
AWS Fault Injection Service	Registre chamadas de API com AWS CloudTrail	15/03/2021

AWS Serviço	CloudTrail Tópicos	O suporte começou
AWS Firewall Manager	Registrando chamadas de AWS Firewall Manager API com AWS CloudTrail	05/04/2018
AWS Global Accelerator	Registrando chamadas de API do AWS Global Accelerator com AWS CloudTrail	26/11/2018
AWS Glue	Registrando AWS Glue operações usando AWS CloudTrail	07/11/2017
AWS Ground Station	Registrando chamadas de AWS Ground Station API com AWS CloudTrail	31/05/2019
AWS Health	Registrando chamadas de AWS Health API com AWS CloudTrail	21/11/2016
AWS Health Dashboard	Registrando chamadas de AWS Health API com AWS CloudTrail	01/12/2016
AWS HealthImaging	Registrando chamadas de AWS HealthImaging API usando AWS CloudTrail	26/07/2023
AWS HealthLake	Registrando chamadas de AWS HealthLake API com AWS CloudTrail	12/07/2020
AWS HealthOmics	Registrando chamadas de AWS HealthOmics API usando AWS CloudTrail	29/11/2022

AWS Serviço	CloudTrail Tópicos	O suporte começou
AWS IAM Identity Center	Registro de chamadas de API do IAM Identity Center com AWS CloudTrail	07/12/2017
AWS Identity and Access Management (IAM)	Registrando eventos do IAM com AWS CloudTrail	13/11/2013
AWS IoT	Registrando chamadas de AWS IoT API com AWS CloudTrail	11/04/2016
AWS IoT 1-Click	Registrando chamadas de AWS IoT 1-Click API com AWS CloudTrail	14/05/2018
AWS IoT Análise	Registrando chamadas da API AWS IoT Analytics com AWS CloudTrail	23/04/2018
AWS IoT Eventos	Registrando chamadas de API de AWS IoT eventos com AWS CloudTrail	06/11/2019
AWS IoT Greengrass	Registrando chamadas de AWS IoT Greengrass API com AWS CloudTrail	29/10/2018
AWS IoT Greengrass V2	Registre chamadas de API AWS IoT Greengrass V2 com AWS CloudTrail	14/12/2020
AWS IoT SiteWise	Registrando chamadas de AWS IoT SiteWise API com AWS CloudTrail	29/04/2020

AWS Serviço	CloudTrail Tópicos	O suporte começou
AWS Key Management Service (AWS KMS)	Registrando chamadas de AWS KMS API usando AWS CloudTrail	12/11/2014
AWS Lake Formation	Registrando chamadas de AWS Lake Formation API usando AWS CloudTrail	08/09/2019
AWS Lambda	Registrando chamadas de AWS Lambda API usando AWS CloudTrail	Eventos de gerenciamento: 09/04/2015 Eventos de dados: 30/11/2017
AWS Launch Wizard	Registrando chamadas de AWS Launch Wizard API usando AWS CloudTrail	11/08/2023
AWS License Manager	Registrando chamadas da API do AWS License Manager com AWS CloudTrail	01/03/2019
AWS Mainframe Modernization	Registrando chamadas de AWS Mainframe Modernization API usando AWS CloudTrail	06/08/2022
AWS Managed Services	Gerenciamento de registros no AMS Accelerate	21/12/2016
AWS Marketplace Acordos	Registrando chamadas de API de contratos usando AWS CloudTrail	09/01/2023
AWS Marketplace Serviço de implantação	Registrando chamadas AWS Marketplace do Serviço de Implantação com CloudTrail	29/11/2023

AWS Serviço	CloudTrail Tópicos	O suporte começou
AWS Marketplace Descoberta	Registrando chamadas da API AWS Marketplace Discovery usando AWS CloudTrail	15/12/2022
AWS Marketplace Serviço de medição	Registrando chamadas de AWS Marketplace API com AWS CloudTrail	08/22/2018
AWS Migration Hub	Registrando chamadas de API do AWS Migration Hub com AWS CloudTrail	14/08/2017
AWS Network Firewall	Registrando chamadas para a AWS Network Firewall API com AWS CloudTrail	17/11/2020
AWS OpsWorks for Chef Automate	Registrando chamadas de AWS OpsWorks for Chef Automate API com AWS CloudTrail	16/07/2018
AWS OpsWorks for Puppet Enterprise	Registro OpsWorks de chamadas de API do Puppet Enterprise com AWS CloudTrail	16/07/2018
AWS OpsWorks Stacks	Registrando chamadas de AWS OpsWorks Stacks API com AWS CloudTrail	04/06/2014
AWS Organizations	Registrando chamadas de AWS Organizations API com AWS CloudTrail	27/02/2017
AWS Outposts	Registrando chamadas de AWS Outposts API com AWS CloudTrail	02/04/2020

AWS Serviço	CloudTrail Tópicos	O suporte começou
AWS Panorama	Referência da API do AWS Panorama	20/10/2021
AWS Payment Cryptography	Registrando chamadas de AWS Payment Cryptography API usando AWS CloudTrail	06/08/2023
AWS 5G privado	Registrando chamadas AWS privadas de API 5G usando AWS CloudTrail	08/11/2022
AWS Private Certificate Authority (AWS Private CA)	Usando CloudTrail	04/04/2018
AWS Proton	Registro e monitoramento em AWS Proton	06/09/2021
AWS re:Post Privado	Registrando chamadas de API AWS re:Post privadas usando AWS CloudTrail	26/11/2023
AWS Resilience Hub	AWS CloudTrail	11/10/2021
AWS Resource Access Manager (AWS RAM)	Registrando chamadas de AWS RAM API com AWS CloudTrail	20/11/2018
Explorador de recursos da AWS	Registrando chamadas de Explorador de recursos da AWS API usando AWS CloudTrail	11/07/2022
AWS Resource Groups	Registro e monitoramento em Resource Groups	29/06/2018

AWS Serviço	CloudTrail Tópicos	O suporte começou
AWS RoboMaker	Registrando chamadas de AWS RoboMaker API com AWS CloudTrail	16/01/2019
AWS Secrets Manager	Monitore o uso de seus AWS Secrets Manager segredos	05/04/2018
AWS Security Hub	Registrando chamadas de AWS Security Hub API com AWS CloudTrail	27/11/2018
AWS Security Token Service (AWS STS)	Registrando eventos do IAM com AWS CloudTrail O tópico do IAM inclui informações sobre AWS STS.	13/11/2013
AWS Serverless Application Repository	Registrando chamadas de AWS Serverless Application Repository API com AWS CloudTrail	20/02/2018
AWS Service Catalog	Registrando chamadas de API do Service Catalog com AWS CloudTrail	06/07/2016
AWS Shield	Chamadas de API do Logging Shield Advanced com AWS CloudTrail	08/02/2018
AWS Snowball Borda	Registrando chamadas de API do AWS Snowball Edge com AWS CloudTrail	25/01/2019
AWS Step Functions	Registrando chamadas de AWS Step Functions API com AWS CloudTrail	01/12/2016

AWS Serviço	CloudTrail Tópicos	O suporte começou
AWS Storage Gateway	Registrando chamadas de API do Storage Gateway usando AWS CloudTrail	16/12/2014
AWS Support	Registrando chamadas de AWS Support API com AWS CloudTrail	21/04/2016
AWS Support Recomendações (pré-visualização)	AWS Support Chamadas da API de recomendações de registro com AWS CloudTrail	22/05/2024
AWS Systems Manager	Registrando chamadas de AWS Systems Manager API com AWS CloudTrail	29/11/2017
AWS Systems Manager Incident Manager	Registrando chamadas da API AWS Systems Manager Incident Manager usando AWS CloudTrail	05/10/2021
AWS Construtor de rede de telecomunicações (AWS TNB)	Registrando chamadas da API do AWS Telco Network Builder usando AWS CloudTrail	21/02/2023
AWS Transfer for SFTP	Registrando chamadas de AWS Transfer for SFTP API com AWS CloudTrail	08/01/2019
AWS Transit Gateway	Registrar chamadas de API para seu Transit Gateway usando o AWS CloudTrail	26/11/2018
AWS Trusted Advisor	Registrando ações AWS Trusted Advisor do console com AWS CloudTrail	22/10/2020

AWS Serviço	CloudTrail Tópicos	O suporte começou
Acesso Verificado pela AWS	Registre chamadas de Acesso Verificado pela AWS API usando AWS CloudTrail	27/04/2023
AWS WAF	Registrando chamadas de AWS WAF API com AWS CloudTrail	28/04/2016
AWS Well-Architected Tool	Registrando chamadas de AWS Well-Architected Tool API com AWS CloudTrail	15/12/2020
AWS X-Ray	Registrando chamadas de AWS X-Ray API com CloudTrail	25/04/2018
Elastic Load Balancing	AWS CloudTrail Registro para seu Classic Load Balancer e AWS CloudTrail registro para seu Application Load Balancer	04/04/2014
Atualizações OTA (over-the-air) do FreeRTOS	Registrando chamadas de API AWS IoT OTA com AWS CloudTrail	05/22/2019
Service Quotas	Registrando chamadas da API Service Quotas usando AWS CloudTrail	24/06/2019

CloudTrail serviços não suportados

Serviços que ainda estão em versão preview, que ainda não foram lançados para disponibilidade geral (GA) ou que não têm APIs públicas não são considerados compatíveis.

Além disso, os seguintes AWS serviços e eventos não são suportados:

- AWS Import/Export

- Eventos específicos da política de endpoint do Amazon VPC

Para obter uma lista dos AWS serviços compatíveis, consulteAWS tópicos de serviço para CloudTrail.

Cotas em AWS CloudTrail

A tabela a seguir descreve as cotas (anteriormente chamadas de limites) dentro de. CloudTrail CloudTrail não tem cotas ajustáveis. Para obter informações sobre outras cotas em AWS, consulte cotas AWS de serviço.

Recurso	Cota padrão	Comentários
Trilhas por região	5	Essa cota não pode ser aumentada.
Obter, descrever e listar APIs	10 transações por segundo (TPS)	O número máximo de solicitações de operação que você pode fazer por segundo sem ser limitado. As `StartQuery` APIs `CancelQuery` `LookupEvents` `ListInsightsMetricData` `PutAuditEvents` ,,, e não estão incluídas nessa categoria.
CancelQuery, StartQuery APIs	3 transações por segundo (TPS)	O número máximo de solicitações de operação que você pode fazer por segundo sem ser limitado. Essa cota não pode ser aumentada.
LookupEvents API	2 transações por segundo (TPS).	O número máximo de solicitações de operação que você

Recurso	Cota padrão	Comentários
		pode fazer por segundo sem ser limitado. Essa cota não pode ser aumentada.
ListInsightsMetricData API	1 transação por segundo (TPS)	O número máximo de solicitações de operação que você pode fazer por segundo sem ser limitado. Essa cota não pode ser aumentada.
PutAuditEvents API	100 transações por segundo (TPS)	O número máximo de solicitações de operação que você pode fazer por segundo sem ser limitado. Essa cota não pode ser aumentada.
Todas as outras APIs	1 transação por segundo (TPS)	O número máximo de solicitações de operação que você pode fazer por segundo sem ser limitado. Essa cota não pode ser aumentada.

Recurso	Cota padrão	Comentários
Armazenamentos de dados de eventos	10	O número máximo de armazenamentos de dados de eventos que você pode ter em qualquer Região da AWS. Isso inclui armazenamentos de dados de eventos de região única para a região, bem como quaisquer armazenamentos de dados de eventos de várias regiões em todas as Regiões da AWS. Isso inclui armazenamentos de dados de eventos em qualquer estágio do ciclo de vida. Essa cota não pode ser aumentada.
Canais	25	Essa cota se aplica aos canais usados para integrações do CloudTrail Lake com fontes de AWS eventos externas e não se aplica aos canais vinculados a serviços. Essa cota não pode ser aumentada.
Consultas simultâneas	10	O número máximo de consultas em fila ou em execução que você pode executar simultaneamente no Lake. CloudTrail Essa cota não pode ser aumentada.

Recurso	Cota padrão	Comentários
Eventos por PutAuditEvents solicitação	100	É possível adicionar até 100 eventos de atividade (ou até 1 MB) por solicitação `PutAuditEvents` . Essa cota não pode ser aumentada.
Seletores de eventos	5 por trilha	Essa cota não pode ser aumentada.
Seletores de eventos avançados	500 condições em todos os seletores de eventos avançados	Se uma trilha ou armazenamento de dados de eventos usar seletores de eventos avançados, será permitido um máximo de 500 valores totais para todas as condições, em todos os seletores de eventos avançados. A menos que uma trilha ou armazenamento de dados de eventos registre em log eventos de dados em todos os recursos, como todos os buckets do S3 ou todas as funções do Lambda, há um limite de 250 recursos de dados. Os recursos de dados podem ser distribuídos entre seletores de eventos, mas o total total geral não pode exceder 250. Essa cota não pode ser aumentada.

Recurso	Cota padrão	Comentários
Recursos de dados nos seletores de eventos	250 em todos os seletores de eventos em uma trilha	Se você optar por limitar eventos de dados usando seletores de eventos ou seletores de eventos avançados, o número total de recursos de dados não poderá exceder 250 em todos os seletores de eventos em uma trilha. O limite de número de recursos em um seletor de evento individual é configurá vel até 250. Esse limite superior é permitido apenas se o número total de recursos de dados não exceder 250 em todos os seletores de eventos. Exemplos: • Uma trilha com 5 seletores de eventos, cada um configurado com 50 recursos de dados, é permitida. (5*50=250) • Uma trilha com 5 seletores de eventos, 3 dos quais estão configurados com 50 recursos de dados, 1 está configurado com 99 recursos de dados e 1 com um recurso de dados, também é permitida. ((3*50)+1+99=250) • Uma trilha configurada com 5 seletores de eventos,

Recurso	Cota padrão	Comentários
		todos configurados com 100 recursos de dados, não é permitida. (5*100=500) Os seletores de eventos se aplicam somente a trilhas. Para armazenamentos de dados de eventos, devem ser usados seletores de eventos avançados. Essa cota não pode ser aumentada. A cota não se aplicará se você optar por registrar eventos de dados em todos os recursos, como todos os buckets do S3 ou todas as funções do Lambda.

Recurso	Cota padrão	Comentários
Tamanho do evento	Todas as versões do evento: eventos com mais de 256 KB não podem ser enviados para o CloudWatch Logs Versão do evento 1.05 e mais recente: limite total de tamanho do evento de 256 KB	O Amazon CloudWatch Logs e o Amazon permitem, EventBridge cada um, um tamanho máximo de evento de 256 KB. CloudTrail não envia eventos com mais de 256 KB para o CloudWatch Logs ou EventBridge. A partir da versão de evento 1.05, os eventos têm um tamanho máximo de 256 KB. Isso ajuda a evitar a exploração por agentes mal-intencionados e permite que os eventos sejam consumido s por outros AWS serviços, como CloudWatch Logs EventBridge e.
CloudTrail tamanho do arquivo enviado para o Amazon S3	Arquivo ZIP de 50 MB, após compactação	Para eventos de gerenciam ento e de dados, CloudTrail envia eventos para o S3 em arquivos ZIP (compactados) de no máximo 50 MB. Se ativada na trilha, as notificações de entrega de registros são enviadas pelo Amazon SNS após o CloudTrail envio dos arquivos ZIP para o S3.

Introdução aos AWS CloudTrail tutoriais

Se você é novato AWS CloudTrail, esses tutoriais podem ajudá-lo a aprender como usar seus recursos.

Tópicos

Conceda permissões de uso CloudTrail

Para criar, atualizar e gerenciar CloudTrail recursos como trilhas, armazenamentos de dados de eventos e canais, você precisa conceder permissões de uso CloudTrail. Esta seção fornece informações sobre as políticas gerenciadas disponíveis para CloudTrail.

> **Note**
>
> As permissões que você concede aos usuários para realizar tarefas CloudTrail administrativas não são as mesmas que CloudTrail exigem a entrega de arquivos de log para buckets do Amazon S3 ou o envio de notificações para tópicos do Amazon SNS. Para obter mais informações sobre essas permissões, consulte Política de bucket do Amazon S3 para CloudTrail.
>
> Se você configurar a integração com o Amazon CloudWatch Logs, CloudTrail também requer uma função que ele possa assumir para entregar eventos a um grupo de CloudWatch logs do Amazon Logs. Você deve criar a função que CloudTrail usa. Para obter mais informações, consulte Conceder permissão para visualizar e configurar as informações do Amazon CloudWatch Logs no console CloudTrail e Envio de eventos para o CloudWatch Logs.

As seguintes políticas AWS gerenciadas estão disponíveis para CloudTrail:

- AWSCloudTrail_FullAccess— Essa política fornece acesso total às CloudTrail ações sobre CloudTrail recursos, como trilhas, armazenamentos de dados de eventos e canais. Essa política fornece as permissões necessárias para criar, atualizar e excluir CloudTrail trilhas, armazenamentos de dados de eventos e canais.

  Essa política também fornece permissões para gerenciar o bucket do Amazon S3, o grupo de CloudWatch logs para Logs e um tópico do Amazon SNS para uma trilha. No entanto, a política `AWSCloudTrail_FullAccess` gerenciada não fornece permissões para excluir o bucket do Amazon S3, o grupo de CloudWatch logs para Logs ou um tópico do Amazon SNS. Para obter informações sobre políticas gerenciadas para outros AWS serviços, consulte o Guia de referência de políticas AWS gerenciadas.

  > **Note**
  >
  > A AWSCloudTrail_FullAccesspolítica não se destina a ser compartilhada amplamente entre seus Conta da AWS. Os usuários com esse perfil podem desativar ou reconfigurar as funções de auditoria mais confidenciais e importantes em suas Contas da AWS. Por esse motivo, você só deve aplicar essa política aos administradores da conta. Você deve controlar e monitorar de perto o uso desta política.

- AWSCloudTrail_ReadOnlyAccess— Essa política concede permissões para visualizar o CloudTrail console, incluindo eventos recentes e histórico de eventos. Essa política também permite visualizar trilhas, armazenamentos de dados de eventos e canais existentes. Os perfis e usuários com essa política podem baixar o histórico de eventos, mas não podem criar ou atualizar trilhas, armazenamentos de dados de eventos ou canais.

Para conceder acesso, adicione as permissões aos seus usuários, grupos ou perfis:

- Usuários e grupos em AWS IAM Identity Center:

  Crie um conjunto de permissões. Siga as instruções em Criação de um conjunto de permissões no Guia do usuário do AWS IAM Identity Center .

- Usuários gerenciados no IAM com provedor de identidades:

  Crie um perfil para a federação de identidades. Siga as instruções em Criar um perfil para um provedor de identidades de terceiros (federação) no Guia do usuário do IAM.

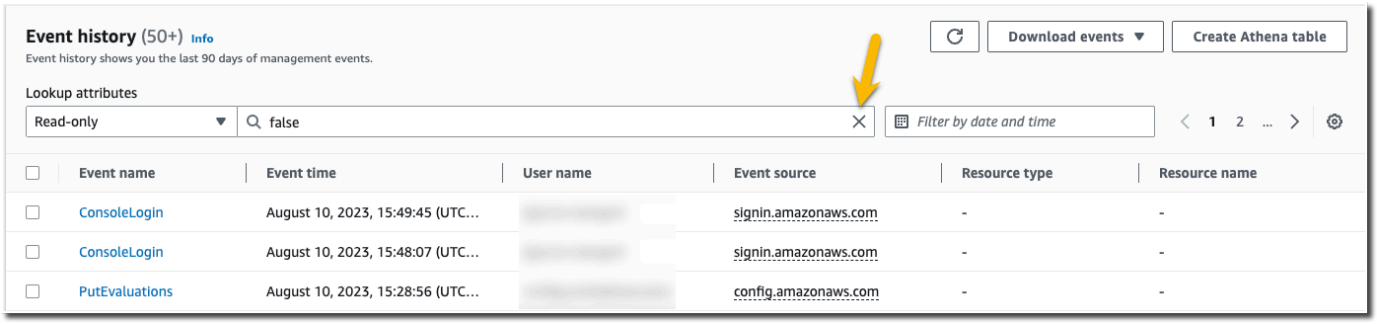
- Usuários do IAM:
  - Crie um perfil que seu usuário possa assumir. Siga as instruções em Criação de um perfil para um usuário do IAM no Guia do usuário do IAM.
  - (Não recomendado) Vincule uma política diretamente a um usuário ou adicione um usuário a um grupo de usuários. Siga as instruções em Adição de permissões a um usuário (console) no Guia do usuário do IAM.

Exibir histórico de eventos

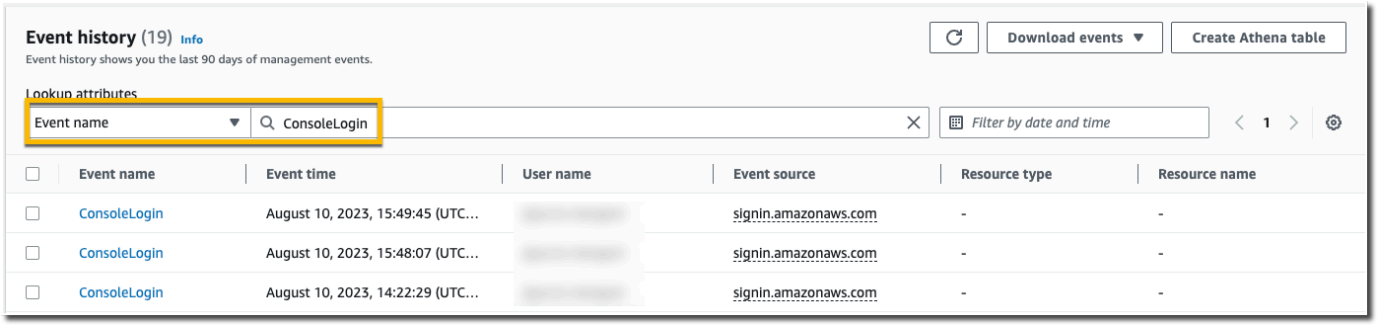
Esta seção descreve como usar a página Histórico de CloudTrail eventos no CloudTrail console para visualizar os últimos 90 dias de eventos de gerenciamento Conta da AWS para você no momento Região da AWS.

Para ver o histórico de eventos

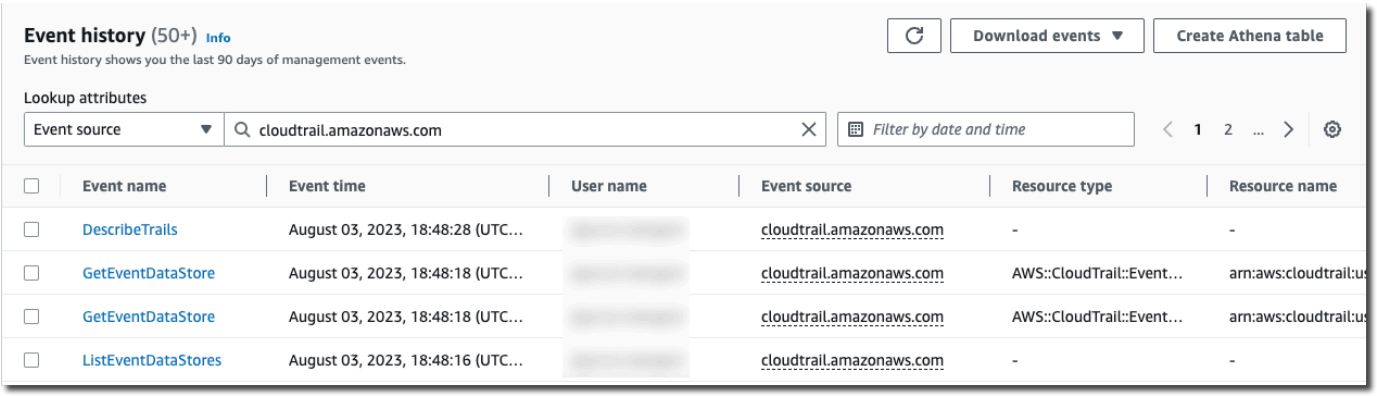
1. Faça login no AWS Management Console e abra o CloudTrail console em https://console.aws.amazon.com/cloudtrail/.
2. No painel de navegação, escolha Event history (Histórico de eventos). Você verá uma lista filtrada de eventos, com os eventos mais recentes exibidos primeiro. O filtro padrão para eventos é somente Read only (Somente leitura), definido como false (falso). Você pode limpar esse filtro escolhendo X à direita do filtro. É possível pesquisar eventos no Histórico de eventos filtrando eventos por um único atributo



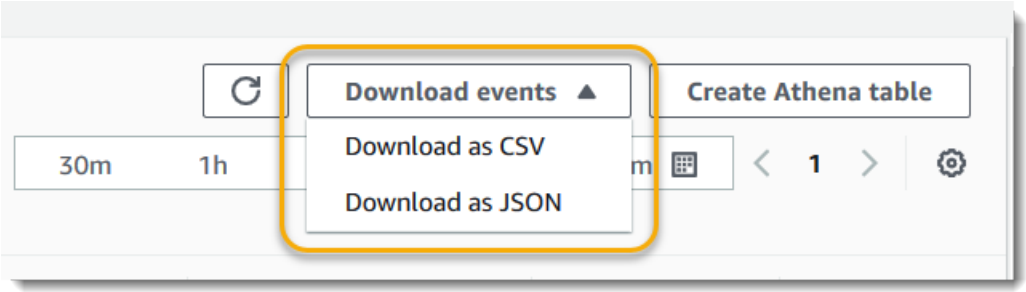
3. Escolha um atributo para filtrar e insira o valor total do atributo. CloudTrail não é possível filtrar por um valor parcial. Por exemplo, para visualizar todos os eventos de login do console, escolha o filtro Nome do evento e especifique ConsoleLogino valor do atributo.



Ou, para visualizar eventos CloudTrail de gerenciamento recentes, escolha Origem do evento e especifique`cloudtrail.amazonaws.com`.



4. Para visualizar um evento de gerenciamento específico, escolha o nome do evento. Na página de detalhes do evento, é possível visualizar detalhes sobre o evento, ver quaisquer recursos referenciados e visualizar o registro do evento.
5. Para comparar eventos, selecione até cinco eventos preenchendo as caixas de seleção na margem esquerda da tabela Event history (Histórico de eventos). Você pode ver os detalhes dos eventos selecionados side-by-side na tabela Comparar detalhes do evento.
6. Você pode salvar o histórico de eventos baixando-o como um arquivo no formato JSON ou CSV. O download do histórico de eventos pode levar alguns minutos.



Para ter mais informações, consulte Trabalhando com o histórico de CloudTrail eventos.

Crie uma trilha para registrar eventos de gerenciamento

Para sua primeira trilha, recomendamos criar uma trilha que registre todos os eventos de gerenciamento em todas as AWS regiões e não registre nenhum evento de dados. Os exemplos de eventos de gerenciamento incluem eventos de segurança, como os eventos do `CreateUser` e `AttachRolePolicy` do IAM, eventos de recurso, como `RunInstances` e `CreateBucket` e muito mais. Você criará um bucket do Amazon S3 onde armazenará os arquivos de log da trilha como parte da criação da trilha no CloudTrail console.

> **Note**
>
> Este tutorial pressupõe que você está criando a primeira trilha. Dependendo do número de trilhas que você tem em sua AWS conta e de como essas trilhas são configuradas, o procedimento a seguir pode ou não gerar despesas. CloudTrail armazena arquivos de log em um bucket do Amazon S3, o que gera custos. Para obter mais informações sobre preços, consulte Preços do AWS CloudTrail e Preços do Amazon S3.

Para criar uma trilha

1. Faça login no AWS Management Console e abra o CloudTrail console em https://console.aws.amazon.com/cloudtrail/.
2. No seletor de região, escolha a AWS região em que você deseja que sua trilha seja criada. Essa é a região inicial da trilha.

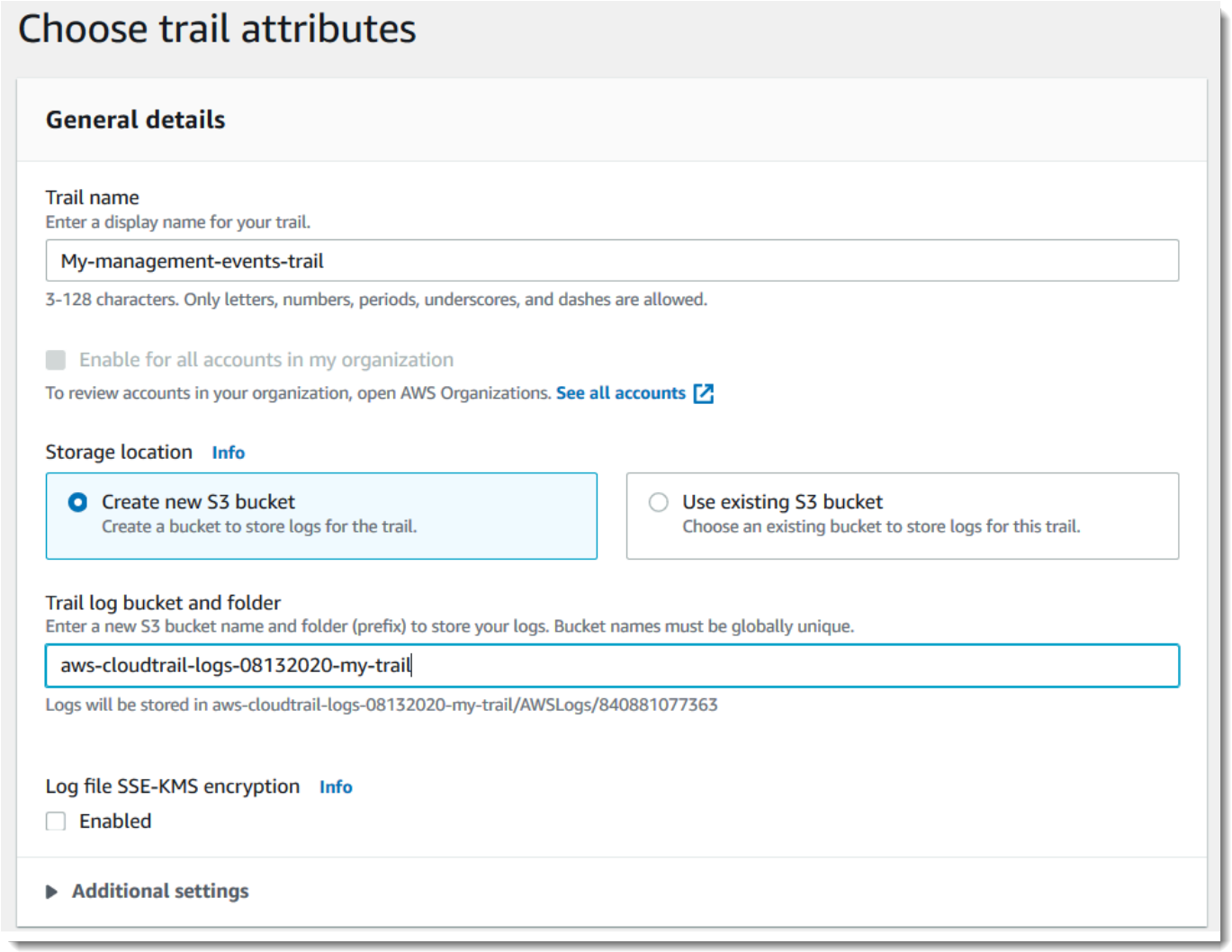
   > **Note**
   >
   > A região de origem é a única AWS região em que você pode visualizar e atualizar a trilha depois de criada, mesmo que a trilha registre eventos em todas as AWS regiões.

3. Na página inicial do CloudTrail serviço, na página Trilhas ou na seção Trilhas da página Painel, escolha Criar trilha.
4. Em Trail name (Nome da trilha), atribua um nome para a trilha, como *`My-Management-Events-Trail`*. Como prática recomendada, use um nome que identifique rapidamente a finalidade da trilha. Nesse caso, você está criando uma trilha que registra eventos de gerenciamento.

5. Mantenha a configuração padrão para Habilitar para todas as contas em minha organização. Essa opção não estará disponível para alteração, a menos que você tenha contas configuradas no Organizations.
6. Em Storage location (Local de armazenamento), escolha Create a S3 bucket (Criar um bucket do S3) para criar um bucket. Quando você cria um bucket, CloudTrail cria e aplica as políticas de bucket necessárias. Se você optar por criar um novo bucket do S3, sua política do IAM precisará incluir permissão para a `s3:PutEncryptionConfiguration` ação porque, por padrão, a criptografia do lado do servidor está habilitada para o bucket. Dê ao seu bucket um nome que o torne fácil de identificar.

   Para facilitar a localização de seus registros, crie uma nova pasta (também conhecida como prefixo) em um bucket existente para armazenar seus CloudTrail registros.

   > **Note**
   >
   > O nome do bucket do Amazon S3 deve ser exclusivo globalmente. Para obter mais informações, consulte as Regras para nomear buckets no Guia do usuário do Amazon Simple Storage Service.

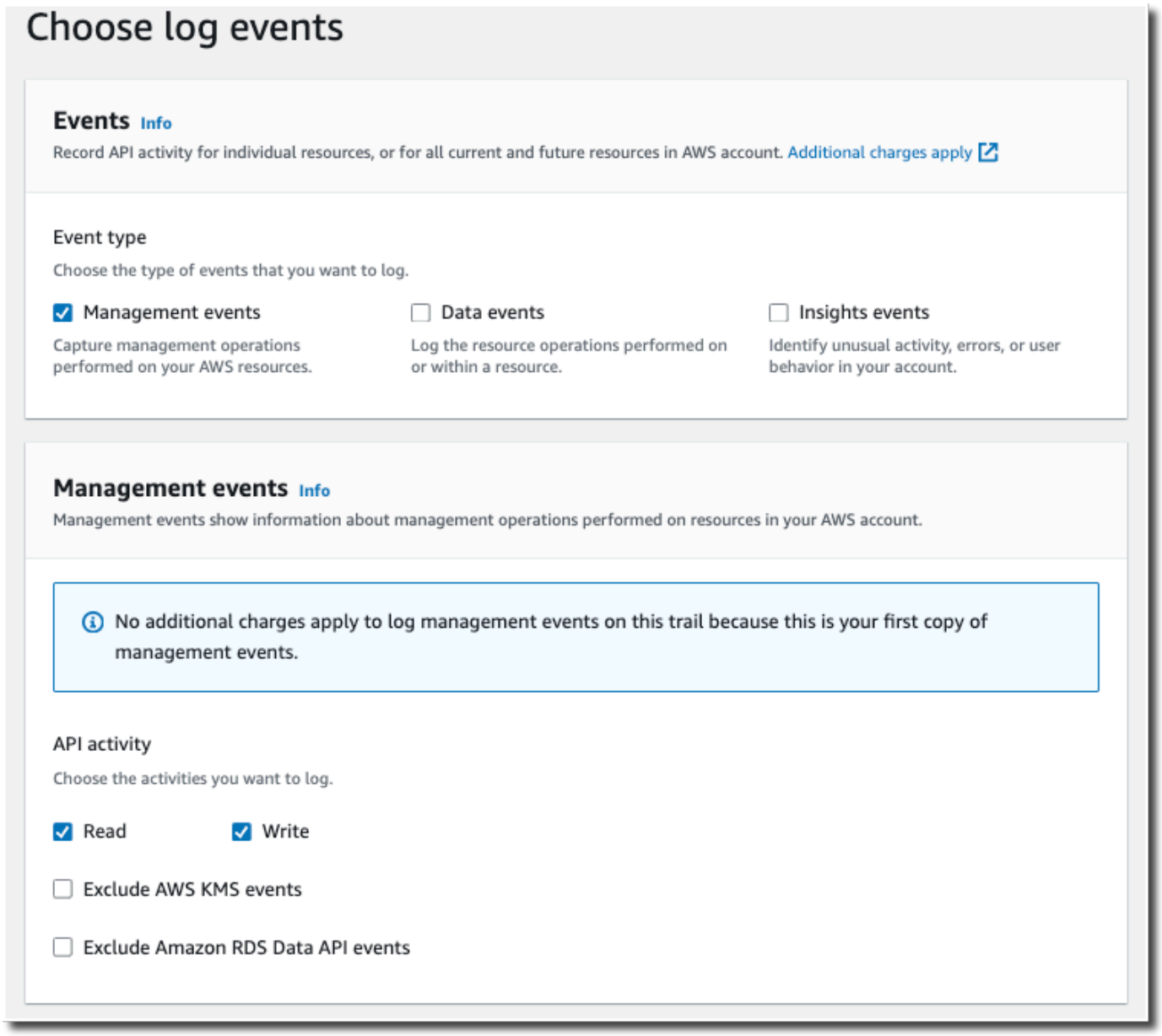


7. Desmarque a caixa de seleção para desabilitar a Log file SSE-KMS encryption (Criptografia SSE-KMS do arquivo de log). Por padrão, os arquivos de log são criptografados com criptografia SSE-S3. Para obter mais informações sobre essa configuração, consulte Uso da criptografia do lado do servidor com chaves gerenciadas do Amazon S3 (SSE-S3).
8. Deixe as configurações padrão em Additional settings (Configurações adicionais).
9. Deixe as configurações padrão para CloudWatch Registros. Por enquanto, não envie registros para o Amazon CloudWatch Logs.
10. (Opcional) Em Tags, adicione uma ou mais tags personalizadas (pares chave-valor) à sua trilha. As tags podem ajudá-lo a identificar suas CloudTrail trilhas e outros recursos, como os buckets do Amazon S3 que contêm CloudTrail arquivos de log. Por exemplo, você poderia anexar uma tag com o nome **`Compliance`** e o valor **`Auditing`**.

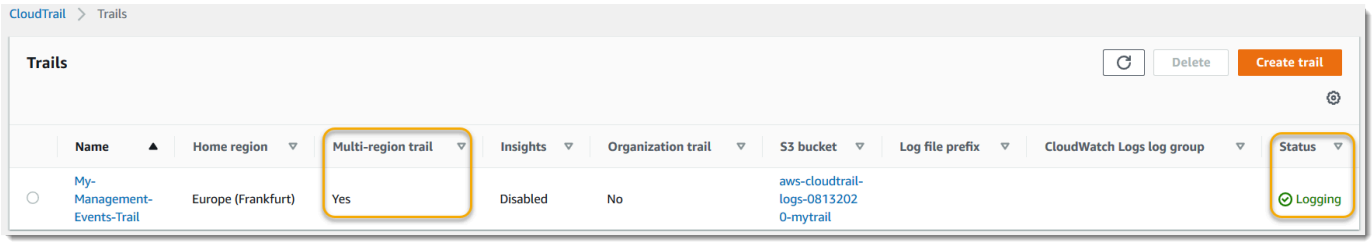
> **Note**
>
> Embora você possa adicionar tags às trilhas ao criá-las no CloudTrail console e criar um bucket do Amazon S3 para armazenar seus arquivos de log no CloudTrail console, você não pode adicionar tags ao bucket do Amazon S3 a partir do console. CloudTrail Para obter mais informações sobre como visualizar e alterar as propriedades de um bucket do Amazon S3, inclusive adicionar tags a um bucket, consulte o Manual do usuário do Amazon S3.

Quando terminar de criar as tags, escolha Next (Próximo).

11. Na página Choose log events (Escolher eventos de log), selecione os tipos de log. Para essa trilha, mantenha o padrão, Management events (Eventos de gerenciamento). Em Management events (Eventos de gerenciamento), escolha para registrar eventos de Read (Leitura) e Write (Gravação) se ainda não estiverem selecionados. Deixe as caixas de seleção Excluir AWS KMS eventos e Excluir eventos da API de dados do Amazon RDS vazias para registrar todos os eventos de gerenciamento.



12. Mantenha as configurações padrão para Eventos de dados e Eventos do Insights. Essa trilha não registrará nenhum dado ou evento do CloudTrail Insights. Escolha Next.
13. Na página Review and create (Analisar e criar), revise as configurações que você escolheu para sua trilha. Selecione Edit (Editar) para voltar e fazer alterações em uma seção. Quando estiver pronto para criar a trilha, escolha Create trail (Criar trilha).
14. A página Trails (Trilhas) mostra sua nova trilha na tabela. Observe que a trilha está definida como Multi-region trail (Trilha de várias regiões) por padrão, e esse registro está ativado para a trilha por padrão.



Visualizar seus arquivos de log

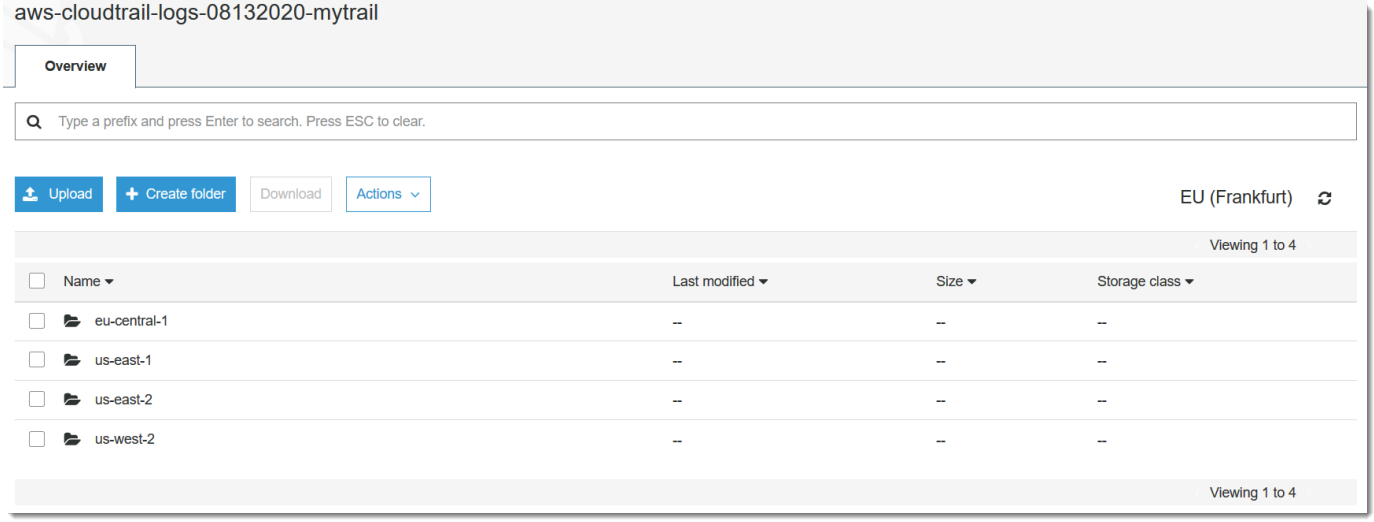
Em uma média de cerca de 5 minutos após a criação da sua primeira trilha, CloudTrail entrega o primeiro conjunto de arquivos de log para o bucket do Amazon S3 para sua trilha. Você pode examinar esses arquivos e saber mais sobre as informações que eles contêm.

> **Note**
>
> CloudTrail normalmente entrega registros em uma média de cerca de 5 minutos após uma chamada de API. Desta vez não há garantias. Consulte o Acordo de Nível de Serviço do AWS CloudTrail para obter mais informações.
> Se você configurar incorretamente sua trilha (por exemplo, o bucket do S3 está inacessível), CloudTrail tentará reenviar os arquivos de log para o bucket do S3 por 30 dias, e esses attempted-to-deliver eventos estarão sujeitos às cobranças padrão. CloudTrail Para evitar cobranças em uma trilha mal configurada, você precisa excluir a trilha.

Para visualizar seus arquivos de log

1. Faça login no AWS Management Console e abra o CloudTrail console em https://console.aws.amazon.com/cloudtrail/.
2. No painel de navegação, selecione Trilhas. Na página Trails (Trilhas), localize o nome da trilha que você acabou de criar (no exemplo, *`My-Management-Events-Trail`*).
3. Na linha da trilha, escolha o valor do bucket do S3 (no exemplo, *`aws-cloudtrail-logs-08132020-mytrail`*).
4. O console do Amazon S3 é aberto e mostra esse bucket, no nível superior para arquivos de log. Como você criou uma trilha que registra eventos em todas as AWS regiões, a tela é aberta no nível que mostra cada pasta da região. *`A hierarquia da navegação do bucket do Amazon S3 nesse nível é bucket-name AWS/Logs/ account-id/.`* CloudTrail

Escolha a pasta da AWS região em que você deseja revisar os arquivos de log. Por exemplo, se você quiser revisar os arquivos de log para a região Leste dos EUA (Ohio), us-east-2.



5. Navegue a estrutura de pastas do bucket até o ano, o mês e o dia em que você deseja revisar os logs de atividade nessa região. Nesse dia, há uma série de arquivos. O nome dos arquivos começa com o ID AWS da sua conta e termina com a extensão `.gz`. *Por exemplo, se o ID da sua conta for 123456789012, você verá arquivos com nomes semelhantes a este: 123456789012 _ _ us-east-2 _ 20190610T1255ABCDEExample .json.gz. CloudTrail*

   Para visualizar esses arquivos, você pode baixá-los, descompactá-los e visualizá-los em um editor de texto simples ou um visualizador de arquivo JSON. Alguns navegadores também oferecem suporte para a visualização de arquivos .gz e JSON diretamente. Recomendamos usar um visualizador JSON, pois facilita a análise das informações nos arquivos de CloudTrail log.

Planejar para as próximas etapas

Agora que você tem uma trilha, tem acesso a um registro contínuo de eventos e atividades em sua AWS conta. Esse registro contínuo ajuda você a atender às necessidades de contabilidade e auditoria da sua conta da AWS . No entanto, há muito mais que você pode fazer com CloudTrail CloudTrail esses dados.

- Adicione segurança adicional aos dados da sua trilha. CloudTrailaplica automaticamente um certo nível de segurança ao criar uma trilha. No entanto, há etapas adicionais que você pode tomar para ajudar a manter seus dados seguros.

  - Por padrão, o bucket do Amazon S3 que você criou como parte da criação de uma trilha tem uma política aplicada que permite CloudTrail gravar arquivos de log nesse bucket. O bucket não pode ser acessado publicamente, mas pode ser acessível a outros usuários em sua AWS conta se eles tiverem permissões para ler e gravar em buckets em sua AWS conta. Analise a política do bucket e, se necessário, faça alterações para restringir o acesso. Para obter mais informações, consulte a documentação de segurança do Amazon S3 e a demonstração de exemplo para proteger um bucket.
  - Os arquivos de log entregues CloudTrail ao seu bucket são criptografados pela criptografia do lado do servidor da Amazon com chaves de criptografia gerenciadas pelo Amazon S3 (SSE-S3). Para fornecer uma camada de segurança que seja diretamente gerenciável, você pode usar criptografia do lado do servidor com chaves AWS KMS gerenciadas (SSE-KMS) para seus arquivos de log. CloudTrail Para usar o SSE-KMS com CloudTrail, você cria e gerencia uma chave KMS, também conhecida como. AWS KMS key Para ter mais informações, consulte Criptografando arquivos de CloudTrail log com AWS KMS chaves (SSE-KMS).
  - Para um planejamento de segurança adicional, revise as melhores práticas de segurança para CloudTrail.
- Crie uma trilha para registrar eventos de dados. Se você estiver interessado em registrar quando objetos são adicionados, recuperados e excluídos em um ou mais buckets do Amazon S3, quando itens são adicionados, alterados ou excluídos nas tabelas do DynamoDB ou quando uma ou AWS Lambda mais funções são invocadas, esses são eventos de dados. A trilha de eventos de gerenciamento que você criou anteriormente neste tutorial não registra esses tipos de eventos. Você pode criar uma trilha separada especificamente para registrar eventos de dados para alguns ou todos os tipos de recursos compatíveis. Para ter mais informações, consulte Eventos de dados.

  > **Note**
  >
  > Há cobranças adicionais para o registro de eventos de dados. Para obter mais informações, consulte Preços do AWS CloudTrail.

- Registre eventos do CloudTrail Insights em sua trilha. AWS CloudTrail O Insights ajuda AWS os usuários a identificar e responder a atividades incomuns associadas a chamadas de API e taxas de erro de API, analisando continuamente os eventos CloudTrail de gerenciamento. CloudTrail O Insights usa modelos matemáticos para determinar os níveis normais de atividade de API e eventos de serviço de uma conta. Ele identifica o comportamento que está fora dos padrões normais, gera eventos do Insights e entrega esses eventos a uma pasta do `/CloudTrail-`

`Insight` no bucket do S3 de destino escolhido para a trilha. Para obter mais informações sobre o CloudTrail Insights, consulteRegistrar eventos do Insights.

> **Note**
>
> Há cobranças adicionais para o registro em log de eventos do Insights. Para obter mais informações, consulte Preços do AWS CloudTrail.

- Configure CloudWatch os alarmes do Logs para alertá-lo quando determinados eventos ocorrerem. CloudWatch Os registros permitem monitorar e receber alertas de eventos específicos capturados pelo CloudTrail. Por exemplo, é possível monitorar eventos de gerenciamento relacionados a rede e segurança de chave, como alterações do grupo de segurança, eventos de login do AWS Management Console com falha ou alterações nas políticas do IAM. Para ter mais informações, consulte Monitoramento CloudTrail de arquivos de log com o Amazon CloudWatch Logs.
- Use ferramentas de análise para identificar tendências em seus CloudTrail registros. Embora os filtros no histórico de eventos possam ajudar você a localizar eventos ou tipos de evento específicos em sua atividade recente, isso não permite pesquisar atividade por longos períodos. Para uma análise mais profunda e mais sofisticada, você pode usar o Amazon Athena. Para obter mais informações, consulte Consultando AWS CloudTrail registros no Guia do usuário do Amazon Athena.

Crie um armazenamento de dados de eventos para eventos de dados do S3

Você pode criar um armazenamento de dados de eventos para registrar CloudTrail eventos (eventos de gerenciamento, eventos de dados), eventos do CloudTrail Insights, AWS Audit Manager evidências, itens de AWS Config configuração ou não AWS eventos.

Ao criar um armazenamento de dados de eventos para eventos de dados, você escolhe os tipos de recursos Serviços da AWS e os quais deseja registrar eventos de dados. Para obter informações sobre Serviços da AWS esses eventos de dados de log, consulteEventos de dados.

Este passo a passo mostra como criar um armazenamento de dados de eventos para eventos de dados do Amazon S3. Neste tutorial, em vez de registrar todos os eventos de dados do Amazon S3, escolheremos um modelo de seletor de log personalizado para registrar eventos somente quando um objeto for excluído de um bucket do S3 específico.

CloudTrail Os armazenamentos de dados de eventos em Lake incorrem em cobranças. Ao criar um armazenamento de dados de eventos, você escolhe a opção de preço que deseja usar para ele. A opção de preço determina o custo para a ingestão e para o armazenamento de eventos, e o período de retenção padrão e máximo para o armazenamento de dados de eventos. Para obter informações sobre CloudTrail preços e gerenciamento de custos do Lake, consulte AWS CloudTrail Preços Gerenciando os custos CloudTrail do Lake e.

Para criar um armazenamento de dados de eventos para eventos de dados do S3

1. Faça login no AWS Management Console e abra o CloudTrail console em https://console.aws.amazon.com/cloudtrail/.
2. No painel de navegação, em Lake, escolha Armazenamentos de dados de eventos.
3. Selecione Create event data store (Criar armazenamento de dados de eventos).
4. Na página Configurar armazenamento de dados de eventos, em Detalhes gerais, dê um nome ao seu armazenamento de dados de eventos, como *`s3- data-events-eds`*. Como prática recomendada, use um nome que identifique rapidamente a finalidade do armazenamento de dados de eventos. Para obter informações sobre os requisitos CloudTrail de nomenclatura, consulteRequisitos de nomenclatura.
5. Escolha a opção de preço que você deseja usar para o armazenamento de dados de eventos. A opção de preço determina o custo para a ingestão e para o armazenamento de eventos, e os períodos de retenção padrão e máximo para o armazenamento de dados de eventos. Para obter mais informações, consulte Preços do AWS CloudTrail e Gerenciando os custos CloudTrail do Lake.

   As seguintes opções estão disponíveis:

   - Preço de retenção extensível de um ano: geralmente recomendado se você espera ingerir menos de 25 TB de dados de eventos por mês e deseja um período de retenção flexível de até 10 anos. Nos primeiros 366 dias (o período de retenção padrão), o armazenamento é incluído sem custo adicional no preço de ingestão. Depois de 366 dias, a retenção estendida está disponível pelo pay-as-you-go preço. Esta é a opção padrão.
     - Período de retenção padrão: 366 dias
     - Período máximo de retenção: 3.653 dias
   - Preço de retenção de sete anos: recomendado se você espera ingerir mais de 25 TB de dados de eventos por mês e precisa de um período de retenção de até 7 anos. A retenção está incluída no preço de ingestão sem custo adicional.

- Período de retenção padrão: 2.557 dias
- Período máximo de retenção: 2.557 dias

6. Especifique um período de retenção para o armazenamento de dados de eventos. Os períodos de retenção podem ser entre 7 dias e 3.653 dias (cerca de 10 anos) para a opção de preço de retenção extensível de um ano ou entre 7 dias e 2.557 dias (cerca de sete anos) para a opção de preço de retenção de sete anos.

   CloudTrail Lake determina se deve reter um evento verificando se o `eventTime` evento está dentro do período de retenção especificado. Por exemplo, se você especificar um período de retenção de 90 dias, CloudTrail removerá eventos quando forem mais antigos do que 90 dias. `eventTime`

7. (Opcional) Em Criptografia, escolha se você deseja criptografar o armazenamento de dados do evento usando sua própria chave do KMS. Por padrão, todos os eventos em um armazenamento de dados de eventos são criptografados CloudTrail usando uma chave KMS que AWS possui e gerencia para você.

   Para habilitar a criptografia usando sua própria chave do KMS, escolha Usar minha própria AWS KMS key. Escolha Novo para AWS KMS key criar uma para você ou escolha Existente para usar uma chave KMS existente. Em Inserir alias KMS, especifique um alias, no formato. `alias/` *`MyAliasName`* Usar sua própria chave KMS exige que você edite sua política de chaves KMS para permitir que CloudTrail os registros sejam criptografados e descriptografados. Para obter mais informações, consulteConfigure as AWS KMS principais políticas para CloudTrail. CloudTrail também suporta chaves AWS KMS multirregionais. Para obter mais informações sobre chaves de várias regiões, consulte Usar chaves de várias regiões no Manual do desenvolvedor do AWS Key Management Service .

   Usar sua própria chave KMS gera AWS KMS custos de criptografia e descriptografia. Após associar um armazenamento de dados de eventos a uma chave do KMS, não será possível remover ou alterar a chave do KMS.

   > **Note**
   >
   > Para habilitar a AWS Key Management Service criptografia para um armazenamento de dados de eventos da organização, você deve usar uma chave KMS existente para a conta de gerenciamento.

8. (Opcional) Se você quiser consultar os dados do seu evento usando o Amazon Athena, escolha Habilitar na federação de consultas do Lake. A federação permite que você visualize os metadados associados ao armazenamento de dados de eventos no Catálogo de Dados do AWS Glue e execute consultas SQL nos dados do evento no Athena. Os metadados da tabela armazenados no Catálogo de AWS Glue Dados permitem que o mecanismo de consulta do Athena saiba como encontrar, ler e processar os dados que você deseja consultar. Para ter mais informações, consulte Federar um armazenamento de dados de eventos.

   Para habilitar a federação de consultas do Lake, escolha Habilitar e faça o seguinte:

   a. Escolha se deseja criar um perfil ou usar um perfil do IAM existente. O AWS Lake Formation usa esse perfil para gerenciar permissões para o armazenamento de dados de eventos federados. Quando você cria uma nova função usando o CloudTrail console, cria CloudTrail automaticamente uma função com as permissões necessárias. Se você escolher um perfil existente, a política do perfil deve fornecer as permissões mínimas necessárias.

   b. Se você estiver criando um perfil, insira um nome para identificá-lo.

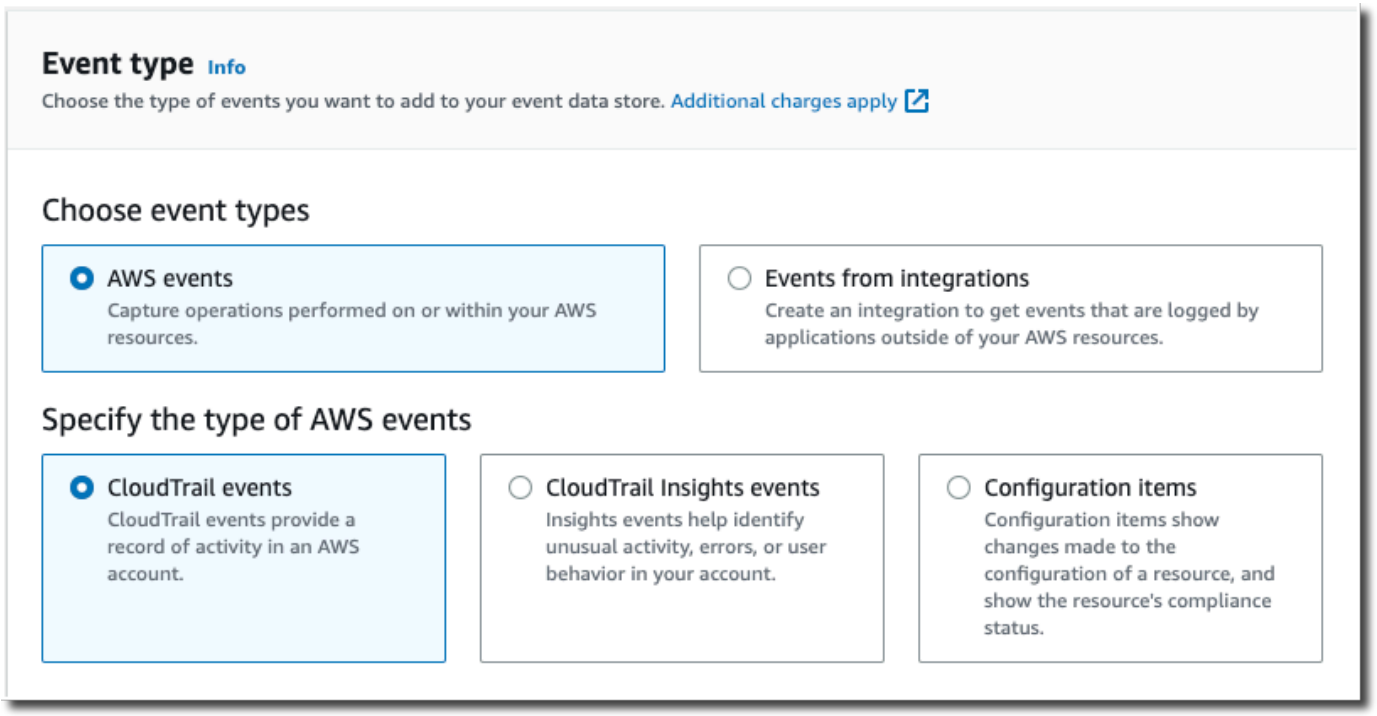
   c. Se você estiver usando um perfil existente, escolha o perfilo que deseja usar. O perfil deve existir em sua conta.

9. (Opcional) Em Tags, adicione uma ou mais tags personalizadas (pares chave-valor) ao armazenamento de dados de eventos. As tags podem ajudar você a identificar seus repositórios de dados de CloudTrail eventos. Por exemplo, você poderia anexar uma tag com o nome **`stage`** e o valor **`prod`**. É possível usar tags para limitar o acesso ao armazenamento de dados de eventos. As tags também podem ser usadas para monitorar os custos de consulta e ingestão do seu armazenamento de dados de eventos.

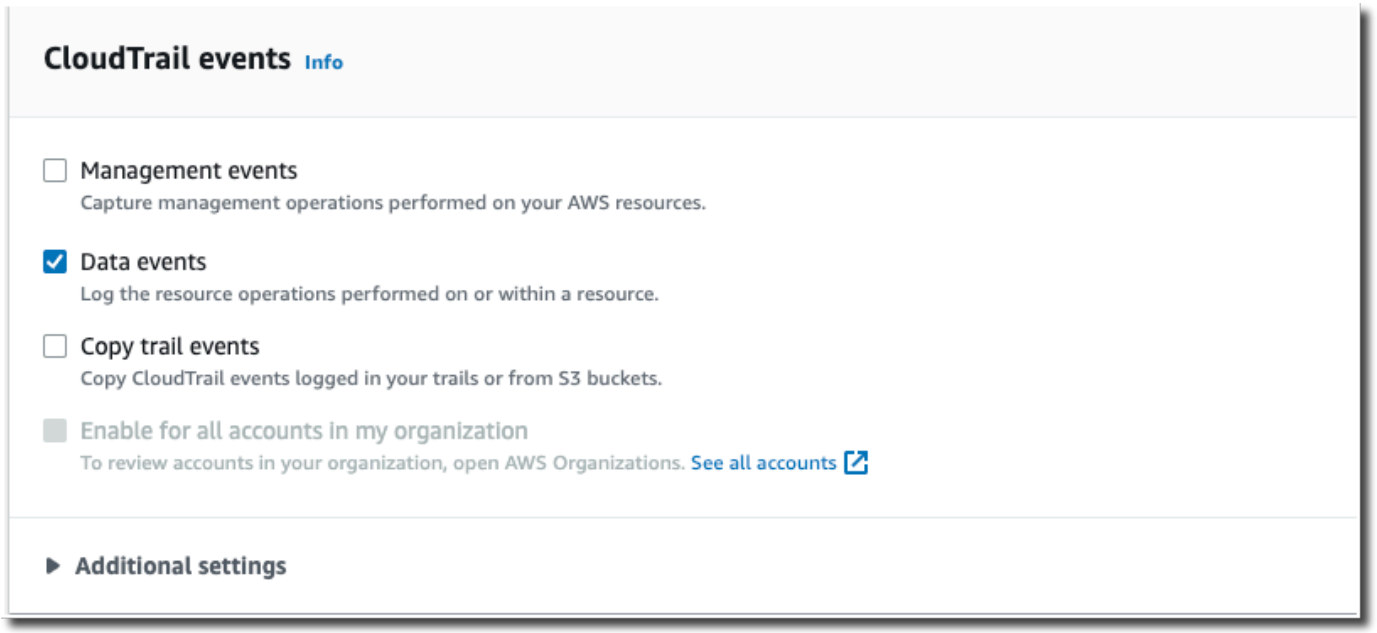
   Para obter informações sobre como usar tags para monitorar os custos, consulte Criação de etiquetas de alocação de custos definidas pelo usuário para armazenamentos de dados de eventos do CloudTrail Lake. Para obter informações sobre como usar políticas do IAM para autorizar o acesso a um armazenamento de dados de eventos com base em tags, consulte Exemplos: negação de acesso para criar ou excluir armazenamentos de dados de eventos com base em tags. Para obter informações sobre como você pode usar tags em AWS, consulte Como marcar seus AWS recursos no Guia do usuário de AWS recursos de marcação.

10. Escolha Next (Avançar) para configurar o armazenamento de dados de eventos.

11. Na página Escolher eventos, mantenha as seleções padrão para Tipo de evento.



12. Para CloudTrail eventos, escolha Eventos de dados e desmarque Eventos de gerenciamento. Para obter mais informações sobre eventos de dados, consulte Eventos de dados de log.



13. Mantenha a configuração padrão para Copiar eventos de trilha. Você usaria essa opção para copiar eventos de trilhas existentes para o armazenamento de dados de eventos. Para ter mais informações, consulte Copiar eventos de trilhas para um armazenamento de dados de eventos.

14. Escolha Habilitar para todas as contas em minha organização se este for um armazenamento de dados de eventos da organização. Essa opção não estará disponível para alteração, a menos que você tenha contas configuradas no AWS Organizations.
15. Em Configurações adicionais, mantenha as seleções padrão. Por padrão, um armazenamento de dados de eventos coleta eventos para todos Regiões da AWS e começa a ingerir eventos quando é criado.
16. Para Eventos de dados, faça as seguintes seleções:

    a. Em Tipo de evento de dados, escolha S3. O tipo de evento de dados identifica o recurso AWS service (Serviço da AWS) e no qual os eventos de dados são registrados.

    b. Em Modelo do seletor de log, escolha Personalizado. Escolher Personalizado permite definir um seletor de eventos personalizado para filtrar os campos `eventName`, `resources.ARN` e `readOnly`. Para obter informações sobre esses campos, consulte AdvancedFieldSelectora Referência AWS CloudTrail da API.

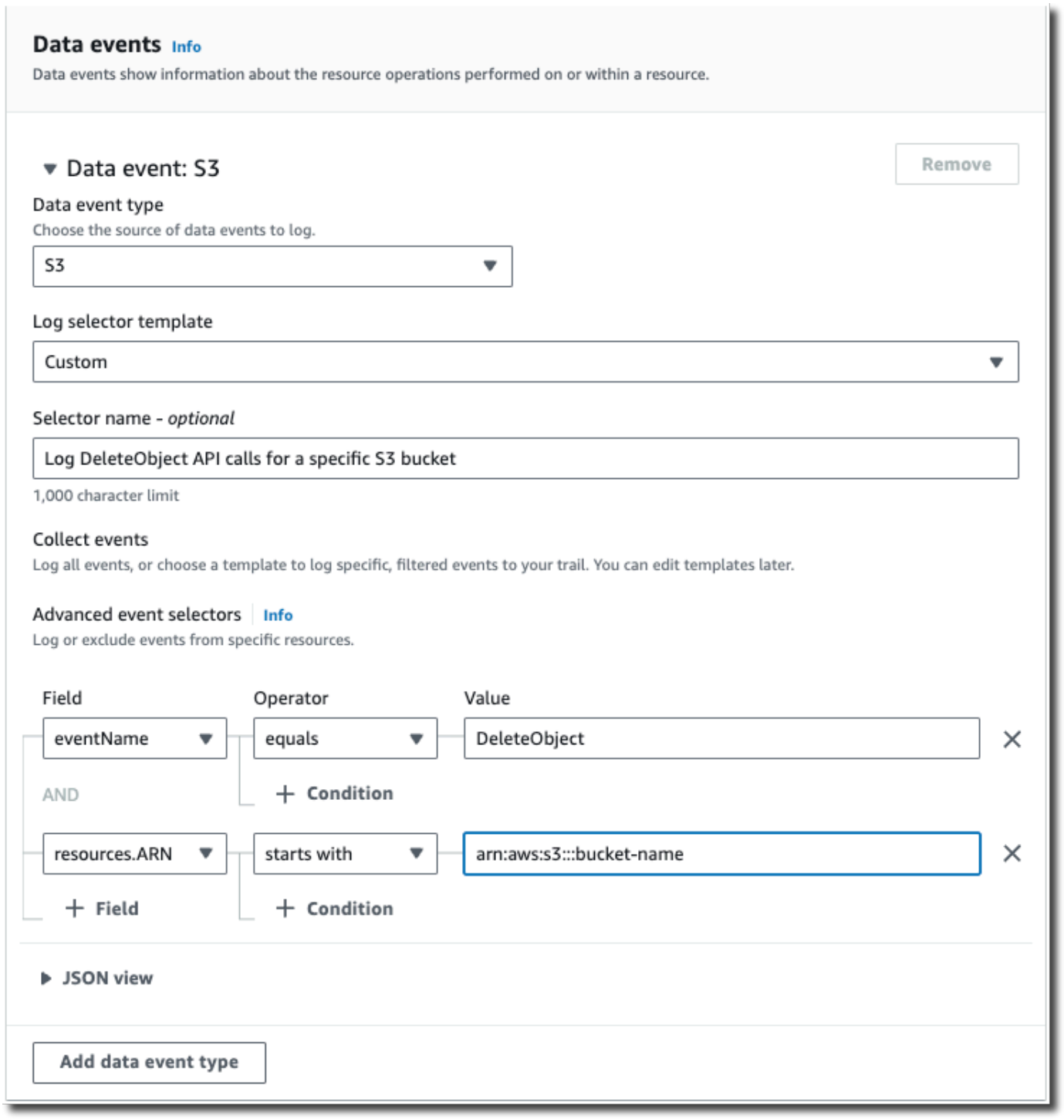
    c. (Opcional) Em Nome do seletor, insira um nome para identificar o seletor. O nome do seletor é um nome descritivo para um seletor de eventos avançado, como “Registrar chamadas de DeleteObject API para um bucket específico do S3”. O nome do seletor é listado como `Name` no seletor de eventos avançado e poderá ser visualizado se você expandir a visualização JSON.

    d. Nos seletores de eventos avançados, criaremos o seletor de eventos personalizado para filtrar os campos `eventName` e. `resources.ARN` Seletores de eventos avançados para

um armazenamento de dados de eventos funcionam da mesma forma que os seletores de eventos avançados que você aplica a uma trilha. Para obter mais informações sobre como criar seletores de eventos avançados, consulte Registro em log de eventos de dados com seletores de eventos avançados.

i. Em Campo, escolha eventName. Em Operador, escolha equals. Em Valor, insira **`DeleteObject`**. Escolha + Campo para filtrar em outro campo.

ii. Em Campo, escolha resources.ARN. Para Operador, escolha StartsWith. Em Valor, insira o ARN do seu bucket (por exemplo, *`arn:aws:s3:::bucket-name`*). Para obter mais informações sobre como obter o ARN, consulte Recursos do Amazon S3 no Guia do usuário do Amazon Simple Storage Service.



17. Selecione Next (Próximo) para revisar suas escolhas.
18. Na página Review and create (Revisar e criar), revise as suas escolhas. Escolha Edit (Editar) para fazer alterações a uma seção. Quando estiver pronto para criar o armazenamento de

dados de eventos, escolha Create event data store (Criar armazenamento de dados de eventos).

19. O novo armazenamento de dados de eventos está visível na tabela Armazenamentos de dados de eventos na página Armazenamento de dados de eventos.

    Deste ponto em diante, o armazenamento de dados de eventos captura eventos que correspondem aos seletores de eventos avançados. Os eventos ocorridos antes da criação do armazenamento de dados de eventos não estarão no armazenamento de dados de eventos, a menos que você tenha optado por copiar eventos de trilha existentes.

Você agora está pronto para executar consultas em seu armazenamento de dados de eventos. Para obter informações sobre como visualizar e executar consultas de exemplo, consulte Visualize e execute exemplos de consultas do CloudTrail Lake.

Copiar eventos de trilha para um armazenamento de dados de eventos do CloudTrail Lake

Este passo a passo mostra como copiar eventos de trilha para um novo armazenamento de dados de eventos do CloudTrail Lake para análise histórica. Para obter mais informações sobre cópia de eventos de trilhas, consulte Copiar eventos de trilhas para um armazenamento de dados de eventos.

CloudTrail Os armazenamentos de dados de eventos em Lake incorrem em cobranças. Ao criar um armazenamento de dados de eventos, você escolhe a opção de preço que deseja usar para ele. A opção de preço determina o custo para a ingestão e para o armazenamento de eventos, e o período de retenção padrão e máximo para o armazenamento de dados de eventos. Para obter informações sobre CloudTrail preços e gerenciamento de custos do Lake, consulte AWS CloudTrail Preços Gerenciando os custos CloudTrail do Lake e.

Ao copiar eventos de trilha para um armazenamento de dados de eventos do CloudTrail Lake, você incorre em cobranças com base na quantidade de dados não compactados que o armazenamento de dados de eventos ingere.

Ao copiar eventos de trilha para o CloudTrail Lake, CloudTrail descompacta os registros armazenados no formato gzip (compactado) e, em seguida, copia os eventos contidos nos registros para seu armazenamento de dados de eventos. O tamanho dos dados não compactados pode ser maior do que o tamanho real do armazenamento do S3. Para obter uma estimativa geral do tamanho dos dados não compactados, é possível multiplicar o tamanho dos registros no bucket do S3 por 10.

É possível pode reduzir os custos especificando um intervalo de tempo mais restrito para os eventos copiados. Se você planeja usar apenas o armazenamento de dados de eventos para consultar seus eventos copiados, poderá desativar a ingestão de eventos para evitar cobranças em eventos futuros. Para obter mais informações sobre custos, consulte AWS CloudTrail Preços Gerenciando os custos CloudTrail do Lake e.

Para copiar eventos de trilhas para um novo armazenamento de dados de eventos

1. Faça login no AWS Management Console e abra o CloudTrail console em https://console.aws.amazon.com/cloudtrail/.
2. No painel de navegação, em Lake, escolha Armazenamentos de dados de eventos.
3. Selecione Create event data store (Criar armazenamento de dados de eventos).
4. Na página Configurar armazenamento de dados de eventos, em Detalhes gerais, dê um nome ao seu armazenamento de dados de eventos, como *my-management-events-eds*. Como prática recomendada, use um nome que identifique rapidamente a finalidade do armazenamento de dados de eventos. Para obter informações sobre os requisitos CloudTrail de nomenclatura, consulteRequisitos de nomenclatura.
5. Escolha a opção de preço que você deseja usar para o armazenamento de dados de eventos. A opção de preço determina o custo para a ingestão e para o armazenamento de eventos, e os períodos de retenção padrão e máximo para o armazenamento de dados de eventos. Para obter mais informações, consulte Preços do AWS CloudTrail e Gerenciando os custos CloudTrail do Lake.

   As seguintes opções estão disponíveis:

   - Preço de retenção extensível de um ano: geralmente recomendado se você espera ingerir menos de 25 TB de dados de eventos por mês e deseja um período de retenção flexível de até 10 anos. Nos primeiros 366 dias (o período de retenção padrão), o armazenamento é incluído sem custo adicional no preço de ingestão. Depois de 366 dias, a retenção estendida está disponível pelo pay-as-you-go preço. Esta é a opção padrão.
     - Período de retenção padrão: 366 dias
     - Período máximo de retenção: 3.653 dias
   - Preço de retenção de sete anos: recomendado se você espera ingerir mais de 25 TB de dados de eventos por mês e precisa de um período de retenção de até 7 anos. A retenção está incluída no preço de ingestão sem custo adicional.
     - Período de retenção padrão: 2.557 dias

- Período máximo de retenção: 2.557 dias

6. Especifique um período de retenção para o armazenamento de dados de eventos. Os períodos de retenção podem ser entre 7 dias e 3.653 dias (cerca de 10 anos) para a opção de preço de retenção extensível de um ano ou entre 7 dias e 2.557 dias (cerca de sete anos) para a opção de preço de retenção de sete anos.

   CloudTrail Lake determina se deve reter um evento verificando se o `eventTime` evento está dentro do período de retenção especificado. Por exemplo, se você especificar um período de retenção de 90 dias, CloudTrail removerá eventos quando forem mais antigos do que 90 dias. `eventTime`

   > **Note**
   >
   > Se você estiver copiando eventos de trilha para esse armazenamento de dados de eventos, não CloudTrail copiará um evento se ele `eventTime` for anterior ao período de retenção especificado. Para determinar o período de retenção adequado, calcule a soma do evento mais antigo que você deseja copiar em dias e o número de dias em que deseja reter os eventos no armazenamento de dados do evento (período de retenção = *`oldest-event-in-days`*+ *`number-days-to-retain`*). Por exemplo, se o evento mais antigo que você está copiando tiver 45 dias e você quiser manter os eventos no armazenamento de dados de eventos por mais 45 dias, defina o período de retenção como 90 dias.

7. (Opcional) Em Criptografia, escolha se você deseja criptografar o armazenamento de dados do evento usando sua própria chave do KMS. Por padrão, todos os eventos em um armazenamento de dados de eventos são criptografados CloudTrail usando uma chave KMS que AWS possui e gerencia para você.

   Para habilitar a criptografia usando sua própria chave do KMS, escolha Usar minha própria AWS KMS key. Escolha Novo para AWS KMS key criar uma para você ou escolha Existente para usar uma chave KMS existente. Em Inserir alias KMS, especifique um alias, no formato. `alias/` *`MyAliasName`* Usar sua própria chave KMS exige que você edite sua política de chaves KMS para permitir que CloudTrail os registros sejam criptografados e descriptografados. Para obter mais informações, consulteConfigure as AWS KMS principais políticas para CloudTrail. CloudTrail também suporta chaves AWS KMS multirregionais. Para obter mais informações sobre chaves de várias regiões, consulte Usar chaves de várias regiões no Manual do desenvolvedor do AWS Key Management Service .

Usar sua própria chave KMS gera AWS KMS custos de criptografia e descriptografia. Após associar um armazenamento de dados de eventos a uma chave do KMS, não será possível remover ou alterar a chave do KMS.

> **Note**
>
> Para habilitar a AWS Key Management Service criptografia para um armazenamento de dados de eventos da organização, você deve usar uma chave KMS existente para a conta de gerenciamento.

8. (Opcional) Se você quiser consultar os dados do seu evento usando o Amazon Athena, escolha Habilitar na federação de consultas do Lake. A federação permite que você visualize os metadados associados ao armazenamento de dados de eventos no Catálogo de Dados do AWS Glue e execute consultas SQL nos dados do evento no Athena. Os metadados da tabela armazenados no Catálogo de AWS Glue Dados permitem que o mecanismo de consulta do Athena saiba como encontrar, ler e processar os dados que você deseja consultar. Para ter mais informações, consulte Federar um armazenamento de dados de eventos.

   Para habilitar a federação de consultas do Lake, escolha Habilitar e faça o seguinte:

   a. Escolha se deseja criar um perfil ou usar um perfil do IAM existente. O AWS Lake Formation usa esse perfil para gerenciar permissões para o armazenamento de dados de eventos federados. Quando você cria uma nova função usando o CloudTrail console, cria CloudTrail automaticamente uma função com as permissões necessárias. Se você escolher um perfil existente, a política do perfil deve fornecer as permissões mínimas necessárias.

   b. Se você estiver criando um perfil, insira um nome para identificá-lo.

   c. Se você estiver usando um perfil existente, escolha o perfilo que deseja usar. O perfil deve existir em sua conta.

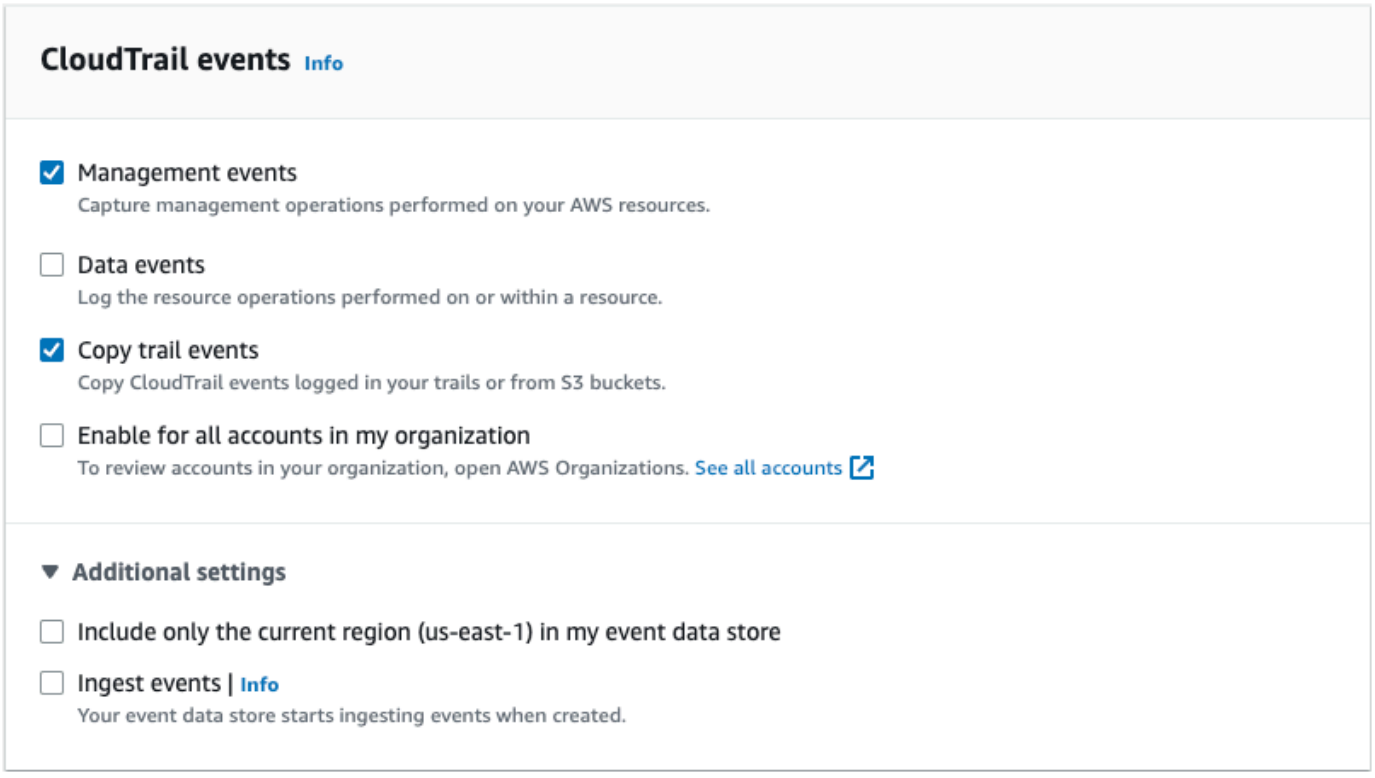
9. (Opcional) Em Tags, adicione uma ou mais tags personalizadas (pares chave-valor) ao armazenamento de dados de eventos. As tags podem ajudar você a identificar seus repositórios de dados de CloudTrail eventos. Por exemplo, você poderia anexar uma tag com o nome **`stage`** e o valor **`prod`**. É possível usar tags para limitar o acesso ao armazenamento de dados de eventos. As tags também podem ser usadas para monitorar os custos de consulta e ingestão do seu armazenamento de dados de eventos.

   Para obter informações sobre como usar tags para monitorar os custos, consulte Criação de etiquetas de alocação de custos definidas pelo usuário para armazenamentos de dados de

eventos do CloudTrail Lake. Para obter informações sobre como usar políticas do IAM para autorizar o acesso a um armazenamento de dados de eventos com base em tags, consulte Exemplos: negação de acesso para criar ou excluir armazenamentos de dados de eventos com base em tags. Para obter informações sobre como você pode usar tags em AWS, consulte Como marcar seus AWS recursos no Guia do usuário de AWS recursos de marcação.

10. Escolha Next (Avançar) para configurar o armazenamento de dados de eventos.
11. Na página Escolher eventos, mantenha as seleções padrão para Tipo de evento.
12. Para CloudTrail eventos, deixaremos os eventos de gerenciamento selecionados e escolheremos Copiar eventos da trilha. Neste exemplo, não estamos preocupados com os tipos de eventos porque estamos usando somente o armazenamento de dados de eventos para analisar eventos passados e não estamos ingerindo eventos futuros.

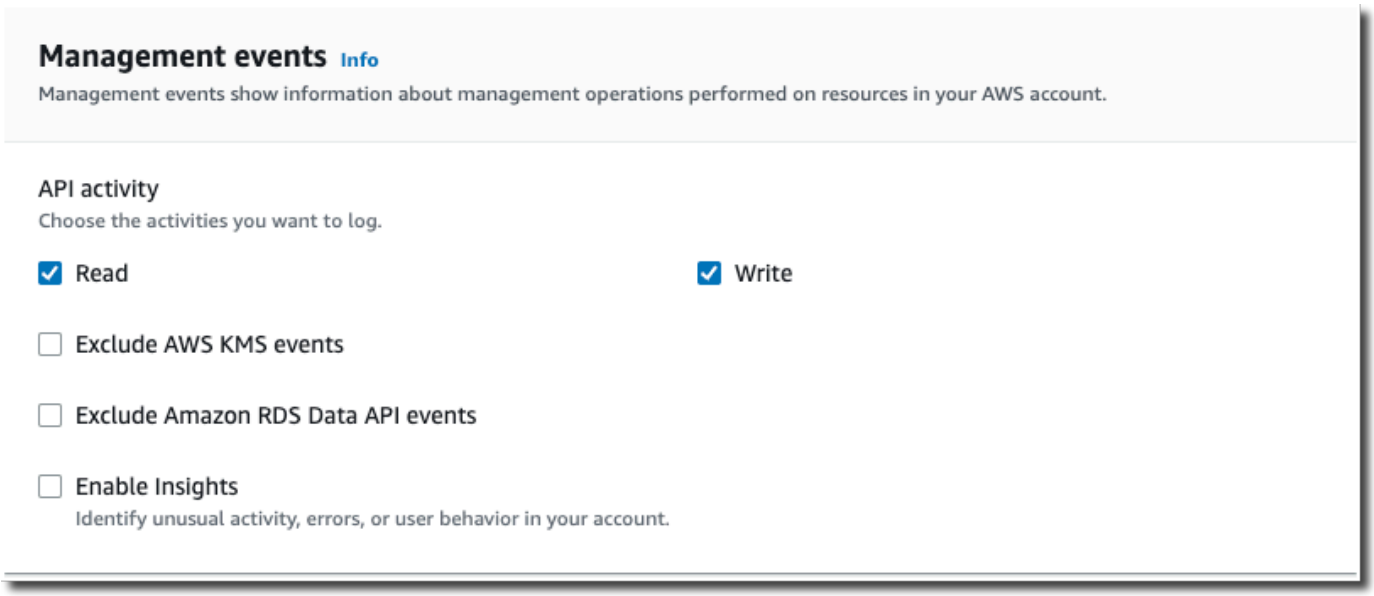
    Se você estiver criando um armazenamento de dados de eventos para substituir uma trilha existente, escolha os mesmos seletores de eventos da sua trilha para garantir que o armazenamento de dados de eventos tenha a mesma cobertura de eventos.



13. Escolha Habilitar para todas as contas em minha organização se este for um armazenamento de dados de eventos da organização. Essa opção não estará disponível para alteração, a menos que você tenha contas configuradas no AWS Organizations.

> **Note**
>
> Ao criar um armazenamento de dados de eventos da organização, você deverá estar conectado com a conta de gerenciamento da organização, pois somente a conta de gerenciamento pode copiar eventos de trilha para um armazenamento de dados de eventos da organização.

14. Em Configurações adicionais, desmarcaremos a opção Ingerir eventos porque, em nosso exemplo, não queremos que o armazenamento de dados de eventos consuma eventos futuros, pois estamos interessados apenas em consultar os eventos copiados. Por padrão, um armazenamento de dados de eventos coleta eventos para todos Regiões da AWS e começa a ingerir eventos quando é criado.
15. Em Eventos de gerenciamento, manteremos as configurações padrão.



16. Na área Copiar eventos da trilha, conclua as etapas a seguir.

    a. Escolha a trilha que você deseja copiar. Neste exemplo, escolheremos uma trilha chamada *`management-events`*.

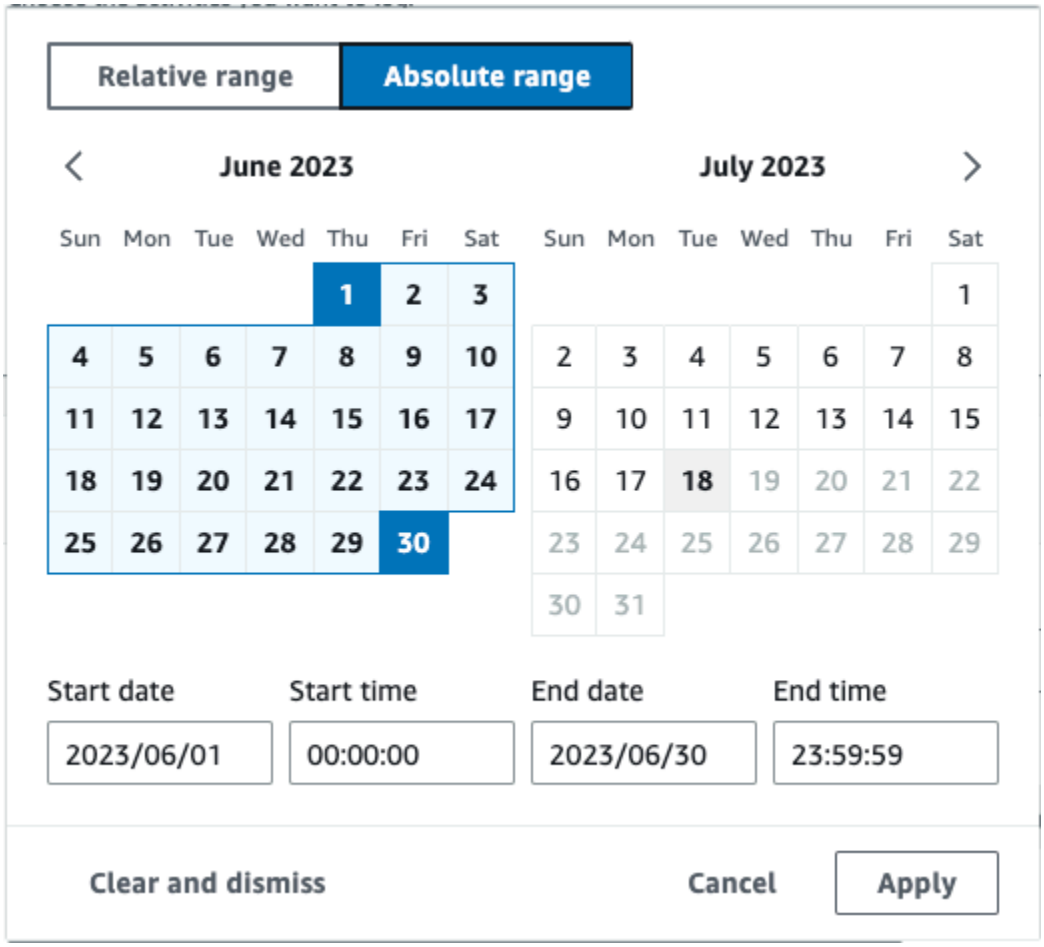
       Por padrão, copia CloudTrail somente CloudTrail os eventos contidos no prefixo do bucket do S3 e os `CloudTrail` prefixos dentro do `CloudTrail` prefixo, e não verifica os prefixos de outros serviços. AWS Se você quiser copiar CloudTrail eventos contidos em outro prefixo, escolha Inserir URI do S3 e, em seguida, escolha Procurar no S3 para navegar até o prefixo. Se o bucket S3 de origem da trilha usar uma chave KMS para criptografia de

dados, certifique-se de que a política de chaves do KMS permita CloudTrail descriptografar os dados. Se seu bucket do S3 de origem usa várias chaves KMS, você deve atualizar a política de cada chave CloudTrail para permitir a descriptografia dos dados no bucket. Para obter mais informações sobre a atualização da política de chaves do KMS, consulte Política de chaves do KMS para descriptografar dados no bucket do S3 de origem.

b. Escolha um intervalo de tempo para copiar os eventos. CloudTrail verifica o prefixo e o nome do arquivo de log para verificar se o nome contém uma data entre as datas de início e término escolhidas antes de tentar copiar os eventos da trilha. É possível escolher entre Relative range (Intervalo relativo) e Absolute range (Intervalo absoluto). Para evitar a duplicação de eventos entre a trilha de origem e o armazenamento de dados de eventos de destino, escolha um intervalo de tempo que seja anterior à criação do armazenamento de dados de eventos.

   - Se você escolher Intervalo relativo, poderá optar por copiar eventos registrados nos últimos 6 meses, 1 ano, 2 anos, 7 anos ou um intervalo personalizado. CloudTrail copia os eventos registrados dentro do período de tempo escolhido.
   - Se você escolher Intervalo absoluto, poderá escolher uma data específica de início e término. CloudTrail copia os eventos que ocorreram entre as datas de início e término escolhidas.

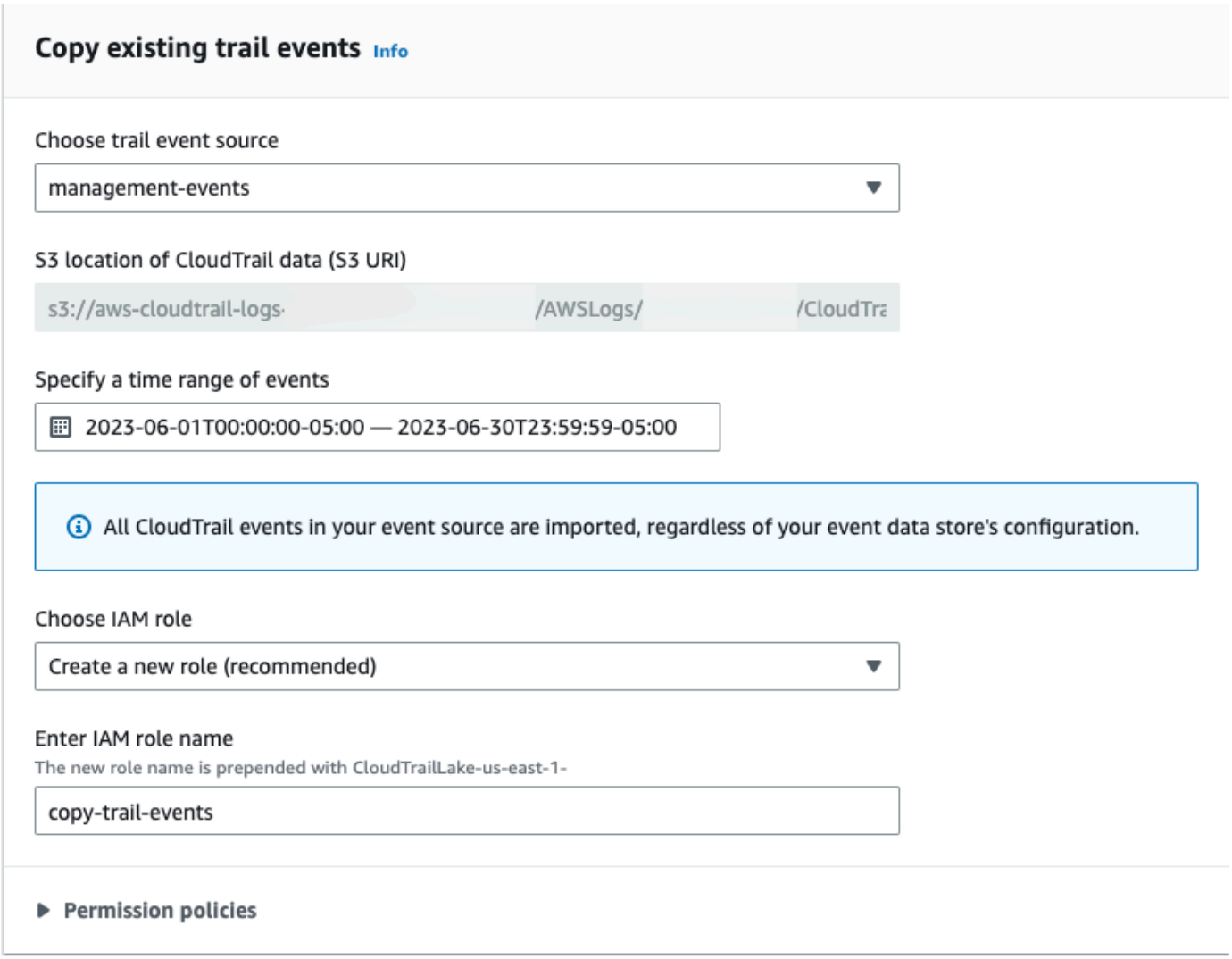
   Neste exemplo, escolheremos Intervalo absoluto e selecionaremos todo o mês de junho.



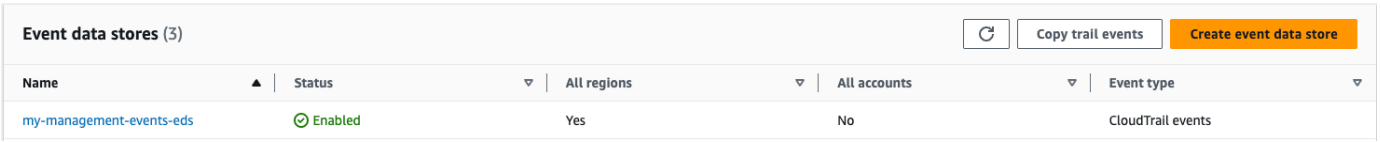
c. Em Permissions (Permissões), escolha uma das opções de perfil do IAM a seguir. Ao escolher um perfil do IAM existente, verifique se a política de perfil do IAM fornece as permissões necessárias. Para obter mais informações sobre como atualizar as permissões do perfil do IAM, consulte Permissões do IAM para copiar eventos da trilha.

- Escolha Create a new role (recommended) (Criar uma nova função [recomendado]) para criar um novo perfil do IAM. Em Inserir nome da função do IAM, insira um nome para a função. CloudTrailcria automaticamente as permissões necessárias para essa nova função.
- Escolha Usar um ARN de função personalizada do IAM para usar uma função personalizada do IAM que não esteja listada. Em Enter IAM role ARN (Inserir ARN do perfil do IAM), insira o ARN do perfil.
- Escolha uma função do IAM existente na lista suspensa.

Neste exemplo, escolheremos Criar um novo perfil (recomendado) e forneceremos o nome **`copy-trail-events`**.

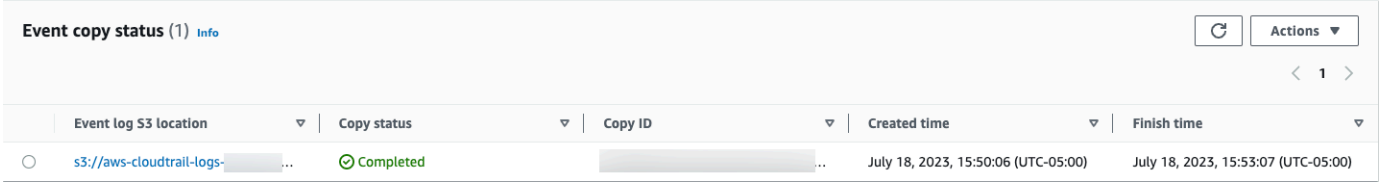


17. Selecione Next (Próximo) para revisar suas escolhas.
18. Na página Review and create (Revisar e criar), revise as suas escolhas. Escolha Edit (Editar) para fazer alterações a uma seção. Quando estiver pronto para criar o armazenamento de dados de eventos, escolha Create event data store (Criar armazenamento de dados de eventos).
19. O novo armazenamento de dados de eventos está visível na tabela Armazenamentos de dados de eventos na página Armazenamento de dados de eventos.

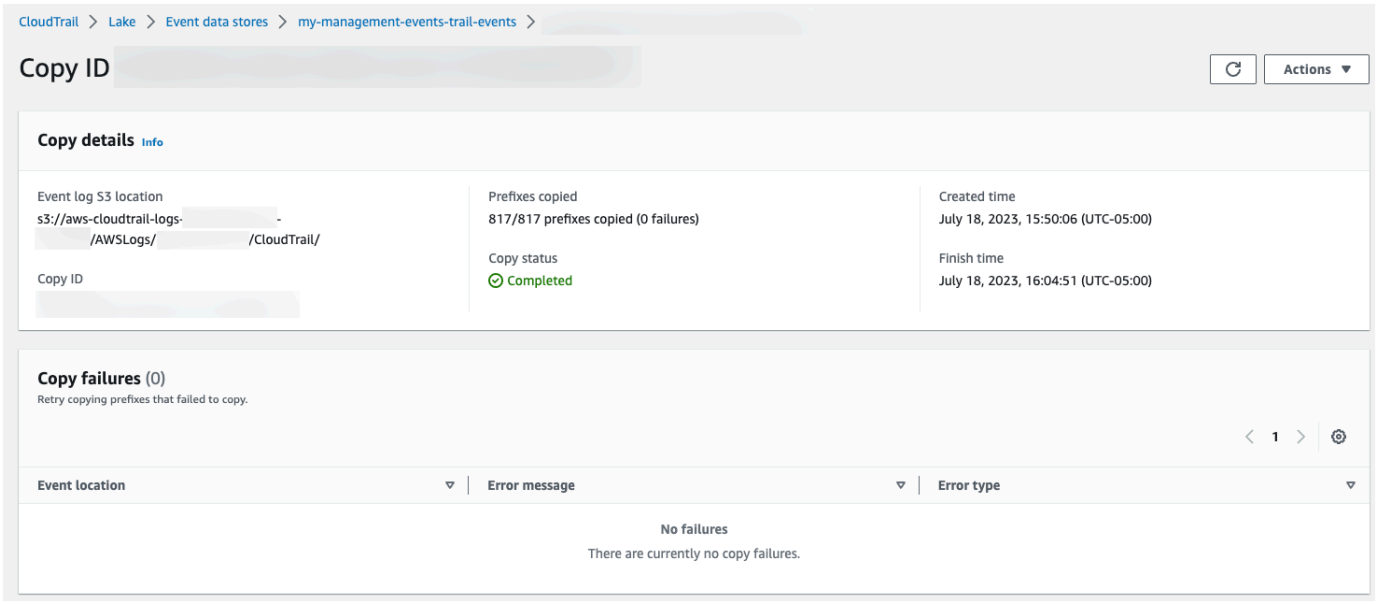


20. Escolha o nome do armazenamento de dados de eventos para visualizar sua página de detalhes. A página de detalhes mostra os detalhes do armazenamento de dados de eventos e o status da cópia. O status da cópia de eventos é mostrado na área Status da cópia de eventos.

    Quando uma cópia de evento de trilha é concluída, seu Copy status (Status de cópia) é definido como Completed (Concluída) se não houve erros ou como Failed (Falha) se houve algum erro.



21. Para visualizar mais detalhes sobre a cópia, escolha o nome da cópia na coluna Localização do log de eventos no S3 ou escolha a opção Visualizar detalhes no menu Ações. Para obter mais informações sobre como visualizar os detalhes de uma cópia de evento de trilha, consulte Detalhes da cópia de um evento.



22. A área Falhas de cópia mostra todos os erros que ocorreram ao copiar eventos de trilha. Se o Copy status (Status da cópia) for Failed (Falha), corrija os erros mostrados em Copy failures (Falhas ao copiar) e, em seguida, escolha Retry copy (Tentar cópia novamente). Quando você tenta fazer uma cópia novamente, CloudTrail retoma a cópia no local em que a falha ocorreu.

Veja os painéis CloudTrail do Lake

Este passo a passo mostra como visualizar os painéis do CloudTrail Lake. CloudTrailOs painéis do Lake permitem que você visualize os eventos em seu armazenamento de dados de eventos e veja tendências, como os principais usuários e os principais erros.

Cada painel consiste em vários widgets e cada widget representa uma consulta SQL. Para preencher o painel, CloudTrail executa consultas geradas pelo sistema. As consultas incorrem em cobranças com base na quantidade de dados examinados.

> **Note**
>
> Atualmente, os painéis só estão disponíveis para armazenamentos de dados de eventos que coletam eventos CloudTrail de gerenciamento, eventos de dados do Amazon S3 e eventos do Insights.

Para visualizar painéis do Lake

1. Faça login no AWS Management Console e abra o CloudTrail console em https://console.aws.amazon.com/cloudtrail/.
2. No painel de navegação, em Lake, escolha Painel.
3. Na primeira vez que você visualiza a página Painéis, CloudTrail solicita que você reconheça os custos associados à execução de consultas. Escolha Eu concordo para confirmar que está ciente do custo da execução de consultas. Essa confirmação é necessária apenas uma vez. Para obter mais informações sobre CloudTrail preços, consulte CloudTrailPreços.
4. Escolha seu armazenamento de dados de eventos na lista e, em seguida, escolha o tipo de painel que deseja visualizar.

   Os possíveis tipos de painel são apresentados a seguir.

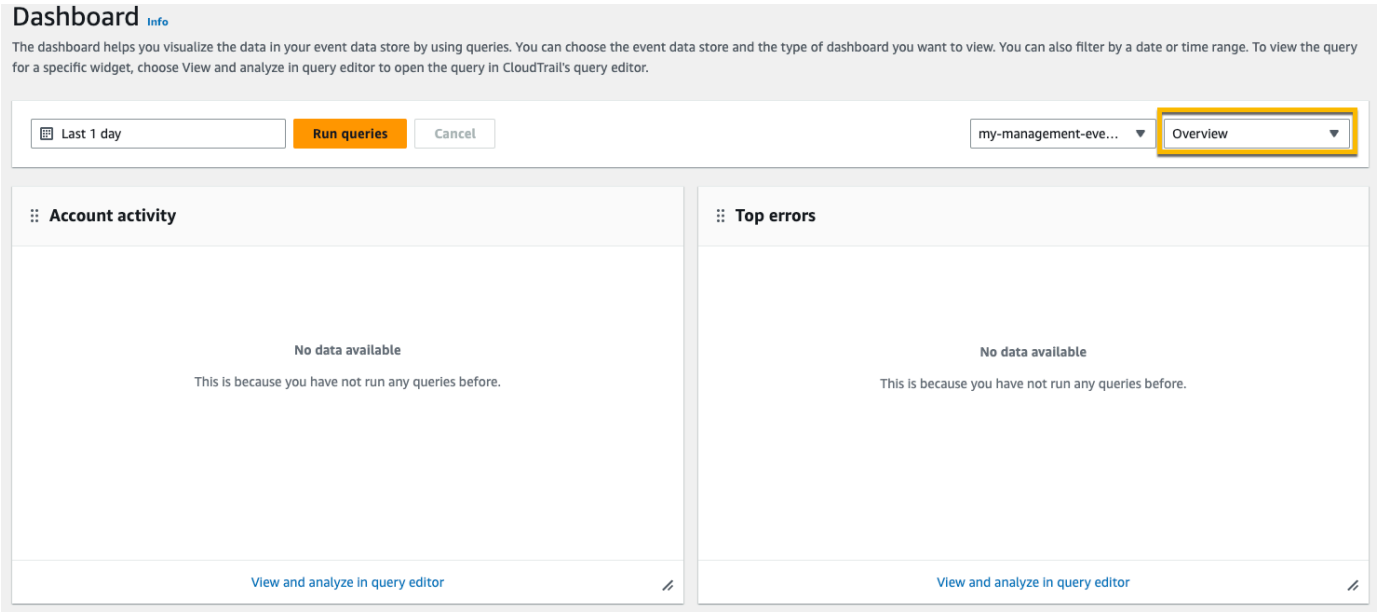
   - Painel de visão geral - Mostra os usuários mais ativos e Serviços da AWS por contagem de eventos. Regiões da AWS Também é possível visualizar informações sobre atividades de eventos de gerenciamento de `read` e `write`, eventos com mais controle de utilização e os principais erros. Esse painel está disponível para armazenamentos de dados de eventos que coletam eventos de gerenciamento.
   - Painel Gerenciamento de eventos: mostra eventos de login do console, eventos de acesso negado, ações destrutivas e principais erros por usuário. Você também pode visualizar

informações sobre versões do TLS e chamadas de TLS desatualizadas por usuário. Esse painel está disponível para armazenamentos de dados de eventos que coletam eventos de gerenciamento.

- Painel Eventos de dados do S3: mostra a atividade da conta do S3, os objetos mais acessados do S3, os principais usuários do S3 e as principais ações do S3. Esse painel está disponível para armazenamentos de dados de eventos que coletam eventos de dados do Amazon S3.
- Painel Eventos do Insights: mostra a proporção geral de eventos do Insights por tipo de Insights, a proporção de eventos do Insights por tipo de Insights para os principais usuários e serviços e o número de eventos do Insights por dia. O painel também inclui um widget que lista até 30 dias de eventos do Insights. Esse painel está disponível somente para armazenamentos de dados de eventos que coletam eventos do Insights.

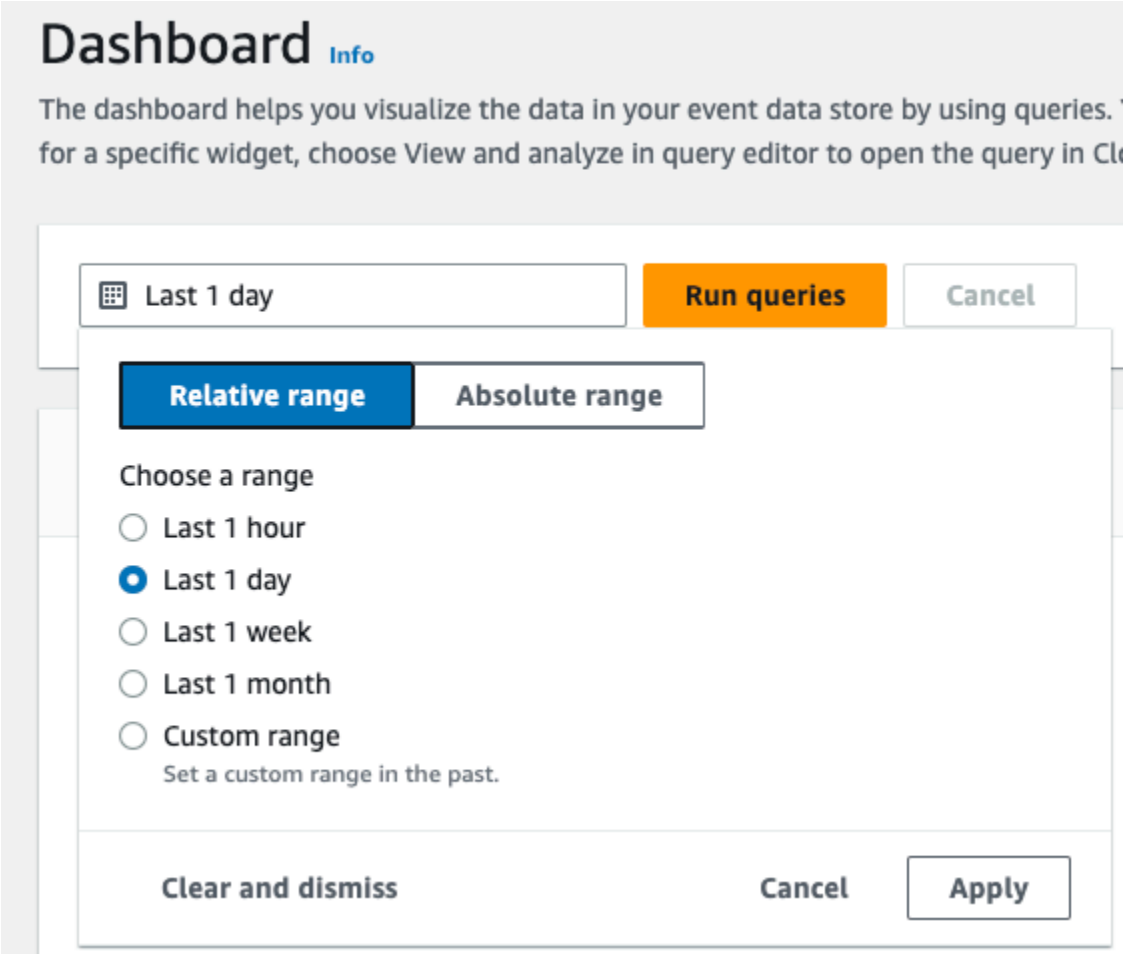
> **Note**
>
> - Depois de ativar o CloudTrail Insights pela primeira vez no armazenamento de dados do evento de origem, pode levar até 7 dias CloudTrail para entregar o primeiro evento do Insights, se uma atividade incomum for detectada. Para ter mais informações, consulte Entender a entrega de eventos do Insights.
> - O painel Eventos do Insights exibe apenas informações sobre os eventos do Insights coletados pelo armazenamento de dados de eventos selecionado, o qual é determinado pela configuração do armazenamento de dados do evento de origem. Por exemplo, se você configurar o armazenamento de dados de eventos de origem para ativar eventos do Insights em `ApiCallRateInsight` mas não `ApiErrorRateInsight`, você não verá informações sobre os eventos do Insights em `ApiErrorRateInsight`.

Neste exemplo, escolhemos o painel Visão geral.



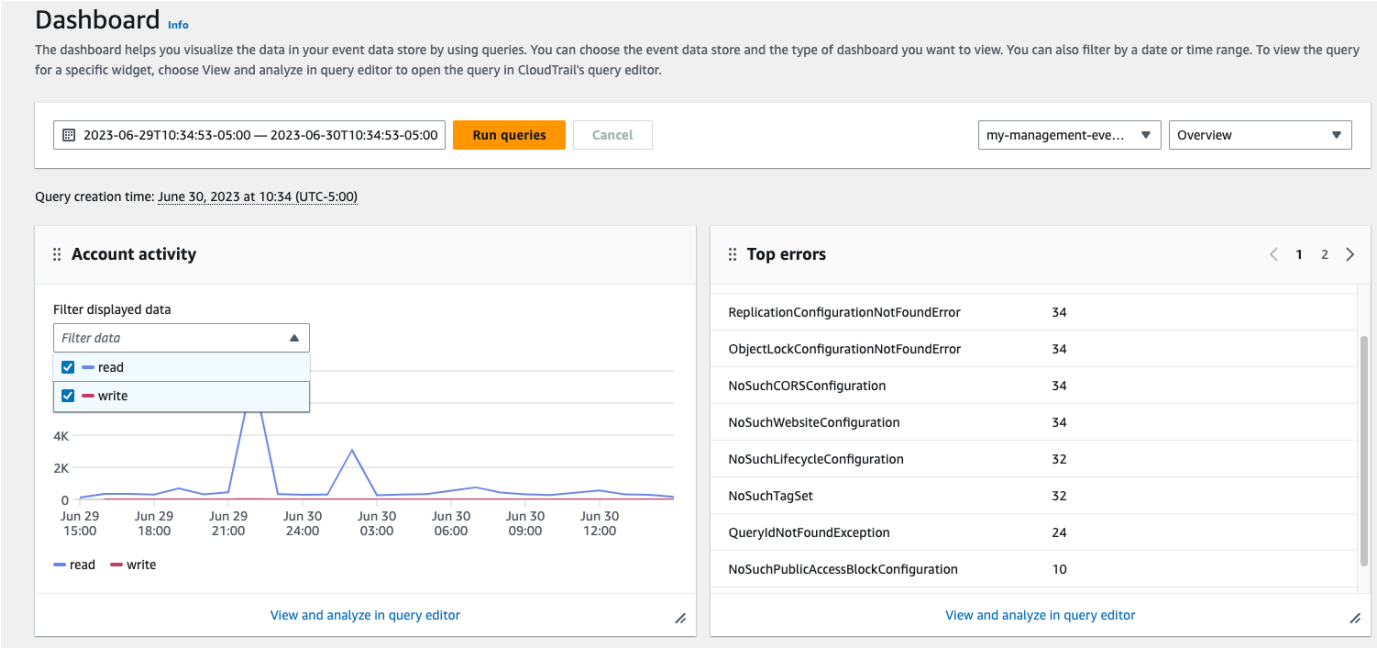
5. Escolha o campo de data para filtrar em um intervalo de tempo e, em seguida, escolha Aplicar. Escolha Intervalo absoluto para selecionar um intervalo específico de data e hora. Escolha Intervalo relativo para selecionar um intervalo de tempo predefinido ou um intervalo personalizado. Por padrão, o painel exibe dados de eventos das últimas 24 horas.

> **Note**
>
> Como CloudTrail as consultas são cobradas com base na quantidade de dados digitalizados, você pode reduzir os custos filtrando em um intervalo de tempo mais restrito.

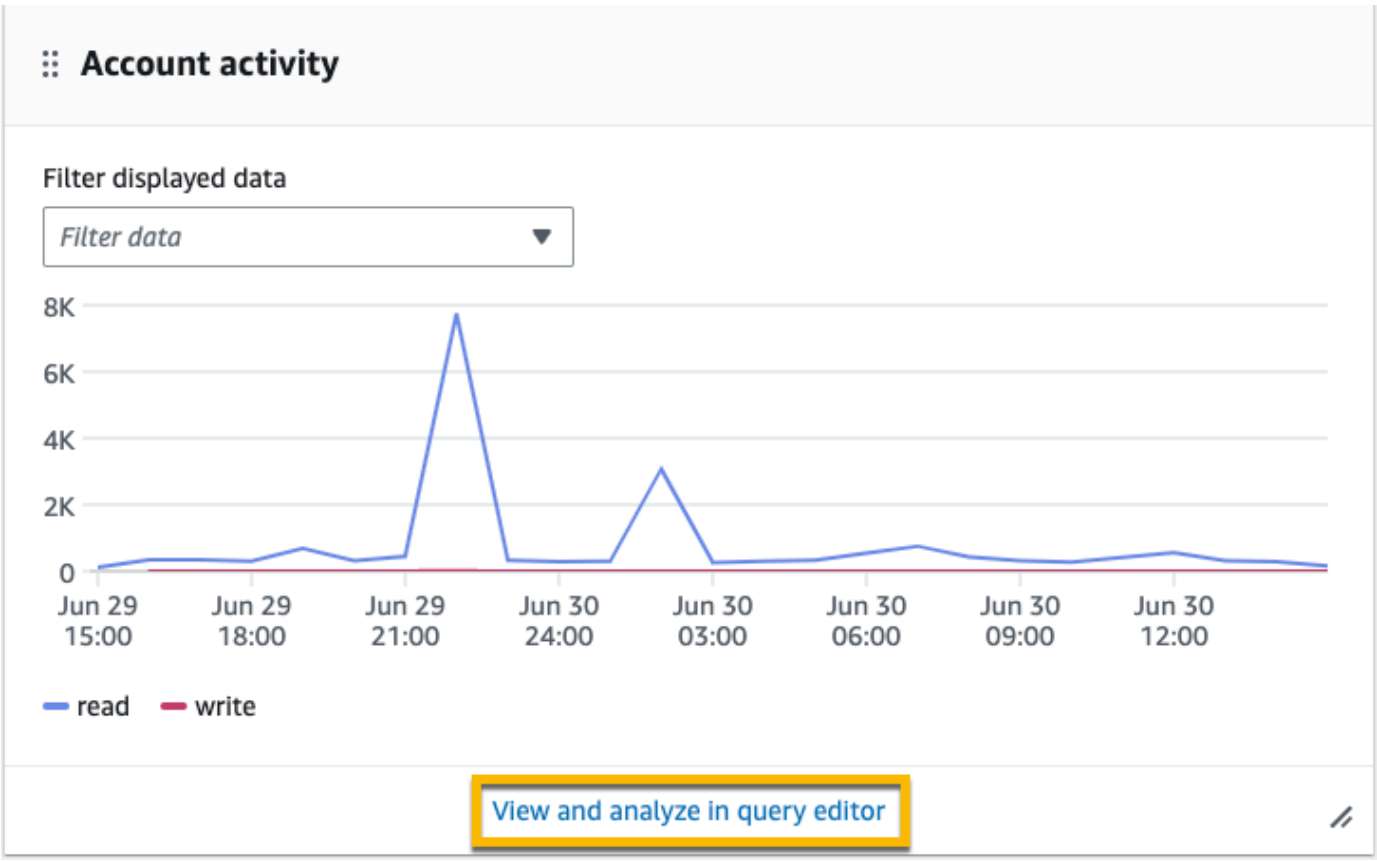


6. Escolha Executar consultas para preencher o painel. Cada widget exibe individualmente o status da consulta associada e apresenta os dados quando a consulta é concluída.

   É possível realizar uma filtragem adicional em alguns widgets, por exemplo, Atividade da conta, que permite filtrar a atividade de um evento de `read` e `write`.

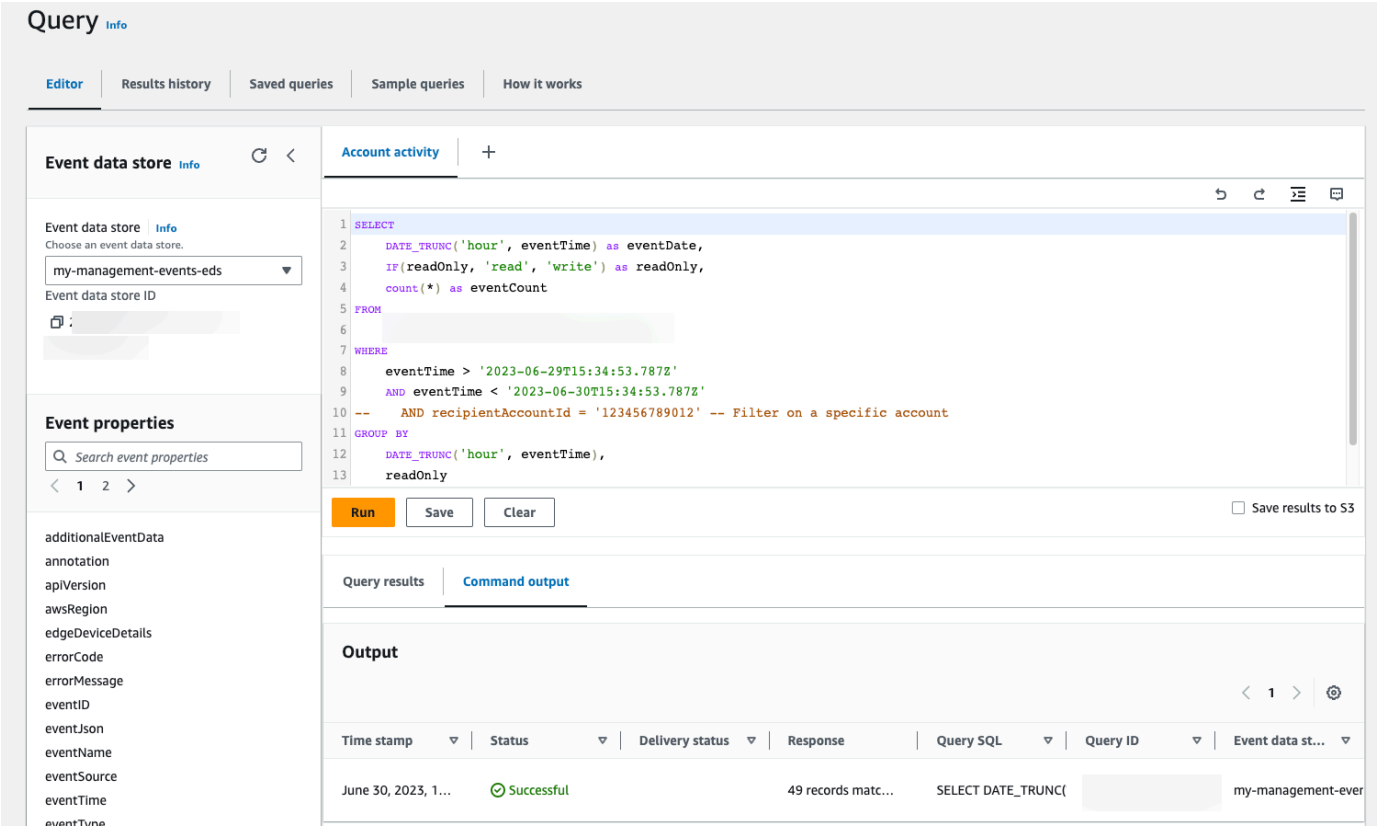


7. Para visualizar a consulta por um widget, escolha Visualizar e analisar no editor de consultas.



Escolher Exibir e analisar no editor de consultas abre a consulta no editor de consultas do CloudTrail Lake, o que permite analisar melhor os resultados da consulta fora do painel. Para

obter mais informações sobre a edição de uma consulta, veja Criar ou editar uma consulta. Para obter mais informações sobre como executar uma consulta e salvar seus resultados, consulte Executar uma consulta e salvar os resultados de consulta.



Para obter mais informações sobre painéis, consulte Veja os painéis CloudTrail do Lake.

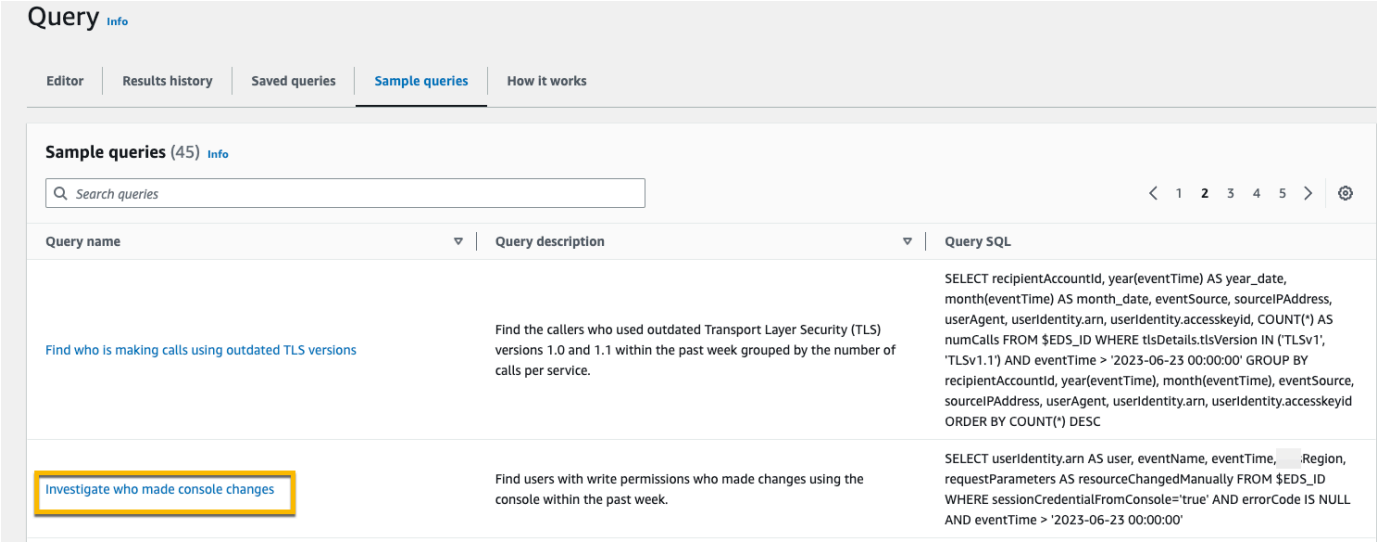
Visualize e execute exemplos de consultas do CloudTrail Lake

CloudTrail O Lake fornece vários exemplos de consultas que podem ajudar você a começar a escrever suas próprias consultas. Este passo a passo mostra como selecionar e executar uma consulta de amostra.

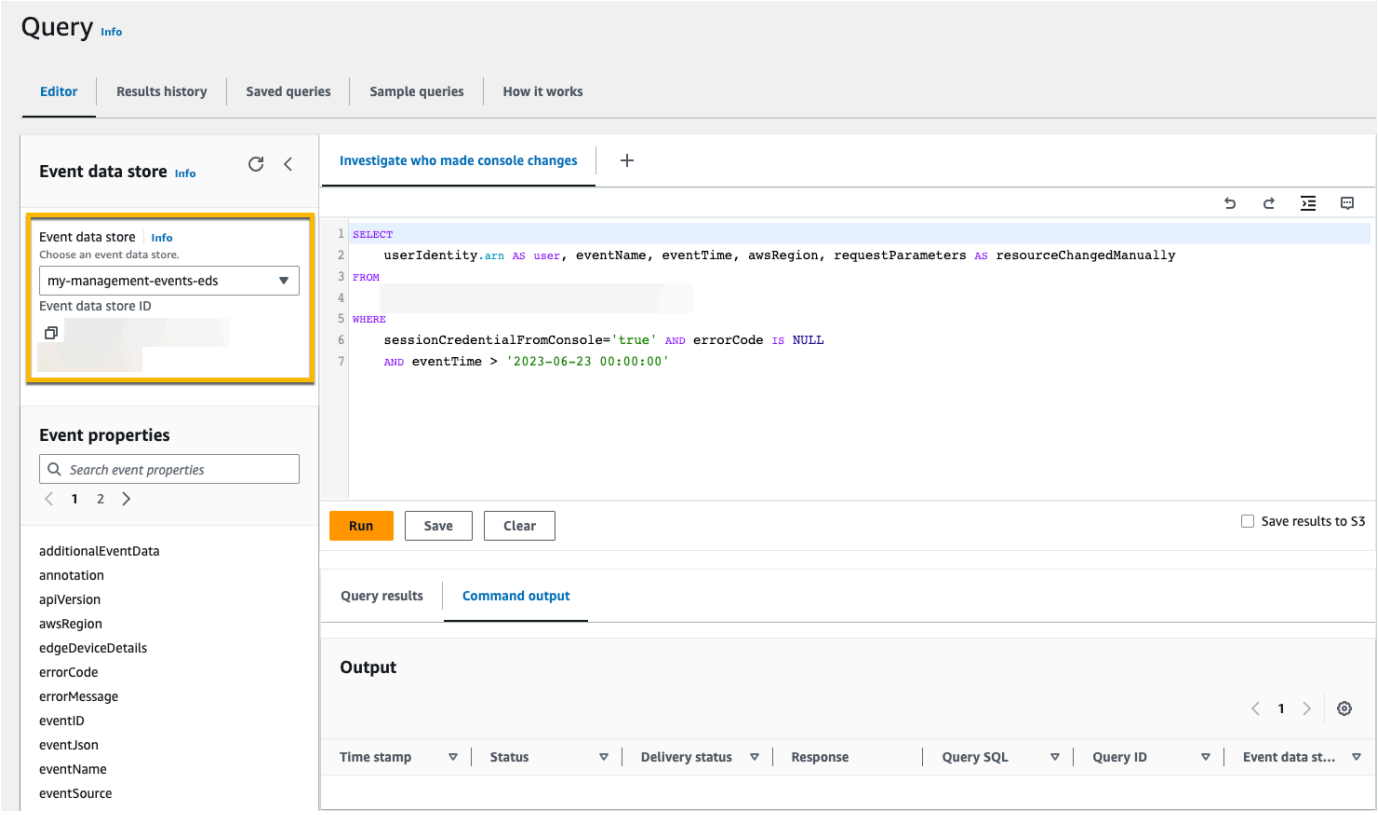
CloudTrail as consultas incorrem em cobranças com base na quantidade de dados digitalizados. Para ajudar a controlar os custos, recomendamos que você restrinja as consultas adicionando carimbos de data/hora `eventTime` de início e término nas consultas. Para obter mais informações sobre CloudTrail preços, consulte AWS CloudTrail Preços.

Para visualizar e executar uma consulta de exemplo

1. Faça login no AWS Management Console e abra o CloudTrail console em https://console.aws.amazon.com/cloudtrail/.
2. No painel de navegação, em Lake, escolha Consulta.
3. Na página Query (Consulta), escolha a guia Sample queries (Consultas de exemplo).
4. Escolha uma consulta de exemplo na lista ou pesquise pela consulta para filtrar a lista. Neste exemplo, abriremos a consulta Investigar quem fez alterações no console escolhendo o Nome da consulta. Isso abre a consulta na guia Editor.

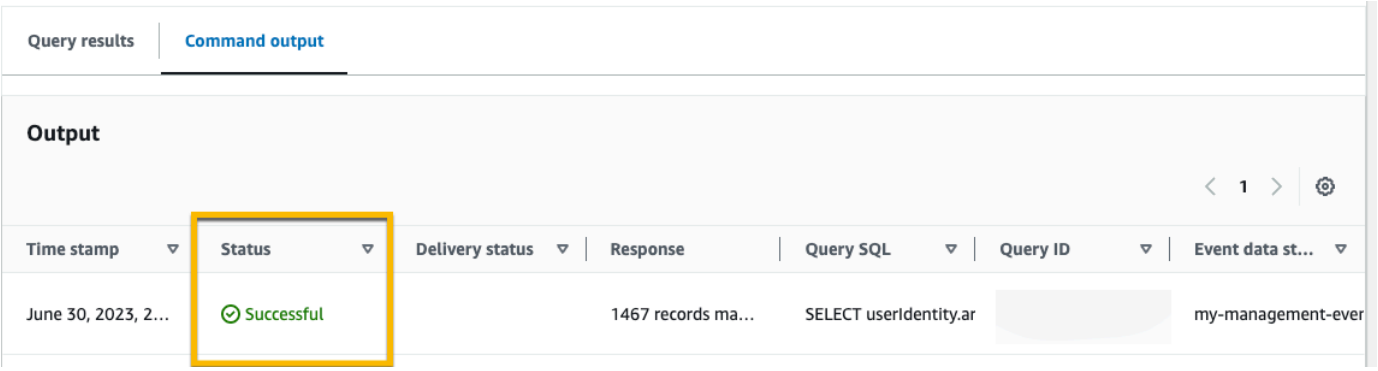


5. Na guia Editor, escolha o armazenamento de dados de eventos para o qual você deseja executar a consulta. Quando você escolhe o armazenamento de dados do evento na lista, preenche CloudTrail automaticamente o ID do armazenamento de dados do evento na `FROM` linha do editor de consultas.

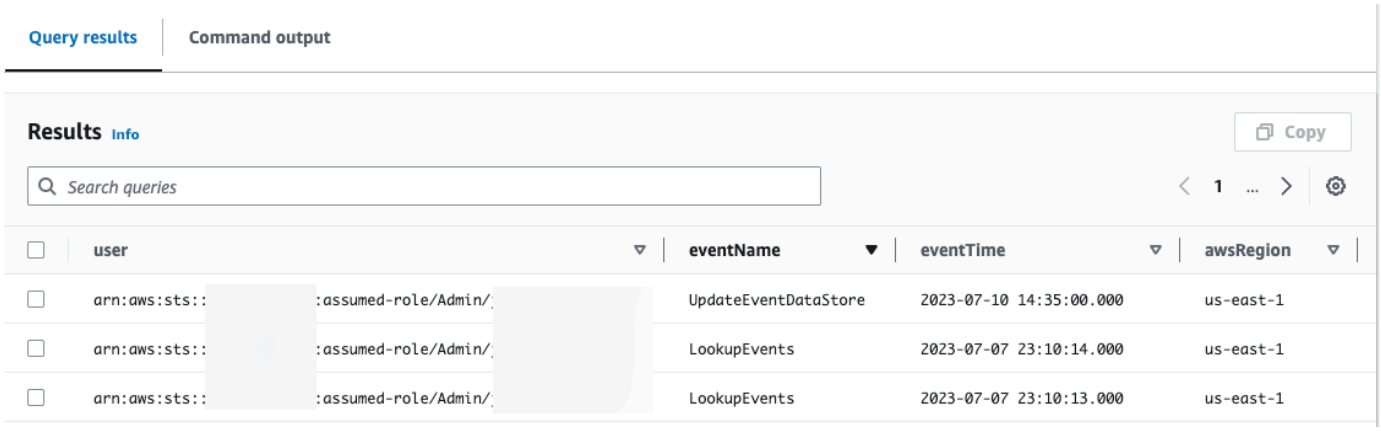


6. Para executar a consulta, escolha Executar.

   A guia Saída do comando mostra metadados sobre a consulta, por exemplo, se a consulta foi bem-sucedida, o número de registros correspondentes e o tempo de execução da consulta.



   A guia Resultados da consulta mostra os dados de eventos no armazenamento de dados de eventos selecionado que correspondem à sua consulta.



Para obter mais informações sobre a edição de uma consulta, veja Criar ou editar uma consulta. Para obter mais informações sobre como executar uma consulta e salvar seus resultados, consulte Executar uma consulta e salvar os resultados de consulta.

Salve os resultados da consulta do CloudTrail Lake em um bucket S3

Este passo a passo mostra como você pode salvar os resultados da consulta do CloudTrail Lake em um bucket do S3 e, em seguida, fazer o download desses resultados.

Ao executar consultas no CloudTrail Lake, você incorre em cobranças com base na quantidade de dados digitalizados pela consulta. Não há cobranças adicionais do CloudTrail Lake para salvar os resultados da consulta em um bucket do S3. No entanto, há cobranças de armazenamento do S3. Para obter mais informações sobre os preços, consulte Preços do Amazon S3.

Quando você salva os resultados da consulta, os resultados da consulta podem ser exibidos no CloudTrail console antes de serem visualizados no bucket do S3, pois CloudTrail entregam os resultados da consulta após a conclusão da verificação da consulta. Embora a maioria das consultas seja concluída em alguns minutos, dependendo do tamanho do seu armazenamento de dados de eventos, pode levar muito mais tempo para entregar os resultados da consulta CloudTrail ao seu bucket do S3. CloudTrail entrega os resultados da consulta ao bucket do S3 no formato gzip compactado. Em média, após a conclusão da análise da consulta, você pode esperar uma latência de 60 a 90 segundos para cada GB de dados entregue ao bucket do S3.

Para salvar resultados de consultas em um bucket do Amazon S3

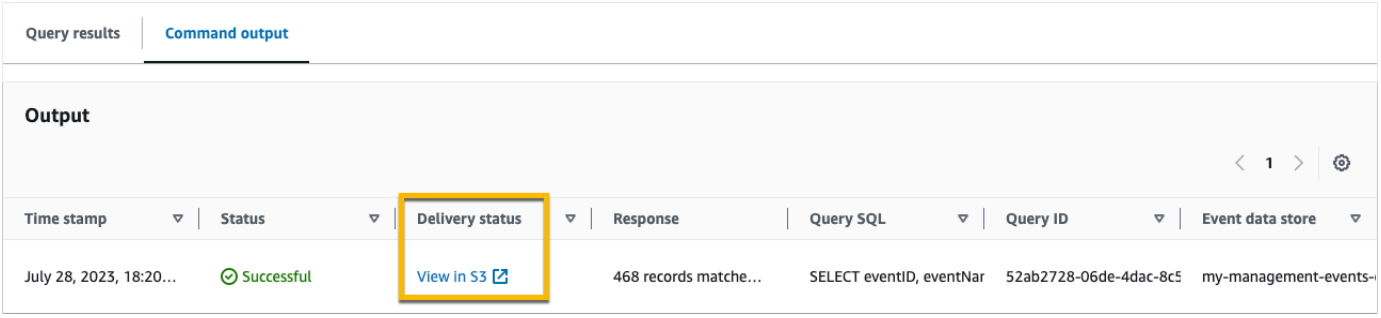
1. Faça login no AWS Management Console e abra o CloudTrail console em https://console.aws.amazon.com/cloudtrail/.
2. No painel de navegação, em Lake, escolha Consulta.
3. Nas guias Consultas de exemplo ou Consultas salvas, escolha uma consulta a ser executada escolhendo o valor na coluna Nome da consulta. Neste exemplo, escolheremos a consulta de exemplo chamada Investigar ações do usuário.
4. Na guia Editor, em Event data store (Armazenamento de dados de eventos), escolha um armazenamento de dados de eventos na lista suspensa. Quando você escolhe o armazenamento de dados do evento na lista, preenche CloudTrail automaticamente o ID do armazenamento de dados do evento na `From` linha.
5. Nesta consulta de exemplo, editaremos o valor `userIdentity.`ARN para especificar um usuário chamado `Admin` e mantermos os valores padrão para `eventTime`. Ao executar uma consulta, você é cobrado pela quantidade de dados examinados. Para ajudar a controlar os custos, recomendamos que você restrinja as consultas adicionando carimbos de data/hora `eventTime` de início e término nas consultas.

6. Escolha Salvar resultados no S3 para salvar os resultados da consulta em um bucket do S3. Quando você escolhe o bucket S3 padrão, CloudTrail cria e aplica as políticas de bucket necessárias. Se você escolher o bucket S3 padrão, sua política do IAM precisará incluir permissão para a `s3:PutEncryptionConfiguration` ação porque, por padrão, a criptografia do lado do servidor está habilitada para o bucket. Para obter mais informações sobre como salvar resultados de consulta, acesse Informações adicionais sobre resultados de consultas salvas. Neste exemplo, usaremos o bucket do S3 padrão.

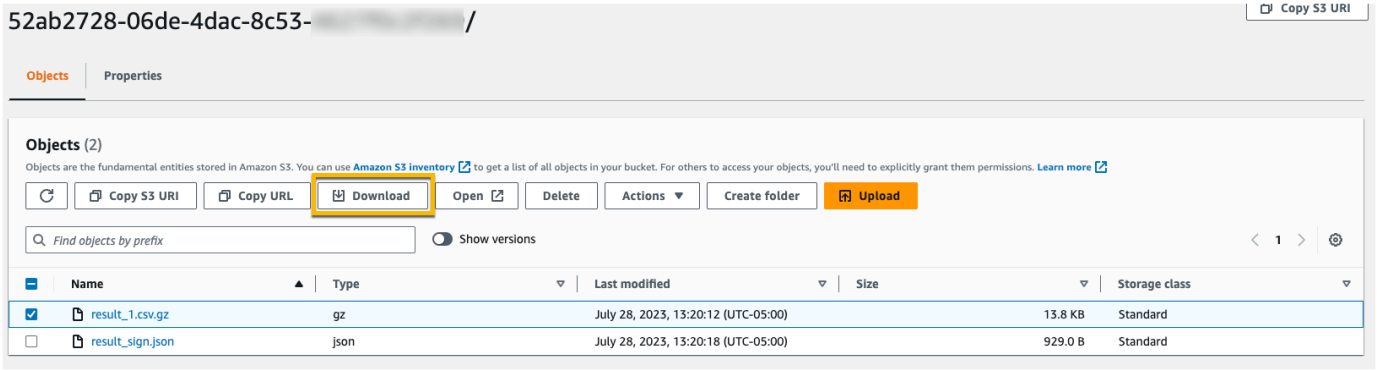
> **Note**
>
> Para usar um bucket diferente, especifique um nome de bucket ou escolha Browse S3 (Procurar S3) para escolher um bucket. A política do bucket deve conceder CloudTrail permissão para entregar os resultados da consulta ao bucket. Para obter informações sobre como editar manualmente a política de bucket, consulte Política de bucket do Amazon S3 para resultados de consulta CloudTrail do Lake.

7. Escolha Executar. Dependendo do tamanho do armazenamento de dados do evento e do número de dias de dados que ele inclui, uma consulta pode levar vários minutos para ser executada. A guia Command output (Saída do comando) mostra o status de uma consulta e se uma consulta tem a execução concluída. Quando uma consulta terminar de ser executada, abra a guia Query results (Resultados da consulta) para ver uma tabela de resultados para a consulta ativa (a consulta atualmente mostrada no editor).
8. Ao CloudTrail concluir a entrega dos resultados da consulta salva no bucket do S3, a coluna Status da entrega fornece um link para o bucket do S3 que contém os arquivos de resultados da consulta salvos, bem como um arquivo de sinal que você pode usar para verificar os resultados da consulta salva. Escolha Visualizar no S3 para visualizar os arquivos de resultados da consulta e os arquivos de assinatura no bucket do S3.

> **Note**
>
> Quando você salva os resultados da consulta, os resultados da consulta podem ser exibidos no CloudTrail console antes de serem visualizados no bucket do S3, pois CloudTrail entregam os resultados da consulta após a conclusão da verificação da consulta. Embora a maioria das consultas seja concluída em alguns minutos, dependendo do tamanho do seu armazenamento de dados de eventos, pode levar muito mais tempo para entregar os resultados da consulta CloudTrail ao seu bucket do S3. CloudTrail entrega os resultados da consulta ao bucket do S3 no formato gzip compactado. Em média, após a conclusão da análise da consulta, você pode esperar uma latência de 60 a 90 segundos para cada GB de dados entregue ao bucket do S3.



9. Para baixar os resultados da consulta, escolha o arquivo de resultados da consulta (neste exemplo, `result_1.csv.gz`) e escolha Baixar.



Para obter mais informações sobre validação de resultados de consultas salvas, acesse Validar resultados de consulta salva.

Visualizando seu CloudTrail custo e uso com AWS Cost Explorer

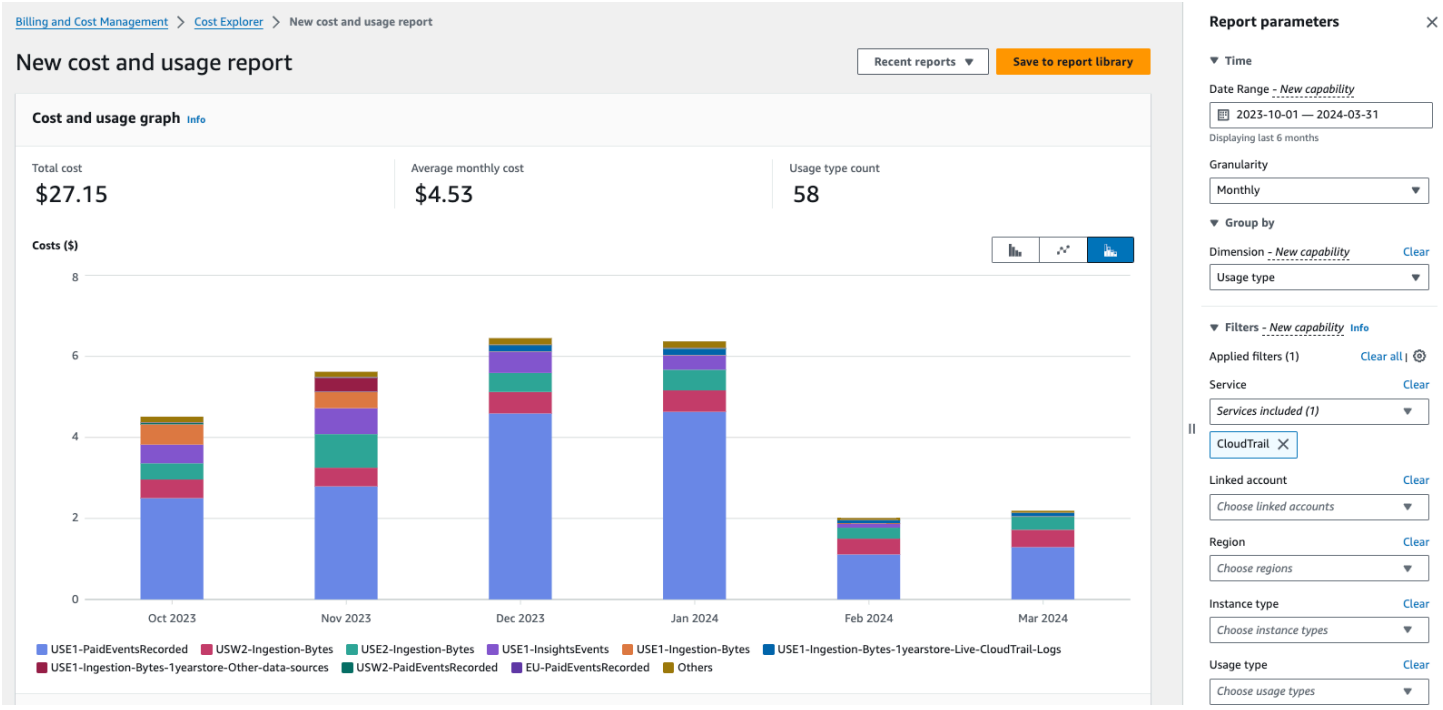
Esta seção descreve como você pode visualizar seus CloudTrail custos e uso usando AWS Cost Explorer. O Cost Explorer oferece a capacidade de visualizar, entender e gerenciar seus AWS custos e uso ao longo do tempo.

Para obter detalhes sobre CloudTrail preços, consulte AWS CloudTrail Preços.

Para ver o CloudTrail custo e o uso com o Cost Explorer

1. Faça login AWS Management Console e abra o console do Cost Explorer em https://console.aws.amazon.com/cost-management/home#/custom.
2. Em Hora, escolha o intervalo de datas que você deseja analisar.
3. Em Agrupar por, em Dimensão, escolha Tipo de uso.
4. Em Filtros, em Serviço, escolha CloudTrail.

A imagem a seguir mostra um exemplo de um relatório de custos filtrado CloudTrail e agrupado por tipo de uso.



Analise o Tipo de uso para ver quais CloudTrail recursos geraram o maior custo. Cada tipo de uso começa com o código do Região da AWS local em que a cobrança foi cobrada.

A tabela a seguir descreve os tipos de CloudTrail uso de cada CloudTrail recurso.

CloudTrail recurso	Tipo de uso	Descrição
CloudTrail trilhas	*region*-FreeEventsRecorded	A primeira cópia dos eventos de gerenciamento entregue gratuitamente a um Região da AWS.
	region-PaidEventsRecorded	A cobrança por cópias adicionais de eventos de gerenciamento entregues a um Região da AWS.
	region-DataEventsRecorded	A cobrança pela entrega de eventos de dados a um Região da AWS. Os eventos de dados sempre incorrem em cobranças.
CloudTrail Lago	*region*-Ingestion-Bytes	A cobrança pela ingestão de eventos em um armazenamento de dados de eventos do

CloudTrail recurso	Tipo de uso	Descrição
		CloudTrail Lake usando a opção de preço de retenção de sete anos. O preço de ingestão é baseado no volume de dados ingeridos e é o mesmo para todos os tipos de eventos.
	region-Ingestion-Bytes-1yearstore-Live-CloudTrail-Logs	A cobrança pela ingestão de eventos de CloudTrail dados e eventos de gerenciamento em um armazenamento de dados de eventos do CloudTrail Lake usando a opção de preço de retenção extensível por um ano.

CloudTrail recurso	Tipo de uso	Descrição
	region-Ingestion-Bytes-1yearstore-Other-data-sources	A cobrança pela ingestão de outras fontes de eventos em um armazenamento de dados de eventos do CloudTrail Lake usando a opção de preço de retenção extensível por um ano. Isso inclui eventos do CloudTrail Insights, itens de configuração AWS Config, evidências de AWS Audit Manager CloudTrail registros históricos (não compactados) importados do S3 e eventos externos ao. AWS

CloudTrail recurso	Tipo de uso	Descrição
	region-QueryScanned-Bytes	A cobrança pela execução de consultas CloudTrail do Lake. Ao executar consultas no CloudTrail Lake, você incorre em cobranças com base na quantidade de dados otimizados e compactados digitalizados.
CloudTrail Percepções	*region*-InsightsEvents	A cobrança pelos eventos do CloudTrail Insights. Para eventos do Insights, você incorre em cobranças com base no número de eventos de gerenciamento analisados por tipo de Insight.

Recursos adicionais do

- AWS CloudTrail Definição de preço
- Gerenciando os custos das CloudTrail trilhas

- Gerenciando os custos CloudTrail do Lake

Trabalhando com o histórico de CloudTrail eventos

CloudTrail está ativado por padrão para sua AWS conta e você tem acesso automático ao histórico de CloudTrail eventos. O Histórico de eventos fornece um registro visualizável, pesquisável, baixável e imutável dos últimos 90 dias de eventos de gerenciamento em uma Região da AWS. Esses eventos capturam atividades feitas por meio de AWS Management Console, AWS Command Line Interface, e AWS SDKs e APIs. O histórico de eventos registra eventos no Região da AWS local em que o evento aconteceu. Não há CloudTrail cobrança pela visualização do histórico de eventos.

Você pode pesquisar eventos relacionados à criação, modificação ou exclusão de recursos (como usuários do IAM ou instâncias do Amazon EC2) por região no Conta da AWS console, visualizando a página CloudTrail de histórico de eventos. Você também pode pesquisar esses eventos executando o comando aws cloudtrail lookup-events ou usando a API `LookupEvents`.

Você pode usar a página Histórico de eventos no CloudTrail console para visualizar, pesquisar, baixar, arquivar, analisar e responder à atividade da conta em toda a sua AWS infraestrutura. É possível personalizar a visualização do Histórico de eventos selecionando quantos eventos devem ser exibidos em cada página e quais colunas serão exibidas ou ocultadas. Você também pode comparar os detalhes dos eventos no histórico de eventos side-by-side. Você pode pesquisar eventos de forma programática usando os AWS SDKs ou. AWS Command Line Interface

> **Note**
>
> Com o tempo, Serviços da AWS pode adicionar eventos adicionais. CloudTrail registra esses eventos no histórico de eventos, mas um registro completo de 90 dias da atividade que inclui eventos adicionados não estará disponível até 90 dias após a adição dos eventos.
> O Histórico de eventos é separado de todas as trilhas ou armazenamentos de dados de eventos que você cria para sua conta. As alterações feitas nos armazenamentos de dados de eventos ou trilhas não afetam o Histórico de eventos.

As seções a seguir descrevem como pesquisar eventos de gerenciamento recentes usando o CloudTrail console e o AWS CLI, e descrevem como baixar um arquivo de eventos. Para obter informações sobre como usar a `LookupEvents` API para recuperar informações de CloudTrail eventos, consulte LookupEventsa Referência da AWS CloudTrail API.

Tópicos

Limitações do histórico de eventos

As limitações a seguir se aplicam ao Histórico de eventos.

- A página Histórico de eventos no CloudTrail console mostra apenas eventos de gerenciamento. Ele não mostra eventos de dados ou eventos do Insights.
- O Histórico de eventos é limitado aos últimos 90 dias de eventos. Para um registro contínuo dos eventos em seu Conta da AWS, crie um armazenamento de dados de eventos ou uma trilha.
- Ao baixar eventos da página Histórico de eventos no CloudTrail console, você pode baixar até 200.000 eventos em um único arquivo. Se você atingir o limite de 200.000 eventos, o CloudTrail console fornecerá a opção de baixar arquivos adicionais.
- O Histórico de eventos não fornece agregação de eventos em nível organizacional. Para registrar eventos em toda a sua organização, crie um armazenamento de dados de eventos ou uma trilha da organização.
- Uma pesquisa no histórico de eventos é limitada a uma única Conta da AWS, retorna somente eventos de uma única Região da AWS e não pode consultar vários atributos. É possível aplicar somente um filtro de atributo e um filtro de intervalo de tempo.

  Você pode criar um armazenamento de dados de eventos do CloudTrail Lake para consultar vários atributos Regiões da AWS e. Você também pode consultar vários Contas da AWS em uma AWS Organizations organização. No CloudTrail Lake, você pode consultar vários tipos de eventos, incluindo eventos de gerenciamento, eventos de dados, eventos do Insights, itens de AWS Config configuração, evidências do Audit Manager e não AWS eventos. CloudTrail As consultas do Lake oferecem uma visão mais profunda e personalizável dos eventos do que pesquisas simples de chaves e valores no histórico de eventos ou em execução. `LookupEvents` Para obter mais informações, consulte Trabalhando com AWS CloudTrail Lake e Crie um armazenamento de dados de CloudTrail eventos para eventos com o console.
- Você não pode excluir AWS KMS nem os eventos da Amazon RDS Data API do histórico de eventos; as configurações que você aplica a um armazenamento de dados de trilhas ou eventos não se aplicam ao histórico de eventos.

Visualizando eventos de gerenciamento recentes com o console

Você pode usar a página Histórico de eventos no CloudTrail console para visualizar os últimos 90 dias de eventos de gerenciamento em um Região da AWS. Você também pode fazer download de um arquivo com essas informações, ou um subconjunto de informações com base no filtro e intervalo de tempo que escolher. É possível personalizar a visualização do Histórico de eventos selecionando quantos eventos devem ser exibidos em cada página e escolhendo quais colunas serão exibidas no console. Você também pode pesquisar e filtrar eventos pelos tipos de recursos disponíveis para um determinado serviço. Você pode selecionar até cinco eventos no histórico de eventos e comparar seus detalhes side-by-side.

Event history (Histórico de eventos) não exibe eventos de dados. Para visualizar eventos de dados, crie um armazenamento de dados de eventos ou uma trilha.

Após 90 dias, os eventos não são mais exibidos em Event history (Histórico de eventos). Você não pode excluir manualmente eventos do Event history (Histórico de eventos).

Você pode saber mais sobre as especificidades de como CloudTrail registrar eventos para um serviço específico consultando a documentação desse serviço. Para ter mais informações, consulte AWS tópicos de serviço para CloudTrail.

> **Note**
>
> Para um registro contínuo de atividades e eventos nos últimos 90 dias, crie um armazenamento de dados de eventos ou uma trilha.

Para visualizar Histórico de eventos

1. Faça login no AWS Management Console e abra o CloudTrail console em https://console.aws.amazon.com/cloudtrail/.
2. No painel de navegação, escolha Event history (Histórico de eventos). Você verá uma lista filtrada de eventos, com os eventos mais recentes exibidos primeiro. O filtro padrão para eventos é somente Read only (Somente leitura), definido como false (falso). Você pode limpar esse filtro escolhendo X à direita do filtro.
3. Você pode filtrar eventos em um único atributo, que pode ser escolhido na lista suspensa. Para filtrar um atributo, escolha o atributo na lista suspensa e insira o valor total do atributo. Por exemplo, para visualizar todos os eventos de login do console, escolha o filtro Nome do evento

e especifique ConsoleLogin. Ou, para visualizar eventos recentes de gerenciamento do S3, escolha o filtro de origem do evento e especifique`s3.amazonaws.com`.

4. Para visualizar um evento de gerenciamento específico, escolha o nome do evento. Na página de detalhes do evento, é possível visualizar detalhes sobre o evento, ver quaisquer recursos referenciados e visualizar o registro do evento.
5. Para comparar eventos, selecione até cinco eventos preenchendo as caixas de seleção na margem esquerda da tabela Event history (Histórico de eventos). Você pode ver os detalhes dos eventos selecionados side-by-side na tabela Comparar detalhes do evento.
6. Você pode salvar o histórico de eventos baixando-o como um arquivo no formato JSON ou CSV. O download do histórico de eventos pode levar alguns minutos.

Sumário

Navegar entre páginas

Você pode navegar entre as páginas no Histórico de eventos escolhendo a página que deseja visualizar. Também é possível a próxima página e a página anterior no Histórico de eventos.

Escolha **<** para ver a página anterior do Histórico de eventos.

Escolha **>** para ver a próxima página do Histórico de eventos.

Personalizar a exibição

Você pode personalizar a exibição do histórico de eventos no CloudTrail console selecionando uma das seguintes preferências.

- Tamanho da página: escolha se deseja exibir 10, 25 ou 50 eventos em cada página.

- Quebrar linhas: quebre o texto para poder ver todo o texto de cada evento.
- Linhas listradas: sombreie linhas alternadas na tabela.
- Exibição da hora do evento: escolha se deseja exibir a hora do evento em UTC ou no fuso horário local.
- Selecionar colunas visíveis: selecione as colunas que serão exibidas. Por padrão, as colunas a seguir são exibidas:
  - Nome do evento
  - Hora do evento
  - Nome do usuário
  - Origem do evento.
  - Tipo de atributo
  - Nome do recurso

> **Note**
>
> Você não pode alterar a ordem das colunas ou excluir manualmente eventos do Event history (Histórico de eventos).

Para personalizar a exibição

1. Faça login no AWS Management Console e abra o CloudTrail console em https://console.aws.amazon.com/cloudtrail/.
2. No painel de navegação, escolha Event history (Histórico de eventos).
3. Escolha o ícone de engrenagem.
4. Em Tamanho da página, escolha o número de eventos a serem exibidos em uma página.
5. Escolha Quebrar linhas para ver todo o texto de cada evento.
6. Escolha Linhas listradas para sombrear linhas alternadas na tabela.
7. Em Exibição da hora do evento, escolha se deseja exibir a hora do evento em UTC ou no fuso horário local. Por padrão, UTC é selecionado.
8. Em Select visible columns (Selecionar colunas visíveis), selecione as colunas que você deseja exibir. Desabilite as colunas que você não deseja exibir.
9. Após terminar de fazer as alterações, escolha Confirmar.

Filtrando eventos CloudTrail

A exibição padrão de eventos em Event history (Histórico de eventos) usa um filtro de atributo para excluir eventos somente leitura da lista de eventos exibidos. Esse filtro de atributo é chamado de Read only (Somente leitura) e está definido como false (falso). É possível remover esse filtro para exibir tanto eventos de leitura, como de gravação. Para visualizar somente os eventos Read (Leitura), você pode alterar o valor do filtro para true (verdadeiro). Também é possível filtrar eventos por outros atributos. Além disso, é possível filtrar por intervalo de tempo.

> **Note**
>
> É possível aplicar somente um filtro de atributo e um filtro de intervalo de tempo. Não é possível aplicar vários filtros de atributo.

AWS chave de acesso

O ID da chave de AWS acesso que foi usado para assinar a solicitação. Se a solicitação foi feita com credenciais de segurança temporárias, esse é o ID da chave de acesso delas.

ID do evento

O CloudTrail ID do evento. Cada evento tem um ID exclusivo.

Nome do evento

O nome do evento. Por exemplo, você pode filtrar eventos do IAM como `CreatePolicy`, ou eventos do Amazon EC2, como `RunInstances`.

Origem do evento.

O AWS serviço para o qual a solicitação foi feita, como `iam.amazonaws.com` ou `us3.amazonaws.com`. Você pode percorrer uma lista de fontes de eventos depois que selecionar o filtro Origem do evento.

Somente leitura

O tipo de leitura do evento. Os eventos são categorizados como eventos de leitura ou eventos de gravação. Se estiverem definidos como false (falso), eventos de leitura não serão incluídos na lista de eventos exibidos. Por padrão, esse filtro de atributo é aplicado e o valor é definido como false (falso).

Nome do recurso

O nome ou o ID do recurso ao qual o evento faz referência. Por exemplo, o nome do recurso pode ser "auto-scaling-test-group" para um grupo de Auto Scaling ou “i-12345678910" para uma instância do EC2.

Tipo de recurso

O tipo de recurso ao qual o evento faz referência. Por exemplo, um tipo de recurso pode ser `Instance` para EC2 ou `DBInstance` para RDS. Os tipos de recursos variam para cada AWS serviço.

Intervalo de tempo

O período no qual você deseja filtrar eventos. É possível escolher entre Intervalo relativo e Intervalo absoluto. Você pode filtrar os eventos dos últimos 90 dias.

Nome do usuário

A identidade ao qual o evento faz referência. Ela pode ser um usuário, um nome de perfil ou um perfil de serviço.

Se não houver eventos registrados para o atributo ou o tempo que você escolher, a lista de resultados estará vazia. Você pode aplicar apenas um filtro de atributo, além do período. Se você escolher um filtro de atributo diferente, o intervalo de tempo especificado será preservado.

As etapas a seguir descrevem como filtrar por atributo.

Para filtrar por atributo

1. Para filtrar os resultados por um atributo, escolha um atributo na lista suspensa Lookup attributes (Atributos de pesquisa) e, em seguida, digite ou escolha um valor para o atributo na caixa de texto.
2. Para remover um filtro de atributo, selecione o X à direita da caixa de filtros de atributos.

As etapas a seguir descrevem como filtrar por data e hora de início e de término.

Para filtrar por data e hora de início e de término

1. Para limitar o período dos eventos que você deseja ver, escolha um período na barra de períodos. É possível escolher entre Intervalo relativo e Intervalo absoluto.

Escolha Intervalo relativo para selecionar um valor predefinido ou escolher um intervalo personalizado. Os valores predefinidos são 30 minutos, 1 hora, 12 horas ou 1 dia. Para especificar um período personalizado, escolha Custom (Personalizado).

Escolha Intervalo absoluto para especificar horas de início e término específicas. Também é possível escolher entre o fuso horário local e UTC.

2. Para remover um filtro de intervalo de tempo, escolha Limpar e dispensar na barra de intervalos de tempo.

Visualizar detalhes de um evento

1. Escolha um evento na lista de resultados para mostrar os detalhes dele.
2. Os recursos referenciados no evento são mostrados na seção Resources referenced (Recursos de referência) na página de detalhes do evento.
3. Alguns recursos referenciados têm links. Selecione o link para abrir o console para esse recurso.
4. Role até Event record (Registro de eventos) na página de detalhes para ver o registro de evento JSON, também chamado de evento payload.
5. Selecione Event history (Histórico de eventos) na página de rastro para fechar a página de detalhes do evento e retornar ao Event history (Histórico de eventos).

Baixar eventos

Você pode fazer download do histórico de eventos registrados como um arquivo no formato JSON ou CSV. Você pode baixar até 200.000 eventos em um único arquivo. Se você atingir o limite de 200.000 eventos, o CloudTrail console fornecerá a opção de baixar arquivos adicionais. Use filtros e intervalos de tempo para reduzir o tamanho do arquivo que você fizer download.

> **Note**
>
> CloudTrail arquivos de histórico de eventos são arquivos de dados que contêm informações (como nomes de recursos) que podem ser configuradas por usuários individuais. Alguns dados podem ser interpretados como comandos em programas usados para ler e analisar esses dados (injeção de CSV). Por exemplo, quando CloudTrail os eventos são exportados para CSV e importados para um programa de planilhas, esse programa pode alertá-lo sobre questões de segurança. Você deve optar por desabilitar esse conteúdo para manter

o sistema seguro. Sempre desabilite links ou macros de arquivos do histórico de eventos obtidos por download.

1. Adicione um filtro e um período para eventos no Event history (Histórico de eventos) que você deseja baixar. Por exemplo, você pode especificar o nome do evento, `StartInstances`, e um período relativo aos últimos três dias de atividade.
2. Escolha Download events (Baixar eventos) e, em seguida, Download as CSV (Baixar como CSV) ou Download as JSON (Baixar como JSON). O download inicia imediatamente.

   > **Note**
   >
   > O download pode levar algum tempo para ser concluído. Para obter resultados mais rápidos, antes de iniciar o processo de download, use um filtro específico ou um período mais curto para restringir os resultados. É possível cancelar um download. Se você cancelar um download, um download parcial incluindo apenas alguns dados de eventos poderá ficar no computador local. Para baixar o histórico de eventos completo, reinicie o download.

3. Quando o download for concluído, abra o arquivo para visualizar os eventos que você especificou.
4. Para cancelar o download, escolha Cancel (Cancelar) e confirme selecionando Cancel download (Cancelar download). Se você precisar reiniciar um download, aguarde até que termine o cancelamento do download anterior.

Visualizar recursos referenciados com AWS Config

AWS Config registra detalhes de configuração, relacionamentos e alterações em seus AWS recursos.

No painel Recursos referenciados, escolha a coluna

na linha do tempo do AWS Config recurso para visualizar o recurso no console. AWS Config

Se o

ícone estiver cinza, AWS Config não estiver ligado ou não estiver registrando o tipo de recurso.

Escolha o ícone para acessar o AWS Config console para ativar o serviço ou começar a gravar esse tipo de recurso. Para obter mais informações, consulte Configurar o AWS Config uso do console no Guia do AWS Config desenvolvedor.

Se Link not available (Link não disponível) for exibido na coluna, o recurso não poderá ser visualizado por um dos seguintes motivos:

- AWS Config não suporta o tipo de recurso. Para obter mais informações, consulte Recursos com suporte, itens de configuração e relacionamentos no Manual do desenvolvedor do AWS Config .
- AWS Config recentemente adicionou suporte para o tipo de recurso, mas ele ainda não está disponível no CloudTrail console. Você pode pesquisar o recurso no AWS Config console para ver o cronograma do recurso.
- O recurso é de propriedade de outro Conta da AWS.
- O recurso pertence a outro AWS service (Serviço da AWS), como uma política gerenciada do IAM.
- O recurso foi criado e excluído imediatamente.
- O recurso foi criado ou atualizado recentemente.

Para conceder aos usuários permissão somente de leitura para visualizar recursos no AWS Config console, consulte. Concedendo permissão para visualizar AWS Config informações no console CloudTrail

Para obter mais informações sobre AWS Config, consulte o Guia do AWS Config desenvolvedor.

Visualizando eventos de gerenciamento recentes com o AWS CLI

Você pode pesquisar eventos CloudTrail de gerenciamento dos últimos 90 dias para os atuais Região da AWS usando o aws cloudtrail lookup-events comando. O aws cloudtrail lookup-events comando mostra os eventos no Região da AWS local em que eles ocorreram.

A pesquisa aceita os seguintes atributos para eventos de gerenciamento:

- AWS chave de acesso
- ID do evento
- Nome do evento
- Origem do evento.
- Somente leitura

- Nome do recurso
- Tipo de recurso
- Nome do usuário

Todos os outros atributos são opcionais.

O comando `lookup-events` inclui as seguintes opções:

- `--max-items <integer>`: o número total de itens para retornar na saída do comando. Se o número total de itens disponíveis for maior que o valor especificado, um `NextToken` será fornecido na saída do comando. Para retomar a paginação, forneça o valor do `NextToken` no argumento starting-token de um comando subsequente. Não use o elemento de resposta `NextToken` diretamente fora da AWS CLI.
- `--start-time <timestamp>`: especifica que apenas os eventos ocorridos no horário especificado ou depois dele são retornados. Se o horário de início especificado for posterior ao de término, um erro será retornado.
- `--lookup-attributes <integer>`: contém uma lista de atributos de pesquisa. No momento, a lista pode conter apenas um item.
- `--generate-cli-skeleton <string>`: imprime um esqueleto JSON na saída padrão sem enviar uma solicitação de API. Se fornecido sem valor ou com a entrada de valor, imprime um exemplo de entrada JSON que pode ser usado como argumento para `--cli-input-json`. Da mesma forma, se fornecido com yaml-input, imprime um exemplo de entrada YAML que pode ser usado com `--cli-input-yaml`. Se fornecido com a saída do valor, valida as entradas do comando e retorna um exemplo de saída JSON para esse comando. O esqueleto JSON gerado não é estável entre as versões do AWS CLI e não há garantias de compatibilidade com versões anteriores no esqueleto JSON gerado.
- `--cli-input-json <string>`: lê argumentos da string JSON fornecida. A string JSON segue o formato fornecido pelo parâmetro `--generate-cli-skeleton`. Se outros argumentos forem fornecidos na linha de comando, esses valores substituirão os valores fornecidos pelo JSON. Não é possível passar valores binários arbitrários usando um valor fornecido pelo JSON, pois a string será interpretada literalmente. Isso não pode ser especificado junto com o parâmetro `--cli-input-yaml`.

Para obter informações gerais sobre o uso da interface de linha de AWS comando, consulte o Guia AWS Command Line Interface do usuário.

Sumário

Pré-requisitos

- Para executar AWS CLI comandos, você deve instalar AWS CLI o. Para obter informações, consulte Começar com AWS CLI o.
- Certifique-se de que sua AWS CLI versão seja maior que 1.6.6. Para verificar a versão da CLI, execute aws --version na linha de comando.
- Para definir a conta e Região da AWS o formato de saída padrão para uma AWS CLI sessão, use o aws configure comando. Para obter mais informações, consulte Configurando a interface de linha de AWS comando.

> **Note**
>
> Os CloudTrail AWS CLI comandos diferenciam maiúsculas de minúsculas.

Receber ajuda da linha de comando

Para ver a ajuda da linha de comando para `lookup-events`, digite o seguinte comando:

```
aws cloudtrail lookup-events help
```

Procurar eventos

> **Important**
>
> A taxa de solicitações de pesquisa é limitada a duas por segundo, por conta, por região. Se esse limite for excedido, ocorrerá um erro de controle de utilização.

Para ver os 10 eventos mais recentes, digite o seguinte comando:

```
aws cloudtrail lookup-events --max-items 10
```

Um evento retornado tem aparência semelhante ao seguinte exemplo fictício, que foi formatado para melhorar a fluência:

```
{
    "NextToken": "kbOt5LlZe+
+mErCebpy2TgaMgmDvF1kYGFcH64JSjIbZFjsuvrSqg66b5YGssKutDYIyII4lrP4IDbeQdiObkp9YAlju3oXd12juy3CIZ
    "Events": [
        {
            "EventId": "0ebbaee4-6e67-431d-8225-ba0d81df5972",
            "Username": "root",
            "EventTime": 1424476529.0,
            "CloudTrailEvent": "{
                  \"eventVersion\":\"1.02\",
                  \"userIdentity\":{
                        \"type\":\"Root\",
                        \"principalId\":\"111122223333\",
                        \"arn\":\"arn:aws:iam::111122223333:root\",
                        \"accountId\":\"111122223333\"},
                  \"eventTime\":\"2015-02-20T23:55:29Z\",
                  \"eventSource\":\"signin.amazonaws.com\",
                  \"eventName\":\"ConsoleLogin\",
                  \"awsRegion\":\"us-east-2\",
                  \"sourceIPAddress\":\"203.0.113.4\",
                  \"userAgent\":\"Mozilla/5.0\",
                  \"requestParameters\":null,
                  \"responseElements\":{\"ConsoleLogin\":\"Success\"},
                  \"additionalEventData\":{
                         \"MobileVersion\":\"No\",
                         \"LoginTo\":\"https://console.aws.amazon.com/console/home",
                         \"MFAUsed\":\"No\"},
```

```
                \"eventID\":\"0ebbaee4-6e67-431d-8225-ba0d81df5972\",
                \"eventType\":\"AwsApiCall\",
                \"recipientAccountId\":\"111122223333\"}",
            "EventName": "ConsoleLogin",
            "Resources": []
        }
    ]
}
```

Para ver uma explicação dos campos relacionados à pesquisa nos resultados, consulte a seção Pesquisar campos de resultados mais adiante neste documento. Para obter uma explicação dos campos no CloudTrail evento, consulteCloudTrail conteúdo do registro.

Especificar o número de eventos a serem retornados

Para especificar o número de eventos a serem retornados, digite o seguinte comando:

```
aws cloudtrail lookup-events --max-items <integer>
```

Os valores possíveis são de 1 a 50. O exemplo a seguir retorna um evento.

```
aws cloudtrail lookup-events --max-items 1
```

Procurar eventos por período

Os eventos dos últimos 90 dias estão disponíveis para pesquisa. Para especificar um período, digite o seguinte comando:

```
aws cloudtrail lookup-events --start-time <timestamp> --end-time <timestamp>
```

`--start-time` *`<timestamp>`* especifica, em UTC, que apenas os eventos ocorridos no horário especificado ou depois dele são retornados. Se o horário de início especificado for posterior ao de término, um erro será retornado.

`--end-time` *`<timestamp>`* especifica, em UTC, que apenas os eventos ocorridos no horário especificado ou antes dele são retornados. Se o horário de término especificado for anterior ao de início, um erro será retornado.

O horário de início padrão é a primeira data em que os dados foram disponibilizados nos últimos 90 dias. O horário de término padrão é o horário de ocorrência de evento mais próximo do momento.

Todos os carimbos de data/hora são exibidos em UTC.

Procurar eventos por atributo

Para filtrar por um atributo, digite o seguinte comando:

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=<attribute>,AttributeValue=<string>
```

Você pode especificar apenas um par de chave/valor de atributo para cada comando lookup-events. Estes são valores válidos para `AttributeKey`. Os nomes dos valores diferenciam maiúsculas de minúsculas.

- `AccessKeyId`
- `EventId`
- `EventName`
- `EventSource`
- `ReadOnly`
- `ResourceName`
- `ResourceType`
- `Username`

O tamanho máximo para o `AttributeValue` é de 2.000 caracteres. Os seguintes caracteres ('_', ' ', ',', '\\n') contam como dois caracteres até o limite de 2.000 caracteres.

Exemplos de consulta de atributo

O exemplo de comando a seguir retorna os eventos nos quais o valor de `AccessKeyId` é `AKIAIOSFODNN7EXAMPLE`.

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=AccessKeyId,AttributeValue=AKIAIOSFODNN7EXAMPLE
```

O comando de exemplo a seguir retorna o evento para o especificado CloudTrail`EventId`.

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=EventId,AttributeValue=b5cc8c40-12ba-4d08-a8d9-2bceb9a3e002
```

O exemplo de comando a seguir retorna os eventos nos quais o valor de `EventName` é `RunInstances`.

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=EventName,AttributeValue=RunInstances
```

O exemplo de comando a seguir retorna os eventos nos quais o valor de `EventSource` é `iam.amazonaws.com`.

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=EventSource,AttributeValue=iam.amazonaws.com
```

O comando de exemplo a seguir retorna eventos de gravação. Ele exclui eventos de leitura, como `GetBucketLocation` e `DescribeStream`.

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=ReadOnly,AttributeValue=false
```

O exemplo de comando a seguir retorna os eventos nos quais o valor de `ResourceName` é `CloudTrail_CloudWatchLogs_Role`.

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=ResourceName,AttributeValue=CloudTrail_CloudWatchLogs_Role
```

O exemplo de comando a seguir retorna os eventos nos quais o valor de `ResourceType` é `AWS::S3::Bucket`.

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=ResourceType,AttributeValue=AWS::S3::Bucket
```

O exemplo de comando a seguir retorna os eventos nos quais o valor de `Username` é `root`.

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=Username,AttributeValue=root
```

Especificar a próxima página de resultados

Para obter a próxima página de resultados de um comando `lookup-events`, digite o seguinte comando:

```
aws cloudtrail lookup-events <same parameters as previous command> --next-token=<token>
```

em que o valor do *<token>* é obtido a partir do primeiro campo de resultados do comando anterior.

Quando você usa `--next-token` em um comando, precisa usar os mesmos parâmetros do comando anterior. Por exemplo, imagine que você executou o seguinte comando:

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=Username,AttributeValue=root
```

Para obter a próxima página de resultados, seu próximo comando teria esta aparência:

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=Username,AttributeValue=root --next-token=kbOt5LlZe+
+mErCebpy2TgaMgmDvF1kYGFcH64JSjIbZFjsuvrSqg66b5YGssKutDYIyII4lrP4IDbeQdiObkp9YAlju3oXd12juy3CIZ
```

Obter entrada JSON de um arquivo

AWS CLI Para alguns AWS serviços, há dois parâmetros`--cli-input-json`, `--generate-cli-skeleton` que você pode usar para gerar um modelo JSON que pode ser modificado e usado como entrada para o `--cli-input-json` parâmetro. Esta seção descreve como usar esses parâmetros com `aws cloudtrail lookup-events`. Para obter mais informações gerais, consulte AWS CLI esqueletos e arquivos de entrada.

Para pesquisar CloudTrail eventos obtendo a entrada JSON de um arquivo

1. Crie um modelo de entrada para uso com `lookup-events` redirecionando os resultados `--generate-cli-skeleton` para um arquivo, como no exemplo a seguir.

   ```
   aws cloudtrail lookup-events --generate-cli-skeleton > LookupEvents.txt
   ```

   O arquivo de modelo gerado (nesse caso, LookupEvents .txt) tem a seguinte aparência:

   ```
   {
       "LookupAttributes": [
           {
               "AttributeKey": "",
   ```

```
            "AttributeValue": ""
        }
    ],
    "StartTime": null,
    "EndTime": null,
    "MaxResults": 0,
    "NextToken": ""
}
```

2. Use um editor de texto para modificar o JSON conforme necessário. A entrada do JSON precisa conter apenas os valores especificados.

> **Important**
>
> Todos os valores nulos ou vazios precisam ser removidos do modelo antes que ele seja usado.

O exemplo a seguir especifica um período e o número máximo de resultados a serem retornados.

```
{
    "StartTime": "2023-11-01",
    "EndTime": "2023-12-12",
    "MaxResults": 10
}
```

3. Para usar o arquivo editado como entrada, use a sintaxe `--cli-input-json file://<filename>`, como no exemplo a seguir:

```
aws cloudtrail lookup-events --cli-input-json file://LookupEvents.txt
```

> **Note**
>
> Você pode usar outros argumentos na mesma linha de comando como `--cli-input-json`.

Pesquisar campos de resultados

Eventos

Uma lista de eventos de pesquisa com base no atributo de pesquisa e no período que foram especificados. A lista de eventos é classificada por tempo, com o último evento listado primeiro. Cada entrada contém informações sobre a solicitação de pesquisa e inclui uma representação em cadeia de caracteres do CloudTrail evento que foi recuperado.

As seguintes entradas descrevem os campos de cada evento de pesquisa.

CloudTrailEvent

Uma string JSON que contém uma representação do objeto do evento retornado. Para obter informações sobre cada um dos elementos retornados, consulte Conteúdo do corpo do registro.

EventId

Uma string que contém a GUID do evento retornado.

EventName

Uma string que contém o nome do evento retornado.

EventSource

O AWS serviço para o qual a solicitação foi feita.

EventTime

A data e a hora, em formato de horário do UNIX, do evento.

Recursos

Uma lista de recursos referenciados pelo evento que foi retornado. Cada entrada de recurso especifica um tipo e um nome do recurso.

ResourceName

Uma string que contém o nome do recurso referenciado pelo evento.

ResourceType

Uma string que contém o tipo de um recurso referenciado pelo evento. Quando o tipo de recurso não pode ser determinado, null é retornado.

Username

Uma string que contém o nome do usuário da conta do evento retornado.

NextToken

Uma string para obter a próxima página de resultados de um comando `lookup-events` anterior. Para usar o token, os parâmetros precisam ser os mesmos do comando original. Se nenhuma entrada `NextToken` aparecer nos resultados, significa que não há mais resultados a serem retornados.

Trabalhando com AWS CloudTrail Lake

AWS CloudTrail O Lake permite que você execute consultas baseadas em SQL em seus eventos. CloudTrail O Lake converte eventos existentes no formato JSON baseado em linhas para o formato Apache ORC. O ORC é um formato colunar de armazenamento otimizado para recuperação rápida de dados. Os eventos são agregados em armazenamentos de dados de eventos, que são coleções imutáveis de eventos com base nos critérios que você seleciona aplicando seletores de eventos avançados. Você pode manter os dados do evento em um armazenamento de dados de eventos por até 3.653 dias (cerca de 10 anos) se escolher a opção de preço de retenção extensível de um ano ou até 2.557 dias (cerca de 7 anos) se escolher a opção de preço de retenção por sete anos. Os seletores que você aplica a um armazenamento de dados de eventos controlam quais eventos persistem e estão disponíveis para você consultar. CloudTrail O Lake é uma solução de auditoria que pode complementar sua pilha de conformidade e ajudá-lo com a solução de problemas quase em tempo real.

CloudTrail Armazenamentos de dados de eventos em Lake

Ao criar um armazenamento de dados de eventos, você escolhe o tipo dos eventos a serem incluídos em seu armazenamento de dados de eventos. Você pode criar um armazenamento de dados de eventos para incluir CloudTrail eventos, eventos do CloudTrail Insights, itens de AWS Config configuração, AWS Audit Manager evidências ou eventos externos AWS. Cada armazenamento de dados de eventos só pode conter uma categoria de evento específica (por exemplo, itens de AWS Config configuração), porque o esquema do evento é exclusivo da categoria do evento. Você pode armazenar eventos de uma organização AWS Organizations em um armazenamento de dados de eventos da organização, incluindo eventos de várias regiões e contas. Você também pode executar consultas SQL em vários armazenamentos de dados de eventos usando as palavras-chave SQL JOIN compatíveis. Para obter informações sobre como executar consultas em vários armazenamentos de dados de eventos, consulte Compatibilidade avançada para consultas com várias tabelas.

Você pode copiar eventos da trilha para um armazenamento de dados de eventos novo ou existente para criar um point-in-time instantâneo dos eventos registrados na trilha. Para ter mais informações, consulte Copiar eventos de trilhas para um armazenamento de dados de eventos.

Você pode federar um armazenamento de dados de eventos para ver os metadados associados a ele no Catálogo de Dados do AWS Glue e executar consultas SQL nos dados do evento usando o

Amazon Athena. Os metadados da tabela armazenados no Catálogo de AWS Glue Dados permitem que o mecanismo de consulta do Athena saiba como encontrar, ler e processar os dados que você deseja consultar. Para ter mais informações, consulte Federar um armazenamento de dados de eventos.

Por padrão, todos os eventos em um armazenamento de dados de eventos são criptografados por CloudTrail. Ao configurar um armazenamento de dados de eventos, você pode optar por usar sua própria AWS Key Management Service chave. Usar sua própria chave KMS gera AWS KMS custos de criptografia e descriptografia. Após associar um armazenamento de dados de eventos a uma chave do KMS, não será possível remover ou alterar a chave do KMS.

Você pode controlar o acesso a ações em armazenamentos de dados de eventos usando a autorização com base em tags. Para obter mais informações e exemplos, consulte Exemplos: negação de acesso para criar ou excluir armazenamentos de dados de eventos com base em tags neste guia.

Você pode usar os painéis do CloudTrail Lake para visualizar os dados em seus armazenamentos de dados de eventos. Cada painel consiste em vários widgets e cada widget representa uma consulta SQL. Para obter mais informações sobre painéis do Lake, consulte Veja os painéis CloudTrail do Lake.

CloudTrail Os armazenamentos de dados de eventos em Lake incorrem em cobranças. Ao criar um armazenamento de dados de eventos, você escolhe a opção de preço que deseja usar para ele. A opção de preço determina o custo para a ingestão e para o armazenamento de eventos, e o período de retenção padrão e máximo para o armazenamento de dados de eventos. Para obter informações sobre CloudTrail preços e gerenciamento de custos do Lake, consulte AWS CloudTrail Preços Gerenciando os custos CloudTrail do Lake e.

CloudTrail O Lake oferece suporte às CloudWatch métricas da Amazon, que fornecem informações sobre dados ingeridos e bytes de armazenamento. Para obter mais informações sobre CloudWatch métricas compatíveis, consulte CloudWatch Métricas suportadas.

> **Note**
>
> CloudTrail normalmente entrega eventos em uma média de cerca de 5 minutos após uma chamada de API. Desta vez não há garantias.

CloudTrail Integrações com o Lake

Você pode usar as integrações do CloudTrail Lake para registrar e armazenar dados de atividades do usuário de fora de AWS; de qualquer fonte em seus ambientes híbridos, como aplicativos internos ou SaaS hospedados no local ou na nuvem, máquinas virtuais ou contêineres. Depois de criar armazenamentos de dados de eventos no CloudTrail Lake e criar um canal para registrar eventos de atividades, você chama a `PutAuditEvents` API para ingerir a atividade do seu aplicativo. CloudTrail Em seguida, você pode usar o CloudTrail Lake para pesquisar, consultar e analisar os dados que são registrados em seus aplicativos.

As integrações também podem registrar eventos em seus armazenamentos de dados de eventos de mais de uma dúzia de CloudTrail parceiros. Em uma integração com parceiros, você cria armazenamentos de dados de eventos de destino, um canal e uma política de recursos. Depois de criar a integração, você fornece o ARN do canal ao parceiro. Há dois tipos de integração: a direta e a de solução. Com integrações diretas, o parceiro chama a `PutAuditEvents` API para entregar eventos ao armazenamento de dados de eventos da sua AWS conta. Com as integrações de soluções, o aplicativo é executado em sua AWS conta e chama a `PutAuditEvents` API para entregar eventos ao armazenamento de dados de eventos de sua AWS conta.

Para obter mais informações sobre integrações, consulte Criar uma integração com uma fonte de eventos externa à AWS.

CloudTrail Consultas sobre o lago

CloudTrail As consultas do Lake oferecem uma visão mais profunda e personalizável dos eventos do que pesquisas simples de chaves e valores no histórico de eventos ou em execução. `LookupEvents` Uma pesquisa no histórico de eventos é limitada a uma única Conta da AWS, retorna somente eventos de uma única Região da AWS e não pode consultar vários atributos. Por outro lado, os usuários do CloudTrail Lake podem executar consultas SQL complexas em vários campos de eventos. CloudTrail O Lake suporta todas as `SELECT` instruções e funções válidas do Presto. Para obter mais informações sobre as funções e os operadores SQL compatíveis, consulte Funções e operadores no site de documentação do Presto.

Você pode salvar as consultas do CloudTrail Lake para uso futuro e visualizar os resultados das consultas por até sete dias. Ao executar consultas, você pode salvar os resultados de consulta em um bucket do Amazon S3.

O CloudTrail console fornece vários exemplos de consultas que podem ajudar você a começar a escrever suas próprias consultas. Para ter mais informações, consulte Veja exemplos de consultas no console CloudTrail .

CloudTrail As consultas sobre o lago incorrem em cobranças. Ao executar consultas no Lake, você paga de acordo com a quantidade de dados examinados. Para obter informações sobre CloudTrail preços e gerenciamento de custos do Lake, consulte AWS CloudTrail Preços Gerenciando os custos CloudTrail do Lake e.

Recursos adicionais do

Os recursos a seguir podem ajudá-lo a entender melhor o que é o CloudTrail Lake e como você pode usá-lo.

- Modernize seu gerenciamento de registros de auditoria usando o CloudTrail Lake (YouTube vídeo)
- Registre eventos de atividades de AWS fontes não pertencentes ao AWS CloudTrail Lake (YouTube vídeo)
- Analise registros de atividades com AWS CloudTrail Lake e Amazon Athena (vídeo) YouTube
- Obtenha visibilidade dos registros de atividades de sua força de trabalho e identidades de clientes (blog)AWS
- Usando o AWS CloudTrail Lake para identificar conexões TLS mais antigas com endpoints AWS de serviço (blog)AWS
- Como a Arctic Wolf usa o AWS CloudTrail Lake para simplificar a segurança e as operações (AWS blog)
- CloudTrail Perguntas frequentes sobre o lago
- AWS CloudTrail API Reference
- AWS CloudTrail Referência da API de dados
- AWS CloudTrail Guia de integração de parceiros

CloudTrail Regiões suportadas por lagos

Atualmente, o CloudTrail Lake é compatível com o seguinte Regiões da AWS:

Nome da região	Região
Leste dos EUA (Norte da Virgínia)	us-east-1
Leste dos EUA (Ohio)	us-east-2
Oeste dos EUA (Norte da Califórnia)	us-west-1
Oeste dos EUA (Oregon)	us-west-2
África (Cidade do Cabo)	af-south-1
Ásia-Pacífico (Hong Kong)	ap-east-1
Ásia-Pacífico (Hyderabad)	ap-south-2
Ásia-Pacífico (Jacarta)	ap-southeast-3
Ásia-Pacífico (Mumbai)	ap-south-1
Asia Pacific (Osaka)	ap-northeast-3
Ásia-Pacífico (Seul)	ap-northeast-2
Ásia-Pacífico (Singapura)	ap-southeast-1
Ásia-Pacífico (Sydney)	ap-southeast-2
Ásia-Pacífico (Tóquio)	ap-northeast-1
Canadá (Central)	ca-central-1
Europa (Frankfurt)	eu-central-1
Europa (Irlanda)	eu-west-1
Europa (Londres)	eu-west-2
Europa (Milão)	eu-south-1
Europa (Paris)	eu-west-3

Nome da região	Região
Europa (Espanha)	eu-south-2
Europa (Estocolmo)	eu-north-1
Europa (Zurique)	eu-central-2
Israel (Tel Aviv)	il-central-1
Oriente Médio (Barém)	me-south-1
Oriente Médio (Emirados Árabes Unidos)	me-central-1
América do Sul (São Paulo)	sa-east-1
AWS GovCloud (Leste dos EUA)	us-gov-east-1
AWS GovCloud (Oeste dos EUA)	us-gov-west-1

Para obter informações sobre endpoints CloudTrail de serviço, consulte AWS CloudTrail endpoints e cotas.

Para obter mais informações sobre o uso CloudTrail no AWS GovCloud (US) Regions, consulte Service Endpoints no Guia do AWS GovCloud (US) usuário.

CloudTrail Conceitos e terminologia do lago

Esta seção descreve os principais conceitos e termos para ajudá-lo a usar o AWS CloudTrail Lake.

Conceitos e termos

- Armazenamentos de dados de eventos
- Integrações
- Consultas
- Painel

Armazenamentos de dados de eventos

Os eventos são agregados em armazenamentos de dados de eventos, que são coleções imutáveis de eventos com base nos critérios que você seleciona aplicando seletores de eventos avançados.

Você pode criar um armazenamento de dados de eventos para registrar eventos CloudTrail de gerenciamento e eventos de dados, eventos do CloudTrail Insights, AWS Audit Manager evidências, itens de AWS Config configuração ou eventos externos AWS.

Seletores de eventos avançados

Seletores de eventos avançados determinam quais eventos incluir em um armazenamento de dados de eventos. Eles ajudam a controlar os custos registrando apenas os eventos que são importantes para você.

Para eventos de gerenciamento e eventos de dados, é possível usar seletores de eventos avançados para filtrar eventos. Por exemplo, se você estiver criando um armazenamento de dados de eventos para coletar eventos de gerenciamento, poderá filtrar AWS Key Management Service (AWS KMS) ou eventos da API de dados do Amazon Relational Database Service (Amazon RDS). Normalmente, AWS KMS ações como `EncryptDecrypt`, e `GenerateDataKey` geram mais de 99% dos eventos.

Para itens de AWS Config configuração, evidências do Audit Manager ou eventos externos AWS, os seletores de eventos avançados são usados somente para incluir eventos desse tipo no armazenamento de dados de eventos.

Federação

A federação permite ver os metadados associados a um armazenamento de dados de evento no Catálogo de Dados do AWS Glue e executar consultas SQL nos dados do evento usando o Amazon Athena. Os metadados da tabela armazenados no Catálogo de AWS Glue Dados permitem que o mecanismo de consulta do Athena saiba como encontrar, ler e processar os dados que você deseja consultar.

Quando você ativa a federação de consultas do Lake, CloudTrail cria os recursos federados em seu nome e registra esses recursos com. AWS Lake Formation Depois que a federação do Lake estiver habilitada, você poderá consultar diretamente os dados do evento no Athena sem precisar realizar nenhuma etapa adicional. Para ter mais informações, consulte Federar um armazenamento de dados de eventos.

Opções de preço

Ao criar um armazenamento de dados de eventos, você escolhe a opção de preço que deseja usar para ele. A opção de preço determina o custo para a ingestão e para o armazenamento de eventos, e os períodos de retenção padrão e máximo para o armazenamento de dados de eventos. Para obter mais informações sobre preços, consulte Definição de preço do AWS CloudTrail e Gerenciando os custos CloudTrail do Lake.

Período de retenção

O período de retenção de um armazenamento de dados de eventos determina por quanto tempo os dados de eventos são mantidos no armazenamento de dados de eventos. CloudTrail Lake determina se deve reter um evento verificando se o `eventTime` evento está dentro do período de retenção especificado. Por exemplo, se você especificar um período de retenção de 90 dias, CloudTrail removerá eventos quando forem mais antigos do que 90 dias. `eventTime`

Período de retenção padrão

O período de retenção padrão de um armazenamento de dados de eventos é o número padrão de dias em que os dados do evento são mantidos no armazenamento de dados de eventos. Durante o período de retenção padrão do armazenamento de dados de eventos, o armazenamento é incluído no preço de ingestão sem custo adicional. Após o período de retenção padrão, o preço do armazenamento é pay-as-you-go.

Período máximo de retenção

O período máximo de retenção de um armazenamento de dados de eventos representa o número máximo de dias em que você pode manter os dados em um armazenamento de dados de eventos.

Termination protection

Por padrão, os armazenamentos de dados de eventos habilitam a proteção contra encerramento, que evita que um armazenamento de dados de eventos seja excluído acidentalmente. Para excluir um armazenamento de dados de eventos com a proteção contra encerramento habilitada, escolha Alterar proteção contra encerramento no menu Ações na página de detalhes do armazenamento de dados de eventos. Em seguida, você pode continuar com a exclusão do armazenamento de dados de eventos. Para ter mais informações, consulte Altere a proteção de rescisão com o console.

Integrações

Você pode usar as integrações do CloudTrail Lake para registrar e armazenar dados de atividades do usuário das seguintes fontes:

- Fora de AWS
- Qualquer fonte em seus ambientes híbridos, como aplicações internas ou de software como serviço (SaaS) hospedados on-premises ou na nuvem, máquinas virtuais ou contêineres

Uma integração requer um canal para entregar os eventos e um armazenamento de dados de eventos para receber os eventos. Depois de configurar sua integração, chame a operação da PutAuditEventsAPI para ingerir a atividade do seu aplicativo. CloudTrail Em seguida, você pode usar o CloudTrail Lake para pesquisar, consultar e analisar os dados que são registrados em seus aplicativos. Para ter mais informações, consulte Crie uma integração com uma fonte de eventos fora do AWS.

Tipo de integração

Há dois tipos de integração: a direta e a de solução. Com as integrações diretas, o parceiro chama a operação da API `PutAuditEvents` para entregar eventos ao armazenamento de dados de eventos da sua Conta da AWS. Com as integrações de soluções, o aplicativo é executado em você Conta da AWS e chama a operação da `PutAuditEvents` API para entregar eventos ao armazenamento de dados de eventos para você Conta da AWS.

Canais

Realize eventos de fontes externas ao AWS trabalho usando canais para trazer eventos para o CloudTrail Lake de parceiros externos que trabalham com CloudTrail ou de suas próprias fontes. Ao criar um canal, você escolhe um ou mais armazenamentos de dados de eventos para armazenar eventos que cheguem da fonte do canal. É possível alterar os armazenamentos de dados de eventos de destino de um canal conforme necessário, desde que os armazenamentos de dados de eventos de destino estejam configurados para registrar em log eventos do `eventCategory="ActivityAuditLog"`. Ao criar um canal para eventos de um parceiro externo, você fornece um nome do recurso da Amazon (ARN) de canal para o parceiro ou aplicação da fonte.

Políticas baseadas em atributos

Políticas baseadas em atributos são documentos de políticas JSON que você anexa a um atributo. A política baseada em atributos anexada ao canal permite que a fonte transmita eventos pelo canal. Se um canal não tiver uma política de recursos para o canal, somente o proprietário do canal poderá chamar a operação da API `PutAuditEvents` no canal. Para ter mais informações, consulte AWS CloudTrail exemplos de políticas baseadas em recursos.

Consultas

As consultas no CloudTrail Lake são criadas em SQL. Você pode criar uma consulta na guia CloudTrail Lake Editor escrevendo a consulta em SQL do zero ou abrindo uma consulta salva ou de amostra e editando-a. Você não pode sobrescrever uma consulta de exemplo incluída por suas alterações, mas você pode salvá-la como uma nova consulta. Para ter mais informações, consulte Criar ou editar uma consulta.

CloudTrail O Lake suporta todas as Presto `SELECT` instruções e funções válidas. Para obter mais informações sobre as funções e os operadores SQL compatíveis, consulte Funções e operadores no site de documentação do Presto.

Painel

Ao usar o painel do CloudTrail Lake, você pode visualizar os eventos em um armazenamento de dados de eventos e ver as tendências dos eventos, como principais Serviços da AWS, usuários e erros. Para ter mais informações, consulte Veja os painéis CloudTrail do Lake.

Tipo de painel

Os tipos de painéis disponíveis para um armazenamento de dados de eventos dependem da configuração dos seletores de eventos avançados do armazenamento de dados de eventos. Por exemplo, se um tipo de painel exibir informações sobre eventos CloudTrail de gerenciamento, você só poderá selecionar o painel se o armazenamento de dados de eventos atualmente selecionado coletar eventos CloudTrail de gerenciamento.

Os tipos de painel disponíveis são apresentados a seguir:

- Painel de visão geral — Mostra os usuários mais ativos e Serviços da AWS por contagem de eventos. Regiões da AWS Também é possível visualizar informações sobre atividades de eventos de gerenciamento de `read` e `write`, eventos com mais controle de utilização e os

principais erros. Esse painel está disponível para armazenamentos de dados de eventos que coletam eventos de gerenciamento.

- Painel Gerenciamento de eventos: mostra eventos de login do console, eventos de acesso negado, ações destrutivas e principais erros por usuário. Você também pode visualizar informações sobre versões do TLS e chamadas de TLS desatualizadas por usuário. Esse painel está disponível para armazenamentos de dados de eventos que coletam eventos de gerenciamento.
- Painel Eventos de dados do S3: mostra a atividade da conta do Amazon S3, os objetos mais acessados do S3, os principais usuários do S3 e as principais ações do S3. Esse painel está disponível para armazenamentos de dados de eventos que coletam eventos de dados do Amazon S3.
- Painel Eventos do Insights: mostra a proporção geral de eventos do Insights por tipo de Insights, a proporção de eventos do Insights por tipo de Insights para os principais usuários e serviços e o número de eventos do Insights por dia. O painel também inclui um widget que lista até 30 dias de eventos do Insights. Esse painel está disponível somente para armazenamentos de dados de eventos que coletam eventos do Insights.

> **Note**
>
> - Depois de ativar o CloudTrail Insights pela primeira vez no armazenamento de dados do evento de origem, pode levar até 7 dias CloudTrail para entregar o primeiro evento do Insights, se uma atividade incomum for detectada. Para ter mais informações, consulte Entender a entrega de eventos do Insights.
> - O painel Eventos do Insights exibe apenas informações sobre os eventos do Insights coletados pelo armazenamento de dados de eventos selecionado, o qual é determinado pela configuração do armazenamento de dados do evento de origem. Por exemplo, se você configurar o armazenamento de dados de eventos de origem para ativar eventos do Insights em `ApiCallRateInsight` mas não `ApiErrorRateInsight`, você não verá informações sobre os eventos do Insights em `ApiErrorRateInsight`.

Widgets

Os widgets são os componentes que compõem um painel e fornecem uma visualização, como um gráfico de linhas ou gráfico de barras. Cada widget representa uma consulta subjacente. Quando você escolhe Executar consultas, CloudTrail executa uma consulta gerada pelo sistema para preencher os dados de cada widget.

CloudTrail Armazenamentos de dados de eventos em Lake

Os eventos são agregados em armazenamentos de dados de eventos, que são coleções imutáveis de eventos baseados nos critérios selecionados com a aplicação de seletores de eventos avançados.

Ao criar um armazenamento de dados de eventos no CloudTrail Lake, você escolhe o tipo de eventos a serem incluídos em seu armazenamento de dados de eventos. Você pode criar um armazenamento de dados de eventos para incluir CloudTrail dados ou eventos de gerenciamento, eventos do CloudTrail Insights, itens de AWS Config configuração ou eventos externos AWS. Cada tipo de armazenamento de dados de eventos só pode conter categorias de eventos específicas (por exemplo, itens de AWS Config configuração), porque o esquema do evento é exclusivo da categoria do evento. Você pode executar consultas SQL em vários armazenamentos de dados de eventos usando as palavras-chave SQL JOIN compatíveis. Para obter informações sobre como executar consultas em vários armazenamentos de dados de eventos, consulte Compatibilidade avançada para consultas com várias tabelas.

A tabela a seguir mostra as categorias de eventos compatível com cada tipo de armazenamento de dados de eventos. A coluna eventCategory mostra o valor que você especificaria nos seletores de eventos avançados para coletar eventos desse tipo.

Tipo de evento (console)	eventCategory (API)	Descrição

CloudTrail eventos	`Management`
	
	`Data`
		Esse tipo de armazenamento de dados de eventos pode coletar eventos CloudTrail de gerenciamento e dados. Para obter mais informações, consulte Criar um armazenamento de dados de CloudTrail eventos para eventos.

CloudTrail Eventos do Insights	`Insight`	Esse tipo de armazenamento de dados de eventos pode coletar eventos do CloudTrail Insights. Para receber eventos do Insights, você precisa de um armazenamento de dados de eventos de origem que registre os eventos CloudTrail de gerenciamento e habilite o Insights. Para obter informações sobre

Tipo de evento (console)	eventCategory (API)	Descrição
		como criar os armazenamentos de dados de eventos de origem e destino, consulte Criar um armazenamento de dados de eventos para eventos do CloudTrail Insights.
Itens de configuração	`ConfigurationItem`	Esse tipo de armazenamento de dados de eventos pode coletar itens AWS Config de configuração. Para obter mais informações, consulte Criar um armazenamento de dados de eventos para itens AWS Config de configuração.
Eventos da integração	`ActivityAuditLog`	Esse tipo de armazenamento de dados de eventos pode coletar AWS não-eventos de integrações. Para obter mais informações, consulte Criar um armazenamento de dados de eventos para eventos fora do AWS.

Você também pode criar um armazenamento de dados de eventos para AWS Audit Manager evidências usando o console do Audit Manager. Para obter mais informações sobre como agregar evidências no CloudTrail Lake usando o Audit Manager, consulte Entendendo como o localizador de evidências funciona com o CloudTrail Lake no Guia do AWS Audit Manager Usuário.

CloudTrail Os armazenamentos de dados de eventos em Lake incorrem em cobranças. Ao criar um armazenamento de dados de eventos, você escolhe a opção de preço que deseja usar para ele. A opção de preço determina o custo para a ingestão e para o armazenamento de eventos, e o período de retenção padrão e máximo para o armazenamento de dados de eventos. Para obter informações sobre CloudTrail preços e gerenciamento de custos do Lake, consulte AWS CloudTrail Preços Gerenciando os custos CloudTrail do Lake e.

As seções a seguir descrevem como criar, atualizar e gerenciar armazenamentos de dados de eventos.

Tópicos

- Crie, atualize e gerencie armazenamentos de dados de eventos com o console

- Crie, atualize e gerencie armazenamentos de dados de eventos com o AWS CLI
- Gerenciar ciclos de vida do armazenamento de dados de eventos
- Copiar eventos de trilhas para um armazenamento de dados de eventos
- Federar um armazenamento de dados de eventos
- Armazenamentos de dados de eventos da organização

Crie, atualize e gerencie armazenamentos de dados de eventos com o console

Você pode usar o CloudTrail console para criar, atualizar e gerenciar seus armazenamentos de dados de eventos. Você também pode iniciar e interromper a ingestão de eventos em um armazenamento de dados de eventos e ativar a federação de consultas do Lake usando o console.

Usar o CloudTrail console para criar ou atualizar um armazenamento de dados de eventos oferece as seguintes vantagens:

- Se for a primeira vez que você cria um armazenamento de dados de eventos, o uso do CloudTrail console permite que você visualize os recursos e opções disponíveis.
- Se você estiver configurando um armazenamento de dados de eventos para registrar eventos de dados, o uso do CloudTrail console permite visualizar os tipos de dados disponíveis. Para obter mais informações, consulte Crie um armazenamento de dados de CloudTrail eventos para eventos com o console e Eventos de dados de log.
- Se você estiver configurando um armazenamento de dados de eventos para registrar eventos externos AWS, o uso do CloudTrail console permite que você visualize informações sobre os parceiros disponíveis. Para ter mais informações, consulte Crie um armazenamento de dados de eventos para eventos externos AWS com o console.

Tópicos

- Crie um armazenamento de dados de CloudTrail eventos para eventos com o console
- Crie um armazenamento de dados de eventos para eventos do CloudTrail Insights com o console
- Crie um armazenamento de dados de eventos para itens de AWS Config configuração com o console
- Crie um armazenamento de dados de eventos para eventos externos AWS com o console
- Atualizar um armazenamento de dados de eventos com o console

- Interrompa e inicie a ingestão de eventos com o console
- Altere a proteção de rescisão com o console
- Excluir um armazenamento de dados de eventos com o console
- Restaurar um armazenamento de dados de eventos com o console

Crie um armazenamento de dados de CloudTrail eventos para eventos com o console

Armazenamentos de dados de CloudTrail eventos para eventos podem registrar eventos CloudTrail de gerenciamento e dados. Você pode manter os dados do evento em um armazenamento de dados de eventos por até 3.653 dias (cerca de 10 anos) se escolher a opção de preço de retenção extensível de um ano ou até 2.557 dias (cerca de 7 anos) se escolher a opção de preço de retenção por sete anos.

CloudTrail Os armazenamentos de dados de eventos em Lake incorrem em cobranças. Ao criar um armazenamento de dados de eventos, você escolhe a opção de preço que deseja usar para ele. A opção de preço determina o custo para a ingestão e para o armazenamento de eventos, e o período de retenção padrão e máximo para o armazenamento de dados de eventos. Para obter informações sobre CloudTrail preços e gerenciamento de custos do Lake, consulte AWS CloudTrail Preços Gerenciando os custos CloudTrail do Lake e.

Para criar um armazenamento de dados de eventos para CloudTrail gerenciamento ou eventos de dados

Use esse procedimento para criar um armazenamento de dados de eventos que registre eventos CloudTrail de gerenciamento, eventos de dados ou eventos de gerenciamento e de dados.

1. Faça login no AWS Management Console e abra o CloudTrail console em https://console.aws.amazon.com/cloudtrail/.
2. No painel de navegação, em Lake, escolha Armazenamentos de dados de eventos.
3. Selecione Create event data store (Criar armazenamento de dados de eventos).
4. Na página Configure event data store (Configurar armazenamento de dados de eventos), em General details (Detalhes gerais), insira um nome para o armazenamento de dados de eventos. Um nome é obrigatório.
5. Escolha a opção de preço que você deseja usar para o armazenamento de dados de eventos. A opção de preço determina o custo para a ingestão e para o armazenamento de eventos, e os períodos de retenção padrão e máximo para o armazenamento de dados de eventos. Para obter

mais informações, consulte Preços do AWS CloudTrail e Gerenciando os custos CloudTrail do Lake.

As seguintes opções estão disponíveis:

- Preço de retenção extensível de um ano: geralmente recomendado se você espera ingerir menos de 25 TB de dados de eventos por mês e deseja um período de retenção flexível de até 10 anos. Nos primeiros 366 dias (o período de retenção padrão), o armazenamento é incluído sem custo adicional no preço de ingestão. Depois de 366 dias, a retenção estendida está disponível pelo pay-as-you-go preço. Esta é a opção padrão.
  - Período de retenção padrão: 366 dias
  - Período máximo de retenção: 3.653 dias
- Preço de retenção de sete anos: recomendado se você espera ingerir mais de 25 TB de dados de eventos por mês e precisa de um período de retenção de até 7 anos. A retenção está incluída no preço de ingestão sem custo adicional.
  - Período de retenção padrão: 2.557 dias
  - Período máximo de retenção: 2.557 dias

6. Especifique um período de retenção para o armazenamento de dados de eventos. Os períodos de retenção podem ser entre 7 dias e 3.653 dias (cerca de 10 anos) para a opção de preço de retenção extensível de um ano ou entre 7 dias e 2.557 dias (cerca de sete anos) para a opção de preço de retenção de sete anos.

   CloudTrail Lake determina se deve reter um evento verificando se o `eventTime` evento está dentro do período de retenção especificado. Por exemplo, se você especificar um período de retenção de 90 dias, CloudTrail removerá eventos quando tiverem `eventTime` mais de 90 dias.

   > **Note**
   >
   > Se você estiver copiando eventos de trilha para esse armazenamento de dados de eventos, não CloudTrail copiará um evento se ele `eventTime` for anterior ao período de retenção especificado. Para determinar o período de retenção adequado, calcule a soma do evento mais antigo que você deseja copiar em dias e o número de dias em que deseja reter os eventos no armazenamento de dados do evento (período de retenção = *`oldest-event-in-days`*+ *`number-days-to-retain`*). Por exemplo, se o evento mais antigo que você está copiando tiver 45 dias e você quiser manter os eventos no

armazenamento de dados de eventos por mais 45 dias, defina o período de retenção como 90 dias.

7. (Opcional) Para ativar o uso da criptografia AWS Key Management Service, escolha Usar minha própria AWS KMS key. Escolha Novo para AWS KMS key criar uma para você ou escolha Existente para usar uma chave KMS existente. Em Inserir alias KMS, especifique um alias, no formato. `alias/` *`MyAliasName`* Usar sua própria chave KMS exige que você edite sua política de chaves KMS para permitir que CloudTrail os registros sejam criptografados e descriptografados. Para obter mais informações, consulteConfigure as AWS KMS principais políticas para CloudTrail. CloudTrail também oferece suporte a chaves AWS KMS multirregionais. Para obter mais informações sobre chaves de várias regiões, consulte Usar chaves de várias regiões no Manual do desenvolvedor do AWS Key Management Service .

   Usar sua própria chave KMS gera AWS KMS custos de criptografia e descriptografia. Após associar um armazenamento de dados de eventos a uma chave do KMS, não será possível remover ou alterar a chave do KMS.

   > **Note**
   >
   > Para habilitar a AWS Key Management Service criptografia para um armazenamento de dados de eventos da organização, você deve usar uma chave KMS existente para a conta de gerenciamento.

8. (Opcional) Se você quiser consultar os dados do seu evento usando o Amazon Athena, escolha Habilitar na federação de consultas do Lake. A federação permite que você visualize os metadados associados ao armazenamento de dados de eventos no Catálogo de Dados do AWS Glue e execute consultas SQL nos dados do evento no Athena. Os metadados da tabela armazenados no Catálogo de AWS Glue Dados permitem que o mecanismo de consulta do Athena saiba como encontrar, ler e processar os dados que você deseja consultar. Para ter mais informações, consulte Federar um armazenamento de dados de eventos.

   Para habilitar a federação de consultas do Lake, escolha Habilitar e faça o seguinte:

   a. Escolha se deseja criar um perfil ou usar um perfil do IAM existente. O AWS Lake Formation usa esse perfil para gerenciar permissões para o armazenamento de dados de eventos federados. Quando você cria uma nova função usando o CloudTrail console, cria CloudTrail automaticamente uma função com as permissões necessárias. Se você escolher um perfil existente, a política do perfil deve fornecer as permissões mínimas necessárias.

b. Se você estiver criando um perfil, insira um nome para identificá-lo.

c. Se você estiver usando um perfil existente, escolha o perfilo que deseja usar. O perfil deve existir em sua conta.

9. (Opcional) Na seção Tags, é possível adicionar até 50 pares de chave de tag para ajudar a identificar, classificar e controlar o acesso ao seu armazenamento de dados de eventos. Para obter mais informações sobre como usar políticas do IAM para autorizar o acesso a um armazenamento de dados de eventos com base em tags, consulte Exemplos: negação de acesso para criar ou excluir armazenamentos de dados de eventos com base em tags. Para obter mais informações sobre como você pode usar tags em AWS, consulte AWS Recursos de marcação no Guia do usuário de AWS recursos de marcação.
10. Escolha Next (Avançar) para configurar o armazenamento de dados de eventos.
11. Na página Escolher eventos, escolha AWS eventos e, em seguida, escolha CloudTraileventos.
12. Para CloudTrail eventos, escolha pelo menos um tipo de evento. Por padrão, Management events (Eventos de gerenciamento) está selecionado. Você pode adicionar eventos de gerenciamento e dados ao armazenamento de dados de eventos. Para obter mais informações sobre gerenciamento de eventos, consulte Log de eventos de gerenciamento. Para obter mais informações sobre eventos de dados, consulte Eventos de dados de log.
13. (Opcional) Escolha Copy trail events (Copiar eventos de trilha) se quiser copiar eventos de uma trilha existente para fazer consultas sobre eventos anteriores. Para copiar eventos de trilha para um armazenamento de dados de eventos da organização, use a conta de gerenciamento da organização. A conta de administrador delegado não pode copiar eventos de trilhas para um armazenamento de dados de eventos da organização. Para obter mais informações sobre considerações da cópia de eventos de trilhas, consulte Considerações para copiar eventos de trilhas.
14. Para que o armazenamento de dados do seu evento colete eventos de todas as contas em uma organização do AWS Organizations , selecione Enable for all accounts in my organization (Habilitar para todas as contas na minha organização). É necessário estar conectado à conta de gerenciamento da organização ou à conta de administrador delegado para criar um armazenamento de dados de eventos que colete eventos de uma organização.

> **Note**
>
> Para copiar eventos de trilhas ou habilitar eventos do Insights, você deve estar conectado à conta de gerenciamento da organização.

15. Expanda Configurações adicionais para escolher se você deseja que seu armazenamento de dados de eventos colete eventos para todos Regiões da AWS ou somente para os atuais Região da AWS, e escolha se o armazenamento de dados de eventos ingere eventos. Por padrão, seu armazenamento de dados de eventos coleta eventos de todas as regiões em sua conta e começa a ingerir eventos ao ser criado.

    a. Opcionalmente, selecione Incluir somente a região atual no armazenamento de dados do meu evento para incluir somente eventos que estejam registrados na região atual. Se você não escolher essa opção, o armazenamento de dados de eventos incluirá eventos de todas as regiões.

    b. Desmarque a opção Ingerir eventos se você não quiser que o armazenamento de dados de eventos comece a ingerir eventos. Por exemplo, talvez você queira desmarcar Ingerir eventos se estiver copiando eventos da trilha e não quiser que o armazenamento de dados de eventos inclua eventos futuros. Por padrão, o armazenamento de dados de eventos começa a ingerir eventos assim que é criado.

16. Se seu armazenamento de dados de eventos incluir eventos de gerenciamento, você poderá escolher entre as opções a seguir. Para obter mais informações sobre gerenciamento de eventos, consulte Log de eventos de gerenciamento.

    a. Escolha se você deseja incluir eventos de leitura, eventos de gravação ou ambos. Pelo menos um é necessário.

    b. Escolha se deseja excluir AWS Key Management Service ou excluir eventos da Amazon RDS Data API do seu armazenamento de dados de eventos.

    c. Escolha se deseja habilitar o Insights. Para habilitar o Insights, é necessário configurar um armazenamento de dados de eventos de destino para coletar eventos do Insights com base na atividade de eventos de gerenciamento nesse armazenamento de dados de eventos.

        Se você optar por ativar o Insights, siga estas instruções.

        i. Em Habilitar Insights, escolha o armazenamento de dados de eventos de destino que registrará os eventos do Insights. O armazenamento de dados de eventos de destino coletará eventos do Insights com base na atividade de gerenciamento de eventos nesse armazenamento de dados de eventos. Para obter informações sobre como criar o armazenamento de dados de eventos de destino, consulte Para criar um armazenamento de dados de eventos de destino que registra eventos do Insights.

        ii. Escolha os tipos de Insights. É possível escolher a Taxa de chamadas à API, a Taxa de erros da API ou ambas. Você deve registrar eventos de gerenciamento de

gravação para registrar em log eventos do Insights sobre a taxa de chamadas à API. É necessário registrar eventos de gerenciamento de leitura ou gravação para registrar em log eventos do Insights sobre a taxa de erros da API.

17. Para incluir eventos de dados no armazenamento de dados de eventos, faça o seguinte.

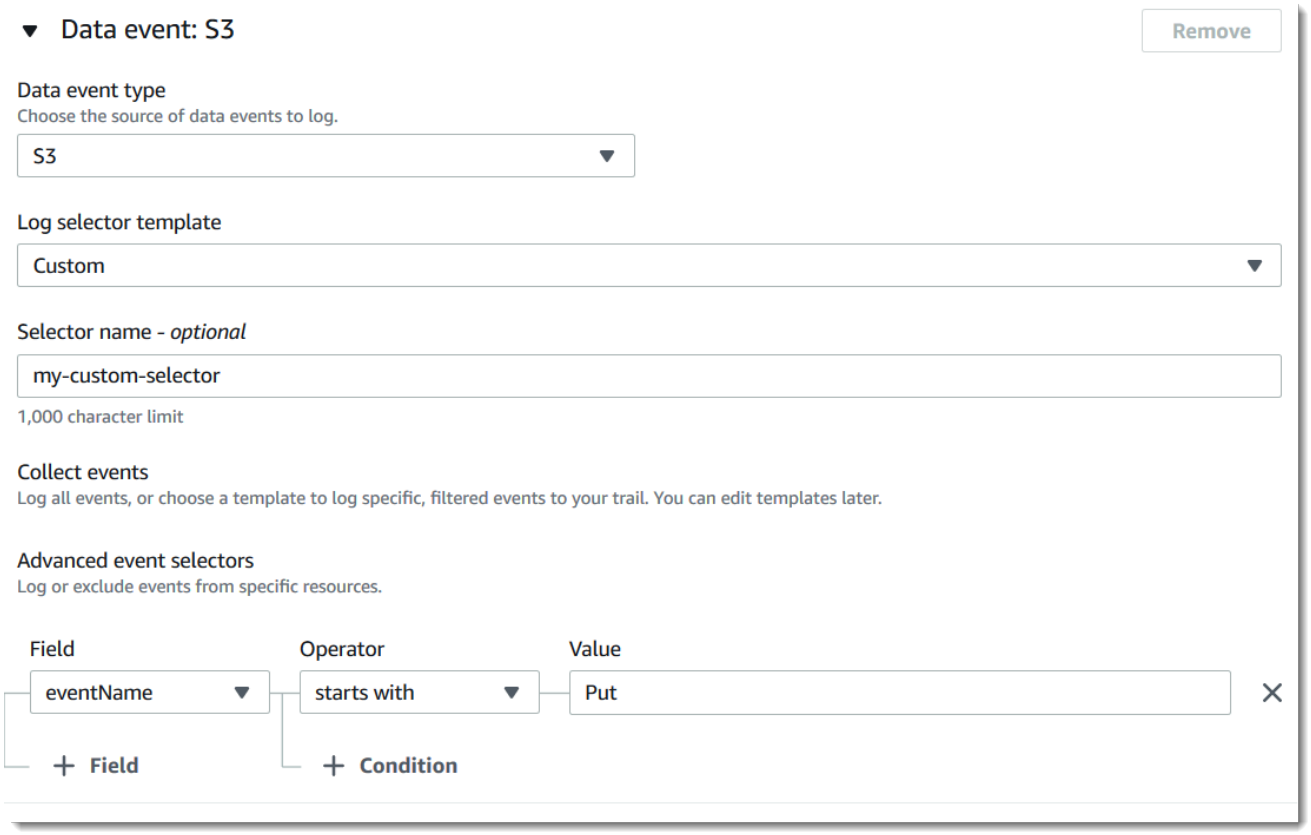
    a. Escolha um tipo de evento de dados. Esse é o AWS service (Serviço da AWS) recurso no qual os eventos de dados são registrados. Para registrar eventos de dados para AWS Glue tabelas criadas pelo Lake Formation, escolha Lake Formation como tipo de dados.

    b. Em Log selector template (Modelo de seletor de logs), escolha um modelo. Você pode optar por registrar em log todos os eventos de dados, eventos `readOnly`, eventos `writeOnly` ou Custom (Personalizado) para criar um seletor de logs personalizado.

    c. (Opcional) Em Nome do seletor, insira um nome para identificar o seletor. O nome do seletor é um nome descritivo para um seletor de eventos avançado, como "Registrar eventos de dados em log para apenas dois buckets do S3". O nome do seletor é listado como `Name` no seletor de eventos avançado e poderá ser visualizado se você expandir a visualização JSON.

    d. Em Advanced event selectors (Seletores de eventos avançados), crie expressões escolhendo valores para Field (Campo), Operator (Operador) e Value (Valor). Seletores de eventos avançados para um armazenamento de dados de eventos funcionam da mesma forma que os seletores de eventos avançados que você aplica a uma trilha. Para obter mais informações sobre como criar seletores de eventos avançados, consulte Filtragem de eventos de dados usando seletores de eventos avançados.

       O exemplo a seguir usa um modelo de seletor de logs Custom (Personalizado) para escolher apenas nomes de eventos de objetos S3 que comecem com `Put`, por exemplo, `PutObject`. Como o seletor de eventos avançados não inclui nem exclui nenhum outro tipo de evento ou ARN de recurso, todos os eventos de dados do S3, tanto de leitura quanto de gravação, que têm nomes de eventos começando com `Put` são armazenados no armazenamento de dados de eventos.



> **Important**
>
> Para excluir ou incluir eventos de dados com seletores de eventos avançados usando um ARN de bucket do S3, sempre use o operador Starts with (Inicia com).

e. Opcionalmente, expanda a JSON view (Exibição de JSON) para ver seus seletores de eventos avançados como um bloco JSON.

f. Para adicionar outro tipo de dados no qual registrar eventos de dados, escolha Add data event type (Adicionar tipo de evento de dados). Repita as etapas de a a esta etapa para configurar seletores de eventos avançados para o tipo de evento de dados.

18. Faça o seguinte para copiar eventos de trilhas existentes para o armazenamento de dados de eventos.

a. Escolha a trilha que você deseja copiar. Por padrão, copia CloudTrail somente CloudTrail os eventos contidos no prefixo do bucket do S3 e os `CloudTrail` prefixos dentro do `CloudTrail` prefixo, e não verifica os prefixos de outros serviços. AWS Se você quiser copiar CloudTrail eventos contidos em outro prefixo, escolha Inserir URI do S3 e, em seguida, escolha Procurar no S3 para navegar até o prefixo. Se o bucket S3 de origem

da trilha usar uma chave KMS para criptografia de dados, certifique-se de que a política de chaves do KMS permita CloudTrail descriptografar os dados. Se seu bucket do S3 de origem usa várias chaves KMS, você deve atualizar a política de cada chave CloudTrail para permitir a descriptografia dos dados no bucket. Para obter mais informações sobre a atualização da política de chaves do KMS, consulte Política de chaves do KMS para descriptografar dados no bucket do S3 de origem.

b. Escolha o intervalo de tempo para copiar os eventos. CloudTrail verifica o prefixo e o nome do arquivo de log para verificar se o nome contém uma data entre as datas de início e término escolhidas antes de tentar copiar os eventos da trilha. É possível escolher entre Relative range (Intervalo relativo) e Absolute range (Intervalo absoluto). Para evitar a duplicação de eventos entre a trilha de origem e o armazenamento de dados de eventos de destino, escolha um intervalo de tempo que seja anterior à criação do armazenamento de dados de eventos.

> **Note**
>
> CloudTrail copia somente eventos de trilha que tenham um período de retenção `eventTime` dentro do armazenamento de dados de eventos. Por exemplo, se o período de retenção de um armazenamento de dados de eventos for de 90 dias, não CloudTrail copiará nenhum evento de trilha com `eventTime` mais de 90 dias.

- Se você escolher Intervalo relativo, poderá optar por copiar eventos registrados nos últimos 6 meses, 1 ano, 2 anos, 7 anos ou um intervalo personalizado. CloudTrail copia os eventos registrados dentro do período de tempo escolhido.
- Se você escolher Intervalo absoluto, poderá escolher uma data específica de início e término. CloudTrail copia os eventos que ocorreram entre as datas de início e término escolhidas.

c. Em Permissions (Permissões), escolha uma das opções de perfil do IAM a seguir. Ao escolher um perfil do IAM existente, verifique se a política de perfil do IAM fornece as permissões necessárias. Para obter mais informações sobre como atualizar as permissões do perfil do IAM, consulte Permissões do IAM para copiar eventos da trilha.

- Escolha Create a new role (recommended) (Criar uma nova função [recomendado]) para criar um novo perfil do IAM. Em Inserir nome da função do IAM, insira um nome para a função. CloudTrail cria automaticamente as permissões necessárias para essa nova função.

- Escolha Usar um ARN de função personalizada do IAM para usar uma função personalizada do IAM que não esteja listada. Em Enter IAM role ARN (Inserir ARN do perfil do IAM), insira o ARN do perfil.
- Escolha uma função do IAM existente na lista suspensa.

19. Selecione Next (Próximo) para revisar suas escolhas.
20. Na página Review and create (Revisar e criar), revise as suas escolhas. Escolha Edit (Editar) para fazer alterações a uma seção. Quando estiver pronto para criar o armazenamento de dados de eventos, escolha Create event data store (Criar armazenamento de dados de eventos).
21. O novo armazenamento de dados de eventos está visível na tabela Armazenamentos de dados de eventos na página Armazenamento de dados de eventos.

    Deste ponto em diante, o armazenamento de dados de eventos captura eventos que correspondem aos seletores de eventos avançados (se você manteve a opção Ingerir eventos selecionada). Os eventos ocorridos antes da criação do armazenamento de dados de eventos não estarão no armazenamento de dados de eventos, a menos que você tenha optado por copiar eventos de trilha existentes.

Agora, você pode executar consultas no novo armazenamento de dados de eventos. A guia Sample queries (Consultas de amostra) fornece exemplos de consultas para você começar. Para obter mais informações sobre como criar e editar consultas, veja Criar ou editar uma consulta.

Você também pode visualizar o painel do CloudTrail Lake para visualizar os eventos em seu armazenamento de dados de eventos. Para obter mais informações sobre painéis do Lake, consulte Veja os painéis CloudTrail do Lake.

Exemplo: criar um armazenamento de dados de eventos para eventos de gerenciamento

Este passo a passo mostra como criar um armazenamento de dados de eventos que registra todos os eventos de gerenciamento em todas as AWS regiões e não registra nenhum evento de dados. Os exemplos de eventos de gerenciamento incluem eventos de segurança, como os eventos do `CreateUser` e `AttachRolePolicy` do IAM, eventos de recurso, como `RunInstances` e `CreateBucket` e muito mais.

Para criar um armazenamento de dados de eventos para eventos de gerenciamento

1. Faça login no AWS Management Console e abra o CloudTrail console em https://console.aws.amazon.com/cloudtrail/.

2. No painel de navegação, em Lake, escolha Armazenamentos de dados de eventos.
3. Selecione Create event data store (Criar armazenamento de dados de eventos).
4. Na página Configurar armazenamento de dados de eventos, em Detalhes gerais, dê um nome ao seu armazenamento de dados de eventos, como *my-management-events-eds*. Como prática recomendada, use um nome que identifique rapidamente a finalidade do armazenamento de dados de eventos. Para obter informações sobre os requisitos CloudTrail de nomenclatura, consulteRequisitos de nomenclatura.
5. Escolha a opção de preço que você deseja usar para o armazenamento de dados de eventos. A opção de preço determina o custo para a ingestão e para o armazenamento de eventos, e os períodos de retenção padrão e máximo para o armazenamento de dados de eventos. Para obter mais informações, consulte Preços do AWS CloudTrail e Gerenciando os custos CloudTrail do Lake.

   As seguintes opções estão disponíveis:

   - Preço de retenção extensível de um ano: geralmente recomendado se você espera ingerir menos de 25 TB de dados de eventos por mês e deseja um período de retenção flexível de até 10 anos. Nos primeiros 366 dias (o período de retenção padrão), o armazenamento é incluído sem custo adicional no preço de ingestão. Depois de 366 dias, a retenção estendida está disponível pelo pay-as-you-go preço. Esta é a opção padrão.
     - Período de retenção padrão: 366 dias
     - Período máximo de retenção: 3.653 dias
   - Preço de retenção de sete anos: recomendado se você espera ingerir mais de 25 TB de dados de eventos por mês e precisa de um período de retenção de até 7 anos. A retenção está incluída no preço de ingestão sem custo adicional.
     - Período de retenção padrão: 2.557 dias
     - Período máximo de retenção: 2.557 dias
6. Especifique um período de retenção para o armazenamento de dados de eventos. Os períodos de retenção podem ser entre 7 dias e 3.653 dias (cerca de 10 anos) para a opção de preço de retenção extensível de um ano ou entre 7 dias e 2.557 dias (cerca de sete anos) para a opção de preço de retenção de sete anos.

   CloudTrail Lake determina se deve reter um evento verificando se o `eventTime` evento está dentro do período de retenção especificado. Por exemplo, se você especificar um período de retenção de 90 dias, CloudTrail removerá eventos quando tiverem `eventTime` mais de 90 dias.

7. (Opcional) Em Criptografia, escolha se você deseja criptografar o armazenamento de dados do evento usando sua própria chave do KMS. Por padrão, todos os eventos em um armazenamento de dados de eventos são criptografados CloudTrail usando uma chave KMS que AWS possui e gerencia para você.

   Para habilitar a criptografia usando sua própria chave do KMS, escolha Usar minha própria AWS KMS key. Escolha Novo para AWS KMS key criar uma para você ou escolha Existente para usar uma chave KMS existente. Em Inserir alias KMS, especifique um alias, no formato. `alias/MyAliasName` Usar sua própria chave KMS exige que você edite sua política de chaves KMS para permitir que CloudTrail os registros sejam criptografados e descriptografados. Para obter mais informações, consulteConfigure as AWS KMS principais políticas para CloudTrail. CloudTrail também oferece suporte a chaves AWS KMS multirregionais. Para obter mais informações sobre chaves de várias regiões, consulte Usar chaves de várias regiões no Manual do desenvolvedor do AWS Key Management Service .

   Usar sua própria chave KMS gera AWS KMS custos de criptografia e descriptografia. Após associar um armazenamento de dados de eventos a uma chave do KMS, não será possível remover ou alterar a chave do KMS.

   > **Note**
   >
   > Para habilitar a AWS Key Management Service criptografia para um armazenamento de dados de eventos da organização, você deve usar uma chave KMS existente para a conta de gerenciamento.

8. (Opcional) Se você quiser consultar os dados do seu evento usando o Amazon Athena, escolha Habilitar na federação de consultas do Lake. A federação permite que você visualize os metadados associados ao armazenamento de dados de eventos no Catálogo de Dados do AWS Glue e execute consultas SQL nos dados do evento no Athena. Os metadados da tabela armazenados no Catálogo de AWS Glue Dados permitem que o mecanismo de consulta do Athena saiba como encontrar, ler e processar os dados que você deseja consultar. Para ter mais informações, consulte Federar um armazenamento de dados de eventos.

   Para habilitar a federação de consultas do Lake, escolha Habilitar e faça o seguinte:

   a. Escolha se deseja criar um perfil ou usar um perfil do IAM existente. O AWS Lake Formation usa esse perfil para gerenciar permissões para o armazenamento de dados de eventos federados. Quando você cria uma nova função usando o CloudTrail console, cria CloudTrail

automaticamente uma função com as permissões necessárias. Se você escolher um perfil existente, a política do perfil deve fornecer as permissões mínimas necessárias.

b. Se você estiver criando um perfil, insira um nome para identificá-lo.

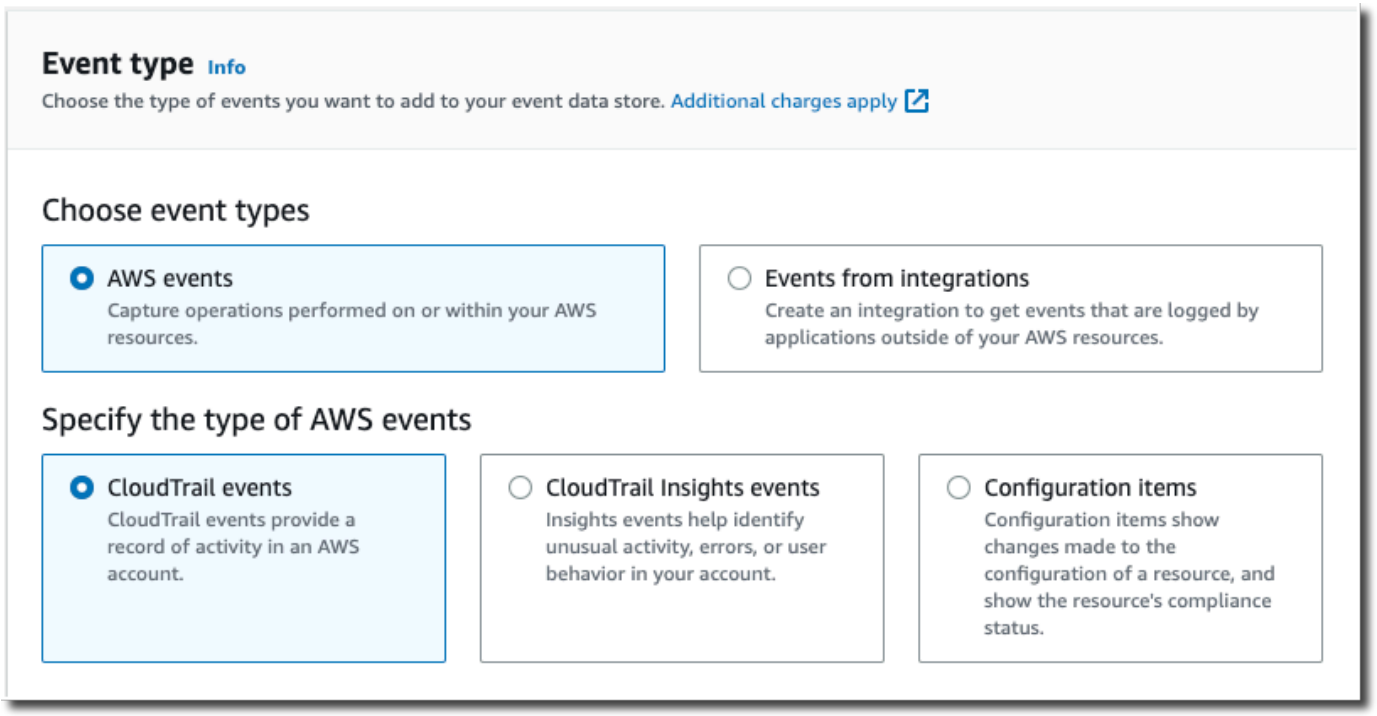
c. Se você estiver usando um perfil existente, escolha o perfilo que deseja usar. O perfil deve existir em sua conta.

9. (Opcional) Em Tags, adicione uma ou mais tags personalizadas (pares chave-valor) ao armazenamento de dados de eventos. As tags podem ajudar você a identificar seus repositórios de dados de CloudTrail eventos. Por exemplo, você poderia anexar uma tag com o nome **`stage`** e o valor **`prod`**. É possível usar tags para limitar o acesso ao armazenamento de dados de eventos. As tags também podem ser usadas para monitorar os custos de consulta e ingestão do seu armazenamento de dados de eventos.

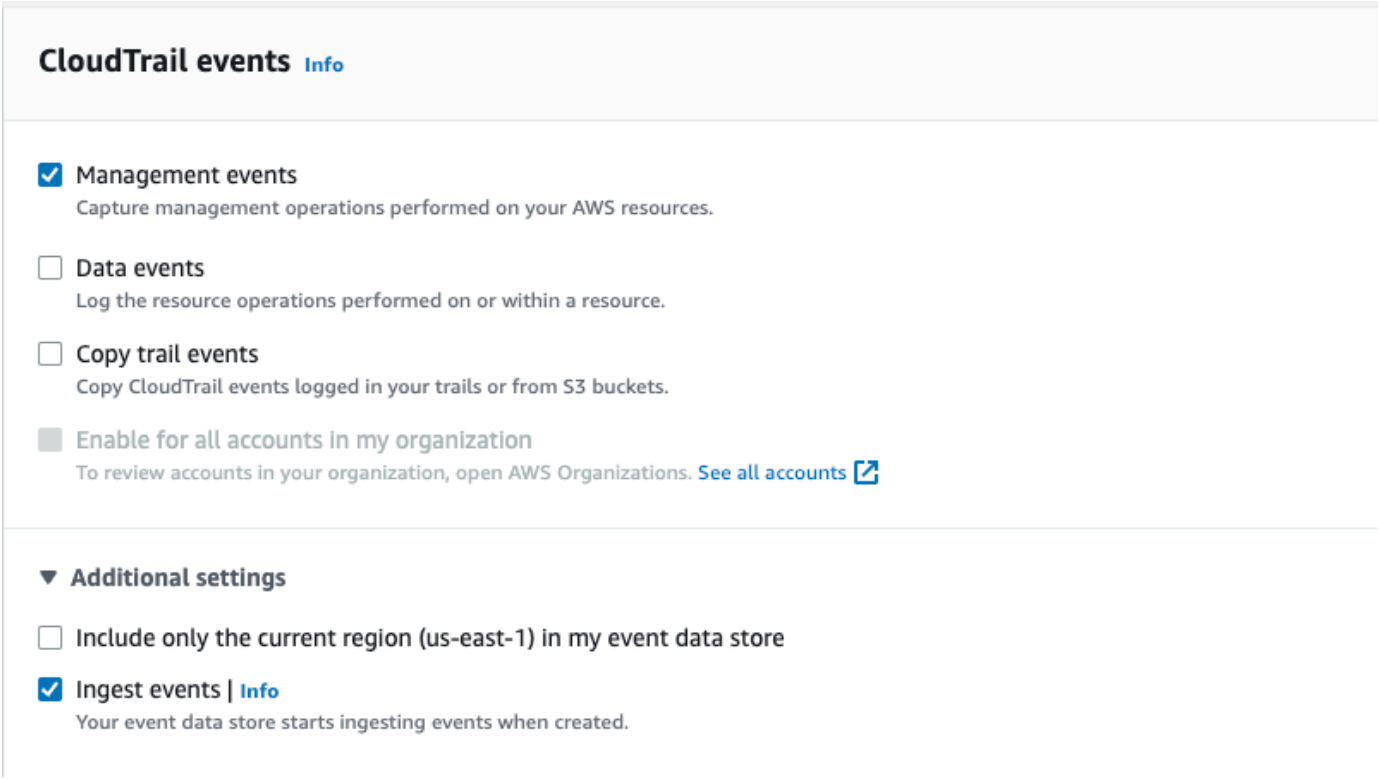
   Para obter informações sobre como usar tags para monitorar os custos, consulte Criação de etiquetas de alocação de custos definidas pelo usuário para armazenamentos de dados de eventos do CloudTrail Lake. Para obter informações sobre como usar políticas do IAM para autorizar o acesso a um armazenamento de dados de eventos com base em tags, consulte Exemplos: negação de acesso para criar ou excluir armazenamentos de dados de eventos com base em tags. Para obter informações sobre como você pode usar tags em AWS, consulte Como marcar seus AWS recursos no Guia do usuário de AWS recursos de marcação.

10. Escolha Next (Avançar) para configurar o armazenamento de dados de eventos.

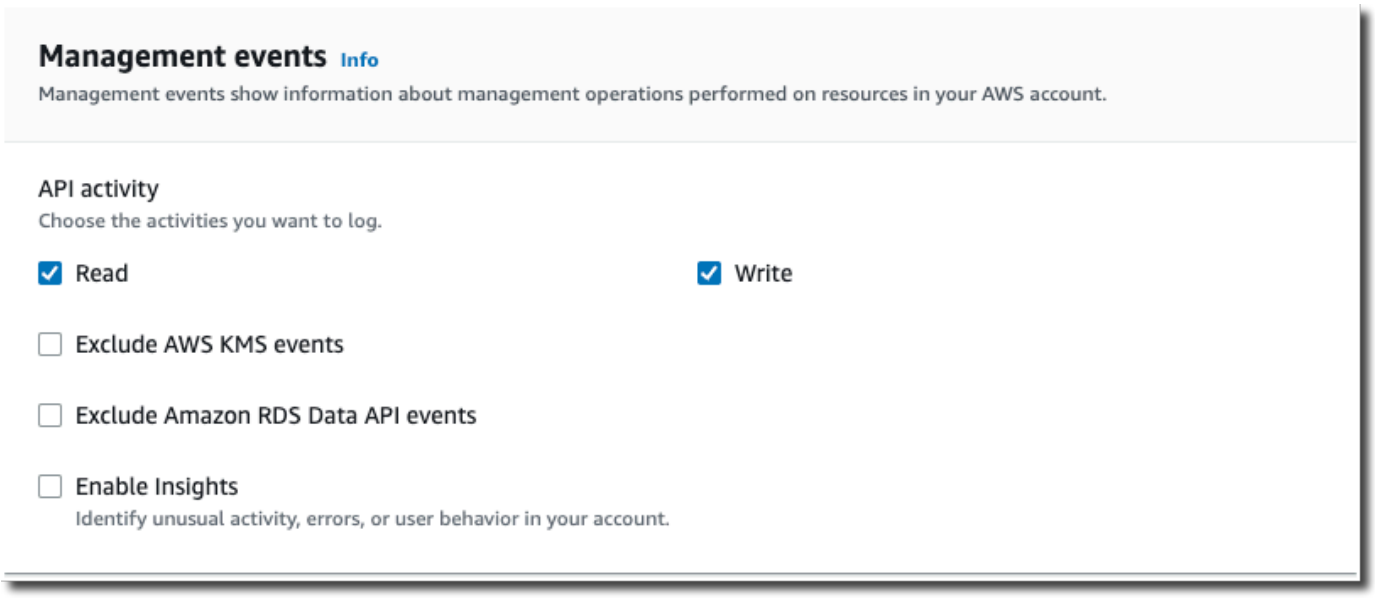
11. Na página Escolher eventos, mantenha as seleções padrão para Tipo de evento.



12. Para CloudTrail eventos, deixe as seleções padrão. Por padrão, os armazenamentos de dados de CloudTrail eventos coletam eventos de gerenciamento e não coletam eventos de dados. Para obter mais informações sobre gerenciamento de eventos, consulte Log de eventos de gerenciamento. Para obter mais informações sobre eventos de dados, consulte Eventos de dados de log.



13. Mantenha a configuração padrão para Copiar eventos de trilha. Você usaria essa opção para copiar eventos de trilhas existentes para o armazenamento de dados de eventos. Para ter mais informações, consulte Copiar eventos de trilhas para um armazenamento de dados de eventos.
14. Escolha Habilitar para todas as contas em minha organização se este for um armazenamento de dados de eventos da organização. Essa opção não estará disponível para alteração, a menos que você tenha contas configuradas no AWS Organizations.
15. Em Configurações adicionais, mantenha as seleções padrão. Por padrão, um armazenamento de dados de eventos coleta eventos para todos Regiões da AWS e começa a ingerir eventos quando é criado.
16. Em Eventos de gerenciamento, escolha coletar eventos de Leitura e Gravação. Deixe as caixas de seleção Excluir AWS KMS eventos e Excluir eventos da API de dados do Amazon RDS vazias para coletar todos os eventos de gerenciamento. Deixe a caixa de seleção Habilitar eventos do Insights vazia.



17. Selecione Next (Próximo) para revisar suas escolhas.
18. Na página Review and create (Revisar e criar), revise as suas escolhas. Escolha Edit (Editar) para fazer alterações a uma seção. Quando estiver pronto para criar o armazenamento de dados de eventos, escolha Create event data store (Criar armazenamento de dados de eventos).
19. O novo armazenamento de dados de eventos está visível na tabela Armazenamentos de dados de eventos na página Armazenamento de dados de eventos.

    Deste ponto em diante, o armazenamento de dados de eventos captura eventos que correspondem aos seletores de eventos avançados. Os eventos ocorridos antes da criação do armazenamento de dados de eventos não estarão no armazenamento de dados de eventos, a menos que você tenha optado por copiar eventos de trilha existentes.

Exemplo: criar um armazenamento de dados de eventos para eventos de dados do S3

Este passo a passo mostra como criar um armazenamento de dados de eventos para eventos de dados do Amazon S3. Nesse cenário, em vez de registrar todos os eventos de dados do Amazon S3, escolheremos um modelo de seletor de log personalizado para registrar eventos somente quando um objeto for excluído de um bucket específico do S3.

Para criar um armazenamento de dados de eventos para eventos de dados do S3

1. Faça login no AWS Management Console e abra o CloudTrail console em https://console.aws.amazon.com/cloudtrail/.

2. No painel de navegação, em Lake, escolha Armazenamentos de dados de eventos.
3. Selecione Create event data store (Criar armazenamento de dados de eventos).
4. Na página Configurar armazenamento de dados de eventos, em Detalhes gerais, dê um nome ao armazenamento de dados de eventos, como *s3- data-events-eds*. Como prática recomendada, use um nome que identifique rapidamente a finalidade do armazenamento de dados de eventos. Para obter informações sobre os requisitos CloudTrail de nomenclatura, consulteRequisitos de nomenclatura.
5. Escolha a opção de preço que você deseja usar para o armazenamento de dados de eventos. A opção de preço determina o custo para a ingestão e para o armazenamento de eventos, e os períodos de retenção padrão e máximo para o armazenamento de dados de eventos. Para obter mais informações, consulte Preços do AWS CloudTrail e Gerenciando os custos CloudTrail do Lake.

   As seguintes opções estão disponíveis:

   - Preço de retenção extensível de um ano: geralmente recomendado se você espera ingerir menos de 25 TB de dados de eventos por mês e deseja um período de retenção flexível de até 10 anos. Nos primeiros 366 dias (o período de retenção padrão), o armazenamento é incluído sem custo adicional no preço de ingestão. Depois de 366 dias, a retenção estendida está disponível pelo pay-as-you-go preço. Esta é a opção padrão.
     - Período de retenção padrão: 366 dias
     - Período máximo de retenção: 3.653 dias
   - Preço de retenção de sete anos: recomendado se você espera ingerir mais de 25 TB de dados de eventos por mês e precisa de um período de retenção de até 7 anos. A retenção está incluída no preço de ingestão sem custo adicional.
     - Período de retenção padrão: 2.557 dias
     - Período máximo de retenção: 2.557 dias
6. Especifique um período de retenção para o armazenamento de dados de eventos. Os períodos de retenção podem ser entre 7 dias e 3.653 dias (cerca de 10 anos) para a opção de preço de retenção extensível de um ano ou entre 7 dias e 2.557 dias (cerca de sete anos) para a opção de preço de retenção de sete anos.

   CloudTrail Lake determina se deve reter um evento verificando se o `eventTime` evento está dentro do período de retenção especificado. Por exemplo, se você especificar um período de retenção de 90 dias, CloudTrail removerá eventos quando tiverem `eventTime` mais de 90 dias.

7. (Opcional) Em Criptografia, escolha se você deseja criptografar o armazenamento de dados do evento usando sua própria chave do KMS. Por padrão, todos os eventos em um armazenamento de dados de eventos são criptografados CloudTrail usando uma chave KMS que AWS possui e gerencia para você.

   Para habilitar a criptografia usando sua própria chave do KMS, escolha Usar minha própria AWS KMS key. Escolha Novo para AWS KMS key criar uma para você ou escolha Existente para usar uma chave KMS existente. Em Inserir alias KMS, especifique um alias, no formato. `alias/MyAliasName` Usar sua própria chave KMS exige que você edite sua política de chaves KMS para permitir que CloudTrail os registros sejam criptografados e descriptografados. Para obter mais informações, consulteConfigure as AWS KMS principais políticas para CloudTrail. CloudTrail também oferece suporte a chaves AWS KMS multirregionais. Para obter mais informações sobre chaves de várias regiões, consulte Usar chaves de várias regiões no Manual do desenvolvedor do AWS Key Management Service .

   Usar sua própria chave KMS gera AWS KMS custos de criptografia e descriptografia. Após associar um armazenamento de dados de eventos a uma chave do KMS, não será possível remover ou alterar a chave do KMS.

   > **Note**
   >
   > Para habilitar a AWS Key Management Service criptografia para um armazenamento de dados de eventos da organização, você deve usar uma chave KMS existente para a conta de gerenciamento.

8. (Opcional) Se você quiser consultar os dados do seu evento usando o Amazon Athena, escolha Habilitar na federação de consultas do Lake. A federação permite que você visualize os metadados associados ao armazenamento de dados de eventos no Catálogo de Dados do AWS Glue e execute consultas SQL nos dados do evento no Athena. Os metadados da tabela armazenados no Catálogo de AWS Glue Dados permitem que o mecanismo de consulta do Athena saiba como encontrar, ler e processar os dados que você deseja consultar. Para ter mais informações, consulte Federar um armazenamento de dados de eventos.

   Para habilitar a federação de consultas do Lake, escolha Habilitar e faça o seguinte:

   a. Escolha se deseja criar um perfil ou usar um perfil do IAM existente. O AWS Lake Formation usa esse perfil para gerenciar permissões para o armazenamento de dados de eventos federados. Quando você cria uma nova função usando o CloudTrail console, cria CloudTrail

automaticamente uma função com as permissões necessárias. Se você escolher um perfil existente, a política do perfil deve fornecer as permissões mínimas necessárias.

b. Se você estiver criando um perfil, insira um nome para identificá-lo.

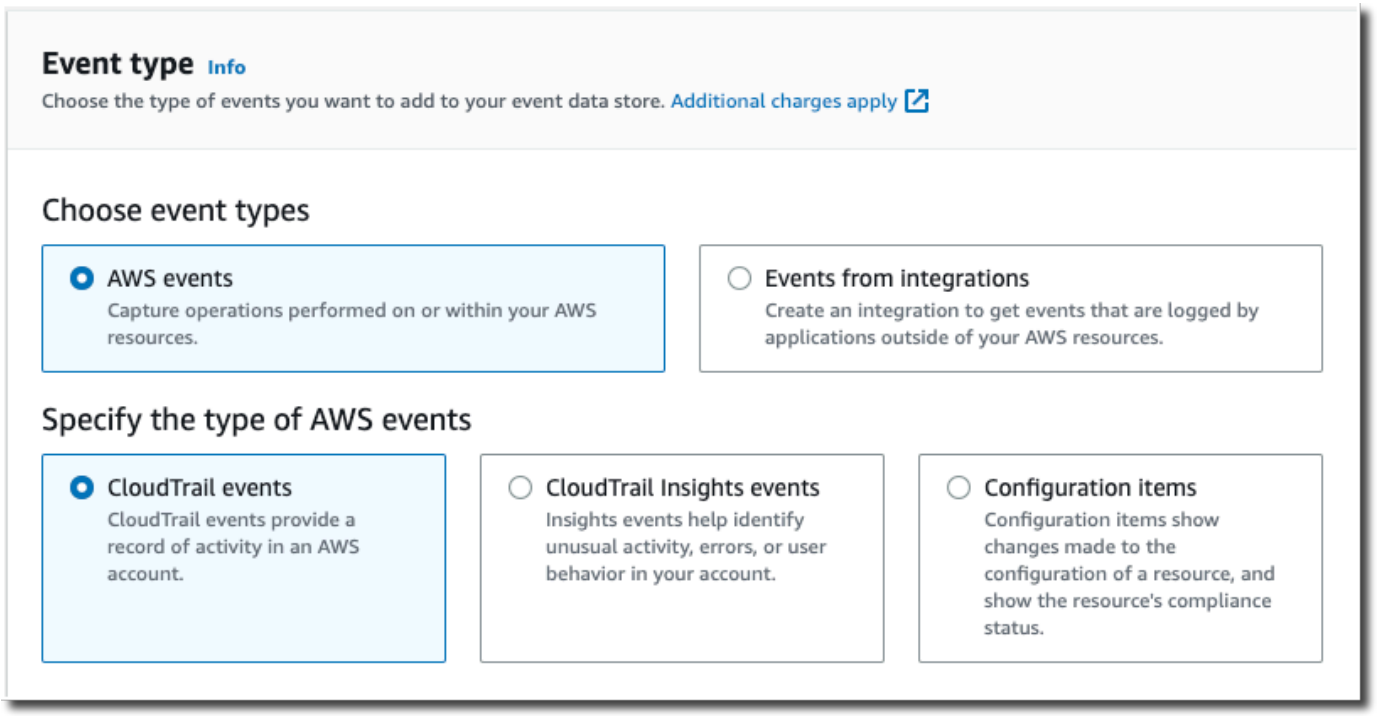
c. Se você estiver usando um perfil existente, escolha o perfilo que deseja usar. O perfil deve existir em sua conta.

9. (Opcional) Em Tags, adicione uma ou mais tags personalizadas (pares chave-valor) ao armazenamento de dados de eventos. As tags podem ajudar você a identificar seus repositórios de dados de CloudTrail eventos. Por exemplo, você poderia anexar uma tag com o nome **`stage`** e o valor **`prod`**. É possível usar tags para limitar o acesso ao armazenamento de dados de eventos. As tags também podem ser usadas para monitorar os custos de consulta e ingestão do seu armazenamento de dados de eventos.

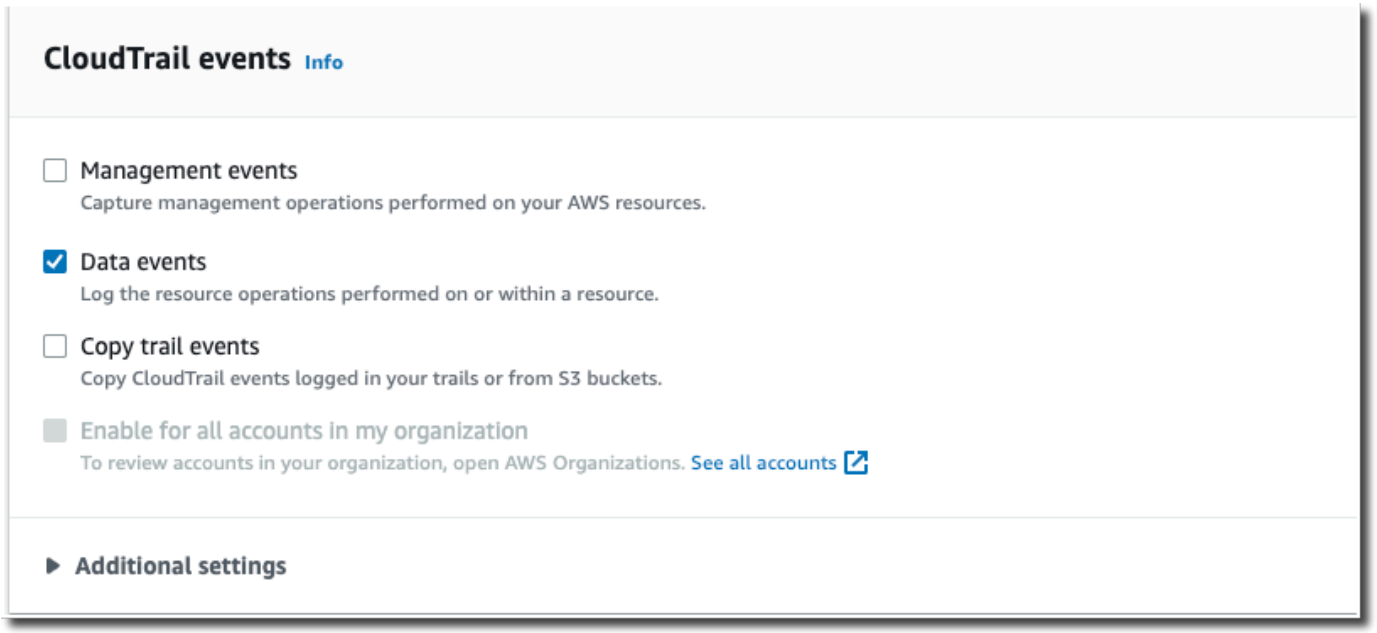
   Para obter informações sobre como usar tags para monitorar os custos, consulte Criação de etiquetas de alocação de custos definidas pelo usuário para armazenamentos de dados de eventos do CloudTrail Lake. Para obter informações sobre como usar políticas do IAM para autorizar o acesso a um armazenamento de dados de eventos com base em tags, consulte Exemplos: negação de acesso para criar ou excluir armazenamentos de dados de eventos com base em tags. Para obter informações sobre como você pode usar tags em AWS, consulte Como marcar seus AWS recursos no Guia do usuário de AWS recursos de marcação.

10. Escolha Next (Avançar) para configurar o armazenamento de dados de eventos.

11. Na página Escolher eventos, mantenha as seleções padrão para Tipo de evento.



12. Para CloudTrail eventos, escolha Eventos de dados e desmarque Eventos de gerenciamento. Para obter mais informações sobre eventos de dados, consulte Eventos de dados de log.



13. Mantenha a configuração padrão para Copiar eventos de trilha. Você usaria essa opção para copiar eventos de trilhas existentes para o armazenamento de dados de eventos. Para ter mais informações, consulte Copiar eventos de trilhas para um armazenamento de dados de eventos.

14. Escolha Habilitar para todas as contas em minha organização se este for um armazenamento de dados de eventos da organização. Essa opção não estará disponível para alteração, a menos que você tenha contas configuradas no AWS Organizations.
15. Em Configurações adicionais, mantenha as seleções padrão. Por padrão, um armazenamento de dados de eventos coleta eventos para todos Regiões da AWS e começa a ingerir eventos quando é criado.
16. Para Eventos de dados, faça as seguintes seleções:

    a. Em Tipo de evento de dados, escolha S3. O tipo de evento de dados identifica o recurso AWS service (Serviço da AWS) e no qual os eventos de dados são registrados.

    b. Em Modelo do seletor de log, escolha Personalizado. Escolher Personalizado permite definir um seletor de eventos personalizado para filtrar os campos `eventName`, `resources.ARN` e `readOnly`. Para obter informações sobre esses campos, consulte AdvancedFieldSelectora Referência AWS CloudTrail da API.

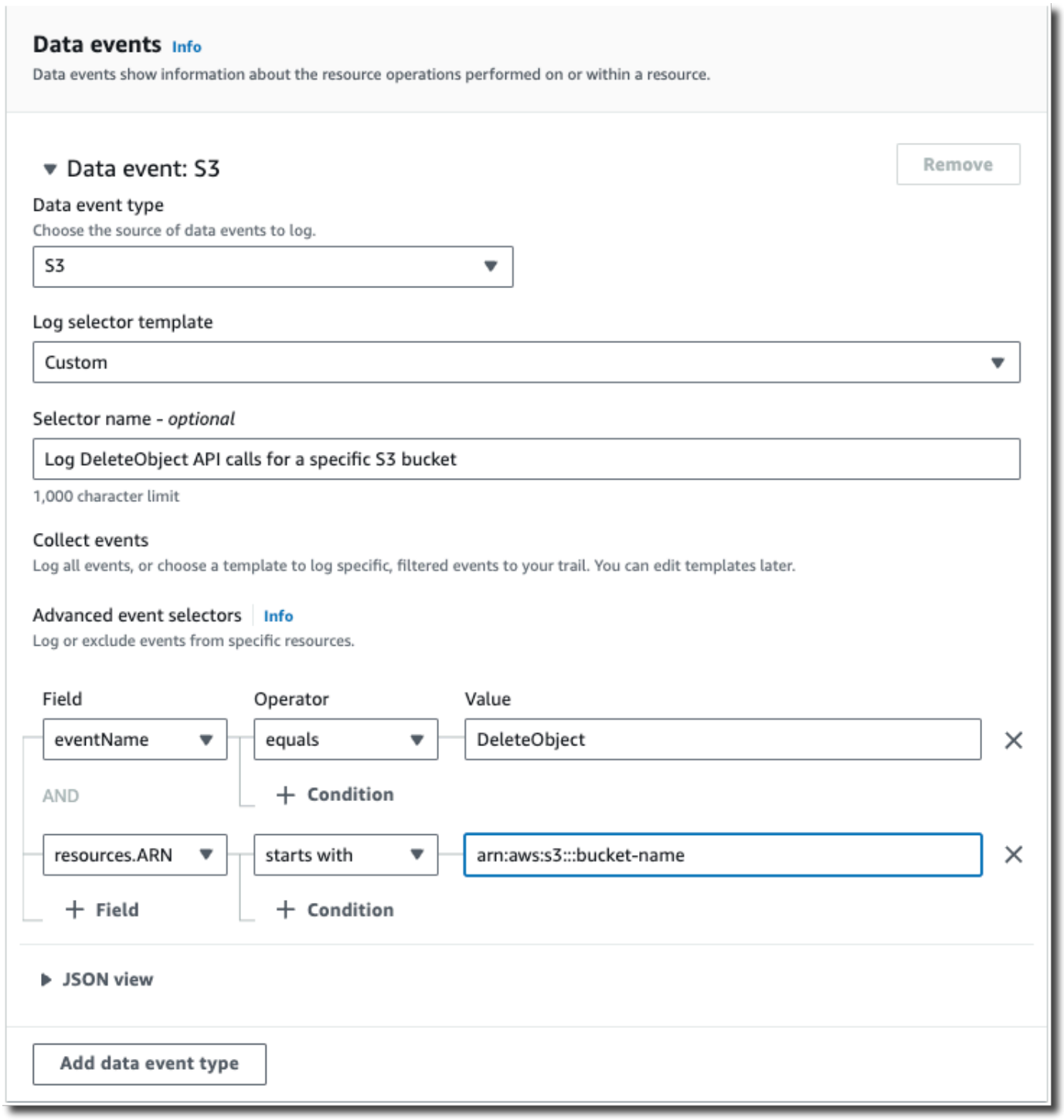
    c. (Opcional) Em Nome do seletor, insira um nome para identificar o seletor. O nome do seletor é um nome descritivo para um seletor de eventos avançado, como “Registrar chamadas de DeleteObject API para um bucket específico do S3”. O nome do seletor é listado como `Name` no seletor de eventos avançado e poderá ser visualizado se você expandir a visualização JSON.

    d. Nos seletores de eventos avançados, criaremos o seletor de eventos personalizado para filtrar os campos `eventName` e. `resources.ARN` Seletores de eventos avançados para

um armazenamento de dados de eventos funcionam da mesma forma que os seletores de eventos avançados que você aplica a uma trilha. Para obter mais informações sobre como criar seletores de eventos avançados, consulte Registro em log de eventos de dados com seletores de eventos avançados.

i. Em Campo, escolha eventName. Em Operador, escolha equals. Em Valor, insira **`DeleteObject`**. Escolha + Campo para filtrar em outro campo.

ii. Em Campo, escolha resources.ARN. Para Operador, escolha StartsWith. Em Valor, insira o ARN do seu bucket (por exemplo, *`arn:aws:s3:::bucket-name`*). Para obter mais informações sobre como obter o ARN, consulte Recursos do Amazon S3 no Guia do usuário do Amazon Simple Storage Service.



17. Selecione Next (Próximo) para revisar suas escolhas.
18. Na página Review and create (Revisar e criar), revise as suas escolhas. Escolha Edit (Editar) para fazer alterações a uma seção. Quando estiver pronto para criar o armazenamento de

dados de eventos, escolha Create event data store (Criar armazenamento de dados de eventos).

19. O novo armazenamento de dados de eventos está visível na tabela Armazenamentos de dados de eventos na página Armazenamento de dados de eventos.

    Deste ponto em diante, o armazenamento de dados de eventos captura eventos que correspondem aos seletores de eventos avançados. Os eventos ocorridos antes da criação do armazenamento de dados de eventos não estarão no armazenamento de dados de eventos, a menos que você tenha optado por copiar eventos de trilha existentes.

Crie um armazenamento de dados de eventos para eventos do CloudTrail Insights com o console

AWS CloudTrail O Insights ajuda AWS os usuários a identificar e responder a atividades incomuns associadas a chamadas de API e taxas de erro de API, analisando continuamente os eventos CloudTrail de gerenciamento. CloudTrail O Insights analisa seus padrões normais de volume de chamadas de API e taxas de erro de API, também chamados de linha de base, e gera eventos do Insights quando o volume de chamadas ou as taxas de erro estão fora dos padrões normais. Eventos de insights no volume de chamadas de API são gerados para `write` APIs de gerenciamento e eventos do Insights na taxa de erros da API são gerados para ambos`read` e `write` APIs de gerenciamento.

Para registrar eventos do Insights no CloudTrail Lake, você precisa de um armazenamento de dados de eventos de destino que registre eventos do Insights e um armazenamento de dados de eventos de origem que permita o Insights e eventos de gerenciamento de registros.

> **Note**
>
> Para registrar em log eventos do Insights sobre o volume de chamadas à API, o armazenamento de dados de eventos de origem deve registrar em log os eventos de gerenciamento de `write`. Para registrar em log eventos do Insights sobre a taxa de erros da API, o armazenamento de dados de eventos de origem deve registrar em log os eventos de gerenciamento de `read` ou `write`.

Se você tiver o CloudTrail Insights ativado em um armazenamento de dados de eventos de origem e CloudTrail detectar atividades incomuns, CloudTrail entrega os eventos do Insights ao

seu armazenamento de dados de eventos de destino. Ao contrário de outros tipos de eventos capturados em um armazenamento de dados de CloudTrail eventos, os eventos do Insights são registrados somente quando CloudTrail detectam alterações no uso da API da sua conta que diferem significativamente dos padrões de uso típicos da conta.

Depois de ativar o CloudTrail Insights pela primeira vez em um armazenamento de dados de eventos, pode levar até 7 dias CloudTrail para entregar o primeiro evento do Insights, se uma atividade incomum for detectada.

CloudTrail O Insights analisa eventos de gerenciamento que ocorrem em uma única região, não globalmente. Um evento do CloudTrail Insights é gerado na mesma região em que seus eventos de gerenciamento de apoio são gerados.

Para um armazenamento de dados de eventos da organização, CloudTrail analisa os eventos de gerenciamento da conta de cada membro em vez de analisar a agregação de todos os eventos de gerenciamento da organização.

Cobranças adicionais se aplicam à ingestão de eventos do Insights em CloudTrail Lake. Você será cobrado separadamente se ativar o Insights tanto para trilhas quanto para armazenamentos de dados de eventos em CloudTrail Lake. Para obter informações sobre CloudTrail preços, consulte AWS CloudTrail Preços.

Tópicos

Para criar um armazenamento de dados de eventos de destino que registra eventos do Insights

Ao criar um armazenamento de dados de eventos do Insights, você tem a opção de escolher um armazenamento de dados de eventos de origem existente que registra os eventos de gerenciamento e, em seguida, especificar os tipos de Insights que deseja receber. Ou, como alternativa, é possível habilitar o Insights em um armazenamento de dados de eventos novo ou existente depois de criar seu armazenamento de dados de eventos do Insights e, em seguida, escolher esse armazenamento de dados de eventos como o armazenamento de dados de eventos de destino.

Este procedimento mostra como criar um armazenamento de dados de eventos de destino que registra eventos do Insights

1. Faça login no AWS Management Console e abra o CloudTrail console em https://console.aws.amazon.com/cloudtrail/.
2. No painel de navegação, abra o submenu Lake e escolha Event data stores (Armazenamentos de dados de eventos).
3. Selecione Create event data store (Criar armazenamento de dados de eventos).
4. Na página Configure event data store (Configurar armazenamento de dados de eventos), em General details (Detalhes gerais), insira um nome para o armazenamento de dados de eventos. Um nome é obrigatório.
5. Escolha a opção de preço que você deseja usar para o armazenamento de dados de eventos. A opção de preço determina o custo para a ingestão e para o armazenamento de eventos, e os períodos de retenção padrão e máximo para o armazenamento de dados de eventos. Para obter mais informações, consulte Preços do AWS CloudTrail e Gerenciando os custos CloudTrail do Lake.

   As seguintes opções estão disponíveis:

   - Preço de retenção extensível de um ano: geralmente recomendado se você espera ingerir menos de 25 TB de dados de eventos por mês e deseja um período de retenção flexível de até 10 anos. Nos primeiros 366 dias (o período de retenção padrão), o armazenamento é incluído sem custo adicional no preço de ingestão. Depois de 366 dias, a retenção estendida está disponível pelo pay-as-you-go preço. Esta é a opção padrão.
     - Período de retenção padrão: 366 dias
     - Período máximo de retenção: 3.653 dias
   - Preço de retenção de sete anos: recomendado se você espera ingerir mais de 25 TB de dados de eventos por mês e precisa de um período de retenção de até 7 anos. A retenção está incluída no preço de ingestão sem custo adicional.
     - Período de retenção padrão: 2.557 dias
     - Período máximo de retenção: 2.557 dias
6. Especifique um período de retenção para o armazenamento de dados de eventos em dias. Os períodos de retenção podem ser entre 7 dias e 3.653 dias (cerca de 10 anos) para a opção de preço de retenção extensível de um ano ou entre 7 dias e 2.557 dias (cerca de sete anos) para a opção de preço de retenção de sete anos. O armazenamento de dados de eventos retém os dados de eventos pelo número especificado de dias.
7. (Opcional) Para ativar o uso da criptografia AWS Key Management Service, escolha Usar minha própria AWS KMS key. Escolha Novo para AWS KMS key criar uma para você ou

escolha Existente para usar uma chave KMS existente. Em Inserir alias KMS, especifique um alias, no formato. `alias/ MyAliasName` Usar sua própria chave KMS exige que você edite sua política de chaves KMS para permitir que CloudTrail os registros sejam criptografados e descriptografados. Para obter mais informações, consulteConfigure as AWS KMS principais políticas para CloudTrail. CloudTrail também oferece suporte a chaves AWS KMS multirregionais. Para obter mais informações sobre chaves de várias regiões, consulte Usar chaves de várias regiões no Manual do desenvolvedor do AWS Key Management Service .

Usar sua própria chave KMS gera AWS KMS custos de criptografia e descriptografia. Após associar um armazenamento de dados de eventos a uma chave do KMS, não será possível remover ou alterar a chave do KMS.

> **Note**
>
> Para habilitar a AWS Key Management Service criptografia para um armazenamento de dados de eventos da organização, você deve usar uma chave KMS existente para a conta de gerenciamento.

8. (Opcional) Se você quiser consultar os dados do seu evento usando o Amazon Athena, escolha Habilitar na federação de consultas do Lake. A federação permite que você visualize os metadados associados ao armazenamento de dados de eventos no Catálogo de Dados do AWS Glue e execute consultas SQL nos dados do evento no Athena. Os metadados da tabela armazenados no Catálogo de AWS Glue Dados permitem que o mecanismo de consulta do Athena saiba como encontrar, ler e processar os dados que você deseja consultar. Para ter mais informações, consulte Federar um armazenamento de dados de eventos.

   Para habilitar a federação de consultas do Lake, escolha Habilitar e faça o seguinte:

   a. Escolha se deseja criar um perfil ou usar um perfil do IAM existente. O AWS Lake Formation usa esse perfil para gerenciar permissões para o armazenamento de dados de eventos federados. Quando você cria uma nova função usando o CloudTrail console, cria CloudTrail automaticamente uma função com as permissões necessárias. Se você escolher um perfil existente, a política do perfil deve fornecer as permissões mínimas necessárias.
   b. Se você estiver criando um perfil, insira um nome para identificá-lo.
   c. Se você estiver usando um perfil existente, escolha o perfilo que deseja usar. O perfil deve existir em sua conta.

9. (Opcional) Na seção Tags, é possível adicionar até 50 pares de chave de tag para ajudar a identificar, classificar e controlar o acesso ao seu armazenamento de dados de eventos. Para obter mais informações sobre como usar políticas do IAM para autorizar o acesso a um armazenamento de dados de eventos com base em tags, consulte Exemplos: negação de acesso para criar ou excluir armazenamentos de dados de eventos com base em tags. Para obter mais informações sobre como você pode usar tags em AWS, consulte Como marcar seus AWS recursos no Guia do usuário de AWS recursos de marcação.
10. Escolha Next (Avançar) para configurar o armazenamento de dados de eventos.
11. Na página Escolher eventos, escolha AWS eventos e, em seguida, escolha Eventos do CloudTrail Insights.
12. Em eventos do CloudTrail Insights, faça o seguinte.

    a. Escolha Permitir acesso de administrador delegado se quiser dar acesso ao administrador delegado da sua organização a esse armazenamento de dados de eventos. Essa opção só está disponível se você estiver conectado com a conta de gerenciamento de uma AWS Organizations organização.

    b. (Opcional) Escolha um armazenamento de dados de eventos de origem existente que registre eventos de gerenciamento e especifique os tipos de Insights que deseja receber.

       Para adicionar um armazenamento de dados de eventos de origem, faça o seguinte:

       i. Escolha Adicionar armazenamento de dados de eventos de origem.

       ii. Escolha o armazenamento de dados de eventos de origem.

       iii. Escolha o Tipo de insights que deseja receber.

       - `ApiCallRateInsight`: o tipo de insight `ApiCallRateInsight` analisa as chamadas à API de gerenciamento somente de gravação que são agregadas por minuto em relação a um volume de chamadas à API de linha de base. Para receber insights de `ApiCallRateInsight`, o armazenamento de dados de eventos de origem deve registrar os eventos de gerenciamento de gravação.
       - `ApiErrorRateInsight`: o tipo de insight `ApiErrorRateInsight` analisa as chamadas à API de gerenciamento que resultam em códigos de erro. O erro será exibido se a chamada à API não for bem-sucedida. Para receber insights de `ApiErrorRateInsight`, o armazenamento de dados de eventos de origem deve registrar os eventos de gerenciamento de gravação ou de leitura.

iv. Repita as duas etapas anteriores (ii e iii) para adicionar outros tipos de insights que você deseja receber.

13. Selecione Next (Próximo) para revisar suas escolhas.
14. Na página Review and create (Revisar e criar), revise as suas escolhas. Escolha Edit (Editar) para fazer alterações a uma seção. Quando estiver pronto para criar o armazenamento de dados de eventos, escolha Create event data store (Criar armazenamento de dados de eventos).
15. O novo armazenamento de dados de eventos está visível na tabela Armazenamentos de dados de eventos na página Armazenamento de dados de eventos.
16. Se você não escolheu um armazenamento de dados de eventos de origem na etapa 10, siga as etapas em Para criar um armazenamento de dados de eventos de origem que registra eventos do Insights para criar um armazenamento de dados de eventos de origem.

Para criar um armazenamento de dados de eventos de origem que registra eventos do Insights

Este procedimento mostra como criar um armazenamento de dados de eventos de origem que habilita eventos do Insights e registra eventos de gerenciamento.

1. Faça login no AWS Management Console e abra o CloudTrail console em https://console.aws.amazon.com/cloudtrail/.
2. No painel de navegação, abra o submenu Lake e escolha Event data stores (Armazenamentos de dados de eventos).
3. Selecione Create event data store (Criar armazenamento de dados de eventos).
4. Na página Configure event data store (Configurar armazenamento de dados de eventos), em General details (Detalhes gerais), insira um nome para o armazenamento de dados de eventos. Um nome é obrigatório.
5. Escolha a opção de preço que você deseja usar para o armazenamento de dados de eventos. A opção de preço determina o custo para a ingestão e para o armazenamento de eventos, e os períodos de retenção padrão e máximo para o armazenamento de dados de eventos. Para obter mais informações, consulte Preços do AWS CloudTrail e Gerenciando os custos CloudTrail do Lake.

   As seguintes opções estão disponíveis:

   - Preço de retenção extensível de um ano: geralmente recomendado se você espera ingerir menos de 25 TB de dados de eventos por mês e deseja um período de retenção flexível de

até 10 anos. Nos primeiros 366 dias (o período de retenção padrão), o armazenamento é incluído sem custo adicional no preço de ingestão. Depois de 366 dias, a retenção estendida está disponível pelo pay-as-you-go preço. Esta é a opção padrão.

- Período de retenção padrão: 366 dias
- Período máximo de retenção: 3.653 dias

- Preço de retenção de sete anos: recomendado se você espera ingerir mais de 25 TB de dados de eventos por mês e precisa de um período de retenção de até 7 anos. A retenção está incluída no preço de ingestão sem custo adicional.
  - Período de retenção padrão: 2.557 dias
  - Período máximo de retenção: 2.557 dias

6. Especifique um período de retenção para o armazenamento de dados de eventos. Os períodos de retenção podem ser entre 7 dias e 3.653 dias (cerca de 10 anos) para a opção de preço de retenção extensível de um ano ou entre 7 dias e 2.557 dias (cerca de sete anos) para a opção de preço de retenção de sete anos.

   CloudTrail Lake determina se deve reter um evento verificando se o `eventTime` evento está dentro do período de retenção especificado. Por exemplo, se você especificar um período de retenção de 90 dias, CloudTrail removerá eventos quando tiverem `eventTime` mais de 90 dias.

7. (Opcional) Para ativar o uso da criptografia AWS Key Management Service, escolha Usar minha própria AWS KMS key. Escolha Novo para AWS KMS key criar uma para você ou escolha Existente para usar uma chave KMS existente. Em Inserir alias KMS, especifique um alias, no formato. `alias/` *`MyAliasName`* Usar sua própria chave KMS exige que você edite sua política de chaves KMS para permitir que CloudTrail os registros sejam criptografados e descriptografados. Para obter mais informações, consulteConfigure as AWS KMS principais políticas para CloudTrail. CloudTrail também oferece suporte a chaves AWS KMS multirregionais. Para obter mais informações sobre chaves de várias regiões, consulte Usar chaves de várias regiões no Manual do desenvolvedor do AWS Key Management Service .

   Usar sua própria chave KMS gera AWS KMS custos de criptografia e descriptografia. Após associar um armazenamento de dados de eventos a uma chave do KMS, não será possível remover ou alterar a chave do KMS.

> **Note**
>
> Para habilitar a AWS Key Management Service criptografia para um armazenamento de dados de eventos da organização, você deve usar uma chave KMS existente para a conta de gerenciamento.

8. (Opcional) Se você quiser consultar os dados do seu evento usando o Amazon Athena, escolha Habilitar na federação de consultas do Lake. A federação permite que você visualize os metadados associados ao armazenamento de dados de eventos no Catálogo de Dados do AWS Glue e execute consultas SQL nos dados do evento no Athena. Os metadados da tabela armazenados no Catálogo de AWS Glue Dados permitem que o mecanismo de consulta do Athena saiba como encontrar, ler e processar os dados que você deseja consultar. Para ter mais informações, consulte Federar um armazenamento de dados de eventos.

   Para habilitar a federação de consultas do Lake, escolha Habilitar e faça o seguinte:

   a. Escolha se deseja criar um perfil ou usar um perfil do IAM existente. O AWS Lake Formation usa esse perfil para gerenciar permissões para o armazenamento de dados de eventos federados. Quando você cria uma nova função usando o CloudTrail console, cria CloudTrail automaticamente uma função com as permissões necessárias. Se você escolher um perfil existente, a política do perfil deve fornecer as permissões mínimas necessárias.

   b. Se você estiver criando um perfil, insira um nome para identificá-lo.

   c. Se você estiver usando um perfil existente, escolha o perfilo que deseja usar. O perfil deve existir em sua conta.

9. (Opcional) Na seção Tags, é possível adicionar até 50 pares de chave de tag para ajudar a identificar, classificar e controlar o acesso ao seu armazenamento de dados de eventos. Para obter mais informações sobre como usar políticas do IAM para autorizar o acesso a um armazenamento de dados de eventos com base em tags, consulte Exemplos: negação de acesso para criar ou excluir armazenamentos de dados de eventos com base em tags. Para obter mais informações sobre como você pode usar tags em AWS, consulte Como marcar seus AWS recursos no Guia do usuário de AWS recursos de marcação.

10. Escolha Next (Avançar) para configurar o armazenamento de dados de eventos.

11. Na página Escolher eventos, escolha AWS eventos e, em seguida, escolha CloudTraileventos.

12. Em CloudTrail eventos, deixe a opção Eventos de gerenciamento selecionada.

13. Para que o armazenamento de dados do seu evento colete eventos de todas as contas em uma organização do AWS Organizations , selecione Enable for all accounts in my organization (Habilitar para todas as contas na minha organização). Você deve estar conectado à conta de gerenciamento da organização para criar um armazenamento de dados de eventos que habilite o Insights.
14. Expanda Configurações adicionais para escolher se você deseja que seu armazenamento de dados de eventos colete eventos para todos Regiões da AWS ou somente para os atuais Região da AWS, e escolha se o armazenamento de dados de eventos ingere eventos. Por padrão, seu armazenamento de dados de eventos coleta eventos de todas as regiões em sua conta e começa a ingerir eventos ao ser criado.

    a. Opcionalmente, selecione Incluir somente a região atual no meu armazenamento de dados de eventos para incluir somente eventos que são registrados em log na região atual. Se você não escolher essa opção, o armazenamento de dados de eventos incluirá eventos de todas as regiões.

    b. Mantenha a opção Ingerir eventos selecionada.
15. Escolha o tipo dos eventos de gerenciamento que você deseja incluir em seu armazenamento de dados de eventos. É possível escolher Ler, Gravar ou ambas. Pelo menos um é necessário.

    > **Note**
    >
    > Para registrar em log eventos do Insights sobre o volume de chamadas à API, o armazenamento de dados de eventos deve registrar em log os eventos de gerenciamento de `write`. Para registrar em log eventos do Insights sobre a taxa de erros da API, o armazenamento de dados de eventos deve registrar em log os eventos de gerenciamento de `read` ou `write`.
16. Você pode optar por excluir AWS Key Management Service ou excluir eventos da Amazon RDS Data API do seu armazenamento de dados de eventos. Para obter mais informações sobre essas opções, consulte Log de eventos de gerenciamento.
17. Escolha Habilitar Insights.
18. Em Habilitar Insights, escolha o armazenamento de dados de eventos de destino que registrará os eventos do Insights. O armazenamento de dados de eventos de destino coletará eventos do Insights com base na atividade de gerenciamento de eventos nesse armazenamento de dados de eventos. Para obter informações sobre como criar o armazenamento de dados de eventos

de destino, consulte Para criar um armazenamento de dados de eventos de destino que registra eventos do Insights.

19. Escolha os tipos de Insights. É possível escolher a Taxa de chamadas à API, a Taxa de erros da API ou ambas. Você deve registrar eventos de gerenciamento de gravação para registrar em log eventos do Insights sobre a taxa de chamadas à API. É necessário registrar eventos de gerenciamento de leitura ou gravação para registrar em log eventos do Insights sobre a taxa de erros da API.
20. Selecione Next (Próximo) para revisar suas escolhas.
21. Na página Review and create (Revisar e criar), revise as suas escolhas. Escolha Edit (Editar) para fazer alterações a uma seção. Quando estiver pronto para criar o armazenamento de dados de eventos, escolha Create event data store (Criar armazenamento de dados de eventos).
22. O novo armazenamento de dados de eventos está visível na tabela Armazenamentos de dados de eventos na página Armazenamento de dados de eventos.

    Deste ponto em diante, o armazenamento de dados de eventos captura eventos que correspondem aos seletores de eventos avançados. Depois de ativar o CloudTrail Insights pela primeira vez em seu armazenamento de dados de eventos de origem, pode levar até 7 dias CloudTrail para entregar o primeiro evento do Insights ao armazenamento de dados de eventos de destino, se uma atividade incomum for detectada.

    Você pode visualizar o painel do CloudTrail Lake para visualizar os eventos do Insights em seu armazenamento de dados de eventos de destino. Para obter mais informações sobre painéis do Lake, consulte Veja os painéis CloudTrail do Lake.

Cobranças adicionais se aplicam à ingestão de eventos do Insights em CloudTrail Lake. Você será cobrado separadamente se ativar o Insights tanto para trilhas quanto para armazenamentos de dados de eventos. Para obter informações sobre CloudTrail preços, consulte AWS CloudTrail Preços.

Crie um armazenamento de dados de eventos para itens de AWS Config configuração com o console

É possível criar um armazenamento de dados de eventos para incluir itens de configuração do AWS Config e usar o armazenamento de dados de eventos para investigar alterações não compatíveis em seus ambientes de produção. Com um armazenamento de dados de eventos, é possível relacionar regras fora de conformidade a usuários e recursos associados às mudanças. Um item de

configuração representa uma point-in-time visualização dos atributos de um AWS recurso compatível que existe em sua conta. AWS Config cria um item de configuração sempre que detecta uma alteração em um tipo de recurso que está gravando. AWS Config também cria itens de configuração quando um instantâneo de configuração é capturado.

Você pode usar ambos AWS Config e o CloudTrail Lake para executar consultas em seus itens de configuração. Você pode usar AWS Config para consultar o estado atual da configuração dos AWS recursos com base nas propriedades de configuração de uma única Conta da AWS conta e/ou de várias contas e regiões. Região da AWS Por outro lado, você pode usar o CloudTrail Lake para consultar diversas fontes de dados, como CloudTrail eventos, itens de configuração e avaliações de regras. CloudTrail As consultas do Lake abrangem todos os itens AWS Config de configuração, incluindo configuração de recursos e histórico de conformidade.

A criação de um armazenamento de dados de eventos para itens de configuração não afeta as consultas AWS Config avançadas existentes nem os AWS Config agregadores configurados. Você pode continuar executando consultas avançadas usando AWS Config e AWS Config entregando arquivos de histórico para seus buckets do S3.

CloudTrail Os armazenamentos de dados de eventos em Lake incorrem em cobranças. Ao criar um armazenamento de dados de eventos, você escolhe a opção de preço que deseja usar para ele. A opção de preço determina o custo para a ingestão e para o armazenamento de eventos, e o período de retenção padrão e máximo para o armazenamento de dados de eventos. Para obter informações sobre CloudTrail preços e gerenciamento de custos do Lake, consulte AWS CloudTrail Preços Gerenciando os custos CloudTrail do Lake e.

Limitações

As limitações a seguir são aplicáveis aos armazenamentos de dados de eventos para itens de configuração.

- Não há compatibilidade com itens de configuração personalizados
- Não há compatibilidade com filtragem de eventos usando seletores de eventos avançados

Pré-requisitos

Antes de criar seu armazenamento de dados de eventos, configure a AWS Config gravação para todas as suas contas e regiões. Você pode usar a Configuração Rápida, um recurso do AWS Systems Manager, para criar rapidamente um gravador de configuração alimentado por AWS Config.

> **Note**
>
> Você paga taxas de uso do serviço quando AWS Config inicia a gravação das configurações. Para obter mais informações sobre precificação, consulte Precificação do AWS Config. Para obter mais informações sobre como gerenciar o gravador de configuração, consulte Managing the Configuration Recorder (Gerenciar o gravador de configurações) no Guia do desenvolvedor do AWS Config .

Além disso, as seguintes ações são recomendadas, mas não são necessárias para criar um armazenamento de dados de eventos.

- Configure um bucket do Amazon S3 para receber um snapshot de configuração mediante solicitação e o histórico de configuração. Para obter mais informações sobre snapshots, consulte Managing the Delivery Channel (Gerenciar o canal de entrega) e Delivering Configuration Snapshot to an Amazon S3 Bucket (Entrega de snapshot de configuração para um bucket do Amazon S3) no Guia do desenvolvedor do AWS Config .
- Especifique as regras que você deseja usar AWS Config para avaliar as informações de conformidade dos tipos de recursos registrados. Vários exemplos de consultas do CloudTrail Lake AWS Config exigem Regras do AWS Config a avaliação do estado de conformidade de seus AWS recursos. Para obter mais informações sobre Regras do AWS Config, consulte Avaliação de recursos Regras do AWS Config no Guia do AWS Config desenvolvedor.

Para criar um armazenamento de dados de eventos para itens de configuração

1. Faça login no AWS Management Console e abra o CloudTrail console em https://console.aws.amazon.com/cloudtrail/.
2. No painel de navegação, em Lake, escolha Armazenamentos de dados de eventos.
3. Selecione Create event data store (Criar armazenamento de dados de eventos).
4. Na página Configure event data store (Configurar armazenamento de dados de eventos), em General details (Detalhes gerais), insira um nome para o armazenamento de dados de eventos. Um nome é obrigatório.
5. Escolha a opção de preço que você deseja usar para o armazenamento de dados de eventos. A opção de preço determina o custo para a ingestão e para o armazenamento de eventos, e os períodos de retenção padrão e máximo para o armazenamento de dados de eventos. Para obter

mais informações, consulte Preços do AWS CloudTrail e Gerenciando os custos CloudTrail do Lake.

As seguintes opções estão disponíveis:

- Preço de retenção extensível de um ano: geralmente recomendado se você espera ingerir menos de 25 TB de dados de eventos por mês e deseja um período de retenção flexível de até 10 anos. Nos primeiros 366 dias (o período de retenção padrão), o armazenamento é incluído sem custo adicional no preço de ingestão. Depois de 366 dias, a retenção estendida está disponível pelo pay-as-you-go preço. Esta é a opção padrão.
  - Período de retenção padrão: 366 dias
  - Período máximo de retenção: 3.653 dias
- Preço de retenção de sete anos: recomendado se você espera ingerir mais de 25 TB de dados de eventos por mês e precisa de um período de retenção de até 7 anos. A retenção está incluída no preço de ingestão sem custo adicional.
  - Período de retenção padrão: 2.557 dias
  - Período máximo de retenção: 2.557 dias

6. Especifique um período de retenção para o armazenamento de dados de eventos. Os períodos de retenção podem ser entre 7 dias e 3.653 dias (cerca de 10 anos) para a opção de preço de retenção extensível de um ano ou entre 7 dias e 2.557 dias (cerca de sete anos) para a opção de preço de retenção de sete anos.

   CloudTrail Lake determina se deve reter um evento verificando se o `eventTime` evento está dentro do período de retenção especificado. Por exemplo, se você especificar um período de retenção de 90 dias, CloudTrail removerá eventos quando tiverem `eventTime` mais de 90 dias.

7. (Opcional) Para ativar o uso da criptografia AWS Key Management Service, escolha Usar minha própria AWS KMS key. Escolha Novo para AWS KMS key criar uma para você ou escolha Existente para usar uma chave KMS existente. Em Inserir alias KMS, especifique um alias, no formato. `alias/` *`MyAliasName`* Usar sua própria chave KMS exige que você edite sua política de chaves KMS para permitir que CloudTrail os registros sejam criptografados e descriptografados. Para obter mais informações, consulteConfigure as AWS KMS principais políticas para CloudTrail. CloudTrail também oferece suporte a chaves AWS KMS multirregionais. Para obter mais informações sobre chaves de várias regiões, consulte Usar chaves de várias regiões no Manual do desenvolvedor do AWS Key Management Service .

Usar sua própria chave KMS gera AWS KMS custos de criptografia e descriptografia. Após associar um armazenamento de dados de eventos a uma chave do KMS, não será possível remover ou alterar a chave do KMS.

> **Note**
>
> Para habilitar a AWS Key Management Service criptografia para um armazenamento de dados de eventos da organização, você deve usar uma chave KMS existente para a conta de gerenciamento.

8. (Opcional) Se você quiser consultar os dados do seu evento usando o Amazon Athena, escolha Habilitar na federação de consultas do Lake. A federação permite que você visualize os metadados associados ao armazenamento de dados de eventos no Catálogo de Dados do AWS Glue e execute consultas SQL nos dados do evento no Athena. Os metadados da tabela armazenados no Catálogo de AWS Glue Dados permitem que o mecanismo de consulta do Athena saiba como encontrar, ler e processar os dados que você deseja consultar. Para ter mais informações, consulte Federar um armazenamento de dados de eventos.

   Para habilitar a federação de consultas do Lake, escolha Habilitar e faça o seguinte:

   a. Escolha se deseja criar um perfil ou usar um perfil do IAM existente. O AWS Lake Formation usa esse perfil para gerenciar permissões para o armazenamento de dados de eventos federados. Quando você cria uma nova função usando o CloudTrail console, cria CloudTrail automaticamente uma função com as permissões necessárias. Se você escolher um perfil existente, a política do perfil deve fornecer as permissões mínimas necessárias.

   b. Se você estiver criando um perfil, insira um nome para identificá-lo.

   c. Se você estiver usando um perfil existente, escolha o perfilo que deseja usar. O perfil deve existir em sua conta.

9. (Opcional) Na seção Tags, é possível adicionar até 50 pares de chave de tag para ajudar a identificar, classificar e controlar o acesso ao seu armazenamento de dados de eventos. Para obter mais informações sobre como usar políticas do IAM para autorizar o acesso a um armazenamento de dados de eventos com base em tags, consulte Exemplos: negação de acesso para criar ou excluir armazenamentos de dados de eventos com base em tags. Para obter mais informações sobre como você pode usar tags em AWS, consulte Como marcar seus AWS recursos no Guia do usuário de AWS recursos de marcação.

10. Escolha Próximo.

11. Na página Escolher eventos, escolha Eventos da AWS e, em seguida, Itens de configuração.
12. CloudTrail armazena o recurso de armazenamento de dados de eventos na região em que você o criou, mas, por padrão, os itens de configuração coletados no armazenamento de dados são de todas as regiões da sua conta que têm a gravação ativada. Opcionalmente, selecione Include only the current region in my event data store (Incluir somente a região atual no armazenamento de dados do meu evento) para incluir somente itens de configuração que sejam capturados na região atual. Se você não escolher essa opção, o armazenamento de dados de eventos incluirá itens de configuração de todas as regiões que estejam com a gravação habilitada.
13. Para que seu armazenamento de dados de eventos colete itens de configuração de todas as contas em uma AWS Organizations organização, selecione Habilitar para todas as contas em minha organização. É necessário estar conectado à conta de gerenciamento da organização ou à conta de administrador delegado para criar um armazenamento de dados de eventos que colete itens de configuração de uma organização.
14. Selecione Next (Próximo) para revisar suas escolhas.
15. Na página Review and create (Revisar e criar), revise as suas escolhas. Escolha Edit (Editar) para fazer alterações a uma seção. Quando estiver pronto para criar o armazenamento de dados de eventos, escolha Create event data store (Criar armazenamento de dados de eventos).
16. O novo armazenamento de dados de eventos está visível na tabela Armazenamentos de dados de eventos na página Armazenamento de dados de eventos.

    Deste ponto em diante, o armazenamento de dados de eventos capturará itens de configuração. Os itens de configuração que tenham ocorrido antes de você criar o armazenamento de dados de eventos não estarão no armazenamento de dados de eventos.

Consultas de exemplo

Agora, você pode executar consultas no novo armazenamento de dados de eventos. A guia Exemplos de consultas no CloudTrail console fornece exemplos de consultas para você começar. A seguir estão alguns exemplos de consultas que você pode executar em seu armazenamento de dados de eventos de itens de configuração.

Descrição	Consulta
Descubra qual usuário executou uma ação que resultou em um status de não conformid	`SELECT`

Descrição	Consulta
ade unindo um armazenamento de dados de eventos de item de configuração a um armazenamento de dados de CloudTrail eventos.	`element_at(config1.eventDat a.configuration, 'targetResourceId') as targetResourceId, element_at(config1.eventDat a.configuration, 'complianceType') as complianceType, config2.eventData.resourceType, cloudtrail.userIdentity FROM config_event_data_store_ID as config1 JOIN config_event_data_store_ID as config2 on element_at(config1 .eventData.configuration, 'targetRe sourceId') = config2.eventData. resourceId JOIN cloudtrail_event_data_store_ID as cloudtrail on config2.eventData. arn = element_at(cloudtrail.resou rces, 1).arn WHERE element_at(config1.eventDat a.configuration, 'configRuleList') is not null AND element_at(config1.eventDat a.configuration, 'complianceType') = 'NON_COMPLIANT' AND cloudtrail.eventTime > '2022-11- 14 00:00:00' AND config2.eventData.resourceType = 'AWS::DynamoDB::Table'`

Descrição	Consulta
Encontre todas AWS Config as regras e retorne o estado de conformidade dos itens de configuração gerados no dia anterior.	`SELECT eventData.configuration, eventData.accountId, eventData.awsRegion, eventData.resourceName, eventData.resourceCreationTime, element_at(eventData.configuration,'complianceType') AS complianceType, element_at(eventData.configuration, 'configRuleList') AS configRuleList, element_at(eventData.configuration, 'resourceId') AS resourceId, element_at(eventData.configuration, 'resourceType') AS resourceType FROM config_event_data_store_ID WHERE eventData.resourceType = 'AWS::Config::ResourceCompliance' AND eventTime > '2022-11-22 00:00:00' ORDER BY eventData.resourceCreationTime DESC limit 10`

Descrição	Consulta

Encontre a contagem total de AWS Config recursos agrupados por tipo de recurso, ID da conta e região.	`SELECT`
	`    eventData.resourceType, eventData`
	`.awsRegion, eventData.accountId,`
	`COUNT (*) AS resourceCount`
	`FROM`
	`    config_event_data_store_ID`
	`WHERE`
	`    eventTime > '2022-11-22 00:00:00'`
	`GROUP BY`
	`    eventData.resourceType, eventData`
	`.awsRegion, eventData.accountId`

Encontre o horário de criação do recurso para todos os itens de AWS Config configuração gerados em uma data específica.	`SELECT`
	`    eventData.configuration,`
	` eventData.accountId,`
	`    eventData.awsRegion, eventData`
	`.resourceId,`
	`    eventData.resourceName, eventData`
	`.resourceType,`
	`    eventData.availabilityZone,`
	` eventData.resourceCreationTime`
	`FROM`
	`    config_event_data_store_ID`
	`WHERE`
	`    eventTime > '2022-11-16 00:00:00'`
	`AND`
	`    eventTime < '2022-11-17 00:00:00'`
	
	`ORDER BY`
	`    eventData.resourceCreationTime`
	`DESC`
	`    limit 10;`

Para obter mais informações sobre como criar e editar consultas, veja Criar ou editar uma consulta.

Esquema de item de configuração

A tabela a seguir descreve os elementos obrigatórios e opcionais de esquema que correspondem aos elementos dos registros de itens de configuração. O conteúdo de `eventData` é fornecido por seus itens de configuração; outros campos são fornecidos CloudTrail após a ingestão.

CloudTrail o conteúdo do registro de eventos é descrito com mais detalhes emCloudTrail conteúdo do registro.

- Campos que são fornecidos por CloudTrail após a ingestão
- Campos que são fornecidos por seus eventos

Campos que são fornecidos por CloudTrail após a ingestão

Nome do campo	Tipo de entrada	Requisito	Descrição
eventVersion	string	Obrigatório	A versão do formato do AWS evento.
eventCategory	string	Obrigatório	A categoria do evento. Para itens de configuração, o valor válido é `ConfigurationItem` .
eventType	string	Obrigatório	O tipo de evento. Para itens de configuração, o valor válido é `AwsConfigurationItem` .
eventID	string	Obrigatório	Um ID exclusivo para um evento.
eventTime	string	Obrigatório	O carimbo de data e hora do evento, em formato `yyyy-MM-DDTHH:mm:ss` , em

Nome do campo	Tipo de entrada	Requisito	Descrição
			Universal Coordinated Time (UTC – Tempo universal coordenado).
awsRegion	string	Obrigatório	O Região da AWS ao qual atribuir um evento.
recipientAccountId	string	Obrigatório	Representa o Conta da AWS ID que recebeu esse evento.
addendum	addendum	Opcional	Mostra informações sobre o motivo de adiamento de um evento. Se as informações estiverem ausentes de um evento existente, o bloco de adendo incluirá as informações ausentes e um motivo pelo qual elas estavam ausentes.

Os campos em **`eventData`** são fornecidos por seus itens de configuração

Nome do campo	Tipo de entrada	Requisito	Descrição
eventData	-	Obrigatório	Os campos em eventData são fornecidos por seus itens de configuração.

Nome do campo	Tipo de entrada	Requisito	Descrição
• configurationItemVersion	string	Opcional	A versão do item de configuração com base em sua origem.
• configurationItemCaptureHora	string	Opcional	A hora em que a gravação da configuração foi iniciada.
• configurationItemStatus	string	Opcional	O status do item de configuração. Os valores válidos são `OK`, `ResourceDiscovered`, `ResourceNotRecorded`, `ResourceDeleted` e `ResourceDeletedNotRecorded`.
• accountId	string	Opcional	O Conta da AWS ID de 12 dígitos associado ao recurso.
• resourceType	string	Opcional	O tipo de AWS recurso. Para obter mais informações sobre tipos de recursos válidos, consulte ConfigurationItem a Referência AWS Config da API.
• resourceId	string	Opcional	O ID do recurso (p. ex., sg-*xxxxxx*).

Nome do campo	Tipo de entrada	Requisito	Descrição
• resourceName	string	Opcional	O nome personalizado do recurso, se disponível.
• arn	string	Opcional	O nome do recurso da Amazon (ARN) associado ao recurso.
• awsRegion	string	Opcional	O Região da AWS local onde o recurso reside.
• availabilityZone	string	Opcional	A zona de disponibilidade associada ao recurso.
• resourceCreationTime	string	Opcional	O carimbo de data e hora de criação do recurso.
• configuration	JSON	Opcional	A descrição da configuração do recurso.
• supplementaryConfiguration	JSON	Opcional	Atributos de configuração que AWS Config retornam para determinados tipos de recursos para complementar as informações retornadas para o parâmetro de configuração.

Nome do campo	Tipo de entrada	Requisito	Descrição
• relatedEvents	string	Opcional	Uma lista de IDs de CloudTrail eventos.
• relationships	-	Opcional	Uma lista de AWS recursos relaciona dos.
• • name	string	Opcional	O tipo de relaciona mento com o recurso relacionado.
• • resourceType	string	Opcional	O tipo de recurso do recurso relacionado.
• • resourceId	string	Opcional	O ID do recurso relacionado (p. ex., sg-*xxxxxx*).
• • resourceName	string	Opcional	O nome personali zado do recurso relacionado, se disponível.
• tags	JSON	Opcional	Um mapeamento das tags de valor de chave associadas ao recurso.

O exemplo a seguir mostra a hierarquia dos elementos de esquema que correspondem aos dos registros de itens de configuração.

```
{
  "eventVersion": String,
  "eventCategory: String,
  "eventType": String,
  "eventID": String,
  "eventTime": String,
```

```
  "awsRegion": String,
  "recipientAccountId": String,
  "addendum": Addendum,
  "eventData": {
      "configurationItemVersion": String,
      "configurationItemCaptureTime": String,
      "configurationItemStatus": String,
      "configurationStateId": String,
      "accountId": String,
      "resourceType": String,
      "resourceId": String,
      "resourceName": String,
      "arn": String,
      "awsRegion": String,
      "availabilityZone": String,
      "resourceCreationTime": String,
      "configuration": {
        JSON,
      },
      "supplementaryConfiguration": {
        JSON,
      },
      "relatedEvents": [
        String
      ],
      "relationships": [
        struct{
          "name" : String,
          "resourceType": String,
          "resourceId": String,
          "resourceName": String
        }
      ],
     "tags": {
       JSON
     }
    }
  }
}
```

Crie um armazenamento de dados de eventos para eventos externos AWS com o console

Você pode criar um armazenamento de dados de eventos para incluir eventos externos e AWS, em seguida, usar o CloudTrail Lake para pesquisar, consultar e analisar os dados que são registrados em seus aplicativos.

Você pode usar as integrações do CloudTrail Lake para registrar e armazenar dados de atividades do usuário de fora de AWS; de qualquer fonte em seus ambientes híbridos, como aplicativos internos ou SaaS hospedados no local ou na nuvem, máquinas virtuais ou contêineres.

Ao criar um armazenamento de dados de eventos para uma integração, você também cria um canal e anexa uma política de recursos ao canal.

CloudTrail Os armazenamentos de dados de eventos em Lake incorrem em cobranças. Ao criar um armazenamento de dados de eventos, você escolhe a opção de preço que deseja usar para ele. A opção de preço determina o custo para a ingestão e para o armazenamento de eventos, e o período de retenção padrão e máximo para o armazenamento de dados de eventos. Para obter informações sobre CloudTrail preços e gerenciamento de custos do Lake, consulte AWS CloudTrail Preços Gerenciando os custos CloudTrail do Lake e.

Para criar um armazenamento de dados de eventos para eventos fora do AWS

1. Faça login no AWS Management Console e abra o CloudTrail console em https://console.aws.amazon.com/cloudtrail/.
2. No painel de navegação, em Lake, escolha Armazenamentos de dados de eventos.
3. Selecione Create event data store (Criar armazenamento de dados de eventos).
4. Na página Configure event data store (Configurar armazenamento de dados de eventos), em General details (Detalhes gerais), insira um nome para o armazenamento de dados de eventos. Um nome é obrigatório.
5. Escolha a opção de preço que você deseja usar para o armazenamento de dados de eventos. A opção de preço determina o custo para a ingestão e para o armazenamento de eventos, e os períodos de retenção padrão e máximo para o armazenamento de dados de eventos. Para obter mais informações, consulte Preços do AWS CloudTrail e Gerenciando os custos CloudTrail do Lake.

   As seguintes opções estão disponíveis:

- Preço de retenção extensível de um ano: geralmente recomendado se você espera ingerir menos de 25 TB de dados de eventos por mês e deseja um período de retenção flexível de até 10 anos. Nos primeiros 366 dias (o período de retenção padrão), o armazenamento é incluído sem custo adicional no preço de ingestão. Depois de 366 dias, a retenção estendida está disponível pelo pay-as-you-go preço. Esta é a opção padrão.
  - Período de retenção padrão: 366 dias
  - Período máximo de retenção: 3.653 dias
- Preço de retenção de sete anos: recomendado se você espera ingerir mais de 25 TB de dados de eventos por mês e precisa de um período de retenção de até 7 anos. A retenção está incluída no preço de ingestão sem custo adicional.
  - Período de retenção padrão: 2.557 dias
  - Período máximo de retenção: 2.557 dias

6. Especifique um período de retenção para o armazenamento de dados de eventos. Os períodos de retenção podem ser entre 7 dias e 3.653 dias (cerca de 10 anos) para a opção de preço de retenção extensível de um ano ou entre 7 dias e 2.557 dias (cerca de sete anos) para a opção de preço de retenção de sete anos.

   CloudTrail Lake determina se deve reter um evento verificando se o `eventTime` evento está dentro do período de retenção especificado. Por exemplo, se você especificar um período de retenção de 90 dias, CloudTrail removerá eventos quando tiverem `eventTime` mais de 90 dias.

7. (Opcional) Para ativar o uso da criptografia AWS Key Management Service, escolha Usar minha própria AWS KMS key. Escolha Novo para AWS KMS key criar uma para você ou escolha Existente para usar uma chave KMS existente. Em Inserir alias KMS, especifique um alias, no formato. `alias/` *`MyAliasName`* Usar sua própria chave KMS exige que você edite sua política de chaves KMS para permitir que CloudTrail os registros sejam criptografados e descriptografados. Para obter mais informações, consulteConfigure as AWS KMS principais políticas para CloudTrail. CloudTrail também oferece suporte a chaves AWS KMS multirregionais. Para obter mais informações sobre chaves de várias regiões, consulte Usar chaves de várias regiões no Manual do desenvolvedor do AWS Key Management Service .

   Usar sua própria chave KMS gera AWS KMS custos de criptografia e descriptografia. Após associar um armazenamento de dados de eventos a uma chave do KMS, não será possível remover ou alterar a chave do KMS.

> **Note**
>
> Para habilitar a AWS Key Management Service criptografia para um armazenamento de dados de eventos da organização, você deve usar uma chave KMS existente para a conta de gerenciamento.

8. (Opcional) Se você quiser consultar os dados do seu evento usando o Amazon Athena, escolha Habilitar na federação de consultas do Lake. A federação permite que você visualize os metadados associados ao armazenamento de dados de eventos no Catálogo de Dados do AWS Glue e execute consultas SQL nos dados do evento no Athena. Os metadados da tabela armazenados no Catálogo de AWS Glue Dados permitem que o mecanismo de consulta do Athena saiba como encontrar, ler e processar os dados que você deseja consultar. Para ter mais informações, consulte Federar um armazenamento de dados de eventos.

   Para habilitar a federação de consultas do Lake, escolha Habilitar e faça o seguinte:

   a. Escolha se deseja criar um perfil ou usar um perfil do IAM existente. O AWS Lake Formation usa esse perfil para gerenciar permissões para o armazenamento de dados de eventos federados. Quando você cria uma nova função usando o CloudTrail console, cria CloudTrail automaticamente uma função com as permissões necessárias. Se você escolher um perfil existente, a política do perfil deve fornecer as permissões mínimas necessárias.

   b. Se você estiver criando um perfil, insira um nome para identificá-lo.

   c. Se você estiver usando um perfil existente, escolha o perfilo que deseja usar. O perfil deve existir em sua conta.

9. (Opcional) Na seção Tags, é possível adicionar até 50 pares de chave de tag para ajudar a identificar, classificar e controlar o acesso ao seu armazenamento de dados de eventos. Para obter mais informações sobre como usar políticas do IAM para autorizar o acesso a um armazenamento de dados de eventos com base em tags, consulte Exemplos: negação de acesso para criar ou excluir armazenamentos de dados de eventos com base em tags. Para obter mais informações sobre como você pode usar tags em AWS, consulte Como marcar seus AWS recursos no Guia do usuário de AWS recursos de marcação.

10. Escolha Next (Avançar) para configurar o armazenamento de dados de eventos.

11. Na página Choose events (Escolher eventos), escolha Events from integrations (Eventos de integrações).

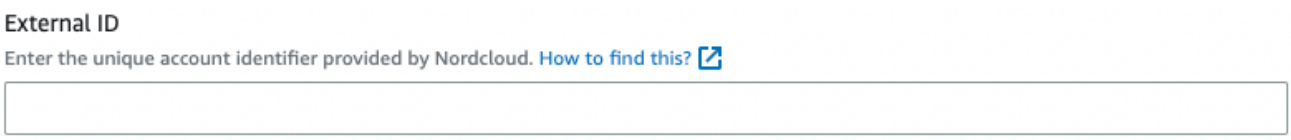
12. Em Events from integration (Eventos de integração), escolha a fonte para entregar os eventos ao armazenamento de dados do evento.
13. Forneça um nome para identificar o canal de integração. O nome pode ter de 3 a 128 caracteres. São permitidas apenas letras, números, pontos, traços e sublinhados.
14. Em Resource policy (Política de recursos), configure a política de recursos para o canal de integração. As políticas de recursos são documentos de políticas em JSON que especificam quais ações uma entidade principal pode executar no recurso e sob quais condições. As contas definidas como entidades principais na política de recursos podem chamar a API `PutAuditEvents` para entregar eventos ao seu canal. O proprietário do recurso tem acesso implícito ao recurso se sua política do IAM permitir a ação `cloudtrail-data:PutAuditEvents`.

    As informações necessárias para a política são determinadas pelo tipo de integração. Para uma integração de direção, adiciona CloudTrail automaticamente os IDs da AWS conta do parceiro e exige que você insira o ID externo exclusivo fornecido pelo parceiro. Para uma integração de soluções, você deve especificar pelo menos uma ID de AWS conta como principal e, opcionalmente, inserir uma ID externa para evitar confusões entre representantes.

    > **Note**
    >
    > Se não for criada uma política de recursos para o canal, somente o proprietário do canal poderá chamar a API `PutAuditEvents` no canal.

    a. Para uma integração direta, insira o ID externo fornecido pelo seu parceiro. O parceiro de integração fornece um ID externo exclusivo, como um ID de conta ou uma string gerada aleatoriamente, para usar na integração e evitar o “confused deputy”. O parceiro é responsável por criar e fornecer um ID externo exclusivo.

    É possível escolher How to find this? (Como encontrar isso?) para ver a documentação do parceiro que descreva como encontrar o ID externo.

> **Note**
>
> Se a política de recursos incluir um ID externo, todas as chamadas para a API `PutAuditEvents` deverão incluir o ID externo. No entanto, se a política não definir um ID externo, o parceiro ainda poderá chamar a API `PutAuditEvents` e especificar um parâmetro `externalId`.

b. Para uma integração de soluções, escolha Adicionar AWS conta para especificar cada ID de AWS conta a ser adicionada como principal na política.

15. Selecione Next (Próximo) para revisar suas escolhas.
16. Na página Review and create (Revisar e criar), revise as suas escolhas. Escolha Edit (Editar) para fazer alterações a uma seção. Quando estiver pronto para criar o armazenamento de dados de eventos, escolha Create event data store (Criar armazenamento de dados de eventos).
17. O novo armazenamento de dados de eventos está visível na tabela Armazenamentos de dados de eventos na página Armazenamento de dados de eventos.
18. Forneça o nome do recurso da Amazon (ARN) do canal para a aplicação do parceiro. As instruções para fornecer o ARN do canal para a aplicação do parceiro estão no site de documentação do parceiro. Para obter mais informações, escolha o link Learn more (Saiba mais) para o parceiro na guia Available sources (Fontes disponíveis) da página Integrations (Integrações) para abrir a página do parceiro no AWS Marketplace.

O armazenamento de dados de eventos começa a ingerir eventos de parceiros CloudTrail por meio do canal de integração quando você, o parceiro ou os aplicativos parceiros chamam a `PutAuditEvents` API no canal.

Atualizar um armazenamento de dados de eventos com o console

Esta seção descreve como atualizar as configurações do armazenamento de dados de eventos usando o AWS Management Console. Para obter informações sobre como atualizar um armazenamento de dados de AWS CLI eventos usando Atualize um armazenamento de dados de eventos com o AWS CLI o.

Atualizar um armazenamento de dados de eventos

1. Faça login no AWS Management Console e abra o CloudTrail console em https://console.aws.amazon.com/cloudtrail/.
2. No painel de navegação, em Lake, escolha Armazenamentos de dados de eventos.
3. Selecione o armazenamento de dados de eventos que você deseja atualizar. Essa ação abre a página de detalhes do armazenamento de dados de eventos.
4. Em Detalhes gerais, escolha Editar para alterar as configurações a seguir:

   - Nome do armazenamento de dados de eventos: altere o nome que identifica seu armazenamento de dados de eventos.
   - Opção de preço : para armazenamentos de dados de eventos que usam a opção de preço de retenção de sete anos, você pode optar por usar o preço de retenção extensível de um ano. Recomendamos preços de retenção extensíveis de um ano para armazenamentos de dados de eventos que ingerem menos de 25 TB de dados de eventos mensalmente. Também recomendamos um preço de retenção extensível de um ano se você estiver buscando um período de retenção flexível de até 10 anos. Para obter mais informações, consulte Preços do AWS CloudTrail e Gerenciando os custos CloudTrail do Lake.

     > **Note**
     >
     > Você não pode alterar a opção de preço para armazenamentos de dados de eventos que usam preços de retenção extensíveis por um ano. Se você quiser usar o preço de retenção de sete anos, interrompa a ingestão em seu armazenamento de dados de eventos atual. Em seguida, crie um novo armazenamento de dados de eventos com a opção de preço de retenção de sete anos.

   - Período de retenção: altere o período de retenção do armazenamento de dados de eventos. O período de retenção determina por quanto tempo os dados do evento são mantidos no armazenamento de dados de eventos. Os períodos de retenção podem ser entre 7 dias e 3.653 dias (cerca de 10 anos) para a opção de preço de retenção extensível de um ano ou entre 7 dias e 2.557 dias (cerca de sete anos) para a opção de preço de retenção de sete anos.

> **Note**
>
> Se você diminuir o período de retenção de um armazenamento de dados de eventos, CloudTrail removerá quaisquer eventos com um período de retenção `eventTime` anterior ao novo. Por exemplo, se o período de retenção anterior foi de 365 dias e você o reduziu para 100 dias, os eventos com `eventTime` mais de 100 dias CloudTrail serão removidos.

- Criptografia: para criptografar seu armazenamento de dados de eventos usando sua própria chave do KMS, escolha Usar minha própria AWS KMS key. Por padrão, todos os eventos em um armazenamento de dados de eventos são criptografados por CloudTrail. Usar sua própria chave KMS gera AWS KMS custos de criptografia e descriptografia.

> **Note**
>
> Após associar um armazenamento de dados de eventos a uma chave do KMS, não será possível remover ou alterar a chave do KMS.

- Para incluir somente eventos registrados na Região da AWS atual, escolha Incluir na região atual em meu armazenamento dados de eventos. Se você não escolher essa opção, o armazenamento de dados de eventos incluirá eventos de todas as regiões.
- Para que seu armazenamento de dados de eventos colete eventos de todas as contas em uma AWS Organizations organização, escolha Habilitar para todas as contas em minha organização. Essa opção só está disponível se você estiver conectado com a conta de gerenciamento da sua organização e o tipo de evento para o armazenamento de dados do evento for CloudTraileventos ou itens de configuração.

Ao concluir, escolha Salvar alterações.

5. Na federação de consultas do Lake, escolha Editar para habilitar ou desabilitar a federação de consultas do Lake. A ativação da federação de consultas do Lake permite que você visualize os metadados do seu armazenamento de dados de eventos no catálogo de AWS Glue dados e execute consultas SQL nos dados do evento usando o Amazon Athena. A desativação da federação de consultas do Lake desativa a integração com AWS Glue AWS Lake Formation, e com o Amazon Athena. Depois de desabilitar a federação de consultas do Lake, você não poderá mais consultar seus dados no Athena. Nenhum dado do CloudTrail Lake é excluído

quando você desativa a federação e você pode continuar executando consultas no CloudTrail Lake.

Para habilitar a federação, faça o seguinte:

a. Escolha Habilitar.

b. Escolha entre criar um novo perfil do IAM ou usar um perfil existente. Quando você cria uma nova função, cria CloudTrail automaticamente uma função com as permissões necessárias. Se você escolher um perfil existente, a política da perfil deve fornecer as permissões mínimas necessárias.

c. Se você estiver criando um perfil do IAM, insira um nome para ele.

d. Se você estiver escolhendo um perfil do IAM existente, escolha o perfil que deseja usar. O perfil deve existir em sua conta.

Após terminar, escolha Salvar alterações.

6. Edite todas as configurações adicionais para seu Tipo de evento.

Tipo de evento	Configurações editáveis
CloudTrail eventos	Você pode editar as seguintes configurações para CloudTrail eventos: • Para alterar quais eventos seu armazenamento de dados de eventos registra, escolha Editar em CloudTrail eventos. • Em Eventos de gerenciamento, escolha Editar para alterar as configurações dos eventos de gerenciamento. Para obter mais informações, consulte Registrando eventos de gerenciamento com o AWS Management Console (etapa 3). • Em Eventos de dados, escolha Editar para alterar as configurações dos eventos de dados. Você pode escolher quais tipos de eventos de dados deseja registrar e escolher o modelo de seletor de registros

Tipo de evento	Configurações editáveis
	que deseja usar. Para ter mais informaçõ es, consulte Atualizando um armazenam ento de dados de eventos existente para registrar eventos de dados no AWS Management Console. Ao concluir, escolha Salvar alterações.
Eventos da integração	Em Integrações, escolha sua integração. Escolha Editar para alterar as configurações a seguir: • Em Detalhes da integração, altere o nome que identifica o canal da sua integração. • Em Local de entrega do evento, escolha o destino para seus eventos. • Em Resource policy (Política de recursos) , configure a política de recursos para o canal de integração. Ao concluir, escolha Salvar alterações. Para ter mais informações sobre essas configurações, consulte Crie uma integração com uma fonte de eventos fora do AWS.

7. Para adicionar, alterar ou remover tags, escolha Editar em Tags. É possível adicionar até 50 pares de chave de tag para ajudar a identificar, classificar e controlar o acesso ao seu armazenamento de dados de eventos. Ao concluir, escolha Salvar alterações.

Interrompa e inicie a ingestão de eventos com o console

Por padrão, os armazenamentos de dados de eventos são configurados para ingerir eventos. Você pode impedir que um armazenamento de dados de eventos consuma eventos usando o console ou as AWS CLI APIs.

As opções de Iniciar ingestão e Interromper ingestão só estão disponíveis em armazenamentos de dados de eventos contendo CloudTrail eventos (eventos de gerenciamento e dados) ou itens de AWS Config configuração.

Quando você interrompe a ingestão em um armazenamento de dados de eventos, o estado do armazenamento de dados de eventos muda para `STOPPED_INGESTION`. Você ainda pode executar consultas em qualquer evento que já esteja no armazenamento de dados de eventos. Você também pode copiar eventos de trilha para o armazenamento de dados de eventos (se ele contiver somente eventos CloudTrail de gerenciamento ou de dados).

Para interromper a ingestão de eventos por um armazenamento de dados de eventos

1. Faça login no AWS Management Console e abra o CloudTrail console em https://console.aws.amazon.com/cloudtrail/.
2. No painel de navegação, em Lake, escolha Armazenamentos de dados de eventos.
3. Escolha o armazenamento de dados de eventos.
4. Em Ações, escolha Interromper ingestão.
5. Quando uma confirmação for solicitada, escolha Interromper ingestão. : o armazenamento de dados de eventos irá parar de ingerir eventos em tempo real.
6. Para retomar a ingestão, escolha Iniciar ingestão.

Para reiniciar a ingestão de eventos

1. Faça login no AWS Management Console e abra o CloudTrail console em https://console.aws.amazon.com/cloudtrail/.
2. No painel de navegação, em Lake, escolha Armazenamentos de dados de eventos.
3. Escolha o armazenamento de dados de eventos.
4. Em Ações, escolha Iniciar ingestão.

Altere a proteção de rescisão com o console

Por padrão, os armazenamentos de dados de eventos no AWS CloudTrail Lake são configurados com a proteção de encerramento ativada. A proteção contra encerramento evita que um armazenamento de dados de eventos seja excluído acidentalmente. Se você quiser excluir o armazenamento de dados de eventos, deverá desativar a proteção contra encerramento. Você pode

desativar a proteção contra encerramento usando as operações de AWS Management Console AWS CLI, ou API.

Desativar a proteção contra encerramento

1. Faça login no AWS Management Console e abra o CloudTrail console em https://console.aws.amazon.com/cloudtrail/.
2. No painel de navegação, em Lake, escolha Armazenamentos de dados de eventos.
3. Escolha o armazenamento de dados de eventos.
4. Escolha Ações e Alterar proteção contra encerramento.
5. Escolha Desabilitado.
6. Escolha Salvar. Agora, você pode excluir o armazenamento de dados de eventos.

Para ativar a proteção contra encerramento

1. Faça login no AWS Management Console e abra o CloudTrail console em https://console.aws.amazon.com/cloudtrail/.
2. No painel de navegação, em Lake, escolha Armazenamentos de dados de eventos.
3. Escolha o armazenamento de dados de eventos.
4. Escolha Ações e Alterar proteção contra encerramento.
5. Para ativar a proteção contra encerramento, escolha Habilitado.
6. Escolha Salvar.

Excluir um armazenamento de dados de eventos com o console

Esta seção descreve como excluir um armazenamento de dados de eventos usando o console do AWS CloudTrail . Para obter informações sobre como excluir um armazenamento de dados de AWS CLI eventos usando Exclua um armazenamento de dados de eventos com o AWS CLI o.

> **Note**
>
> Você não pode excluir um armazenamento de dados de eventos se a proteção contra encerramento ou a federação de consultas do Lake estiverem ativadas. Por padrão, CloudTrail ativa a proteção contra encerramento para evitar que um armazenamento de dados de eventos seja excluído acidentalmente.

> Para excluir um armazenamento de dados de eventos com um tipo de evento Eventos da integração, você deve primeiro excluir o canal da integração. Você pode excluir o canal da página de detalhes da integração ou usando o comando aws cloudtrail delete-channel. Para mais informações, consulte Exclua um canal para excluir uma integração com o AWS CLI.

Excluir um armazenamento de dados de eventos

1. Faça login no AWS Management Console e abra o CloudTrail console em https://console.aws.amazon.com/cloudtrail/.
2. No painel de navegação, em Lake, escolha Armazenamentos de dados de eventos.
3. Escolha o armazenamento de dados de eventos.
4. Em Actions (Ações), selecione Delete (Excluir).
5. Digite o nome do armazenamento de dados de eventos para confirmar que deseja excluí-lo.
6. Escolha Excluir.

Depois de excluir um armazenamento de dados de eventos, o status do armazenamento de dados de eventos muda para `PENDING_DELETION` e permanece nesse estado por 7 dias. É possível restaurar um armazenamento de dados de eventos durante o período de espera de sete dias. No estado `PENDING_DELETION`, um armazenamento de dados de eventos não está disponível para consultas e nenhuma outra operação pode ser executada no armazenamento de dados de eventos, exceto as operações de restauração. Um armazenamento de dados de eventos que está pendente de exclusão não ingere eventos e não incorre em custos. Os armazenamentos de dados de eventos que estão pendentes de exclusão contam para a cota de armazenamentos de dados de eventos que podem existir em um. Região da AWS

Restaurar um armazenamento de dados de eventos com o console

Depois de excluir um armazenamento de dados de eventos no AWS CloudTrail Lake, seu status muda para `PENDING_DELETION` e permanece nesse estado por 7 dias. Durante esse período, você pode restaurar o armazenamento de dados do evento usando a operação AWS Management Console AWS CLI, ou da RestoreEventDataStoreAPI.

Esta seção descreve como restaurar um armazenamento de dados de eventos usando o console. Para obter informações sobre como restaurar um armazenamento de dados de AWS CLI eventos usando Restaure um armazenamento de dados de eventos com o AWS CLI o.

Restaurar um armazenamento de dados de eventos

1. Faça login no AWS Management Console e abra o CloudTrail console em https://console.aws.amazon.com/cloudtrail/.
2. No painel de navegação, em Lake, escolha Armazenamentos de dados de eventos.
3. Escolha o armazenamento de dados de eventos.
4. Em Ações, escolha Restaurar.

Crie, atualize e gerencie armazenamentos de dados de eventos com o AWS CLI

Você pode usar o AWS CLI para criar, atualizar e gerenciar seus armazenamentos de dados de eventos. Ao usar o AWS CLI, lembre-se de que seus comandos são Região da AWS executados no configurado para seu perfil. Se você deseja executar os comandos em uma região diferente, altere a região padrão para o seu perfil ou use o parâmetro --region com o comando.

Comandos disponíveis para armazenamentos de dados de eventos

Os comandos para criar e atualizar armazenamentos de dados de eventos no CloudTrail Lake incluem:

- `create-event-data-store`para criar um armazenamento de dados de eventos.
- `get-event-data-store`para retornar informações sobre o armazenamento de dados de eventos, incluindo os seletores de eventos avançados configurados para o armazenamento de dados de eventos.
- `update-event-data-store`para alterar a configuração de um armazenamento de dados de eventos existente.
- `list-event-data-stores`para listar os armazenamentos de dados do evento.
- `delete-event-data-store`para excluir um armazenamento de dados de eventos.
- `restore-event-data-store`para restaurar um armazenamento de dados de eventos que está pendente de exclusão.
- `start-import`para iniciar uma importação de eventos de trilha para um armazenamento de dados de eventos ou tentar novamente uma importação com falha.
- `get-import`para retornar informações sobre uma importação específica.

- `stop-import`para interromper a importação de eventos de trilha para um armazenamento de dados de eventos.
- `list-imports`para retornar informações sobre todas as importações ou um conjunto selecionado de importações por `ImportStatus` ou`Destination`.
- `list-import-failures`para listar falhas de importação para a importação especificada.
- `stop-event-data-store-ingestion`para interromper a ingestão de eventos em um armazenamento de dados de eventos.
- `start-event-data-store-ingestion`para reiniciar a ingestão de eventos em um armazenamento de dados de eventos.
- `enable-federation`para habilitar a federação em um armazenamento de dados de eventos para consultar o armazenamento de dados de eventos no Amazon Athena.
- `disable-federation`para desativar a federação em um armazenamento de dados de eventos. Depois de desativar a federação, você não poderá mais consultar os dados do armazenamento de dados de eventos no Amazon Athena. Você pode continuar a consultar no CloudTrail Lake.
- `put-insight-selectors`para adicionar ou modificar seletores de eventos do Insights para um armazenamento de dados de eventos existente e ativar ou desativar eventos do Insights.
- `get-insight-selectors`para retornar informações sobre os seletores de eventos do Insights configurados para um armazenamento de dados de eventos.
- `add-tags`para adicionar uma ou mais tags (pares de valores-chave) a um armazenamento de dados de eventos existente.
- `remove-tags`para remover uma ou mais tags de um armazenamento de dados de eventos.
- `list-tags`para retornar uma lista de tags associadas a um armazenamento de dados de eventos.

Para obter uma lista dos comandos disponíveis para consultas do CloudTrail Lake, consulteComandos disponíveis para consultas CloudTrail do Lake.

Para obter uma lista dos comandos disponíveis para integrações com o CloudTrail Lake, consulteComandos disponíveis para integrações com o CloudTrail Lake.

Crie um armazenamento de dados de eventos com o AWS CLI

Use o comando `create-event-data-store` para criar um armazenamento de dados de eventos.

Quando você cria um armazenamento de dados de eventos, o único parâmetro necessário é `--name`, usado para identificar o armazenamento de dados de eventos. Você pode configurar parâmetros opcionais adicionais, incluindo:

- `--advanced-event-selectors`: especifica o tipo dos eventos a serem incluídos no armazenamento de dados de eventos. Por padrão, os armazenamentos de dados de eventos registram todos os eventos de gerenciamento. Para obter mais informações sobre seletores de eventos avançados, consulte AdvancedEventSelectora Referência da CloudTrail API.
- `--kms-key-id`- Especifica a ID da chave do AWS KMS a ser usada para criptografar os eventos entregues por. CloudTrail O valor pode ser um nome de alias com o prefixo `alias/`, um ARN totalmente especificado para um alias, um ARN totalmente especificado para uma chave ou um identificador globalmente exclusivo.
- `--multi-region-enabled`- Cria um armazenamento de dados de eventos multirregional que registra eventos de todos Regiões da AWS em sua conta. Por padrão, `--multi-region-enabled` é definido, mesmo que o parâmetro não seja adicionado.
- `--organization-enabled`: permite que um armazenamento de dados de eventos colete eventos para todas as contas em uma organização. Por padrão, o armazenamento de dados de eventos não está habilitado para todas as contas em uma organização.
- `--billing-mode`: determina o custo de ingestão e armazenamento de eventos e o período de retenção padrão e máximo para o armazenamento de dados de eventos.

  Os valores possíveis são os seguintes:

  - `EXTENDABLE_RETENTION_PRICING`: esse modo de cobrança geralmente é recomendado se você ingerir menos de 25 TB de dados de eventos por mês e quiser um período de retenção flexível de até 3653 dias (cerca de 10 anos). O período de retenção padrão para esse modo de cobrança é de 366 dias.
  - `FIXED_RETENTION_PRICING`: esse modo de cobrança é recomendado se você espera ingerir mais de 25 TB de dados de eventos por mês e precisa de um período de retenção de até 2557 dias (cerca de 7 anos). O período de retenção padrão para esse modo de cobrança é de 2557 dias.

  O valor padrão é `EXTENDABLE_RETENTION_PRICING`.
- `--retention-period`: o número de dias para manter eventos no armazenamento de dados de eventos. Os valores válidos são números inteiros entre 7 e 3653, se `--billing-mode` for `EXTENDABLE_RETENTION_PRICING`, ou entre 7 e 2557, se `--billing-mode` for definido como

`FIXED_RETENTION_PRICING`. Se você não especificar`--retention-period`, CloudTrail usa o período de retenção padrão para `--billing-mode` o.

- `--start-ingestion`: o parâmetro `--start-ingestion` inicia a ingestão de eventos no armazenamento de dados de eventos quando ele é criado. Esse parâmetro é definido mesmo se o parâmetro não for adicionado.

  Especifique `--no-start-ingestion` se você não quiser que o armazenamento de dados de eventos ingira eventos ao vivo. Por exemplo, talvez você queira definir esse parâmetro se estiver copiando eventos para o armazenamento de dados de eventos e planeja usar os dados de eventos para analisar eventos passados. O parâmetro `--no-start-ingestion` é válido somente quando o `eventCategory` for `Management`, `Data` ou `ConfigurationItem`.

Os exemplos a seguir mostram como criar diferentes tipos de armazenamento de dados de eventos.

Tópicos

- Crie um armazenamento de dados de eventos para eventos de dados do S3 com o AWS CLI
- Crie um armazenamento de dados de eventos para itens AWS Config de configuração com o AWS CLI
- Crie um armazenamento de dados de eventos da organização para eventos de gerenciamento com o AWS CLI
- Crie armazenamentos de dados de eventos para eventos do Insights com o AWS CLI

Crie um armazenamento de dados de eventos para eventos de dados do S3 com o AWS CLI

O create-event-data-store comando de exemplo a seguir AWS Command Line Interface (AWS CLI) cria um armazenamento de dados de eventos chamado `my-event-data-store` que seleciona todos os eventos de dados do Amazon S3 e é criptografado usando uma chave KMS.

```
aws cloudtrail create-event-data-store \
--name my-event-data-store \
--kms-key-id "arn:aws:kms:us-east-1:123456789012:alias/KMS_key_alias" \
--advanced-event-selectors '[
        {
            "Name": "Select all S3 data events",
            "FieldSelectors": [
                { "Field": "eventCategory", "Equals": ["Data"] },
                { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
                { "Field": "resources.ARN", "StartsWith": ["arn:aws:s3"] }
```

```
            ]
        }
    ]'
```

A seguir, uma exemplo de resposta.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE-ee54-4813-92d5-999aeEXAMPLE",
    "Name": "my-event-data-store",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Select all S3 data events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3::Object"
                    ]
                },
                {
                    "Field": "resources.ARN",
                    "StartsWith": [
                        "arn:aws:s3"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:alias/KMS_key_alias",
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-09T22:19:39.417000-05:00",
```

```
    "UpdatedTimestamp": "2023-11-09T22:19:39.603000-05:00"
}
```

Crie um armazenamento de dados de eventos para itens AWS Config de configuração com o AWS CLI

O AWS CLI create-event-data-store comando de exemplo a seguir cria um armazenamento de dados de eventos chamado `config-items-eds` que seleciona itens AWS Config de configuração. Para coletar itens de configuração, especifique que o campo `eventCategory` é igual a `ConfigurationItem` nos seletores de eventos avançados.

```
aws cloudtrail create-event-data-store \
--name config-items-eds \
--advanced-event-selectors '[
    {
        "Name": "Select AWS Config configuration items",
        "FieldSelectors": [
            { "Field": "eventCategory", "Equals": ["ConfigurationItem"] }
        ]
    }
]'
```

A seguir, uma exemplo de resposta.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE-ee54-4813-92d5-999aeEXAMPLE",
    "Name": "config-items-eds",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Select AWS Config configuration items",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "ConfigurationItem"
                    ]
                }
            ]
        }
    ],
```

```
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-07T19:03:24.277000+00:00",
    "UpdatedTimestamp": "2023-11-07T19:03:24.468000+00:00"
}
```

Crie um armazenamento de dados de eventos da organização para eventos de gerenciamento com o AWS CLI

O AWS CLI create-event-data-store comando de exemplo a seguir cria um armazenamento de dados de eventos da organização que coleta todos os eventos de gerenciamento e define o `--billing-mode` parâmetro como. `FIXED_RETENTION_PRICING`

```
aws cloudtrail create-event-data-store --name org-management-eds --organization-enabled
 --billing-mode FIXED_RETENTION_PRICING
```

A seguir, uma exemplo de resposta.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE6-d493-4914-9182-e52a7934b207",
    "Name": "org-management-eds",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": true,
    "BillingMode": "FIXED_RETENTION_PRICING",
```

```
    "RetentionPeriod": 2557,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-16T15:30:50.689000+00:00",
    "UpdatedTimestamp": "2023-11-16T15:30:50.851000+00:00"
}
```

Crie armazenamentos de dados de eventos para eventos do Insights com o AWS CLI

Para registrar eventos do Insights no CloudTrail Lake, você precisa de um armazenamento de dados de eventos de destino que colete eventos do Insights e um armazenamento de dados de eventos de origem que habilite o Insights e eventos de gerenciamento de registros.

Este procedimento mostra como criar os armazenamentos de dados de eventos de destino e origem e, em seguida, habilitar os eventos do Insights.

1. Execute o comando aws cloudtrail create-event-data-store para criar um armazenamento de dados de eventos de destino que coleta eventos do Insights. O valor de `eventCategory` deve ser `Insight`. *`retention-period-days`*Substitua pelo número de dias em que você gostaria de reter eventos em seu armazenamento de dados de eventos. Os valores válidos são números inteiros entre 7 e 3653, se `--billing-mode` for `EXTENDABLE_RETENTION_PRICING`, ou entre 7 e 2557, se `--billing-mode` for definido como `FIXED_RETENTION_PRICING`. Se você não especificar`--retention-period`, CloudTrail usa o período de retenção padrão para `--billing-mode` o.

   Se você estiver conectado com a conta de gerenciamento de uma AWS Organizations organização, inclua o `--organization-enabled` parâmetro se quiser dar ao administrador delegado acesso ao armazenamento de dados do evento.

   ```
   aws cloudtrail create-event-data-store \
   --name insights-event-data-store \
   --no-multi-region-enabled \
   --retention-period retention-period-days \
   --advanced-event-selectors '[
       {
         "Name": "Select Insights events",
         "FieldSelectors": [
             { "Field": "eventCategory", "Equals": ["Insight"] }
           ]
       }
     ]'
   ```

A seguir, uma exemplo de resposta.

```
{
    "Name": "insights-event-data-store",
    "ARN": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE",
    "AdvancedEventSelectors": [
        {
           "Name": "Select Insights events",
           "FieldSelectors": [
              {
                  "Field": "eventCategory",
                  "Equals": [
                      "Insight"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": false,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": "90",
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-05-08T15:22:33.578000+00:00",
    "UpdatedTimestamp": "2023-05-08T15:22:33.714000+00:00"
}
```

Você usará o ARN (ou o sufixo de ID do ARN) da resposta como o valor do parâmetro `--insights-destination` na etapa 3.

2. Execute o comando aws cloudtrail create-event-data-store para criar um armazenamento de dados de eventos que registre eventos de gerenciamento no log. Por padrão, os armazenamentos de dados de eventos registram todos os eventos de gerenciamento. Não é necessário especificar nenhum seletor de eventos avançado para registrar todos os eventos de gerenciamento. *`retention-period-days`*Substitua pelo número de dias em que você gostaria de reter eventos em seu armazenamento de dados de eventos. Os valores válidos são números inteiros entre 7 e 3653, se `--billing-mode` for `EXTENDABLE_RETENTION_PRICING`, ou entre 7 e 2557, se `--billing-mode` for definido como `FIXED_RETENTION_PRICING`. Se você não especificar`--retention-period`, CloudTrail usa o período de retenção padrão para `--billing-mode` o. Se você estiver

criando um armazenamento de dados de eventos da organização, inclua o parâmetro `--organization-enabled`.

```
aws cloudtrail create-event-data-store --name source-event-data-store --retention-period retention-period-days
```

A seguir, uma exemplo de resposta.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/EXAMPLE9952-4ab9-49c0-b788-f4f3EXAMPLE",
    "Name": "source-event-data-store",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 90,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-05-08T15:25:35.578000+00:00",
    "UpdatedTimestamp": "2023-05-08T15:25:35.714000+00:00"
}
```

Você usará o ARN (ou o sufixo de ID do ARN) da resposta como o valor do parâmetro `--event-data-store` na etapa 3.

3. Execute o comando put-insight-selectors para ativar os eventos do Insights. Os valores do seletor Insights podem ser `ApiCallRateInsight`, `ApiErrorRateInsight` ou ambos. Para o parâmetro `--event-data-store`, especifique o ARN (ou sufixo de ID do ARN) do armazenamento de dados de eventos de origem que registra os eventos de gerenciamento e

ativará o Insights. Para o parâmetro `--insights-destination`, especifique o ARN (ou sufixo de ID do ARN) do armazenamento de dados de eventos de destino que registrará os eventos do Insights.

```
aws cloudtrail put-insight-selectors --event-data-store arn:aws:cloudtrail:us-
east-1:111122223333:eventdatastore/EXAMPLE9952-4ab9-49c0-b788-f4f3EXAMPLE --
insights-destination arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE --insight-selectors '[{"InsightType":
 "ApiCallRateInsight"},{"InsightType": "ApiErrorRateInsight"}]'
```

O resultado a seguir mostra o seletor de eventos do Insights que está configurado para o armazenamento de dados de eventos.

```
{
  "EventDataStoreARN": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLE9952-4ab9-49c0-b788-f4f3EXAMPLE",
  "InsightsDestination": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE",
  "InsightSelectors":
      [
         {
            "InsightType": "ApiErrorRateInsight"
         },
         {
            "InsightType": "ApiCallRateInsight"
         }
      ]
}
```

Depois de ativar o CloudTrail Insights pela primeira vez em um armazenamento de dados de eventos, pode levar até 7 dias CloudTrail para entregar o primeiro evento do Insights, se uma atividade incomum for detectada.

CloudTrail O Insights analisa eventos de gerenciamento que ocorrem em uma única região, não globalmente. Um evento do CloudTrail Insights é gerado na mesma região em que seus eventos de gerenciamento de apoio são gerados.

Para um armazenamento de dados de eventos da organização, CloudTrail analisa os eventos de gerenciamento da conta de cada membro em vez de analisar a agregação de todos os eventos de gerenciamento da organização.

Cobranças adicionais se aplicam à ingestão de eventos do Insights em CloudTrail Lake. Você será cobrado separadamente se ativar o Insights tanto para trilhas quanto para armazenamentos de dados de eventos. Para obter informações sobre CloudTrail preços, consulte AWS CloudTrail Preços.

Importe eventos de trilha para um armazenamento de dados de eventos com o AWS CLI

No AWS CLI, você pode importar eventos de trilha para um armazenamento de dados de eventos. O procedimento nesta seção demonstra como criar e configurar um armazenamento de dados de eventos executando o comando create-event-data-storee, em seguida, importar os eventos para esse armazenamento de dados de eventos usando o comando start-import. Para obter mais informações sobre a importação de eventos de trilha, incluindo informações sobre considerações e permissões necessárias, consulte Copiar eventos de trilhas para um armazenamento de dados de eventos.

Preparando-se para importar eventos de trilhas

Antes de importar eventos de trilha, faça os seguintes preparativos.

- Certifique-se de ter um perfil com as permissões necessárias para importar eventos de trilhas para um armazenamento de dados de eventos.
- Determine o valor de --billing-mode que você deseja especificar para o armazenamento de dados de eventos. O `--billing-mode` determina o custo de ingestão e armazenamento de eventos e o período de retenção padrão e máximo para o armazenamento de dados de eventos.

  Ao importar eventos de trilha para o CloudTrail Lake, CloudTrail descompacta os registros armazenados no formato gzip (compactado). Em seguida, CloudTrail copia os eventos contidos nos registros para seu armazenamento de dados de eventos. O tamanho dos dados não compactados pode ser maior do que o tamanho real do armazenamento do Amazon S3. Para obter uma estimativa geral do tamanho dos dados não compactados, multiplique o tamanho dos registros no bucket do S3 por 10. Você pode usar essa estimativa para escolher o valor de `--billing-mode` para seu caso de uso.
- Determine o valor que você deseja especificar para `--retention-period`. CloudTrail não copiará um evento se ele `eventTime` for anterior ao período de retenção especificado.

  Para determinar o período de retenção adequado, calcule a soma do evento mais antigo que você deseja copiar em dias e o número de dias em que deseja reter os eventos no armazenamento de dados de eventos, conforme demonstrado nesta equação:

Período de retenção = *oldest-event-in-days*+ *number-days-to-retain*

Por exemplo, se o evento mais antigo que você está copiando tiver 45 dias e você quiser manter os eventos no armazenamento de dados de eventos por mais 45 dias, defina o período de retenção como 90 dias.

- Decida se deseja usar o armazenamento de dados de eventos para analisar quaisquer eventos futuros. Se você não quiser ingerir nenhum evento futuro, inclua o parâmetro `--no-start-ingestion` ao criar o armazenamento de dados de eventos. Por padrão, o armazenamento de dados de eventos começa a ingerir eventos assim que é criado.

Para criar um armazenamento de dados de eventos e importar eventos de trilha para esse armazenamento de dados de eventos

1. Execute o comando create-event-data-store para criar um armazenamento de dados de eventos. Neste exemplo, `--retention-period` é definido como `120` porque o evento mais antigo que está sendo copiado tem 90 dias e queremos reter os eventos por 30 dias. O parâmetro `--no-start-ingestion` é definido porque não queremos ingerir nenhum evento futuro. Neste exemplo, `--billing-mode` não foi definido, porque estamos usando o valor padrão `EXTENDABLE_RETENTION_PRICING`, já que esperamos ingerir menos de 25 TB de dados de eventos.

   > **Note**
   >
   > Se você estiver criando um armazenamento de dados de eventos para substituir sua trilha, recomendamos configurar `--advanced-event-selectors` para corresponder aos seletores de eventos da sua trilha para garantir que você tenha a mesma cobertura de eventos. Por padrão, os armazenamentos de dados de eventos registram todos os eventos de gerenciamento.

   ```
   aws cloudtrail create-event-data-store  --name import-trail-eds  --retention-period
    120 --no-start-ingestion
   ```

   Esta é uma resposta de exemplo:

   ```
   {
   ```

```
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLEa-4357-45cd-bce5-17ec652719d9",
    "Name": "import-trail-eds",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 120,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-09T16:52:25.444000+00:00",
    "UpdatedTimestamp": "2023-11-09T16:52:25.569000+00:00"
}
```

O `Status` inicial é `CREATED` para que executemos o comando get-event-data-store para verificar se a ingestão foi interrompida.

```
aws cloudtrail get-event-data-store --event-data-store eds-id
```

A resposta mostra que `Status` agora é`STOPPED_INGESTION`, o que indica que o armazenamento de dados de eventos não está ingerindo eventos ao vivo.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLEa-4357-45cd-bce5-17ec652719d9",
    "Name": "import-trail-eds",
    "Status": "STOPPED_INGESTION",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
```

```
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 120,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-09T16:52:25.444000+00:00",
    "UpdatedTimestamp": "2023-11-09T16:52:25.569000+00:00"
}
```

2. Execute o comando start-import para importar eventos de trilha para o armazenamento de dados de eventos criado na etapa 1. Especifique o ARN (ou sufixo de ID do ARN) do armazenamento de dados de eventos como o valor para o parâmetro `--destinations`. Para `--start-event-time` especificar o `eventTime` para o evento mais antigo que você deseja copiar, e para `--end-event-time` especificar o `eventTime` do evento mais recente que você deseja copiar. Para `--import-source` especificar o URI do S3 para o bucket do S3 contendo seus registros de trilha, o do bucket do S3 e o ARN da função usada Região da AWS para importar eventos de trilha.

```
aws cloudtrail start-import \
--destinations ["arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLEa-4357-45cd-bce5-17ec652719d9"] \
--start-event-time 2023-08-11T16:08:12.934000+00:00 \
--end-event-time 2023-11-09T17:08:20.705000+00:00 \
--import-source {"S3": {"S3LocationUri": "s3://aws-cloudtrail-
logs-123456789012-612ff1f6/AWSLogs/123456789012/CloudTrail/","S3BucketRegion":"us-
east-1","S3BucketAccessRoleArn": "arn:aws:iam::123456789012:role/service-role/
CloudTrailLake-us-east-1-copy-events-eds"}}
```

A seguir, uma exemplo de resposta.

```
{
   "CreatedTimestamp": "2023-11-09T17:08:20.705000+00:00",
   "Destinations": [
        "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLEa-4357-45cd-bce5-17ec652719d9"
    ],
   "EndEventTime": "2023-11-09T17:08:20.705000+00:00",
   "ImportId": "EXAMPLEe-7be2-4658-9204-b38c3257fcd1",
   "ImportSource": {
      "S3": {
         "S3BucketAccessRoleArn": "arn:aws:iam::123456789012:role/service-role/
CloudTrailLake-us-east-1-copy-events-eds",
         "S3BucketRegion":"us-east-1",
         "S3LocationUri": "s3://aws-cloudtrail-logs-123456789012-111ff1f6/
AWSLogs/123456789012/CloudTrail/"
      }
   },
   "ImportStatus": "INITIALIZING",
   "StartEventTime": "2023-08-11T16:08:12.934000+00:00",
   "UpdatedTimestamp": "2023-11-09T17:08:20.806000+00:00"
}
```

3. Execute o comando get-import para obter informações sobre a importação.

```
aws cloudtrail get-import --import-id import-id
```

A seguir, uma exemplo de resposta.

```
{
    "ImportId": "EXAMPLEe-7be2-4658-9204-b38c3EXAMPLE",
    "Destinations": [
        "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLEa-4357-45cd-bce5-17ec652719d9"
    ],
    "ImportSource": {
        "S3": {
            "S3LocationUri": "s3://aws-cloudtrail-logs-123456789012-111ff1f6/
AWSLogs/123456789012/CloudTrail/",
            "S3BucketRegion":"us-east-1",
            "S3BucketAccessRoleArn": "arn:aws:iam::123456789012:role/service-role/
CloudTrailLake-us-east-1-copy-events-eds"
        }
```

```
    },
    "StartEventTime": "2023-08-11T16:08:12.934000+00:00",
    "EndEventTime": "2023-11-09T17:08:20.705000+00:00",
    "ImportStatus": "COMPLETED",
    "CreatedTimestamp": "2023-11-09T17:08:20.705000+00:00",
    "ImportStatistics": {
        "PrefixesFound": 1548,
        "PrefixesCompleted": 1548,
        "FilesCompleted": 92845,
        "EventsCompleted": 577249,
        "FailedEntries": 0
    }
}
```

Uma importação termina com um `ImportStatus` de `COMPLETED`, se não houve falhas, ou `FAILED`, se houve falhas.

Se a importação teve `FailedEntries`, você pode executar o comando list-import-failures para retornar uma lista de falhas.

```
aws cloudtrail list-import-failures --import-id import-id
```

Para repetir uma importação que teve falhas, execute o comando start-import somente com o parâmetro `--import-id`. Quando você repete uma importação, a importação é CloudTrail retomada no local em que a falha ocorreu.

```
aws cloudtrail start-import --import-id import-id
```

Obtenha um armazenamento de dados de eventos com o AWS CLI

O AWS CLI get-event-data-store comando de exemplo a seguir retorna informações sobre o armazenamento de dados do evento especificado pelo `--event-data-store` parâmetro necessário, que aceita um ARN ou o sufixo de ID do ARN.

```
aws cloudtrail get-event-data-store
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE
```

A seguir, uma exemplo de resposta. A criação e os horários da última atualização estão no formato `timestamp`.

```
{
    "EventDataStoreARN": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "s3-data-events-eds",
    "Status": "ENABLED",
    "AdvancedEventSelectors": [
        {
            "Name": "Log DeleteObject API calls for a specific S3 bucket",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
                {
                    "Field": "eventName",
                    "Equals": [
                        "DeleteObject"
                    ]
                },
                {
                    "Field": "resources.ARN",
                    "StartsWith": [
                        "arn:aws:s3:::bucketName"
                    ]
                },
                {
                    "Field": "readOnly",
                    "Equals": [
                        "false"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3::Object"
                    ]
                }
            ]
```

```
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "FIXED_RETENTION_PRICING",
    "RetentionPeriod": 2557,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-09T22:20:36.344000+00:00",
    "UpdatedTimestamp": "2023-11-09T22:20:36.476000+00:00"
}
```

Liste todos os armazenamentos de dados de eventos em uma conta com o AWS CLI

O AWS CLI list-event-data-stores comando de exemplo a seguir retorna informações sobre todos os armazenamentos de dados de eventos em uma conta, na região atual. Parâmetros opcionais incluem `--max-results` para especificar um número máximo de resultados que você deseja que o comando retorne em uma única página. Se houver mais resultados do que o valor especificado para `--max-results`, execute o comando novamente adicionando o valor retornado `NextToken` para obter a próxima página de resultados.

```
aws cloudtrail list-event-data-stores
```

A seguir, uma exemplo de resposta.

```
{
    "EventDataStores": [
        {
            "EventDataStoreArn": "arn:aws:cloudtrail:us-
east-1:123456789012:eventdatastore/EXAMPLE7-cad6-4357-a84b-318f9868e969",
            "Name": "management-events-eds"
        },
        {
            "EventDataStoreArn": "arn:aws:cloudtrail:us-
east-1:123456789012:eventdatastore/EXAMPLE6-88e1-43b7-b066-9c046b4fd47a",
            "Name": "config-items-eds"
        },
        {
            "EventDataStoreArn": "arn:aws:cloudtrail:us-
east-1:123456789012:eventdatastore/EXAMPLEf-b314-4c85-964e-3e43b1e8c3b4",
            "Name": "s3-data-events"
        }
```

```
    ]
}
```

Atualize um armazenamento de dados de eventos com o AWS CLI

Os exemplos a seguir mostram como atualizar um armazenamento de dados de eventos.

Tópicos

- Atualize o modo de cobrança com o AWS CLI
- Atualize o modo de retenção, ative a proteção contra rescisão e especifique um AWS KMS key com o AWS CLI
- Desative a proteção contra rescisão com o AWS CLI

Atualize o modo de cobrança com o AWS CLI

O `--billing-mode` para o armazenamento de dados de eventos determina o custo de ingestão e armazenamento de eventos e o período de retenção padrão e máximo para o armazenamento de dados de eventos. Se o `--billing-mode` de um armazenamento de dados de eventos estiver definido como `FIXED_RETENTION_PRICING`, você poderá alterar o valor para `EXTENDABLE_RETENTION_PRICING`. `EXTENDABLE_RETENTION_PRICING` geralmente é recomendado se seu armazenamento de dados de eventos ingere menos de 25 TB de dados de eventos por mês e você deseja um período de retenção flexível de até 3653 dias. Para obter mais informações sobre preços, consulte Definição de preço do AWS CloudTrail e Gerenciando os custos CloudTrail do Lake.

> **Note**
>
> Não é possível alterar o valor de `--billing-mode` de `EXTENDABLE_RETENTION_PRICING` para `FIXED_RETENTION_PRICING`. Se o modo de cobrança do armazenamento de dados de eventos estiver definido como `EXTENDABLE_RETENTION_PRICING` e você quiser usar `FIXED_RETENTION_PRICING`, poderá interromper a ingestão no armazenamento de dados de eventos e criar um novo armazenamento de dados de eventos que use `FIXED_RETENTION_PRICING`.

O AWS CLI update-event-data-store comando de exemplo a seguir altera o `--billing-mode` para o armazenamento de dados de eventos de `FIXED_RETENTION_PRICING`

para`EXTENDABLE_RETENTION_PRICING`. O valor do parâmetro `--event-data-store` é um ARN (ou o sufixo de ID do ARN) e é obrigatório; outros parâmetros são opcionais.

```
aws cloudtrail update-event-data-store \
--region us-east-1 \
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE \
--billing-mode EXTENDABLE_RETENTION_PRICING
```

A seguir, uma exemplo de resposta.

```
{
    "EventDataStoreArn": "event-data-store arn:aws:cloudtrail:us-
east-1:123456789012:eventdatastore/EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "management-events-eds",
    "Status": "ENABLED",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 2557,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-10-27T10:55:55.384000-04:00",
    "UpdatedTimestamp": "2023-10-27T10:57:05.549000-04:00"
}
```

Atualize o modo de retenção, ative a proteção contra rescisão e especifique um AWS KMS key com o AWS CLI

O AWS CLI update-event-data-store comando de exemplo a seguir atualiza um armazenamento de dados de eventos para alterar seu período de retenção para 100 dias e ativar a proteção contra rescisão. O valor do parâmetro `--event-data-store` é um ARN (ou o sufixo de ID do ARN) e é obrigatório; outros parâmetros são opcionais. Neste exemplo, o parâmetro `--retention-period` é adicionado para alterar o período de retenção para 100 dias. Opcionalmente, você pode optar por ativar a AWS Key Management Service criptografia e especificar um AWS KMS key adicionando `--kms-key-id` ao comando e especificando um ARN da chave KMS como valor. `--termination-protection-enabled`é adicionado para ativar a proteção de encerramento em um armazenamento de dados de eventos que não tinha a proteção de encerramento ativada.

Um armazenamento de dados de eventos que registra eventos externos AWS não pode ser atualizado para registrar AWS eventos. Da mesma forma, um armazenamento de dados de AWS eventos que registra eventos não pode ser atualizado para registrar eventos externos AWS.

> **Note**
>
> Se você diminuir o período de retenção de um armazenamento de dados de eventos, CloudTrail removerá todos os eventos com um período de retenção `eventTime` mais antigo que o novo. Por exemplo, se o período de retenção anterior foi de 365 dias e você o reduziu para 100 dias, os eventos com `eventTime` mais de 100 dias CloudTrail serão removidos.

```
aws cloudtrail update-event-data-store \
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE \
--retention-period 100 \
--kms-key-id "arn:aws:kms:us-east-1:0123456789:alias/KMS_key_alias" \
--termination-protection-enabled
```

A seguir, uma exemplo de resposta.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE-ee54-4813-92d5-999aeEXAMPLE",
    "Name": "my-event-data-store",
    "Status": "ENABLED",
```

```
    "AdvancedEventSelectors": [
        {
            "Name": "Select all S3 data events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3::Object"
                    ]
                },
                {
                    "Field": "resources.ARN",
                    "StartsWith": [
                        "arn:aws:s3"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 100,
    "KmsKeyId": "arn:aws:kms:us-east-1:0123456789:alias/KMS_key_alias",
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-10-27T10:55:55.384000-04:00",
    "UpdatedTimestamp": "2023-10-27T10:57:05.549000-04:00"
}
```

Desative a proteção contra rescisão com o AWS CLI

Por padrão, a proteção contra encerramento é habilitada em um armazenamento de dados de eventos para proteger o armazenamento de dados de eventos contra exclusão acidental. Você não pode excluir um armazenamento de dados de eventos quando a proteção contra encerramento está habilitada. Se você quiser excluir o armazenamento de dados de eventos, primeiro deverá desativar a proteção contra encerramento.

O AWS CLI update-event-data-store comando de exemplo a seguir desativa a proteção contra terminação passando o `--no-termination-protection-enabled` parâmetro.

```
aws cloudtrail update-event-data-store \
--region us-east-1 \
--no-termination-protection-enabled \
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE
```

A seguir, uma exemplo de resposta.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "management-events-eds",
    "Status": "ENABLED",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": false,
    "CreatedTimestamp": "2023-10-27T10:55:55.384000-04:00",
    "UpdatedTimestamp": "2023-10-27T10:57:05.549000-04:00"
}
```

Interrompa a ingestão em um armazenamento de dados de eventos com o AWS CLI

O AWS CLI stop-event-data-store-ingestion comando de exemplo a seguir impede que um armazenamento de dados de eventos ingira eventos. Para interromper a ingestão, o `Status` do

armazenamento de dados de eventos deve ser `ENABLED` e `eventCategory` deve ser `Management`, `Data` ou `ConfigurationItem`. O armazenamento de dados de eventos é especificado por `--event-data-store`, que aceita um ARN de armazenamento de dados de evento ou o sufixo de ID do ARN. Após a execução de stop-event-data-store-ingestion, o estado do armazenamento de dados do evento muda para `STOPPED_INGESTION`.

O armazenamento de dados de eventos não é contabilizado para o máximo de dez armazenamentos de dados de eventos da conta quando seu estado é `STOPPED_INGESTION`

```
aws cloudtrail stop-event-data-store-ingestion
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE
```

Se o comando tiver êxito, não haverá resposta.

Inicie a ingestão em um armazenamento de dados de eventos com o AWS CLI

O AWS CLI start-event-data-store-ingestion comando de exemplo a seguir inicia a ingestão de eventos em um armazenamento de dados de eventos. Para iniciar a ingestão, o `Status` do armazenamento de dados de eventos deve ser `STOPPED_INGESTION` e `eventCategory` deve ser `Management`, `Data` ou `ConfigurationItem`. O armazenamento de dados de eventos é especificado por `--event-data-store`, que aceita um ARN de armazenamento de dados de evento ou o sufixo de ID do ARN. Após a execução de start-event-data-store-ingestion, o estado do armazenamento de dados do evento muda para `ENABLED`.

```
aws cloudtrail start-event-data-store-ingestion --event-data-store
 arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-f852-4e8f-8bd1-
bcf6cEXAMPLE
```

Se o comando tiver êxito, não haverá resposta.

Habilitar federação em um armazenamento de dados de eventos

Para ativar a federação, execute o comando aws cloudtrail enable-federation, fornecendo os parâmetros obrigatórios `--event-data-store` e `--role`. Para `--event-data-store`, forneça o ARN do armazenamento de dados de eventos (ou o sufixo de ID do ARN). Para `--role`, forneça o ARN para seu perfil na federação. O perfil deve existir em sua conta e fornecer as permissões mínimas necessárias.

```
aws cloudtrail enable-federation
--event-data-store arn:aws:cloudtrail:region:account-id:eventdatastore/eds-id
--role arn:aws:iam::account-id:role/federation-role-name
```

Este exemplo mostra como um administrador delegado pode habilitar a federação em um armazenamento de dados de eventos da organização especificando o ARN do armazenamento de dados de eventos na conta de gerenciamento e o ARN do perfil de federação na conta de administrador delegado.

```
aws cloudtrail enable-federation
--event-data-store arn:aws:cloudtrail:region:management-account-id:eventdatastore/eds-id
--role arn:aws:iam::delegated-administrator-account-id:role/federation-role-name
```

Desabilitar federação em um armazenamento de dados de eventos

Para desabilitar a federação no armazenamento de dados de eventos, execute o comando aws cloudtrail disable-federation. O armazenamento de dados de eventos é especificado por `--event-data-store`, que aceita um ARN de armazenamento de dados de evento ou o sufixo de ID do ARN.

```
aws cloudtrail disable-federation
--event-data-store arn:aws:cloudtrail:region:account-id:eventdatastore/eds-id
```

> **Note**
>
> Se esse elemento for um armazenamento de dados de eventos da organização, use o ID de conta para a conta de gerenciamento.

Exclua um armazenamento de dados de eventos com o AWS CLI

O comando da AWS CLI delete-event-data-store do exemplo a seguir desabilita o armazenamento de dados do evento especificado por `--event-data-store`, que aceita um ARN de armazenamento de dados de evento ou o sufixo de ID do ARN. Depois de executar delete-event-data-store, o estado final do armazenamento de dados de eventos é`PENDING_DELETION` , e o armazenamento de dados de eventos é excluído automaticamente após um período de espera de sete dias.

Depois de executar delete-event-data-store em um armazenamento de dados de eventos, você não pode executar list-queries, describe-query ou get-query-results em consultas que estejam usando o armazenamento de dados desabilitado. O armazenamento de dados do evento é contabilizado para o máximo de dez armazenamentos de dados de eventos da conta quando sua exclusão está pendente.

> **Note**
>
> Você não pode excluir um armazenamento de dados de eventos se `--termination-protection-enabled` estiver definido ou se `FederationStatus` for `ENABLED`.

```
aws cloudtrail delete-event-data-store
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
```

Se o comando tiver êxito, não haverá resposta.

Restaure um armazenamento de dados de eventos com o AWS CLI

O comando da AWS CLI restore-event-data-store do exemplo a seguir restaura um armazenamento de dados de eventos que está pendente de exclusão. O armazenamento de dados de eventos é especificado por `--event-data-store`, que aceita um ARN de armazenamento de dados de evento ou o sufixo de ID do ARN. Você só pode restaurar um armazenamento de dados de eventos excluído dentro do período de espera de sete dias após a exclusão.

```
aws cloudtrail restore-event-data-store
--event-data-store EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
```

A resposta inclui informações sobre o armazenamento de dados de eventos, incluindo seu ARN, seletores de eventos avançados e o status da restauração.

Gerenciar ciclos de vida do armazenamento de dados de eventos

A seguir estão os estágios do ciclo de vida de um armazenamento de dados de eventos:

- `CREATED`: um estado de curto prazo indicando que o armazenamento de dados de eventos foi criado.

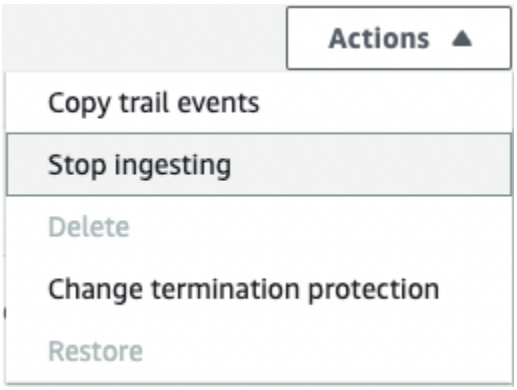
- `ENABLED`: o armazenamento de dados de eventos está ativo e ingerindo eventos. É possível executar consultas e copiar eventos de trilha para o armazenamento de dados de eventos.
- `STARTING_INGESTION`: um estado de curto prazo que indica que o armazenamento de dados de eventos começará a ingerir eventos em tempo real.
- `STOPPING_INGESTION`: um estado de curto prazo que indica que o armazenamento de dados de eventos irá parar de ingerir eventos em tempo real.
- `STOPPED_INGESTION`: o armazenamento de dados de eventos não está ingerindo eventos em tempo real. Você ainda pode executar consultas em qualquer evento que já esteja no armazenamento de dados de eventos e copiar eventos de trilha para o armazenamento de dados de eventos.
- `PENDING_DELETION`: o armazenamento de dados de eventos estava em um estado `ENABLED` ou `STOPPED_INGESTION` e foi excluído, mas está dentro do período de espera de sete dias antes da exclusão permanente. Não é possível executar consultas no armazenamento de dados de eventos e nenhuma operação pode ser executada no armazenamento de dados, exceto a restauração.

Somente será possível excluir um armazenamento de dados de eventos se tanto a federação como a proteção contra encerramento estiver desabilitada. A proteção contra encerramento evita que um armazenamento de dados de eventos seja excluído acidentalmente. Por padrão, a proteção contra término está habilitada em um armazenamento de dados de eventos. A federação permite que você consulte os dados do armazenamento de dados de eventos no Athena e está desabilitada por padrão.

Depois de excluir um armazenamento de dados de eventos, ele permanece no estado `PENDING_DELETION` por sete dias antes de ser excluído permanentemente. É possível restaurar um armazenamento de dados de eventos durante o período de espera de sete dias. No estado `PENDING_DELETION`, um armazenamento de dados de eventos não está disponível para consultas e nenhuma outra operação pode ser executada no armazenamento de dados de eventos, exceto as operações de restauração. Um armazenamento de dados de eventos que está pendente de exclusão não ingere eventos e não incorre em custos. No entanto, os armazenamentos de dados de eventos que estão pendentes de exclusão contam para a cota de armazenamentos de dados de eventos que podem existir em um. Região da AWS

Ações disponíveis em armazenamentos de dados de eventos

Para excluir ou restaurar um armazenamento de dados de eventos, copiar eventos de trilha, iniciar ou parar a ingestão de eventos ou ativar ou desativar sua proteção contra término, use comandos no menu Ações da página de detalhes do armazenamento de dados de eventos.



A opção de copiar eventos de trilha só está disponível em armazenamentos de dados de eventos que contêm eventos CloudTrail de gerenciamento e dados. As opções de Iniciar ingestão e Interromper ingestão só estão disponíveis em armazenamentos de dados de eventos contendo CloudTrail eventos (eventos de gerenciamento e dados) ou itens de AWS Config configuração.

Copiar eventos de trilhas para um armazenamento de dados de eventos

Você pode copiar eventos da trilha para um armazenamento de dados de eventos do CloudTrail Lake para criar um point-in-time instantâneo dos eventos registrados na trilha. Copiar os eventos de uma trilha não interfere na capacidade da trilha de registrar eventos e não modifica a trilha de nenhuma forma.

Você pode copiar eventos de trilha para um armazenamento de dados de eventos existente configurado para CloudTrail eventos ou pode criar um novo armazenamento de dados de CloudTrail eventos e escolher a opção Copiar eventos de trilha como parte da criação do armazenamento de dados de eventos. Para obter mais informações sobre cópia de eventos de trilhas para um armazenamento de dados de eventos existente, consulte Copiar eventos de trilhas para um armazenamento de dados de eventos existente. Para obter mais informações sobre como criar um armazenamento de dados de eventos, consulte Crie um armazenamento de dados de CloudTrail eventos para eventos com o console.

Se estiver copiando eventos de trilha para um armazenamento de dados de eventos da organização, você deve usar a conta de gerenciamento da respectiva organização. Não é possível copiar eventos de trilha usando uma conta de administrador delegado para uma organização.

CloudTrail Os armazenamentos de dados de eventos em Lake incorrem em cobranças. Ao criar um armazenamento de dados de eventos, você escolhe a opção de preço que deseja usar para ele. A opção de preço determina o custo para a ingestão e para o armazenamento de eventos, e o período de retenção padrão e máximo para o armazenamento de dados de eventos. Para obter

informações sobre CloudTrail preços e gerenciamento de custos do Lake, consulte AWS CloudTrail Preços Gerenciando os custos CloudTrail do Lake e.

Ao copiar eventos de trilha para um armazenamento de dados de eventos do CloudTrail Lake, você incorre em cobranças com base na quantidade de dados não compactados que o armazenamento de dados de eventos ingere.

Ao copiar eventos de trilha para o CloudTrail Lake, CloudTrail descompacta os registros armazenados no formato gzip (compactado) e, em seguida, copia os eventos contidos nos registros para seu armazenamento de dados de eventos. O tamanho dos dados não compactados pode ser maior do que o tamanho real do armazenamento do S3. Para obter uma estimativa geral do tamanho dos dados não compactados, é possível multiplicar o tamanho dos registros no bucket do S3 por 10.

É possível pode reduzir os custos especificando um intervalo de tempo mais restrito para os eventos copiados. Se você planeja usar apenas o armazenamento de dados de eventos para consultar seus eventos copiados, poderá desativar a ingestão de eventos para evitar cobranças em eventos futuros. Para obter mais informações, consulte Preços do AWS CloudTrail e Gerenciando os custos CloudTrail do Lake.

Cenários

A tabela a seguir descreve alguns cenários comuns para copiar eventos de trilha e como você realiza cada cenário usando o console.

Cenário	Como faço isso no console?
Analise e consulte eventos históricos de trilhas em CloudTrail Lake sem ingerir novos eventos	Crie um novo armazenamento de dados de eventos e escolha a opção Copiar eventos da trilha como parte da criação do armazenamento de dados de eventos. Ao criar o armazenam ento de dados de eventos, desmarque a opção Ingerir eventos (etapa 15 do procedimento) para garantir que o armazenamento de dados de eventos contenha somente os eventos históricos da sua trilha e nenhum evento futuro.
Substitua sua trilha existente por um armazenamento de dados de eventos do CloudTrail Lake	Crie um armazenamento de dados de eventos com os mesmos seletores de eventos que sua trilha para garantir que o armazenamento de dados de eventos tenha a mesma cobertura da trilha.

Cenário	Como faço isso no console?
	Para evitar a duplicação de eventos entre a trilha de origem e o armazenamento de dados de eventos de destino, escolha um intervalo de datas para os eventos copiados que seja anterior à criação do armazenamento de dados de eventos. Após a criação do armazenamento de dados de eventos, você poderá desativar o registro em log da trilha para evitar cobranças adicionais.

Tópicos

Considerações para copiar eventos de trilhas

Considere os seguintes fatores ao copiar eventos de trilhas.

- Ao copiar eventos de trilha, CloudTrail usa a operação da `GetObject`API do S3 para recuperar os eventos de trilha no bucket do S3 de origem. Há algumas classes de armazenamento arquivadas no S3, como os níveis de S3 Glacier Flexible Retrieval, S3 Glacier Deep Archive, S3 Outposts e S3 Intelligent-Tiering Deep Archive que não são acessíveis via `GetObject`. Para copiar eventos de trilhas armazenados nessas classes de armazenamento arquivadas, primeiro é necessário restaurar uma cópia usando a operação `RestoreObject` do S3. Para obter informações sobre como restaurar objetos arquivados, consulte Restaurar objetos arquivados no Guia do usuário do Amazon S3.
- Quando você copia eventos de trilha para um armazenamento de dados de eventos, CloudTrail copia todos os eventos de trilha, independentemente da configuração dos tipos de eventos do armazenamento de dados de eventos de destino, seletores de eventos avançados ou Região da AWS.

- Antes de copiar eventos de trilha para um armazenamento de dados de eventos existente, certifique-se de que a opção de preço e o período de retenção do armazenamento de dados de eventos estejam configurados adequadamente para seu caso de uso.
  - Opção de preço: a opção de preço determina o custo de ingestão e armazenamento de eventos. Para obter mais informações sobre opções de preço, consulte Preço do AWS CloudTrail e Opções de preços do armazenamento de dados de eventos.
  - Período de retenção: o período de retenção determina por quanto tempo os dados do evento são mantidos no armazenamento de dados do evento. CloudTrail copia somente eventos de trilha que tenham um período de retenção `eventTime` dentro do armazenamento de dados de eventos. Para determinar o período de retenção adequado, calcule a soma do evento mais antigo que você deseja copiar em dias e o número de dias em que deseja reter os eventos no armazenamento de dados do evento (período de retenção = *`oldest-event-in-days`*+ *`number-days-to-retain`*). Por exemplo, se o evento mais antigo que você está copiando tiver 45 dias e você quiser manter os eventos no armazenamento de dados de eventos por mais 45 dias, defina o período de retenção como 90 dias.
- Se você estiver copiando eventos de trilha para um armazenamento de dados de eventos para investigação e não quiser ingerir nenhum evento futuro, poderá interromper a ingestão no armazenamento de dados de eventos. Ao criar o armazenamento de dados de eventos, desmarque a opção Ingerir eventos (etapa 15 do procedimento) para garantir que o armazenamento de dados de eventos contenha somente os eventos históricos da sua trilha e nenhum evento futuro.
- Antes de copiar os eventos da trilha, desative todas as listas de controle de acesso (ACLs) anexadas ao bucket do S3 de origem e atualize a política do bucket do S3 para o armazenamento de dados de eventos de destino. Para obter mais informações sobre a atualização da política de bucket do S3, consulte Política de buckets do Amazon S3 para copiar eventos da trilha. Para obter mais informações sobre desabilitação de ACLs, consulte Controlar a propriedade de objetos e desabilitar ACLs para seu bucket no Guia do usuário do Amazon S3.
- CloudTrail copia somente eventos de trilha de arquivos de log compactados Gzip que estão no bucket S3 de origem. CloudTrail não copia eventos de trilha de arquivos de log não compactados ou arquivos de log que foram compactados usando um formato diferente de Gzip.
- Para evitar a duplicação de eventos entre a trilha de origem e o armazenamento de dados de eventos de destino, escolha um intervalo de tempo para os eventos copiados que seja anterior à criação do armazenamento de dados de eventos.
- Por padrão, copia CloudTrail somente CloudTrail os eventos contidos no prefixo do bucket do S3 e os `CloudTrail` prefixos dentro do `CloudTrail` prefixo, e não verifica os prefixos de outros

serviços. AWS Se quiser copiar CloudTrail eventos contidos em outro prefixo, você deve escolher o prefixo ao copiar eventos de trilha.

- Para copiar eventos de trilha para um armazenamento de dados de eventos da organização, use a conta de gerenciamento da organização. A conta de administrador delegado não pode copiar eventos de trilhas para um armazenamento de dados de eventos da organização.

Permissões necessárias para copiar eventos da trilha

Antes de copiar os eventos da trilha, verifique se você tem todas as permissões necessárias para sua função do IAM. Se você escolher um perfil do IAM existente para copiar os eventos da trilha, atualizar as permissões do perfil do IAM será o suficiente. Se você optar por criar uma nova função do IAM, CloudTrail forneça todas as permissões necessárias para a função.

Se o bucket do S3 de origem usar uma chave KMS para criptografia de dados, certifique-se de que a política de chaves do KMS permita CloudTrail descriptografar dados no bucket. Se o bucket do S3 de origem usar várias chaves KMS, você deverá atualizar a política de cada chave CloudTrail para permitir a descriptografia de dados no bucket.

Tópicos

- Permissões do IAM para copiar eventos da trilha
- Política de buckets do Amazon S3 para copiar eventos da trilha
- Política de chaves do KMS para descriptografar dados no bucket do S3 de origem

Permissões do IAM para copiar eventos da trilha

Ao copiar os eventos da trilha, você tem a opção de criar um perfil do IAM ou usar um perfil do IAM existente. Quando você escolhe uma nova função do IAM, CloudTrail cria uma função do IAM com as permissões necessárias e nenhuma ação adicional é necessária de sua parte.

Se você escolher uma função existente, certifique-se de que as políticas da função do IAM CloudTrail permitam copiar eventos de trilha do bucket S3 de origem. Esta seção fornece exemplos das políticas de confiança e permissões do perfil do IAM necessárias.

O exemplo a seguir fornece a política de permissões, que CloudTrail permite copiar eventos de trilha do bucket S3 de origem. Substitua *myBucketNamemyAccountId*, *region*, *prefix* e *eventDataStoreId* pelos valores apropriados para sua configuração. O *myAccountID* é o ID da

AWS conta usado para o CloudTrail Lake, que pode não ser o mesmo que o ID da AWS conta do bucket do S3.

Substitua *key-region*, *keyAccountID* e *keyID* pelos valores da chave do KMS usada para criptografar o bucket do S3 de origem. Você poderá omitir a instrução `AWSCloudTrailImportKeyAccess` se o bucket do S3 de origem não usar uma chave KMS para criptografia.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSCloudTrailImportBucketAccess",
      "Effect": "Allow",
      "Action": ["s3:ListBucket", "s3:GetBucketAcl"],
      "Resource": [
        "arn:aws:s3:::myBucketName"
      ],
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "myAccountID",
          "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdataStore/eventDataStoreId"
        }
       }
    },
    {
      "Sid": "AWSCloudTrailImportObjectAccess",
      "Effect": "Allow",
      "Action": ["s3:GetObject"],
      "Resource": [
        "arn:aws:s3:::myBucketName/prefix",
        "arn:aws:s3:::myBucketName/prefix/*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "myAccountID",
          "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdataStore/eventDataStoreId"
        }
       }
    },
    {
```

```
      "Sid": "AWSCloudTrailImportKeyAccess",
      "Effect": "Allow",
      "Action": ["kms:GenerateDataKey","kms:Decrypt"],
      "Resource": [
        "arn:aws:kms:key-region:keyAccountID:key/keyID"
      ]
    }
  ]
}
```

O exemplo a seguir fornece a política de confiança do IAM, que CloudTrail permite assumir uma função do IAM para copiar eventos de trilha do bucket S3 de origem. Substitua *myAccountId*, *region* e *eventDataStoreArn* pelos valores apropriados para sua configuração. O *myAccountID* é o Conta da AWS ID usado para o CloudTrail Lake, que pode não ser o mesmo que o ID da AWS conta para o bucket do S3.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "myAccountID",
          "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdataStore/eventDataStoreId"
        }
      }
    }
  ]
}
```

Política de buckets do Amazon S3 para copiar eventos da trilha

Por padrão, os buckets e objetos do Amazon S3 são privados. Somente o proprietário do recurso (a conta da AWS que criou o bucket) pode acessar o bucket e os objetos que ele contém. O proprietário

do recurso pode conceder permissões de acesso a outros recursos e usuários ao criar uma política de acesso padrão.

Antes de copiar eventos de trilha, você deve atualizar a política de bucket do S3 CloudTrail para permitir a cópia de eventos de trilha do bucket do S3 de origem.

Você pode adicionar a seguinte declaração à política de bucket do S3 para conceder essas permissões. Substitua *roLearn* e *myBucketName*pelos valores apropriados para sua configuração.

```
{
  "Sid": "AWSCloudTrailImportBucketAccess",
  "Effect": "Allow",
  "Action": [
    "s3:ListBucket",
    "s3:GetBucketAcl",
    "s3:GetObject"
  ],
  "Principal": {
    "AWS": "roleArn"
  },
  "Resource": [
    "arn:aws:s3:::myBucketName",
    "arn:aws:s3:::myBucketName/*"
  ]
},
```

Política de chaves do KMS para descriptografar dados no bucket do S3 de origem

Se o bucket do S3 de origem usar uma chave KMS para criptografia de dados, certifique-se de que a política de chaves do KMS forneça CloudTrail `kms:GenerateDataKey` as permissões `kms:Decrypt` e as permissões necessárias para copiar eventos de trilha de um bucket do S3 com a criptografia SSE-KMS ativada. Se o bucket do S3 de origem usar várias chaves do KMS, será necessário atualizar a política de cada chave. A atualização da política de chaves do KMS permite CloudTrail descriptografar dados no bucket S3 de origem, executar verificações de validação para garantir que os eventos estejam em conformidade com os CloudTrail padrões e copiar eventos para o armazenamento de dados de eventos do Lake. CloudTrail

O exemplo a seguir fornece a política de chaves do KMS, que permite CloudTrail descriptografar os dados no bucket S3 de origem. Substitua *roLearn myBucketName*, *myAccountId*, *region* e

eventDataStoreId pelos valores apropriados para sua configuração. O *myAccountID* é o ID da AWS conta usado para o CloudTrail Lake, que pode não ser o mesmo que o ID da AWS conta do bucket do S3.

```
{
  "Sid": "AWSCloudTrailImportDecrypt",
  "Effect": "Allow",
  "Action": [
          "kms:Decrypt",
          "kms:GenerateDataKey"
  ],
  "Principal": {
    "AWS": "roleArn"
  },
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::myBucketName/*"
    },
    "StringEquals": {
      "aws:SourceAccount": "myAccountID",
      "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdataStore/eventDataStoreId"
    }
  }
}
```

Copiar eventos de trilhas para um armazenamento de dados de eventos existente

Use o procedimento a seguir para copiar eventos de trilha para um armazenamento de dados de eventos existentes. Para obter informações sobre como criar um armazenamento de dados de eventos, consulte Crie um armazenamento de dados de CloudTrail eventos para eventos com o console.

> **Note**
>
> Antes de copiar eventos de trilha para um armazenamento de dados de eventos existente, certifique-se de que a opção de preço e o período de retenção do armazenamento de dados de eventos estejam configurados adequadamente para seu caso de uso.

- Opção de preço: a opção de preço determina o custo de ingestão e armazenamento de eventos. Para obter mais informações sobre opções de preço, consulte Preço do AWS CloudTrail e Opções de preços do armazenamento de dados de eventos.
- Período de retenção: o período de retenção determina por quanto tempo os dados do evento são mantidos no armazenamento de dados do evento. CloudTrail copia somente eventos de trilha que tenham um período de retenção `eventTime` dentro do armazenamento de dados de eventos. Para determinar o período de retenção adequado, calcule a soma do evento mais antigo que você deseja copiar em dias e o número de dias em que deseja reter os eventos no armazenamento de dados do evento (período de retenção = *`oldest-event-in-days`*+ *`number-days-to-retain`*). Por exemplo, se o evento mais antigo que você está copiando tiver 45 dias e você quiser manter os eventos no armazenamento de dados de eventos por mais 45 dias, defina o período de retenção como 90 dias.

Para copiar eventos de trilhas para um armazenamento de dados de eventos

1. Faça login no AWS Management Console e abra o CloudTrail console em https://console.aws.amazon.com/cloudtrail/.
2. No painel de navegação, em Lake, escolha Armazenamentos de dados de eventos.
3. Escolha Copy trail events (Copiar eventos de trilha).
4. Na página Copy trail events (Copiar eventos da trilha), em Event source (Origem dos eventos), escolha a trilha que deseja copiar. Por padrão, copia CloudTrail somente CloudTrail os eventos contidos no prefixo do bucket do S3 e os `CloudTrail` prefixos dentro do `CloudTrail` prefixo, e não verifica os prefixos de outros serviços. AWS Se você quiser copiar CloudTrail eventos contidos em outro prefixo, escolha Inserir URI do S3 e, em seguida, escolha Procurar no S3 para navegar até o prefixo. Se o bucket S3 de origem da trilha usar uma chave KMS para criptografia de dados, certifique-se de que a política de chaves do KMS permita CloudTrail descriptografar os dados. Se seu bucket do S3 de origem usa várias chaves KMS, você deve atualizar a política de cada chave CloudTrail para permitir a descriptografia dos dados no bucket. Para obter mais informações sobre a atualização da política de chaves do KMS, consulte Política de chaves do KMS para descriptografar dados no bucket do S3 de origem.

   A política de bucket do S3 deve conceder CloudTrail acesso a eventos de trilha de cópia do seu bucket do S3. Para obter mais informações sobre a atualização da política de bucket do S3, consulte Política de buckets do Amazon S3 para copiar eventos da trilha.

5. Em Especificar um intervalo de tempo de eventos, escolha o intervalo de tempo para copiar os eventos. CloudTrail verifica o prefixo e o nome do arquivo de log para verificar se o nome contém uma data entre as datas de início e término escolhidas antes de tentar copiar os eventos da trilha. É possível escolher entre Relative range (Intervalo relativo) e Absolute range (Intervalo absoluto). Para evitar a duplicação de eventos entre a trilha de origem e o armazenamento de dados de eventos de destino, escolha um intervalo de tempo que seja anterior à criação do armazenamento de dados de eventos.

   > **Note**
   >
   > CloudTrail copia somente eventos de trilha que tenham um período de retenção `eventTime` dentro do armazenamento de dados de eventos. Por exemplo, se o período de retenção de um armazenamento de dados de eventos for de 90 dias, não CloudTrail copiará nenhum evento de trilha com `eventTime` mais de 90 dias.

   - Se você escolher Intervalo relativo, poderá optar por copiar eventos registrados nos últimos 6 meses, 1 ano, 2 anos, 7 anos ou um intervalo personalizado. CloudTrail copia os eventos registrados dentro do período de tempo escolhido.
   - Se você escolher Intervalo absoluto, poderá escolher uma data específica de início e término. CloudTrail copia os eventos que ocorreram entre as datas de início e término escolhidas.
6. Em Delivery location (Local de entrega), escolha o armazenamento de dados de eventos de destino na lista suspensa.
7. Em Permissions (Permissões), escolha uma das opções de perfil do IAM a seguir. Ao escolher um perfil do IAM existente, verifique se a política de perfil do IAM fornece as permissões necessárias. Para obter mais informações sobre como atualizar as permissões do perfil do IAM, consulte Permissões do IAM para copiar eventos da trilha.

   - Escolha Create a new role (recommended) (Criar uma nova função [recomendado]) para criar um novo perfil do IAM. Em Enter IAM role name (Inserir nome do perfil do IAM), insira um nome exclusivo para o perfil. CloudTrail cria automaticamente as permissões necessárias para essa nova função.
   - Escolha Usar um ARN de função personalizada do IAM para usar uma função personalizada do IAM que não esteja listada. Em Enter IAM role ARN (Inserir ARN do perfil do IAM), insira o ARN do perfil.
   - Escolha uma função do IAM existente na lista suspensa.

8. Escolha Copy events (Copiar eventos).
9. Em seguida, sua confirmação será necessária. Quando estiver pronto para confirmar, escolha Copy trail events to Lake (Copiar eventos da trilha para o Lake) e, em seguida, escolha Copy events (Copiar eventos).
10. Na página Copy details (Copiar detalhes), é possível ver o status da cópia e revisar quaisquer falhas. Quando uma cópia de evento de trilha é concluída, seu Copy status (Status de cópia) é definido como Completed (Concluída) se não houve erros ou como Failed (Falha) se houve algum erro.

    > **Note**
    >
    > Os detalhes apresentados na página de detalhes da cópia do evento não estão em tempo real. Os valores reais dos detalhes, como Prefixes copied (prefixos copiados), podem ser maiores do que os apresentados na página. CloudTrail atualiza os detalhes de forma incremental ao longo da cópia do evento.

11. Se o Copy status (Status da cópia) for Failed (Falha), corrija os erros mostrados em Copy failures (Falhas ao copiar) e, em seguida, escolha Retry copy (Tentar cópia novamente). Quando você tenta fazer uma cópia novamente, CloudTrail retoma a cópia no local em que a falha ocorreu.

Para obter mais informações sobre como visualizar os detalhes de uma cópia de evento de trilha, consulte Detalhes da cópia de um evento.

Detalhes da cópia de um evento

Após o início de uma cópia do evento da trilha, você poderá visualizar os detalhes da cópia do evento, incluindo o status da cópia e informações sobre qualquer falha na cópia.

> **Note**
>
> Os detalhes apresentados na página de detalhes da cópia do evento não estão em tempo real. Os valores reais dos detalhes, como Prefixes copied (prefixos copiados), podem ser maiores do que os apresentados na página. CloudTrail atualiza os detalhes de forma incremental ao longo da cópia do evento.

Para acessar a página de detalhes da cópia de um evento

1. Faça login no AWS Management Console e abra o CloudTrail console em https://console.aws.amazon.com/cloudtrail/.
2. No painel de navegação esquerdo, em Lake, escolha Armazenamentos de dados de eventos.
3. Escolha o armazenamento de dados de eventos.
4. Escolha a cópia do evento na seção Event copy status (Status da cópia de um evento).

Detalhes da cópia

Em Copy details (Detalhes da cópia), é possível visualizar os seguintes detalhes sobre a cópia de evento da trilha.

- Event log S3 location (Local do log de eventos no S3): a localização do bucket do S3 de origem que contém os arquivos de log de eventos da trilha.
- Copy ID (ID da cópia): a identificação da cópia.
- Prefixes copied (Prefixos copiados): representa o número de prefixos do S3 copiados. Durante a cópia de um evento de trilha, CloudTrail copia os eventos nos arquivos de registro de trilha que estão armazenados nos prefixos.
- Copy status (Status da cópia): o status da cópia.
  - Initializing (Inicializando): status inicial exibido quando a cópia do evento da trilha é iniciada.
  - In progress (Em andamento): indica que a cópia do evento da trilha está em andamento.

    > **Note**
    >
    > Não é possível copiar eventos da trilha quando há outra cópia de evento da trilha In progress(Em andamento). Para parar uma cópia de evento da trilha, escolha Stop copy (Parar cópia).

  - Stopped (Parada): indica que uma ação Stop copy (Parar cópia) ocorreu. Para repetir uma cópia de evento da trilha, escolha Retry copy (Tentar cópia novamente).
  - Failed (Falha): a cópia terminou, mas não foi possível copiar alguns eventos da trilha. Revise as mensagens de erro em Copy failures (Falhas da cópia). Para repetir uma cópia de evento da trilha, escolha Retry copy (Tentar cópia novamente). Quando você tenta fazer uma cópia novamente, CloudTrail retoma a cópia no local em que a falha ocorreu.
  - Completed (Concluída): a cópia terminou sem erros. É possível consultar os eventos da trilha copiados no armazenamento de dados de eventos.

- Created time (Hora da criação): indica quando a cópia do evento da trilha foi iniciada.
- Finish time (Hora de término): indica quando a cópia do evento da trilha foi concluída ou interrompida.

Falhas da cópia

Em Copy failures (Falhas de cópia), é possível revisar o local do erro, a mensagem de erro e o tipo de erro para cada falha de cópia. Os motivos comuns de falha incluem se um prefixo S3 continha um arquivo não compactado ou continha um arquivo fornecido por um serviço diferente de. CloudTrail Outra possível causa de falha está relacionada a problemas de acesso. Por exemplo, se o bucket S3 do repositório de dados de eventos não concedesse CloudTrail acesso para importar os eventos, você receberia um `AccessDenied` erro.

Para cada falha de cópia, revise as informações de erro a seguir.

- Error location (Local do erro) indica o local no bucket do S3 em que o erro ocorreu. Se ocorresse um erro porque o bucket do S3 de origem continha um arquivo não compactado, Error location (Local do erro) incluiria o prefixo em que você encontraria esse arquivo.
- Error message (Mensagem de erro) fornece uma explicação do motivo pelo qual o erro ocorreu.
- Error type (Tipo de erro) fornece o tipo de erro. Por exemplo, o Error type (Tipo de erro) `AccessDenied` indica que o erro ocorreu devido a um problema de permissões. Para obter mais informações sobre as permissões necessárias para copiar eventos da trilha, consultePermissões necessárias para copiar eventos da trilha.

Após resolver qualquer falha, escolha Retry copy (Tentar cópia novamente). Quando você tenta fazer uma cópia novamente, CloudTrail retoma a cópia no local em que a falha ocorreu.

Exemplo: copiar eventos de trilha para um novo armazenamento de dados de eventos

Este passo a passo mostra como copiar eventos de trilha para um novo armazenamento de dados de eventos do CloudTrail Lake para análise histórica. Para obter mais informações sobre cópia de eventos de trilhas, consulte Copiar eventos de trilhas para um armazenamento de dados de eventos.

Para copiar eventos de trilhas para um novo armazenamento de dados de eventos

1. Faça login no AWS Management Console e abra o CloudTrail console em https://console.aws.amazon.com/cloudtrail/.

2. No painel de navegação, em Lake, escolha Armazenamentos de dados de eventos.
3. Selecione Create event data store (Criar armazenamento de dados de eventos).
4. Na página Configurar armazenamento de dados de eventos, em Detalhes gerais, dê um nome ao seu armazenamento de dados de eventos, como *my-management-events-eds*. Como prática recomendada, use um nome que identifique rapidamente a finalidade do armazenamento de dados de eventos. Para obter informações sobre os requisitos CloudTrail de nomenclatura, consulteRequisitos de nomenclatura.
5. Escolha a opção de preço que você deseja usar para o armazenamento de dados de eventos. A opção de preço determina o custo para a ingestão e para o armazenamento de eventos, e os períodos de retenção padrão e máximo para o armazenamento de dados de eventos. Para obter mais informações, consulte Preços do AWS CloudTrail e Gerenciando os custos CloudTrail do Lake.

   As seguintes opções estão disponíveis:

   - Preço de retenção extensível de um ano: geralmente recomendado se você espera ingerir menos de 25 TB de dados de eventos por mês e deseja um período de retenção flexível de até 10 anos. Nos primeiros 366 dias (o período de retenção padrão), o armazenamento é incluído sem custo adicional no preço de ingestão. Depois de 366 dias, a retenção estendida está disponível pelo pay-as-you-go preço. Esta é a opção padrão.
     - Período de retenção padrão: 366 dias
     - Período máximo de retenção: 3.653 dias
   - Preço de retenção de sete anos: recomendado se você espera ingerir mais de 25 TB de dados de eventos por mês e precisa de um período de retenção de até 7 anos. A retenção está incluída no preço de ingestão sem custo adicional.
     - Período de retenção padrão: 2.557 dias
     - Período máximo de retenção: 2.557 dias
6. Especifique um período de retenção para o armazenamento de dados de eventos. Os períodos de retenção podem ser entre 7 dias e 3.653 dias (cerca de 10 anos) para a opção de preço de retenção extensível de um ano ou entre 7 dias e 2.557 dias (cerca de sete anos) para a opção de preço de retenção de sete anos.

   CloudTrail Lake determina se deve reter um evento verificando se o `eventTime` evento está dentro do período de retenção especificado. Por exemplo, se você especificar um período de retenção de 90 dias, CloudTrail removerá eventos quando tiverem `eventTime` mais de 90 dias.

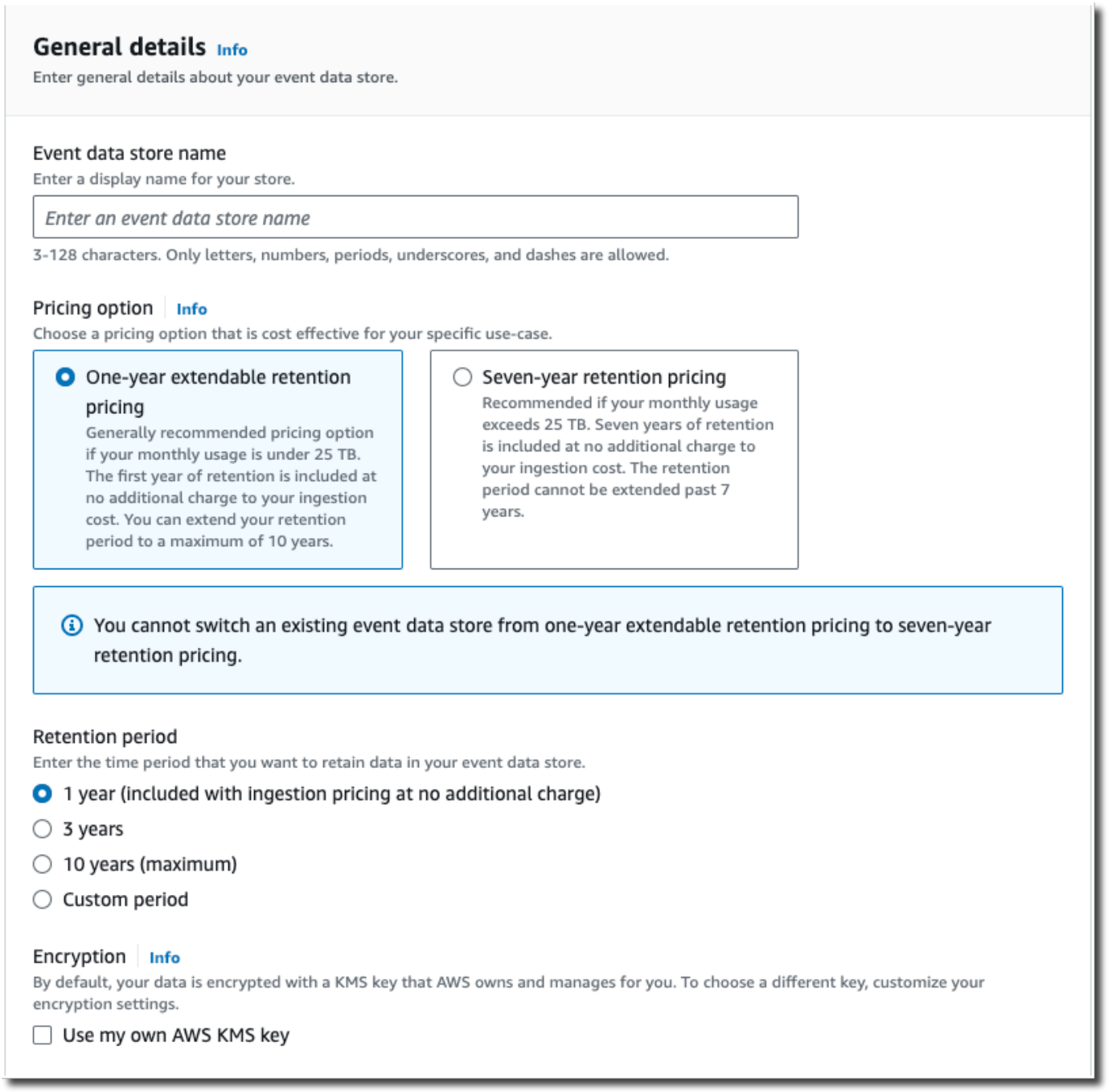
> **Note**
>
> CloudTrail não copiará um evento se ele `eventTime` for anterior ao período de retenção especificado.
> Para determinar o período de retenção adequado, calcule a soma do evento mais antigo que você deseja copiar em dias e o número de dias em que deseja reter os eventos no armazenamento de dados do evento (período de retenção = *`oldest-event-in-days`*+ *`number-days-to-retain`*). Por exemplo, se o evento mais antigo que você está copiando tiver 45 dias e você quiser manter os eventos no armazenamento de dados de eventos por mais 45 dias, defina o período de retenção como 90 dias.

7. (Opcional) Em Criptografia, escolha se você deseja criptografar o armazenamento de dados do evento usando sua própria chave do KMS. Por padrão, todos os eventos em um armazenamento de dados de eventos são criptografados CloudTrail usando uma chave KMS que AWS possui e gerencia para você.

   Para habilitar a criptografia usando sua própria chave do KMS, escolha Usar minha própria AWS KMS key. Escolha Novo para AWS KMS key criar uma para você ou escolha Existente para usar uma chave KMS existente. Em Inserir alias KMS, especifique um alias, no formato. `alias/`*`MyAliasName`* Usar sua própria chave KMS exige que você edite sua política de chaves KMS para permitir que CloudTrail os registros sejam criptografados e descriptografados. Para obter mais informações, consulteConfigure as AWS KMS principais políticas para CloudTrail. CloudTrail também oferece suporte a chaves AWS KMS multirregionais. Para obter mais informações sobre chaves de várias regiões, consulte Usar chaves de várias regiões no Manual do desenvolvedor do AWS Key Management Service .

   Usar sua própria chave KMS gera AWS KMS custos de criptografia e descriptografia. Após associar um armazenamento de dados de eventos a uma chave do KMS, não será possível remover ou alterar a chave do KMS.

   > **Note**
   >
   > Para habilitar a AWS Key Management Service criptografia para um armazenamento de dados de eventos da organização, você deve usar uma chave KMS existente para a conta de gerenciamento.



8. (Opcional) Se você quiser consultar os dados do seu evento usando o Amazon Athena, escolha Habilitar na federação de consultas do Lake. A federação permite que você visualize os metadados associados ao armazenamento de dados de eventos no Catálogo de Dados do AWS Glue e execute consultas SQL nos dados do evento no Athena. Os metadados da tabela armazenados no Catálogo de AWS Glue Dados permitem que o mecanismo de consulta do

Athena saiba como encontrar, ler e processar os dados que você deseja consultar. Para ter mais informações, consulte Federar um armazenamento de dados de eventos.

Para habilitar a federação de consultas do Lake, escolha Habilitar e faça o seguinte:

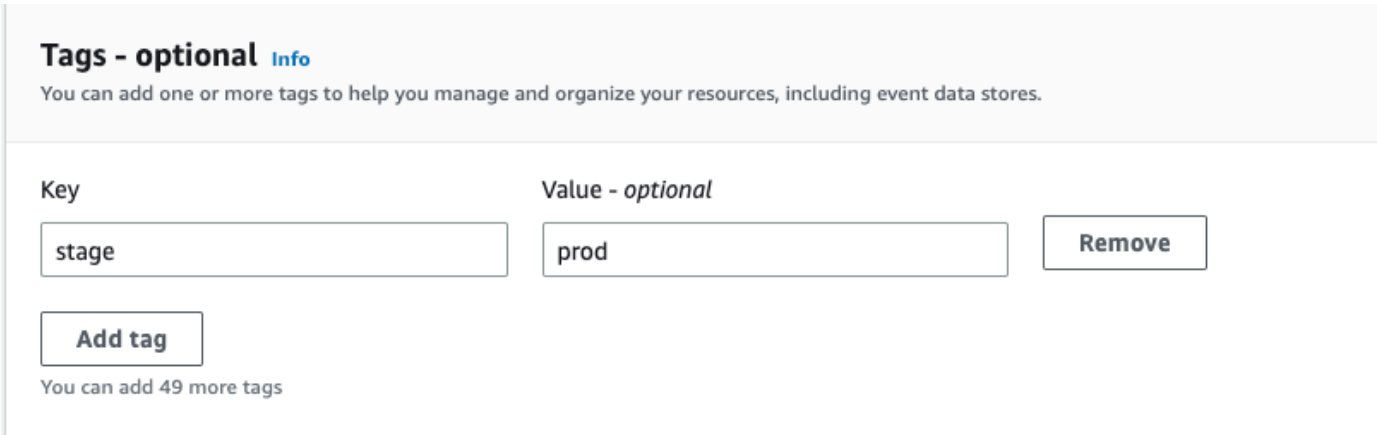
a. Escolha se deseja criar um perfil ou usar um perfil do IAM existente. O AWS Lake Formation usa esse perfil para gerenciar permissões para o armazenamento de dados de eventos federados. Quando você cria uma nova função usando o CloudTrail console, cria CloudTrail automaticamente uma função com as permissões necessárias. Se você escolher um perfil existente, a política do perfil deve fornecer as permissões mínimas necessárias.

b. Se você estiver criando um perfil, insira um nome para identificá-lo.

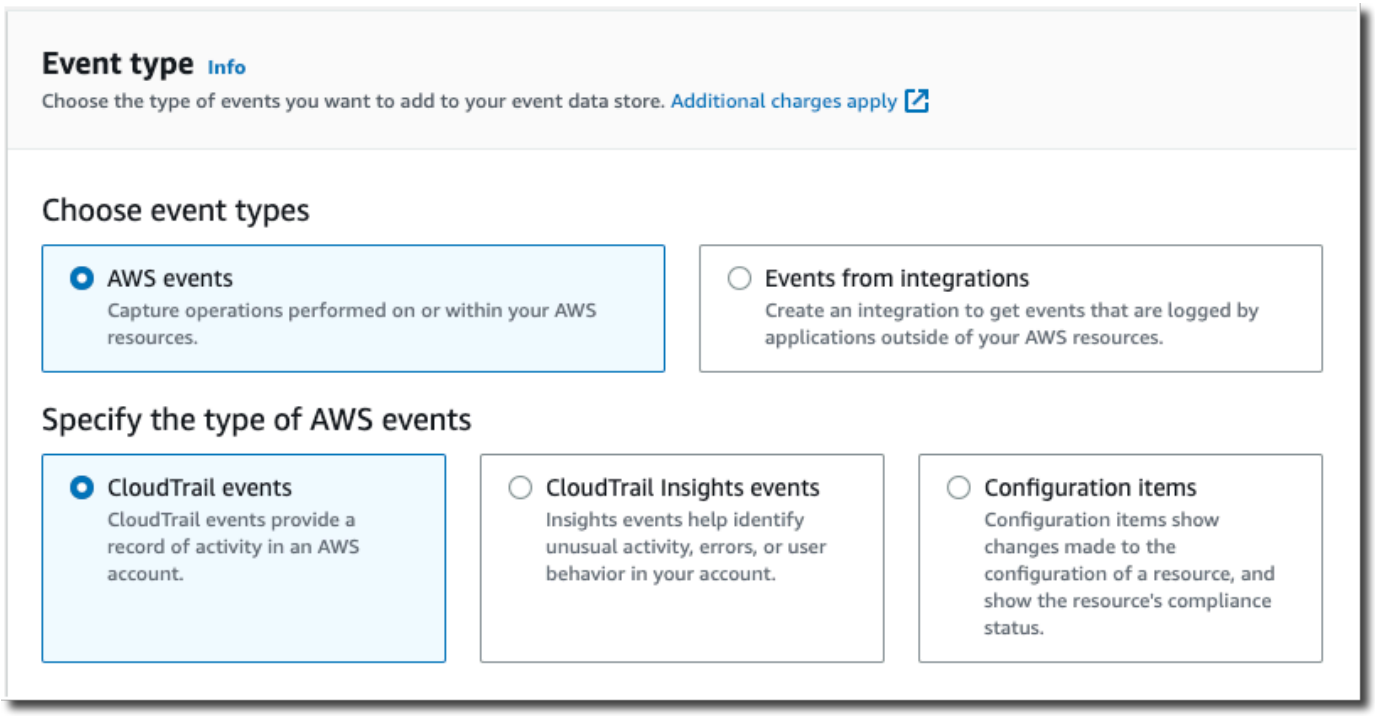
c. Se você estiver usando um perfil existente, escolha o perfilo que deseja usar. O perfil deve existir em sua conta.

9. (Opcional) Em Tags, adicione uma ou mais tags personalizadas (pares chave-valor) ao armazenamento de dados de eventos. As tags podem ajudar você a identificar seus repositórios de dados de CloudTrail eventos. Por exemplo, você poderia anexar uma tag com o nome **`stage`** e o valor **`prod`**. É possível usar tags para limitar o acesso ao armazenamento de dados de eventos. As tags também podem ser usadas para monitorar os custos de consulta e ingestão do seu armazenamento de dados de eventos.

   Para obter informações sobre como usar tags para monitorar os custos, consulte Criação de etiquetas de alocação de custos definidas pelo usuário para armazenamentos de dados de eventos do CloudTrail Lake. Para obter informações sobre como usar políticas do IAM para autorizar o acesso a um armazenamento de dados de eventos com base em tags, consulte Exemplos: negação de acesso para criar ou excluir armazenamentos de dados de eventos com base em tags. Para obter informações sobre como você pode usar tags em AWS, consulte Como marcar seus AWS recursos no Guia do usuário de AWS recursos de marcação.

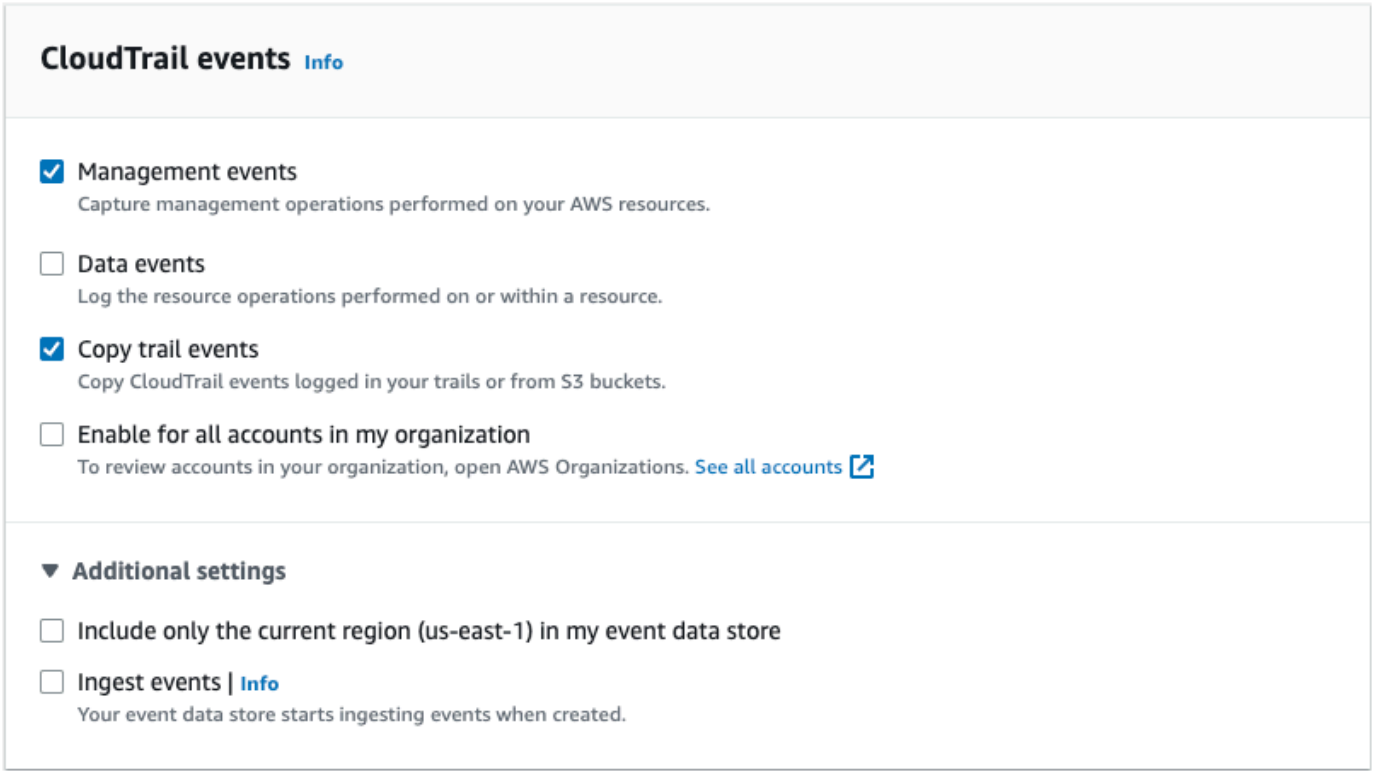


10. Escolha Next (Avançar) para configurar o armazenamento de dados de eventos.
11. Na página Escolher eventos, mantenha as seleções padrão para Tipo de evento.



12. Para CloudTrail eventos, deixaremos os eventos de gerenciamento selecionados e escolheremos Copiar eventos da trilha. Neste exemplo, não estamos preocupados com os tipos de eventos porque estamos usando somente o armazenamento de dados de eventos para analisar eventos passados e não estamos ingerindo eventos futuros.

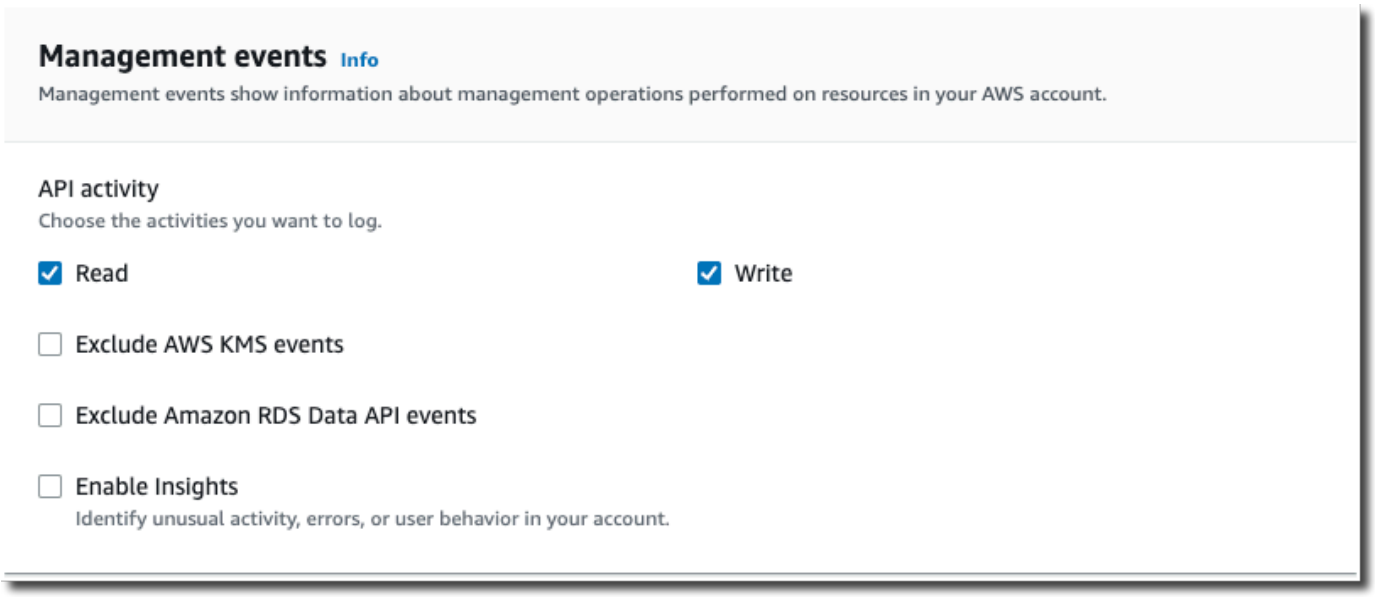
    Se você estiver criando um armazenamento de dados de eventos para substituir uma trilha existente, escolha os mesmos seletores de eventos da sua trilha para garantir que o armazenamento de dados de eventos tenha a mesma cobertura de eventos.



13. Escolha Habilitar para todas as contas em minha organização se este for um armazenamento de dados de eventos da organização. Essa opção não estará disponível para alteração, a menos que você tenha contas configuradas no AWS Organizations.

> **Note**
>
> Ao criar um armazenamento de dados de eventos da organização, você deverá estar conectado com a conta de gerenciamento da organização, pois somente a conta de gerenciamento pode copiar eventos de trilha para um armazenamento de dados de eventos da organização.

14. Em Configurações adicionais, desmarcaremos a opção Ingerir eventos porque, em nosso exemplo, não queremos que o armazenamento de dados de eventos consuma eventos futuros, pois estamos interessados apenas em consultar os eventos copiados. Por padrão, um armazenamento de dados de eventos coleta eventos para todos Regiões da AWS e começa a ingerir eventos quando é criado.
15. Em Eventos de gerenciamento, manteremos as configurações padrão.



16. Na área Copiar eventos da trilha, conclua as etapas a seguir.

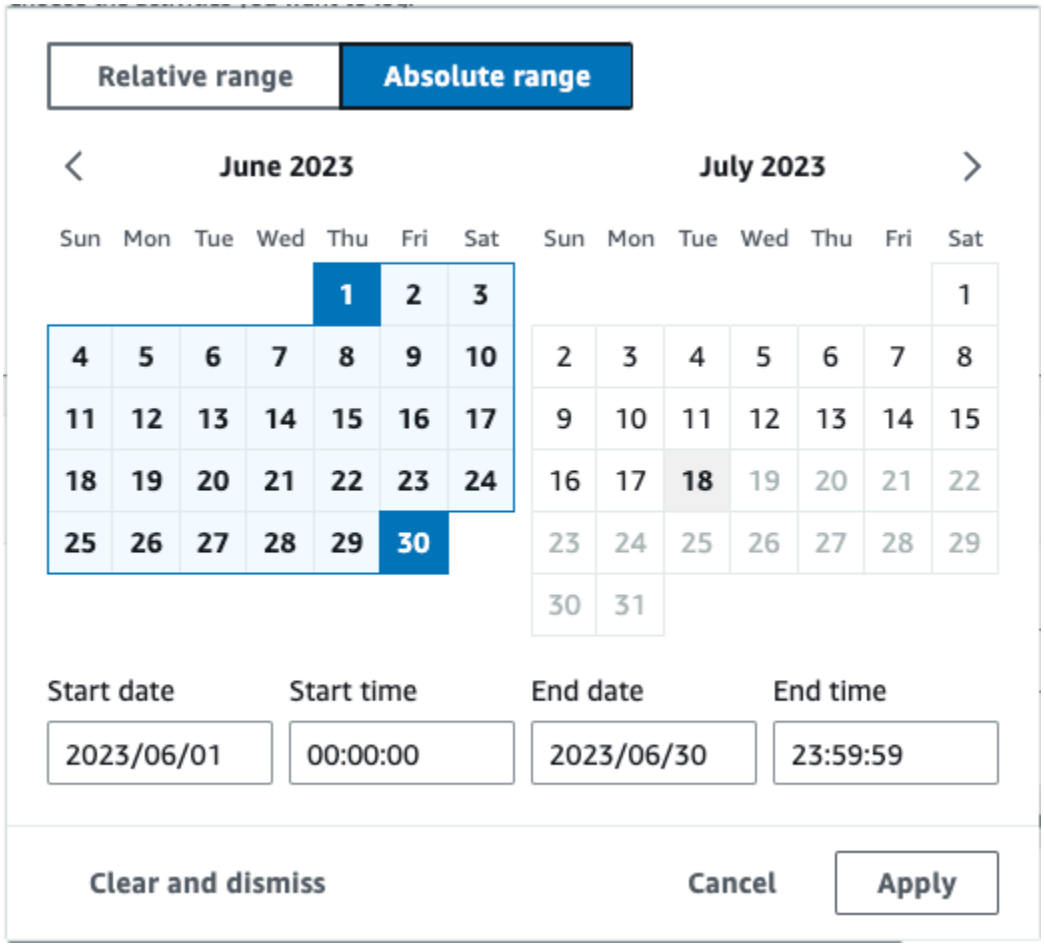
    a. Escolha a trilha que você deseja copiar. Neste exemplo, escolheremos uma trilha chamada *`management-events`*.

       Por padrão, copia CloudTrail somente CloudTrail os eventos contidos no prefixo do bucket do S3 e os `CloudTrail` prefixos dentro do `CloudTrail` prefixo, e não verifica os prefixos de outros serviços. AWS Se você quiser copiar CloudTrail eventos contidos em outro prefixo, escolha Inserir URI do S3 e, em seguida, escolha Procurar no S3 para navegar até o prefixo. Se o bucket S3 de origem da trilha usar uma chave KMS para criptografia de dados, certifique-se de que a política de chaves do KMS permita CloudTrail descriptografar os dados. Se seu bucket do S3 de origem usa várias chaves KMS, você deve atualizar a política de cada chave CloudTrail para permitir a descriptografia dos dados no bucket. Para obter mais informações sobre a atualização da política de chaves do KMS, consulte Política de chaves do KMS para descriptografar dados no bucket do S3 de origem.

    b. Escolha um intervalo de tempo para copiar os eventos. CloudTrail verifica o prefixo e o nome do arquivo de log para verificar se o nome contém uma data entre as datas de início e término escolhidas antes de tentar copiar os eventos da trilha. É possível escolher entre Relative range (Intervalo relativo) e Absolute range (Intervalo absoluto). Para evitar a duplicação de eventos entre a trilha de origem e o armazenamento de dados de eventos de destino, escolha um intervalo de tempo que seja anterior à criação do armazenamento de dados de eventos.

- Se você escolher Intervalo relativo, poderá optar por copiar eventos registrados nos últimos 6 meses, 1 ano, 2 anos, 7 anos ou um intervalo personalizado. CloudTrail copia os eventos registrados dentro do período de tempo escolhido.
- Se você escolher Intervalo absoluto, poderá escolher uma data específica de início e término. CloudTrail copia os eventos que ocorreram entre as datas de início e término escolhidas.

Neste exemplo, escolheremos Intervalo absoluto e selecionaremos todo o mês de junho.



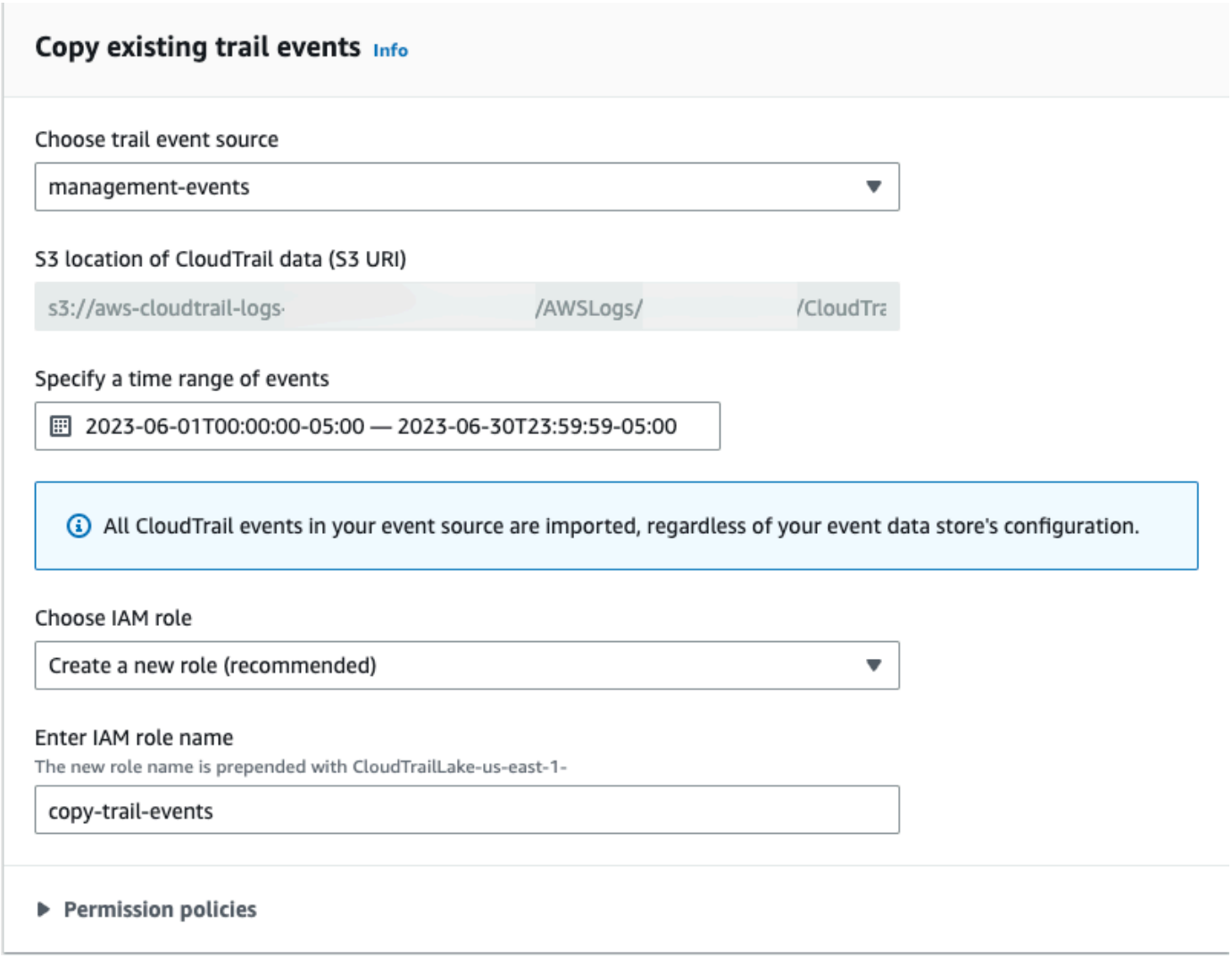
c. Em Permissions (Permissões), escolha uma das opções de perfil do IAM a seguir. Ao escolher um perfil do IAM existente, verifique se a política de perfil do IAM fornece as permissões necessárias. Para obter mais informações sobre como atualizar as permissões do perfil do IAM, consulte Permissões do IAM para copiar eventos da trilha.

- Escolha Create a new role (recommended) (Criar uma nova função [recomendado]) para criar um novo perfil do IAM. Em Inserir nome da função do IAM, insira um nome para

a função. CloudTrail cria automaticamente as permissões necessárias para essa nova função.

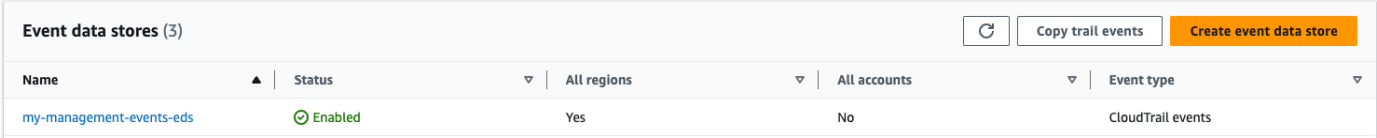
- Escolha Usar um ARN de função personalizada do IAM para usar uma função personalizada do IAM que não esteja listada. Em Enter IAM role ARN (Inserir ARN do perfil do IAM), insira o ARN do perfil.
- Escolha uma função do IAM existente na lista suspensa.

Neste exemplo, escolheremos Criar um novo perfil (recomendado) e forneceremos o nome **`copy-trail-events`**.



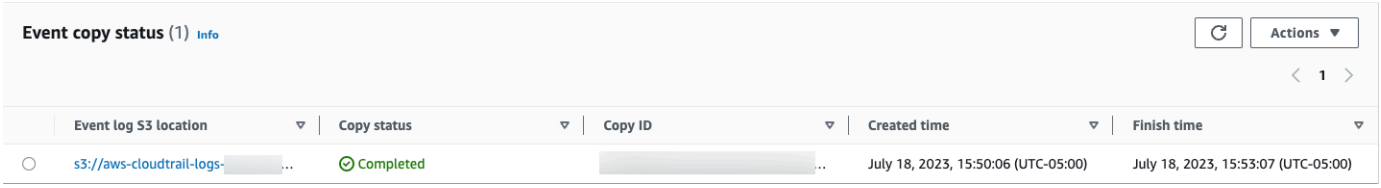
17. Selecione Next (Próximo) para revisar suas escolhas.

18. Na página Review and create (Revisar e criar), revise as suas escolhas. Escolha Edit (Editar) para fazer alterações a uma seção. Quando estiver pronto para criar o armazenamento de dados de eventos, escolha Create event data store (Criar armazenamento de dados de eventos).
19. O novo armazenamento de dados de eventos está visível na tabela Armazenamentos de dados de eventos na página Armazenamento de dados de eventos.

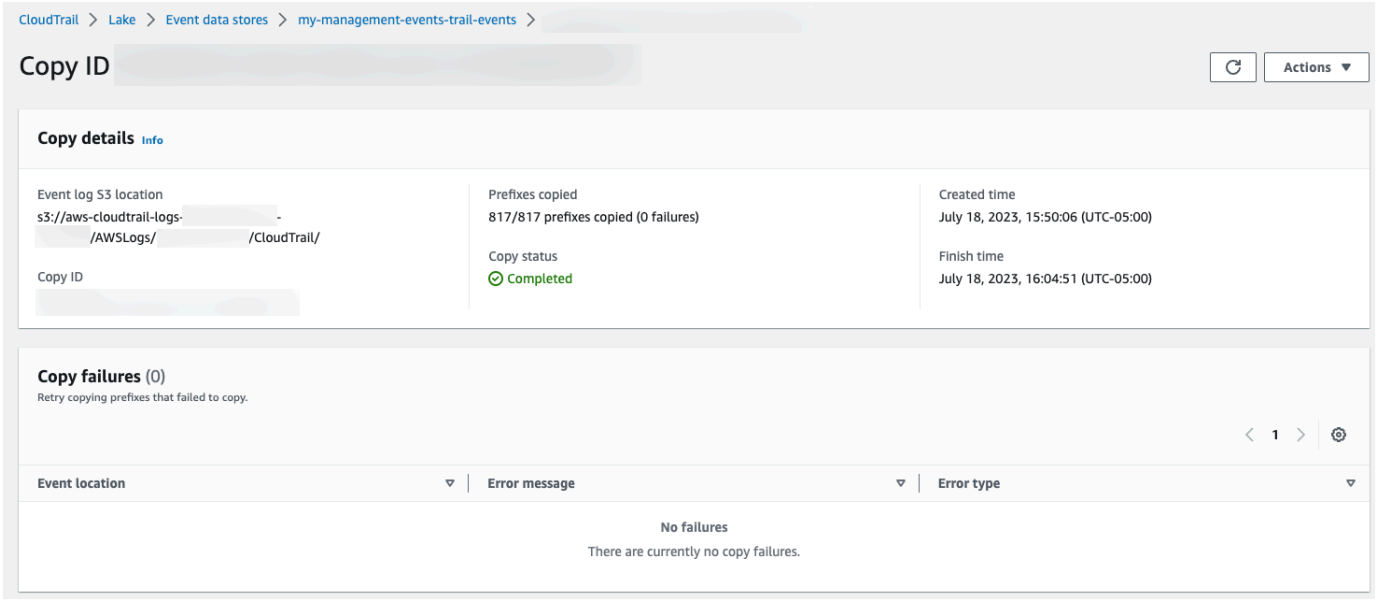


20. Escolha o nome do armazenamento de dados de eventos para visualizar sua página de detalhes. A página de detalhes mostra os detalhes do armazenamento de dados de eventos e o status da cópia. O status da cópia de eventos é mostrado na área Status da cópia de eventos.

    Quando uma cópia de evento de trilha é concluída, seu Copy status (Status de cópia) é definido como Completed (Concluída) se não houve erros ou como Failed (Falha) se houve algum erro.



21. Para visualizar mais detalhes sobre a cópia, escolha o nome da cópia na coluna Localização do log de eventos no S3 ou escolha a opção Visualizar detalhes no menu Ações. Para obter mais informações sobre como visualizar os detalhes de uma cópia de evento de trilha, consulte Detalhes da cópia de um evento.



22. A área Falhas de cópia mostra todos os erros que ocorreram ao copiar eventos de trilha. Se o Copy status (Status da cópia) for Failed (Falha), corrija os erros mostrados em Copy failures (Falhas ao copiar) e, em seguida, escolha Retry copy (Tentar cópia novamente). Quando você tenta fazer uma cópia novamente, CloudTrail retoma a cópia no local em que a falha ocorreu.

Federar um armazenamento de dados de eventos

A federação de um armazenamento de dados de eventos permite que você visualize os metadados associados ao armazenamento de dados de eventos no catálogo de AWS Glue dados, registre o catálogo de dados com AWS Lake Formation e permita executar consultas SQL em seus dados de eventos usando o Amazon Athena. Os metadados da tabela armazenados no Catálogo de AWS Glue Dados permitem que o mecanismo de consulta do Athena saiba como encontrar, ler e processar os dados que você deseja consultar.

Você pode ativar a federação usando o CloudTrail console ou AWS CLI a operação EnableFederationda API. Quando você ativa a federação de consultas do Lake, CloudTrail cria um banco de dados gerenciado chamado `aws:cloudtrail` (se o banco de dados ainda não existir) e uma tabela federada gerenciada no Catálogo de AWS Glue Dados. O ID do armazenamento de dados do evento é usado para o nome da tabela. CloudTrail registra o ARN da função de federação e o armazenamento de dados de eventos AWS Lake Formationno, o serviço responsável por permitir o controle de acesso refinado dos recursos federados no Catálogo de Dados. AWS Glue

Para habilitar a federação de consultas do Lake, você deve criar um perfil do IAM ou escolher um perfil existente. O Lake Formation usa esse perfil para gerenciar permissões para o armazenamento de dados de eventos federados. Quando você cria uma nova função usando o CloudTrail console, cria CloudTrail automaticamente as permissões necessárias para a função. Se você escolher um perfil existente, certifique-se de que ele forneça as permissões mínimas.

Você pode desativar a federação usando o CloudTrail console ou AWS CLI a operação DisableFederationda API. Quando você desativa a federação, CloudTrail desativa a integração com AWS Glue AWS Lake Formation, e com o Amazon Athena. Depois de desabilitar a federação de consultas do Lake, você não poderá mais consultar seus dados de eventos no Athena. Nenhum dado do CloudTrail Lake é excluído quando você desativa a federação e você pode continuar executando consultas no CloudTrail Lake.

Não há CloudTrail cobranças pela federação de um armazenamento de dados de eventos do CloudTrail Lake. Há custos para realizar consultas no Amazon Athena. Para obter informações sobre preços do Athena, consulte os Preços do Amazon Athena.

Analise registros de atividades com o AWS CloudTrail Lake e o Amazon Athena

Tópicos

Considerações

Considere os seguintes fatores ao federar um armazenamento de dados de eventos:

- Não há CloudTrail cobranças pela federação de um armazenamento de dados de eventos do CloudTrail Lake. Há custos para realizar consultas no Amazon Athena. Para obter informações sobre preços do Athena, consulte os Preços do Amazon Athena.
- O Lake Formation é usado para gerenciar permissões para os recursos federados. Se você excluir a função da federação ou revogar as permissões para os recursos do Lake Formation ou AWS Glue não puder executar consultas do Athena. Para obter mais informações sobre como trabalhar com o Lake Formation, consulte Gerenciando os recursos da Federação do CloudTrail Lago com AWS Lake Formation.
- Qualquer pessoa que usa o Amazon Athena para consultar dados registrados no Lake Formation deve ter uma política de permissões do IAM que permita a ação `lakeformation:GetDataAccess`. A política AWS gerenciada: AmazonAthenaFullAccesspermite essa ação. Se você usar políticas em linha, atualize as políticas de permissões para permitir essa ação. Para obter mais informações, consulte Gerenciar permissões de usuário do Lake Formation e do Athena.
- Para criar visualizações em tabelas federadas no Athena, você precisa de um banco de dados de destino diferente de `aws:cloudtrail`. Isso ocorre porque o `aws:cloudtrail` banco de dados é gerenciado pelo CloudTrail.
- Para criar um conjunto de dados na Amazon QuickSight, você deve escolher a opção Usar SQL personalizado. Para obter mais informações, consulte Creating a dataset using Amazon Athena data.

- Se a federação estiver habilitada, não será possível excluir um armazenamento de dados de eventos. Para excluir um armazenamento de dados de eventos federados, primeiro você deve desabilitar a federação e a proteção contra encerramento, se estiver habilitada.
- As seguintes considerações se aplicam aos armazenamentos de dados de eventos da organização:
  - Somente uma única conta de administrador delegado ou a conta de gerenciamento pode habilitar a federação em um armazenamento de dados de eventos da organização. Outras contas de administrador delegado ainda podem consultar e compartilhar informações usando o atributo de compartilhamento de dados do Lake Formation.
  - Qualquer conta de administrador delegado ou conta de gerenciamento da organização pode desabilitar a federação.

Permissões necessárias para federação

Antes de federar um armazenamento de dados de eventos, certifique-se de ter todas as permissões necessárias para o perfil de federação e para habilitar e desabilitar a federação. Se você escolher um perfil do IAM existente para habilitar a federação, somente precisará atualizar as permissões do perfil da federação. Se você optar por criar uma nova função do IAM usando o CloudTrail console, CloudTrail fornecerá todas as permissões necessárias para a função.

Tópicos

Permissões do IAM para federar um armazenamento de dados de eventos

Ao habilitar uma federação, você tem a opção de criar um perfil do IAM ou usar um perfil do IAM existente. Quando você escolhe uma nova função do IAM, CloudTrail cria uma função do IAM com as permissões necessárias e nenhuma ação adicional é necessária de sua parte.

Se você escolher um perfil existente, certifique-se de que as políticas de perfil do IAM forneçam as permissões necessárias para habilitar a federação. Esta seção fornece exemplos das políticas de confiança e permissões do perfil do IAM necessárias.

O exemplo a seguir fornece a política de permissões para o perfil de federação. Para a primeira declaração, forneça o ARN completo do seu armazenamento de dados de eventos para o `Resource`.

A segunda declaração nesta política permite que o Lake Formation decifre dados para um armazenamento de dados de eventos criptografado com uma chave KMS. Substitua *`key-region`*, *`account-id`* e *`key-id`* pelos valores da sua chave KMS. Você poderá omitir essa instrução se o armazenamento de dados de eventos não usar uma chave KMS para criptografia.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "LakeFederationEDSDataAccess",
            "Effect": "Allow",
            "Action": "cloudtrail:GetEventDataStoreData",
            "Resource": "arn:aws:cloudtrail:eds-region:account-id:eventdatastore/eds-
id"
        },
        {
          "Sid": "LakeFederationKMSDecryptAccess",
          "Effect": "Allow",
          "Action": [
              "kms:Decrypt",
              "kms:GenerateDataKey"
          ],
          "Resource": "arn:aws:kms:key-region:account-id:key/key-id"
      }
    ]
}
```

O exemplo a seguir fornece a política de confiança do IAM que permite ao AWS Lake Formation presumir um perfil do IAM para gerenciar permissões para o armazenamento de dados de eventos federados.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "lakeformation.amazonaws.com"
```

```
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Permissões necessárias para habilitar a federação

O exemplo de política a seguir fornece as permissões obrigatórias mínimas para habilitar a federação em um armazenamento de dados de eventos. Essa política permite CloudTrail habilitar a federação no armazenamento de dados de eventos, AWS Glue criar os recursos federados no Catálogo de AWS Glue Dados e AWS Lake Formation gerenciar o registro de recursos.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow CloudTrail to enable federation on the event data store",
            "Effect": "Allow",
            "Action": "cloudtrail:EnableFederation",
            "Resource": "arn:aws:cloudtrail:region:account-id:eventdatastore/eds-id"
        },
        {
            "Sid": "Allow access to the federation role",
            "Effect": "Allow",
            "Action": [
                "iam:PassRole",
                "iam:GetRole"
            ],
            "Resource": "arn:aws:iam::region:role/federation-role-name"
        },
        {
            "Sid": "Allow AWS Glue to create the federated resources in the Data
 Catalog",
            "Effect": "Allow",
            "Action": [
                "glue:CreateDatabase",
                "glue:CreateTable",
                "glue:PassConnection"
            ],
            "Resource": [
                "arn:aws:glue:region:account-id:catalog",
                "arn:aws:glue:region:account-id:database/aws:cloudtrail",
```

```
                "arn:aws:glue:region:account-id:table/aws:cloudtrail/eds-id",
                "arn:aws:glue:region:account-id:connection/aws:cloudtrail"
            ]
        },
        {
            "Sid": "Allow Lake Formation to manage resource registration",
            "Effect": "Allow",
            "Action": [
                "lakeformation:RegisterResource",
                "lakeformation:DeregisterResource"
            ],
            "Resource": "arn:aws:lakeformation:region:account-id:catalog:account-id"
        }
    ]
}
```

Permissões necessárias para desabilitar a federação

O exemplo de política a seguir fornece os recursos mínimos necessários para desabilitar a federação em um armazenamento de dados de eventos. Essa política permite desativar CloudTrail a federação no armazenamento de dados do evento, excluir AWS Glue a tabela federada gerenciada no Catálogo de AWS Glue Dados e o Lake Formation cancelar o registro do recurso federado.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow CloudTrail to disable federation on the event data store",
            "Effect": "Allow",
            "Action": "cloudtrail:DisableFederation",
            "Resource": "arn:aws:cloudtrail:region:account-id:eventdatastore/eds-id"
        },
        {
            "Sid": "Allow AWS Glue to delete the managed federated table from the AWS
 Glue Data Catalog",
            "Effect": "Allow",
            "Action": "glue:DeleteTable",
            "Resource": [
                "arn:aws:glue:region:account-id:catalog",
                "arn:aws:glue:region:account-id:database/aws:cloudtrail",
                "arn:aws:glue:region:account-id:table/aws:cloudtrail/eds-id"
            ]
        },
```

```
        {
            "Sid": "Allow Lake Formation to deregister the resource",
            "Effect": "Allow",
            "Action": "lakeformation:DeregisterResource",
            "Resource": "arn:aws:lakeformation:region:account-id:catalog:account-id"
        }
    ]
}
```

Habilitar a federação de consultas do Lake

Você pode ativar a federação de consultas do Lake usando o CloudTrail console ou a operação EnableFederationda API. AWS CLI Quando você ativa a federação de consultas do Lake, CloudTrail cria um banco de dados gerenciado chamado `aws:cloudtrail` (se o banco de dados ainda não existir) e uma tabela federada gerenciada no Catálogo de AWS Glue Dados. O ID do armazenamento de dados do evento é usado para o nome da tabela. CloudTrail registra o ARN da função de federação e o armazenamento de dados de eventos AWS Lake Formationno, o serviço responsável por permitir o controle de acesso refinado dos recursos federados no Catálogo de Dados. AWS Glue

Esta seção descreve como habilitar a federação usando o CloudTrail console AWS CLI e.

CloudTrail console

O procedimento a seguir mostra como habilitar a federação de consultas do Lake em um armazenamento de dados de eventos existente.

1. Faça login no AWS Management Console e abra o CloudTrail console em https://console.aws.amazon.com/cloudtrail/.
2. No painel de navegação, em Lake, escolha Armazenamentos de dados de eventos.
3. Selecione o armazenamento de dados de eventos que você deseja atualizar. A página de detalhes do armazenamento de dados de eventos é aberta.
4. Na federação de consultas do Lake, escolha Editar e, em seguida, escolha Habilitar.
5. Escolha entre criar um novo perfil do IAM ou usar um perfil existente. Quando você cria uma nova função, cria CloudTrail automaticamente uma função com as permissões necessárias. Se você escolher um perfil existente, a política da perfil deve fornecer as permissões mínimas necessárias.
6. Se você estiver criando um perfil do IAM, insira um nome para ele.

7. Se você estiver escolhendo um perfil do IAM existente, escolha o perfil que deseja usar. O perfil deve existir em sua conta.
8. Escolha Salvar alterações. O status da Federação muda para `Enabled`.

AWS CLI

Para ativar a federação, execute o comando aws cloudtrail enable-federation, fornecendo os parâmetros obrigatórios --event-data-store e --role. Para --event-data-store, forneça o ARN do armazenamento de dados de eventos (ou o sufixo de ID do ARN). Para --role, forneça o ARN para seu perfil na federação. O perfil deve existir em sua conta e fornecer as permissões mínimas necessárias.

```
aws cloudtrail enable-federation
--event-data-store arn:aws:cloudtrail:region:account-id:eventdatastore/eds-id
--role arn:aws:iam::account-id:role/federation-role-name
```

Este exemplo mostra como um administrador delegado pode habilitar a federação em um armazenamento de dados de eventos da organização especificando o ARN do armazenamento de dados de eventos na conta de gerenciamento e o ARN do perfil de federação na conta de administrador delegado.

```
aws cloudtrail enable-federation
--event-data-store arn:aws:cloudtrail:region:management-account-
id:eventdatastore/eds-id
--role arn:aws:iam::delegated-administrator-account-id:role/federation-role-name
```

Desabilitar a federação de consultas do Lake

Você pode desativar a federação usando o CloudTrail console ou AWS CLI a operação DisableFederationda API. Quando você desativa a federação, CloudTrail desativa a integração com AWS Glue AWS Lake Formation, e com o Amazon Athena. Depois de desabilitar a federação de consultas do Lake, você não poderá mais consultar seus dados de eventos no Athena. Nenhum dado do CloudTrail Lake é excluído quando você desativa a federação e você pode continuar executando consultas no CloudTrail Lake.

Esta seção descreve como desabilitar a federação usando o CloudTrail console AWS CLI e.

CloudTrail console

O procedimento a seguir mostra como desabilitar a federação de consultas do Lake em um armazenamento de dados de eventos existente.

1. Faça login no AWS Management Console e abra o CloudTrail console em https://console.aws.amazon.com/cloudtrail/.
2. No painel de navegação, em Lake, escolha Armazenamentos de dados de eventos.
3. Selecione o armazenamento de dados de eventos que você deseja atualizar. A página de detalhes do armazenamento de dados de eventos é aberta.
4. Na federação de consultas do Lake, escolha Editar e, em seguida, escolha Desabilitar.
5. Escolha Salvar alterações. O status da Federação muda para `Disabled`.

AWS CLI

Para desabilitar a federação no armazenamento de dados de eventos, execute o comando aws cloudtrail disable-federation. O armazenamento de dados de eventos é especificado por `--event-data-store`, que aceita um ARN de armazenamento de dados de evento ou o sufixo de ID do ARN.

```
aws cloudtrail disable-federation
--event-data-store arn:aws:cloudtrail:region:account-id:eventdatastore/eds-id
```

> **Note**
>
> Se esse elemento for um armazenamento de dados de eventos da organização, use o ID de conta para a conta de gerenciamento.

Gerenciando os recursos da Federação do CloudTrail Lago com AWS Lake Formation

Quando você federa um armazenamento de dados de eventos, CloudTrail registra o ARN da função de federação e o armazenamento de dados de eventos em AWS Lake Formation, o serviço responsável por permitir o controle de acesso refinado dos recursos federados no Catálogo de Dados. AWS Glue Esta seção descreve como você pode usar o Lake Formation para gerenciar os recursos da federação CloudTrail Lake.

Quando você ativa a federação, CloudTrail cria os seguintes recursos no Catálogo AWS Glue de Dados.

- Banco de dados gerenciado — CloudTrail cria 1 banco de dados com o nome `aws:cloudtrail` por conta. CloudTrail gerencia o banco de dados. Você não pode excluir ou modificar o banco de dados em AWS Glue.
- Tabela federada gerenciada — CloudTrail cria 1 tabela para cada armazenamento de dados de eventos federados e usa a ID do armazenamento de dados de eventos para o nome da tabela. CloudTrail gerencia as tabelas. Você não pode excluir ou modificar as tabelas em AWS Glue. Para excluir uma tabela, você deve desabilitar a federação no armazenamento de dados de eventos.

Controlar o acesso aos recursos federados

Você pode usar um dos dois métodos de permissões para controlar o acesso ao banco de dados gerenciado e às tabelas.

- Controle de acesso somente do IAM: com o controle de acesso somente do IAM, todos os usuários na conta com as permissões necessárias do IAM têm acesso a todos os recursos do catálogo de dados. Para obter informações sobre como AWS Glue funciona com o IAM, consulte Como AWS Glue funciona com o IAM.

  No console do Lake Formation, esse método aparece como Use apenas controle de acesso do IAM.

  > **Note**
  >
  > Se quiser criar filtros de dados e usar outros atributos do Lake Formation, você deve usar o controle de acesso do Lake Formation.

- Controle de acesso do Lake Formation: este método oferece as seguintes vantagens.
  - É possível implementar segurança por coluna, por linha e por célula ao criar filtros de dados.
  - O banco de dados e as tabelas só são visíveis para os administradores e criadores do banco de dados e dos recursos do Lake Formation. Se outro usuário precisar acessar esses recursos, você deverá conceder acesso explicitamente usando as permissões do Lake Formation.

Para obter mais informações sobre o controle de acesso, consulte Métodos de controle de acesso granular.

Determinar o método de permissões para um recurso federado

Quando você ativa a federação pela primeira vez, CloudTrail cria um banco de dados gerenciado e uma tabela federada gerenciada usando as configurações do data lake do Lake Formation.

Depois de CloudTrail habilitar a federação, você pode verificar qual método de permissões está usando para o banco de dados gerenciado e a tabela federada gerenciada verificando as permissões desses recursos. Se `ALL` (Super) da configuração `IAM_ALLOWED_PRINCIPALS` estiver presente para o recurso, ele será gerenciado exclusivamente pelas permissões do IAM. Se a configuração estiver ausente, o recurso será gerenciado pelas permissões do Lake Formation. Para obter mais informações sobre as permissões do Lake Formation, consulte a Referência de permissões do Lake Formation.

O método de permissões para o banco de dados gerenciado e a tabela federada gerenciada pode ser diferente. Por exemplo, se você verificar os valores do banco de dados e da tabela, poderá ver o seguinte:

- Para o banco de dados, o valor atribuído a `ALL` (Super) para `IAM_ALLOWED_PRINCIPALS` está presente nas permissões, indicando que você está usando apenas o controle de acesso do IAM para o banco de dados.
- Para a tabela, o valor que atribui `ALL` (Super) a `IAM_ALLOWED_PRINCIPALS` não está presente, indicando o controle de acesso pelas permissões do Lake Formation.

Você pode alternar entre os métodos de acesso a qualquer momento, adicionando ou removendo `ALL` (Super) à permissão `IAM_ALLOWED_PRINCIPALS` em qualquer recurso federado no Lake Formation.

Compartilhamento entre contas no Lake Formation

Esta seção descreve como compartilhar um banco de dados gerenciado e uma tabela federada gerenciada entre contas usando o Lake Formation.

Você pode compartilhar um banco de dados gerenciado entre contas seguindo estas etapas:

1. Atualize a versão de compartilhamento de dados entre contas para 4.
2. Remova `Super` das permissões `IAM_ALLOWED_PRINCIPALS` do banco de dados, se houver, para alternar para o controle de acesso do Lake Formation.
3. Conceda permissões `Describe` para a conta externa no banco de dados.

4. Se um recurso do Catálogo de Dados for compartilhado com você Conta da AWS e sua conta não estiver na mesma AWS organização da conta de compartilhamento, aceite o convite de compartilhamento de recursos AWS Resource Access Manager (AWS RAM). Para obter mais informações, consulte Aceitar um convite de compartilhamento de recursos da AWS RAM.

Depois de concluir essas etapas, o banco de dados deverá estar visível para a conta externa. Por padrão, o compartilhamento do banco de dados não dá acesso a nenhuma tabela no banco de dados.

Você pode compartilhar todas as tabelas federadas gerenciadas ou individuais com uma conta externa seguindo estas etapas:

1. Atualize a versão de compartilhamento de dados entre contas para 4.
2. Remova `Super` das permissões `IAM_ALLOWED_PRINCIPALS` da tabela, se houver, para alternar para o controle de acesso do Lake Formation.
3. (Opcional) Especifique filtros de dados para restringir colunas ou linhas.
4. Conceda permissões `Select` para a conta externa na tabela.
5. Se um recurso do Catálogo de Dados for compartilhado com você Conta da AWS e sua conta não estiver na mesma AWS organização da conta de compartilhamento, aceite o convite de compartilhamento de recursos AWS Resource Access Manager (AWS RAM). Para uma organização, você pode aceitar automaticamente o uso das configurações de RAM. Para obter mais informações, consulte Aceitar um convite de compartilhamento de recursos da AWS RAM.
6. A tabela agora deverá estar visível. Para habilitar consultas do Amazon Athena nessa tabela, crie um link de recurso nesta conta com a tabela compartilhada.

A conta proprietária pode revogar o compartilhamento a qualquer momento removendo as permissões da conta externa do Lake Formation ou desativando a federação em. CloudTrail

Armazenamentos de dados de eventos da organização

Se você criou uma organização em AWS Organizations, você pode criar um armazenamento de dados de eventos da organização que registra todos os eventos de todos Contas da AWS nessa organização. Os armazenamentos de dados de eventos da organização podem ser aplicados a todas Regiões da AWS ou à região atual. Você não pode usar um armazenamento de dados de eventos da organização para coletar eventos de fora da AWS.

Você pode criar um armazenamento de dados de eventos da organização usando a conta de gerenciamento ou a conta de administrador delegado. Quando um administrador delegado cria um armazenamento de dados de eventos da organização, o armazenamento de dados de eventos da organização existe na conta de gerenciamento da respectiva organização. Essa abordagem ocorre porque a conta de gerenciamento mantém a propriedade de todos os recursos da organização.

A conta de gerenciamento de uma organização pode atualizar um armazenamento de dados de eventos no nível da conta para aplicá-lo a uma organização.

Quando um armazenamento de dados de eventos da organização é especificado como aplicável a uma organização, será aplicado automaticamente a todas as contas de membro da organização. As contas de membro não podem ver o armazenamento de dados de eventos da organização, nem podem modificá-lo ou excluí-lo. Por padrão, as contas de membro não têm acesso ao armazenamento de dados de eventos da organização, nem podem executar consultas em armazenamentos de dados de eventos da organização.

A tabela a seguir mostra os recursos da conta de gerenciamento e das contas de administrador delegado na AWS Organizations organização.

Capacidades	Conta de gerenciamento	Conta de administrador delegado
Registrar ou remover contas de administrador delegado.	Sim	Não
Crie um armazenamento de dados de eventos da organização para AWS CloudTrail eventos ou itens AWS Config de configuração.	Sim	Sim
Habilitar o Insights em um armazenamento de dados de eventos da organização.	Sim	Não
Atualizar um armazenamento de dados de eventos da organização.	Sim	Sim[1]
Habilitar a federação de consultas do Lake em um armazenamento de dados de eventos da organização.[2]	Sim	Sim

Capacidades	Conta de gerenciamento	Conta de administrador delegado
Desabilitar a federação de consultas do Lake em um armazenamento de dados de eventos da organização.	Sim	Sim
Excluir um armazenamento de dados de eventos da organização.	Sim	Sim
Copiar eventos de trilhas para um armazenamento de dados de eventos.	Sim	Não
Executar consultas em armazenamentos de dados de eventos da organização.	Sim	Sim
Veja o painel do CloudTrail Lake para um armazenamento de dados de eventos da organização.	Sim	Sim

[1] Somente a conta de gerenciamento pode converter um armazenamento de dados de eventos da organização em um armazenamento de dados de eventos no nível da conta ou converter um armazenamento de dados de eventos no nível da conta em um armazenamento de dados de eventos da organização. Essas ações não são permitidas para o administrador delegado porque os armazenamentos de dados de eventos da organização só existem na conta de gerenciamento. Quando um armazenamento de dados de eventos da organização é convertido em um armazenamento de dados de eventos no nível da conta, somente a conta de gerenciamento tem acesso ao armazenamento de dados do evento. Da mesma forma, somente um armazenamento de dados de eventos em nível de conta na conta de gerenciamento pode ser convertido em um armazenamento de dados de eventos da organização.

[2]Somente uma única conta de administrador delegado ou a conta de gerenciamento pode habilitar a federação em um armazenamento de dados de eventos da organização. Outras contas de administrador delegado podem consultar e compartilhar informações usando o atributo de compartilhamento de dados do Lake Formation. Qualquer conta de administrador delegado, bem como a conta de gerenciamento da organização, pode desabilitar a federação.

Crie um armazenamento de dados de eventos da organização

A conta de gerenciamento ou a conta de administrador delegado de uma organização pode criar um armazenamento de dados de eventos da organização para coletar CloudTrail eventos (eventos de gerenciamento, eventos de dados) ou itens de AWS Config configuração.

> **Note**
>
> Somente a conta de gerenciamento da organização pode copiar eventos de trilhas para um armazenamento de dados de eventos.

CloudTrail console

Para criar um armazenamento de dados de eventos da organização usando o console

1. Siga as etapas do procedimento criar um armazenamento de dados de CloudTrail eventos para eventos para criar um armazenamento de dados de eventos da organização para CloudTrail gerenciamento ou eventos de dados.

   OU

   Siga as etapas do procedimento criar um armazenamento de dados de eventos para itens de AWS Config configuração para criar um armazenamento de dados de eventos da organização para itens de AWS Config configuração.
2. Na página Escolher eventos, escolha Habilitar para todas as contas em minha organização.

AWS CLI

Para criar um armazenamento de dados de eventos da organização, execute o create-event-data-storecomando e inclua a `--organization-enabled` opção.

O AWS CLI `create-event-data-store` comando de exemplo a seguir cria um armazenamento de dados de eventos da organização que coleta todos os eventos de gerenciamento. Como CloudTrail registra eventos de gerenciamento por padrão, você não precisa especificar seletores de eventos avançados se seu armazenamento de dados de eventos estiver registrando todos os eventos de gerenciamento e não estiver coletando nenhum evento de dados.

```
aws cloudtrail create-event-data-store --name org-management-eds --organization-
enabled
```

A seguir, uma exemplo de resposta.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE6-d493-4914-9182-e52a7934b207",
    "Name": "org-management-eds",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": true,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-16T15:30:50.689000+00:00",
    "UpdatedTimestamp": "2023-11-16T15:30:50.851000+00:00"
}
```

O próximo AWS CLI `create-event-data-store` comando de exemplo cria um armazenamento de dados de eventos da organização chamado `config-items-org-eds` que coleta itens AWS Config de configuração. Para coletar itens de configuração, especifique que o `eventCategory` campo seja igual `ConfigurationItem` nos seletores de eventos avançados.

```
aws cloudtrail create-event-data-store --name config-items-org-eds \
--organization-enabled \
--advanced-event-selectors '[
    {
        "Name": "Select AWS Config configuration items",
```

```
        "FieldSelectors": [
            { "Field": "eventCategory", "Equals": ["ConfigurationItem"] }
        ]
    }
]'
```

Aplique um armazenamento de dados de eventos em nível de conta a uma organização

A conta de gerenciamento da organização pode converter um armazenamento de dados de eventos no nível da conta para aplicá-lo a uma organização.

CloudTrail console

Para atualizar um armazenamento de dados de eventos no nível da conta usando o console

1. Faça login no AWS Management Console e abra o CloudTrail console em https://console.aws.amazon.com/cloudtrail/.
2. No painel de navegação, em Lake, escolha Armazenamentos de dados de eventos.
3. Selecione o armazenamento de dados de eventos que você deseja atualizar. Essa ação abre a página de detalhes do armazenamento de dados de eventos.
4. Em General details (Detalhes gerais), escolha Edit (Editar).
5. Escolha Habilitar para todas as contas em minha organização.
6. Escolha Salvar alterações.

Para obter informações adicionais sobre a atualização de um armazenamento de dados de eventos, consulteAtualizar um armazenamento de dados de eventos com o console.

AWS CLI

Para atualizar um armazenamento de dados de eventos no nível da conta para aplicá-lo a uma organização, execute o update-event-data-storecomando e inclua a `--organization-enabled` opção.

```
aws cloudtrail update-event-data-store --region us-east-1 \
--organization-enabled \
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
```

Consulte também

- Administrador delegado de organização
- Adicionar um administrador CloudTrail delegado
- Remover um CloudTrail administrador delegado

Crie uma integração com uma fonte de eventos fora do AWS

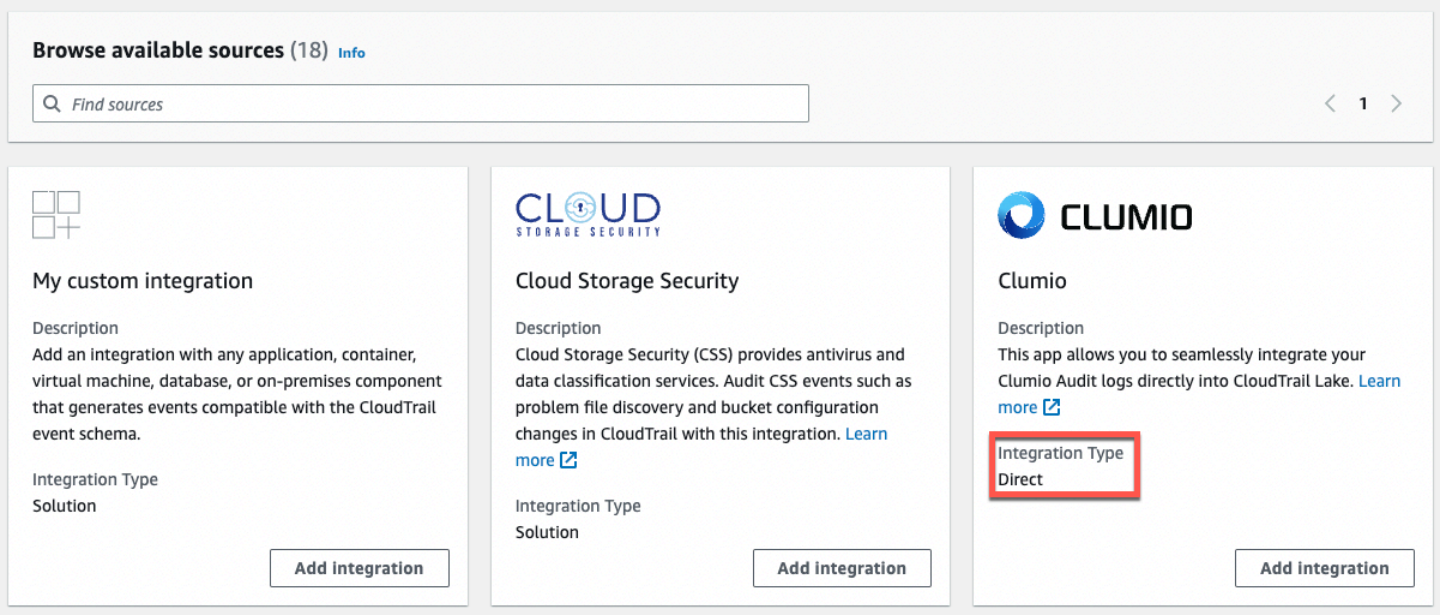
Você pode usar CloudTrail para registrar e armazenar dados de atividades do usuário de qualquer fonte em seus ambientes híbridos, como aplicativos internos ou SaaS hospedados localmente ou na nuvem, máquinas virtuais ou contêineres. É possível armazenar, acessar, analisar, solucionar problemas e agir com base nesses dados sem manter vários agregadores de logs e ferramentas de geração de relatórios.

Os eventos de atividades de AWS outras fontes funcionam usando canais para trazer eventos para o CloudTrail Lake de parceiros externos que trabalham com CloudTrail ou de suas próprias fontes. Ao criar um canal, você escolhe um ou mais armazenamentos de dados de eventos para armazenar eventos que cheguem da fonte do canal. É possível alterar os armazenamentos de dados de eventos de destino de um canal conforme necessário, desde que os armazenamentos de dados de eventos de destino estejam configurados para registrar em log eventos do `eventCategory="ActivityAuditLog"`. Ao criar um canal para eventos de um parceiro externo, você fornece um ARN de canal para o parceiro ou aplicação da fonte. A política de recursos anexada ao canal permite que a fonte transmita eventos pelo canal. Se um canal não tiver uma política de recursos para o canal, somente o proprietário do canal poderá chamar a API `PutAuditEvents` no canal.

CloudTrail fez parceria com muitos fornecedores de fontes de eventos, como Okta e. LaunchDarkly Ao criar uma integração com uma fonte de eventos externa AWS, você pode escolher um desses parceiros como sua fonte de eventos ou escolher Minha integração personalizada para integrar eventos de suas próprias fontes CloudTrail. É permitido no máximo um canal por fonte.

Há dois tipos de integração: a direta e a de solução. Com integrações diretas, o parceiro chama a `PutAuditEvents` API para entregar eventos ao armazenamento de dados de eventos da sua AWS conta. Com as integrações de soluções, o aplicativo é executado em sua AWS conta e chama a `PutAuditEvents` API para entregar eventos ao armazenamento de dados de eventos de sua AWS conta.

Na página Integrations (Integrações), é possível escolher a guia Available sources (Fontes disponíveis) para visualizar o Integration type (Tipo de integração) para parceiros.



Para começar, crie uma integração para registrar eventos do parceiro ou de outras fontes de aplicativos usando o CloudTrail console.

Tópicos

- Crie uma integração com um CloudTrail parceiro com o console
- Crie uma integração personalizada com o console
- Crie, atualize e gerencie integrações do CloudTrail Lake com o AWS CLI
- Informações adicionais sobre parceiros de integração
- CloudTrail Esquema de eventos de integrações do Lake

Crie uma integração com um CloudTrail parceiro com o console

Ao criar uma integração com uma fonte de eventos externa AWS, você pode escolher um desses parceiros como sua fonte de eventos. Quando você cria uma integração CloudTrail com um aplicativo de parceiro, o parceiro precisa do Amazon Resource Name (ARN) do canal que você cria nesse fluxo de trabalho para enviar eventos. CloudTrail Depois de criar a integração, a configuração é concluída seguindo as instruções do parceiro para fornecer o ARN do canal necessário ao parceiro. A integração começa a ingerir eventos do parceiro CloudTrail depois que o parceiro `PutAuditEvents` liga para o canal da integração.

1. Faça login no AWS Management Console e abra o CloudTrail console em https://console.aws.amazon.com/cloudtrail/.
2. No painel de navegação, em Lake, escolha Integrações.
3. Na página Add integration (Adicionar integração), insira um nome para seu canal. O nome pode ter de 3 a 128 caracteres. São permitidas apenas letras, números, pontos, traços e sublinhados.
4. Escolha a fonte da aplicação do parceiro da qual deseja obter eventos. Se você estiver se integrando com eventos de suas próprias aplicações hospedadas on-premises ou na nuvem, escolha My custom integration (Minha integração personalizada).
5. Em Event delivery location (Local de entrega do evento), escolha registrar em log os mesmos eventos de atividade nos armazenamentos de dados de eventos existentes ou criar um novo armazenamento de dados de eventos.

   Se você optar por criar um novo armazenamento de dados de eventos, insira um nome para o armazenamento de dados de eventos, escolha a opção de preço e especifique o período de retenção em dias. O armazenamento de dados de eventos retém os dados de eventos pelo número especificado de dias.

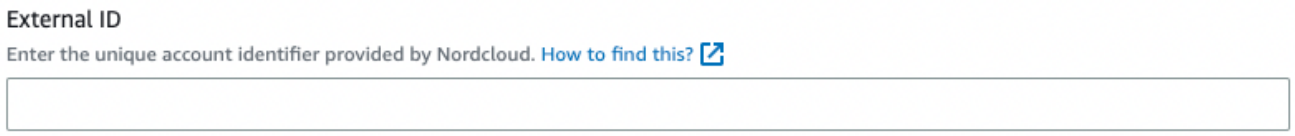
   Se você optar por registrar em log eventos de atividade em um ou mais armazenamentos de dados de eventos existentes, escolha os armazenamentos de dados de eventos na lista. Os armazenamentos de dados de eventos só podem incluir eventos de atividades. O tipo de evento no console deve ser Events from integrations (Eventos de integrações). Na API, o valor de `eventCategory` deve ser `ActivityAuditLog`.
6. Em Resource policy (Política de recursos), configure a política de recursos para o canal de integração. As políticas de recursos são documentos de políticas em JSON que especificam quais ações uma entidade principal pode executar no recurso e sob quais condições.
   As contas definidas como entidades principais na política de recursos podem chamar a API `PutAuditEvents` para entregar eventos ao seu canal. O proprietário do recurso tem acesso implícito ao recurso se sua política do IAM permitir a ação `cloudtrail-data:PutAuditEvents`.

   As informações necessárias para a política são determinadas pelo tipo de integração. Para uma integração de direção, adiciona CloudTrail automaticamente os IDs da AWS conta do parceiro e exige que você insira o ID externo exclusivo fornecido pelo parceiro. Para uma integração de soluções, você deve especificar pelo menos uma ID de AWS conta como principal e, opcionalmente, inserir uma ID externa para evitar confusões entre representantes.

> **Note**
>
> Se não for criada uma política de recursos para o canal, somente o proprietário do canal poderá chamar a API `PutAuditEvents` no canal.

a. Para uma integração direta, insira o ID externo fornecido pelo seu parceiro. O parceiro de integração fornece um ID externo exclusivo, como um ID de conta ou uma string gerada aleatoriamente, para usar na integração e evitar o “confused deputy”. O parceiro é responsável por criar e fornecer um ID externo exclusivo.

   É possível escolher How to find this? (Como encontrar isso?) para ver a documentação do parceiro que descreva como encontrar o ID externo.



> **Note**
>
> Se a política de recursos incluir um ID externo, todas as chamadas para a API `PutAuditEvents` deverão incluir o ID externo. No entanto, se a política não definir um ID externo, o parceiro ainda poderá chamar a API `PutAuditEvents` e especificar um parâmetro `externalId`.

b. Para uma integração de soluções, escolha Adicionar AWS conta para especificar uma ID de AWS conta a ser adicionada como principal na política.

7. (Opcional) Na área Tags, é possível adicionar até 50 pares de chave e valor de tag para ajudar a identificar, classificar e controlar o acesso ao armazenamento de dados de eventos. Para obter mais informações sobre como usar políticas do IAM para autorizar o acesso a um armazenamento de dados de eventos com base em tags, consulte Exemplos: negação de acesso para criar ou excluir armazenamentos de dados de eventos com base em tags. Para obter mais informações sobre como você pode usar tags em AWS, consulte AWS Recursos de marcação no Referência geral da AWS.
8. Quando estiver pronto para criar a nova integração, escolha Add integration (Adicionar integração). Não há página de avaliação. CloudTrail cria a integração, mas você deve fornecer o canal Amazon Resource Name (ARN) para o aplicativo parceiro. As instruções para fornecer

o ARN do canal para a aplicação do parceiro estão no site de documentação do parceiro. Para obter mais informações, escolha o link Learn more (Saiba mais) para o parceiro na guia Available sources (Fontes disponíveis) da página Integrations (Integrações) para abrir a página do parceiro no AWS Marketplace.

Para concluir a configuração da sua integração, forneça o ARN do canal ao parceiro ou à aplicação fonte. Dependendo do tipo de integração, você, o parceiro ou a aplicação executam a API `PutAuditEvents` para entregar eventos de atividade ao armazenamento de dados de eventos da sua conta da AWS . Depois que seus eventos de atividade forem entregues, você poderá usar o CloudTrail Lake para pesquisar, consultar e analisar os dados que são registrados em seus aplicativos. Seus dados de eventos incluem campos que correspondem à carga útil do CloudTrail evento`eventVersion`, como`eventSource`, e. `userIdentity`

Crie uma integração personalizada com o console

Você pode usar CloudTrail para registrar e armazenar dados de atividades do usuário de qualquer fonte em seus ambientes híbridos, como aplicativos internos ou SaaS hospedados localmente ou na nuvem, máquinas virtuais ou contêineres. Execute a primeira metade desse procedimento no console do CloudTrail Lake e, em seguida, chame a `PutAuditEvents`API para ingerir eventos, fornecendo o ARN do canal e a carga útil do evento. Depois de usar a `PutAuditEvents` API para ingerir a atividade do seu aplicativo CloudTrail, você pode usar o CloudTrail Lake para pesquisar, consultar e analisar os dados que são registrados nos seus aplicativos.

1. Faça login no AWS Management Console e abra o CloudTrail console em https://console.aws.amazon.com/cloudtrail/.
2. No painel de navegação, em Lake, escolha Integrações.
3. Na página Add integration (Adicionar integração), insira um nome para seu canal. O nome pode ter de 3 a 128 caracteres. São permitidas apenas letras, números, pontos, traços e sublinhados.
4. Escolha My custom integration (Minha integração personalizada).
5. Em Event delivery location (Local de entrega do evento), escolha registrar em log os mesmos eventos de atividade nos armazenamentos de dados de eventos existentes ou criar um novo armazenamento de dados de eventos.

   Se você optar por criar um novo armazenamento de dados de eventos, insira um nome para o armazenamento de dados de eventos e especifique o período de retenção em dias. Você pode manter os dados do evento em um armazenamento de dados de eventos por até 3.653 dias

(cerca de 10 anos) se escolher a opção de preço de retenção extensível de um ano ou até 2.557 dias (cerca de 7 anos) se escolher a opção de preço de retenção por sete anos.

Se você optar por registrar em log eventos de atividade em um ou mais armazenamentos de dados de eventos existentes, escolha os armazenamentos de dados de eventos na lista. Os armazenamentos de dados de eventos só podem incluir eventos de atividades. O tipo de evento no console deve ser Events from integrations (Eventos de integrações). Na API, o valor de `eventCategory` deve ser `ActivityAuditLog`.

6. Em Resource policy (Política de recursos), configure a política de recursos para o canal de integração. As políticas de recursos são documentos de políticas em JSON que especificam quais ações uma entidade principal pode executar no recurso e sob quais condições. As contas definidas como entidades principais na política de recursos podem chamar a API `PutAuditEvents` para entregar eventos ao seu canal.

   > **Note**
   >
   > Se não for criada uma política de recursos para o canal, somente o proprietário do canal poderá chamar a API `PutAuditEvents` no canal.

   a. (Opcional) Insira um ID externo exclusivo para fornecer uma camada extra de proteção. O ID externo é uma string exclusiva, como um ID de conta ou uma string gerada aleatoriamente, para evitar o “confused deputy”.

      > **Note**
      >
      > Se a política de recursos incluir um ID externo, todas as chamadas para a API `PutAuditEvents` deverão incluir o ID externo. No entanto, se a política não definir um ID externo, você ainda poderá chamar a API `PutAuditEvents` e especificar um parâmetro `externalId`.

   b. Escolha Adicionar AWS conta para especificar cada ID de AWS conta a ser adicionada como principal na política de recursos do canal.

7. (Opcional) Na área Tags, é possível adicionar até 50 pares de chave e valor de tag para ajudar a identificar, classificar e controlar o acesso ao armazenamento de dados de eventos. Para obter mais informações sobre como usar políticas do IAM para autorizar o acesso a um armazenamento de dados de eventos com base em tags, consulte Exemplos: negação de

acesso para criar ou excluir armazenamentos de dados de eventos com base em tags. Para obter mais informações sobre como você pode usar tags em AWS, consulte Como marcar seus AWS recursos no Referência geral da AWS.

8. Quando estiver pronto para criar a nova integração, escolha Add integration (Adicionar integração). Não há página de avaliação. CloudTrail cria a integração, mas para integrar seus eventos personalizados, você deve especificar o ARN do canal em uma `PutAuditEvents`solicitação.
9. Chame a `PutAuditEvents` API para incluir seus eventos de atividade em CloudTrail. É possível adicionar até 100 eventos de atividade (ou até 1 MB) por solicitação `PutAuditEvents`. Você precisará do ARN do canal que criou nas etapas anteriores, da carga de eventos que deseja CloudTrail adicionar e do ID externo (se especificado para sua política de recursos). Certifique-se de que não haja informações confidenciais ou de identificação pessoal na carga útil do evento antes de inseri-las. CloudTrail Os eventos nos quais você ingere CloudTrail devem seguir o. CloudTrail Esquema de eventos de integrações do Lake

> **Tip**
>
> Use AWS CloudShellpara ter certeza de que você está executando as AWS APIs mais atuais.

Os exemplos a seguir mostram como usar o comando put-audit-events da CLI. Os parâmetros --audit-events e --channel-arn são obrigatórios. Você precisa do ARN do canal criado nas etapas anteriores, que pode ser copiado da página de detalhes da integração. O valor de --audit-events é uma matriz JSON de objetos de eventos. `--audit-events`inclui uma ID exigida do evento, a carga útil necessária do evento como valor de e uma soma de `EventData` verificação opcional para ajudar a validar a integridade do evento após a ingestão. CloudTrail

```
aws cloudtrail-data put-audit-events \
--region region \
--channel-arn $ChannelArn \
--audit-events \
id="event_ID",eventData='"{event_payload}"' \
id="event_ID",eventData='"{event_payload}"',eventDataChecksum="optional_checksum"
```

A seguir há um exemplo de comando com dois exemplos de eventos.

```
aws cloudtrail-data put-audit-events \
--region us-east-1 \
--channel-arn arn:aws:cloudtrail:us-east-1:01234567890:channel/EXAMPLE8-0558-4f7e-
a06a-43969EXAMPLE \
--audit-events \
id="EXAMPLE3-0f1f-4a85-9664-d50a3EXAMPLE",eventData='"{\"eventVersion\":\0.01\",
\"eventSource\":\"custom1.domain.com\", ...
\}"' \
id="EXAMPLE7-a999-486d-b241-b33a1EXAMPLE",eventData='"{\"eventVersion\":\0.02\",
\"eventSource\":\"custom2.domain.com\", ...
\}"',eventDataChecksum="EXAMPLE6e7dd61f3ead...93a691d8EXAMPLE"
```

O comando de exemplo a seguir adiciona o parâmetro `--cli-input-json` para especificar um arquivo JSON (`custom-events.json`) de carga útil do evento.

```
aws cloudtrail-data put-audit-events \
--channel-arn $channelArn \
--cli-input-json file://custom-events.json \
--region us-east-1
```

A seguir há a amostra de conteúdo do arquivo JSON do exemplo, `custom-events.json`.

```
{
    "auditEvents": [
      {
        "eventData": "{\"version\":\"eventData.version\",\"UID\":\"UID\",
        \"userIdentity\":{\"type\":\"CustomUserIdentity\",\"principalId\":
\"principalId\",
        \"details\":{\"key\":\"value\"}},\"eventTime\":\"2021-10-27T12:13:14Z\",
\"eventName\":\"eventName\",
        \"userAgent\":\"userAgent\",\"eventSource\":\"eventSource\",
        \"requestParameters\":{\"key\":\"value\"},\"responseElements\":{\"key\":
\"value\"},
        \"additionalEventData\":{\"key\":\"value\"},
        \"sourceIPAddress\":\"source_IP_address\",\"recipientAccountId\":
\"recipient_account_ID\"}",
        "id": "1"
      }
   ]
}
```

(Opcional) Calcular um valor de soma de verificação

A soma de verificação que você especifica como o valor de `EventDataChecksum` em uma `PutAuditEvents` solicitação ajuda a verificar se CloudTrail recebe o evento que corresponde à soma de verificação; ajuda a verificar a integridade dos eventos. O valor da soma de verificação é obtido por um algoritmo base64-SHA256 calculado com a execução do comando a seguir.

```
printf %s "{"eventData": "{\"version\":\"eventData.version\",\"UID\":\"UID\",
        \"userIdentity\":{\"type\":\"CustomUserIdentity\",\"principalId\":\"principalId
\",
        \"details\":{\"key\":\"value\"}},\"eventTime\":\"2021-10-27T12:13:14Z\",
\"eventName\":\"eventName\",
        \"userAgent\":\"userAgent\",\"eventSource\":\"eventSource\",
        \"requestParameters\":{\"key\":\"value\"},\"responseElements\":{\"key\":\"value
\"},
        \"additionalEventData\":{\"key\":\"value\"},
        \"sourceIPAddress\":\"source_IP_address\",
        \"recipientAccountId\":\"recipient_account_ID\"}",
        "id": "1"}" \
 | openssl dgst -binary -sha256 | base64
```

O comando retorna a soma de verificação . Veja um exemplo a seguir.

```
EXAMPLEHjkI8iehvCUCWTIAbNYkOgO/t0YNw+7rrQE=
```

O valor da soma de verificação se torna o valor de `EventDataChecksum` em sua solicitação `PutAuditEvents`. Se a soma de verificação não corresponder à do evento fornecido, CloudTrail rejeitará o evento com um `InvalidChecksum` erro.

Crie, atualize e gerencie integrações do CloudTrail Lake com o AWS CLI

Você pode usar o AWS CLI para criar, atualizar e gerenciar suas integrações com o CloudTrail Lake. Ao usar o AWS CLI, lembre-se de que seus comandos são Região da AWS executados no configurado para seu perfil. Se você deseja executar os comandos em uma região diferente, altere a região padrão para o seu perfil ou use o parâmetro --region com o comando.

Comandos disponíveis para integrações com o CloudTrail Lake

Os comandos para criar, atualizar e gerenciar integrações no CloudTrail Lake incluem:

- `create-event-data-store`para criar um armazenamento de dados de eventos para eventos fora do AWS.
- `delete-channel`para excluir um canal usado para uma integração.
- `delete-resource-policy`para excluir a política de recursos anexada a um canal para uma integração com o CloudTrail Lake.
- `get-channel`para retornar informações sobre um CloudTrail canal.
- `get-resource-policy`para recuperar o texto JSON do documento de política baseado em recursos anexado ao canal. CloudTrail
- `list-channels`para listar os canais na conta atual e seus nomes de origem.
- `put-audit-events`para ingerir os eventos do seu aplicativo no CloudTrail Lake. Um parâmetro obrigatório,`auditEvents`, aceita os registros JSON (também chamados de carga) dos eventos que você deseja CloudTrail ingerir. Você pode adicionar até 100 desses eventos (ou até 1 MB) por `PutAuditEvents` solicitação.
- `put-resource-policy`para anexar uma política de permissão baseada em recursos a um CloudTrail canal que é usado para uma integração com uma fonte de eventos externa. AWS Para obter mais informações sobre políticas baseadas em recursos, consulte exemplos de políticas baseadas em AWS CloudTrail recursos.
- `update-channel`para atualizar um canal especificado pelo ARN ou UUID de um canal necessário.

Para obter uma lista dos comandos disponíveis para armazenamentos de dados de eventos do CloudTrail Lake, consulteComandos disponíveis para armazenamentos de dados de eventos.

Para obter uma lista dos comandos disponíveis para consultas do CloudTrail Lake, consulteComandos disponíveis para consultas CloudTrail do Lake.

Crie uma integração para registrar eventos externos AWS com o AWS CLI

No AWS CLI, você cria uma integração que registra eventos externos AWS em quatro comandos (três se você já tiver um armazenamento de dados de eventos que atenda aos critérios). Os armazenamentos de dados de eventos que você usa como destinos para uma integração devem ser para uma única região e uma única conta; eles não podem ser multirregionais, não podem registrar eventos para organizações e só podem incluir eventos de atividades. AWS Organizations O tipo de evento no console deve ser Events from integrations (Eventos de integrações). Na API, o valor de `eventCategory` deve ser `ActivityAuditLog`. Para obter mais informações sobre integrações, consulte Crie uma integração com uma fonte de eventos fora do AWS.

1. Execute create-event-data-store para criar um armazenamento de dados de eventos, se ainda não houver um ou mais armazenamentos de dados de eventos que possam ser usados para a integração.

   O AWS CLI comando de exemplo a seguir cria um armazenamento de dados de eventos que registra eventos externos AWS. Para eventos de atividade, o valor do seletor do campo `eventCategory` é `ActivityAuditLog`. O armazenamento de dados do evento tem um período de retenção configurado de 90 dias. Por padrão, o armazenamento de dados de eventos coleta eventos de todas as regiões, mas como não são AWS eventos, defina-o como uma única região adicionando a `--no-multi-region-enabled` opção. A proteção contra encerramento é ativada por padrão, e o armazenamento de dados de eventos não coleta eventos para contas em uma organização.

   ```
   aws cloudtrail create-event-data-store \
   --name my-event-data-store \
   --no-multi-region-enabled \
   --retention-period 90 \
   --advanced-event-selectors '[
       {
         "Name": "Select all external events",
         "FieldSelectors": [
             { "Field": "eventCategory", "Equals": ["ActivityAuditLog"] }
           ]
       }
     ]'
   ```

   A seguir, uma exemplo de resposta.

   ```
   {
       "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
   EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE",
       "Name": "my-event-data-store",
       "AdvancedEventSelectors": [
           {
              "Name": "Select all external events",
              "FieldSelectors": [
                 {
                     "Field": "eventCategory",
                     "Equals": [
                         "ActivityAuditLog"
                       ]
   ```

```
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 90,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-10-27T10:55:55.384000-04:00",
    "UpdatedTimestamp": "2023-10-27T10:57:05.549000-04:00"
}
```

Será necessário o ID do armazenamento de dados do evento (o sufixo do ARN, ou `EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE` no exemplo da resposta anterior) para passar para a próxima etapa e criar seu canal.

2. Execute o create-channelcomando para criar um canal que permita que um parceiro ou aplicativo de origem envie eventos para um armazenamento de dados de eventos em CloudTrail.

   Um canal tem os seguintes componentes:

   Origem

   CloudTrail usa essas informações para determinar os parceiros para os quais estão enviando dados de eventos CloudTrail em seu nome. Uma fonte é necessária, e ela pode ser `Custom` para todos os eventos válidos não da AWS , ou o nome de uma fonte de eventos do parceiro. É permitido no máximo um canal por fonte.

   Para obter informações sobre os valores da `Source` dos parceiros disponíveis, consulte Informações adicionais sobre parceiros de integração.

   Status da ingestão

   O status do canal mostra quando os últimos eventos foram recebidos de uma fonte de canal.

   Destinos

   Os destinos são os armazenamentos de dados de eventos do CloudTrail Lake que estão recebendo eventos do canal. É possível alterar os armazenamentos de dados de eventos de destino de um canal.

Para parar de receber eventos de uma fonte, exclua o canal.

É necessário o ID de pelo menos um armazenamento de dados de eventos de destino para executar esse comando. O tipo de destino válido é `EVENT_DATA_STORE`. É possível enviar eventos ingeridos para mais de um armazenamento de dados de eventos. O exemplo de comando a seguir cria um canal que envia eventos para dois armazenamentos de dados de eventos, representados por seus IDs no atributo `Location` do parâmetro `--destinations`. Os parâmetros `--destinations`, `--name` e `--source` são obrigatórios. Para ingerir eventos de um CloudTrail parceiro, especifique o nome do parceiro como o valor de`--source`. Para ingerir eventos de seus próprios aplicativos externos AWS, especifique `Custom` como o valor de`--source`.

```
aws cloudtrail create-channel \
    --region us-east-1 \
    --destinations '[{"Type": "EVENT_DATA_STORE", "Location":
 "EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE"}, {"Type": "EVENT_DATA_STORE", "Location":
 "EXAMPLEg922-5n2l-3vz1- apqw8EXAMPLE"}]'
    --name my-partner-channel \
    --source $partnerSourceName \
```

Na resposta ao seu comando create-channel, copie o ARN do novo canal. O ARN é necessário para executar os comandos `put-resource-policy` e `put-audit-events` nas próximas etapas.

3. Execute o put-resource-policycomando para anexar uma política de recursos ao canal. As políticas de recursos são documentos de políticas em JSON que especificam quais ações uma entidade principal pode executar no recurso e sob quais condições. As contas definidas como entidades principais na política de recursos do canal podem chamar a API `PutAuditEvents` para entregar eventos.

> **Note**
>
> Se não for criada uma política de recursos para o canal, somente o proprietário do canal poderá chamar a API `PutAuditEvents` no canal.

As informações necessárias para a política são determinadas pelo tipo de integração.

- Para uma integração de direção, CloudTrail exige que a política contenha os IDs da AWS conta do parceiro e exige que você insira o ID externo exclusivo fornecido pelo parceiro. CloudTrail adiciona automaticamente os IDs da AWS conta do parceiro à política de recursos quando você cria uma integração usando o CloudTrail console. Consulte a documentação do parceiro para saber como obter os números de AWS conta necessários para a apólice.
- Para uma integração de soluções, você deve especificar pelo menos uma ID de AWS conta como principal e, opcionalmente, inserir uma ID externa para evitar confusões entre representantes.

Veja a seguir os requisitos para a política de recursos:

- O ARN do recurso definido na política deve corresponder ao ARN do canal ao qual a política está anexada.
- A política contém apenas uma ação: cloudtrail-data: PutAuditEvents
- Cada uma deve incluir pelo menos uma instrução. A política pode ter um máximo de 20 instruções.
- Cada instrução contém pelo menos uma entidade principal. Uma instrução pode ter um máximo de 50 entidades principais.

```
aws cloudtrail put-resource-policy \
    --resource-arn "channelARN" \
    --policy "{
    "Version": "2012-10-17",
    "Statement":
    [
        {
            "Sid": "ChannelPolicy",
            "Effect": "Allow",
            "Principal":
            {
                "AWS":
                [
                    "arn:aws:iam::111122223333:root",
                    "arn:aws:iam::444455556666:root",
                    "arn:aws:iam::123456789012:root"
                ]
            },
```

```
            "Action": "cloudtrail-data:PutAuditEvents",
            "Resource": "arn:aws:cloudtrail:us-east-1:777788889999:channel/
EXAMPLE-80b5-40a7-ae65-6e099392355b",
            "Condition":
            {
                "StringEquals":
                {
                    "cloudtrail:ExternalId": "UniqueExternalIDFromPartner"
                }
            }
        }
    ]
}"
```

Para obter mais informações sobre políticas de recursos, consulte AWS CloudTrail exemplos de políticas baseadas em recursos.

4. Execute a `PutAuditEvents`API para incluir seus eventos de atividade em CloudTrail. Você precisará da carga de eventos que deseja CloudTrail adicionar. Certifique-se de que não haja informações confidenciais ou de identificação pessoal na carga útil do evento antes de inseri-las. CloudTrail Observe que a API `PutAuditEvents` usa o endpoint da CLI `cloudtrail-data`, não o endpoint `cloudtrail`.

   Os exemplos a seguir mostram como usar o comando put-audit-events da CLI. Os parâmetros --audit-events e --channel-arn são obrigatórios. O parâmetro --external-id é necessário se um ID externo for definido na política de recursos. Será necessário o ARN do canal criado na etapa anterior. O valor de --audit-events é uma matriz JSON de objetos de eventos. `--audit-events`inclui uma ID exigida do evento, a carga útil necessária do evento como valor de e uma soma de `EventData` verificação opcional para ajudar a validar a integridade do evento após a ingestão. CloudTrail

   ```
   aws cloudtrail-data put-audit-events \
   --channel-arn $ChannelArn \
   --external-id $UniqueExternalIDFromPartner \
   --audit-events \
   id="event_ID",eventData='"{event_payload}"' \
   id="event_ID",eventData='"{event_payload}"',eventDataChecksum="optional_checksum"
   ```

   A seguir há um exemplo de comando com dois exemplos de eventos.

```
aws cloudtrail-data put-audit-events \
--channel-arn arn:aws:cloudtrail:us-east-1:123456789012:channel/EXAMPLE8-0558-4f7e-
a06a-43969EXAMPLE \
--external-id UniqueExternalIDFromPartner \
--audit-events \
id="EXAMPLE3-0f1f-4a85-9664-d50a3EXAMPLE",eventData='"{\"eventVersion\":\0.01\",
\"eventSource\":\"custom1.domain.com\", ...
\}"' \
id="EXAMPLE7-a999-486d-b241-b33a1EXAMPLE",eventData='"{\"eventVersion\":\0.02\",
\"eventSource\":\"custom2.domain.com\", ...
\}"',eventDataChecksum="EXAMPLE6e7dd61f3ead...93a691d8EXAMPLE"
```

O comando de exemplo a seguir adiciona o parâmetro `--cli-input-json` para especificar um arquivo JSON (`custom-events.json`) de carga útil do evento.

```
aws cloudtrail-data put-audit-events --channel-arn $channelArn --external-id
 $UniqueExternalIDFromPartner --cli-input-json file://custom-events.json --region
 us-east-1
```

A seguir há a amostra de conteúdo do arquivo JSON do exemplo, `custom-events.json`.

```
{
    "auditEvents": [
      {
        "eventData": "{\"version\":\"eventData.version\",\"UID\":\"UID\",
        \"userIdentity\":{\"type\":\"CustomUserIdentity\",\"principalId\":
\"principalId\",
        \"details\":{\"key\":\"value\"}},\"eventTime\":\"2021-10-27T12:13:14Z\",
\"eventName\":\"eventName\",
        \"userAgent\":\"userAgent\",\"eventSource\":\"eventSource\",
        \"requestParameters\":{\"key\":\"value\"},\"responseElements\":{\"key\":
\"value\"},
        \"additionalEventData\":{\"key\":\"value\"},
        \"sourceIPAddress\":\"12.34.56.78\",\"recipientAccountId\":
\"152089810396\"}",
        "id": "1"
      }
   ]
}
```

Você pode verificar se a integração está funcionando e se CloudTrail está ingerindo eventos da fonte corretamente executando o get-channelcomando. A saída de get-channel mostra o registro de data e hora mais recente que CloudTrail recebeu os eventos.

```
aws cloudtrail get-channel --channel arn:aws:cloudtrail:us-east-1:01234567890:channel/
EXAMPLE8-0558-4f7e-a06a-43969EXAMPLE
```

(Opcional) Calcular um valor de soma de verificação

A soma de verificação que você especifica como o valor de `EventDataChecksum` em uma `PutAuditEvents` solicitação ajuda a verificar se CloudTrail recebe o evento que corresponde à soma de verificação; ajuda a verificar a integridade dos eventos. O valor da soma de verificação é obtido por um algoritmo base64-SHA256 calculado com a execução do comando a seguir.

```
printf %s "{"eventData": "{\"version\":\"eventData.version\",\"UID\":\"UID\",
        \"userIdentity\":{\"type\":\"CustomUserIdentity\",\"principalId\":\"principalId
\",
        \"details\":{\"key\":\"value\"}},\"eventTime\":\"2021-10-27T12:13:14Z\",
\"eventName\":\"eventName\",
        \"userAgent\":\"userAgent\",\"eventSource\":\"eventSource\",
        \"requestParameters\":{\"key\":\"value\"},\"responseElements\":{\"key\":\"value
\"},
        \"additionalEventData\":{\"key\":\"value\"},
        \"sourceIPAddress\":\"source_IP_address\",
        \"recipientAccountId\":\"recipient_account_ID\"}",
        "id": "1"}" \
 | openssl dgst -binary -sha256 | base64
```

O comando retorna a soma de verificação . Veja um exemplo a seguir.

```
EXAMPLEDHjkI8iehvCUCWTIAbNYkOgO/t0YNw+7rrQE=
```

O valor da soma de verificação se torna o valor de `EventDataChecksum` em sua solicitação `PutAuditEvents`. Se a soma de verificação não corresponder à do evento fornecido, CloudTrail rejeitará o evento com um `InvalidChecksum` erro.

Atualize um canal com o AWS CLI

Para atualizar o nome de um canal ou os armazenamentos de dados de eventos de destino, execute o comando update-channel. O parâmetro `--channel` é obrigatório. A fonte de um canal não pode ser atualizada. Veja um exemplo a seguir.

```
aws cloudtrail update-channel \
--channel aws:cloudtrail:us-east-1:123456789012:channel/EXAMPLE8-0558-4f7e-
a06a-43969EXAMPLE \
--name "new-channel-name" \
--destinations '[{"Type": "EVENT_DATA_STORE", "Location": "EXAMPLEf852-4e8f-8bd1-
bcf6cEXAMPLE"}, {"Type": "EVENT_DATA_STORE", "Location": "EXAMPLEg922-5n2l-3vz1-
 apqw8EXAMPLE"}]'
```

Exclua um canal para excluir uma integração com o AWS CLI

Para parar de ingerir eventos de parceiros ou outras atividades externas AWS, exclua o canal executando o delete-channel comando. O ARN ou ID do canal (o sufixo do ARN) do canal que você deseja excluir é obrigatório. Veja um exemplo a seguir.

```
aws cloudtrail delete-channel \
--channel EXAMPLE8-0558-4f7e-a06a-43969EXAMPLE
```

Informações adicionais sobre parceiros de integração

A tabela nesta seção fornece o nome da fonte de cada parceiro de integração e identifica o tipo de integração (direta ou de solução).

As informações na coluna Nome da fonte são necessárias ao chamar a API `CreateChannel`. O nome da fonte é especificado como o valor do parâmetro `Source`.

Nome do parceiro (console)	Nome da fonte (API)	Tipo de integração
Minha integração personalizada	`Custom`	solução
Cloud Storage Security	`CloudStorageSecurityConsole`	solução
Clumio	`Clumio`	direta
CrowdStrike	`CrowdStrike`	solução
CyberArk	`CyberArk`	solução
GitHub	`GitHub`	solução

Nome do parceiro (console)	Nome da fonte (API)	Tipo de integração
Kong Inc	`KongGatewayEnterprise`	solução
LaunchDarkly	`LaunchDarkly`	direta
Netskope	`NetskopeCloudExchange`	solução
Nordcloud, uma empresa da IBM	`IBMMulticloud`	direta
MontyCloud	`MontyCloud`	direta
Okta	`OktaSystemLogEvents`	solução
One Identity	`OneLogin`	solução
Shoreline.io	`Shoreline`	solução
Snyk.io	`Snyk`	direta
Wiz	`WizAuditLogs`	solução

Visualizar a documentação do parceiro

Você pode saber mais sobre a integração de um parceiro com o CloudTrail Lake visualizando sua documentação.

Para visualizar a documentação do parceiro

1. Faça login no AWS Management Console e abra o CloudTrail console em https://console.aws.amazon.com/cloudtrail/.
2. No painel de navegação, em Lake, escolha Integrações.
3. Na página Integrations (Integrações), escolha Available sources (Fontes disponíveis) e, em seguida, escolha Learn more (Saiba mais) para o parceiro cuja documentação você deseja visualizar.

CloudTrail Esquema de eventos de integrações do Lake

A tabela a seguir descreve os elementos de esquema obrigatórios e opcionais que correspondem aos dos registros de CloudTrail eventos. O conteúdo de `eventData` é fornecido por seus eventos; outros campos são fornecidos CloudTrail após a ingestão.

CloudTrail o conteúdo do registro de eventos é descrito com mais detalhes emCloudTrail conteúdo do registro.

- Campos fornecidos por CloudTrail após a ingestão
- Campos que são fornecidos por seus eventos

Campos fornecidos por CloudTrail após a ingestão

Nome do campo	Tipo de entrada	Requisito	Descrição
eventVersion	string	Obrigatório	A versão do evento.
eventCategory	string	Obrigatório	A categoria do evento. Para não AWS eventos, o valor é`ActivityAuditLog` .
eventType	string	Obrigatório	O tipo de evento. Para não AWS eventos, o valor válido é`ActivityLog` .
eventID	string	Obrigatório	Um ID exclusivo para um evento.
eventTime	string	Obrigatório	O carimbo de data e hora do evento, no formato `yyyy-MM-DDTHH:mm:ss` , em Universal Coordinated Time (UTC – Tempo

Nome do campo	Tipo de entrada	Requisito	Descrição
			universal coordenado).
awsRegion	string	Obrigatório	O Região da AWS local onde a `PutAuditEvents` ligação foi feita.
recipientAccountId	string	Obrigatório	Representa o ID da conta que recebeu esse evento. CloudTrail preenche esse campo calculando-o a partir da carga útil do evento.
addendum	-	Opcional	Exibe informações sobre o motivo do atraso no processamento de um evento. Se as informações estiverem ausentes de um evento existente, o bloco de adendo incluirá as informações ausentes e um motivo pelo qual elas estavam ausentes.
• razão	string	Opcional	A razão pela qual o evento ou parte de seu conteúdo estavam faltando.

Nome do campo	Tipo de entrada	Requisito	Descrição
• updatedFields	string	Opcional	Os campos de registro de eventos que são atualizados pelo adendo. Isso só será fornecido se o motivo for `UPDATED_DATA` .
• originalUID	string	Opcional	O UID original do evento da fonte. Isso só será fornecido se o motivo for `UPDATED_DATA` .
• originalEventID	string	Opcional	O ID do evento original. Isso só será fornecido se o motivo for `UPDATED_DATA` .
metadata	-	Obrigatório	Informações sobre o canal usado pelo evento.
• ingestionTime	string	Obrigatório	O carimbo de data e hora de quando o evento foi processado, no formato `yyyy-MM-DDTHH:mm:ss` , em Universal Coordinated Time (UTC – Tempo universal coordenado).
• channelARN	string	Obrigatório	O ARN do canal que o evento usou.

Campos que são fornecidos por eventos de clientes

Nome do campo	Tipo de entrada	Requisito	Descrição
eventData	-	Obrigatório	Os dados de auditoria enviados CloudTrail em uma `PutAuditEvents` chamada.
• versão	string	Obrigatório	A versão do evento com base em sua fonte. Restrições de tamanho: tamanho máximo de 256.
• userIdentity	-	Obrigatório	Informações sobre o usuário que fez uma solicitação.
• • tipo	string	Obrigatório	O tipo de identidade do usuário. Restrições de tamanho: tamanho máximo de 128.
• • principalId	string	Obrigatório	Um identificador exclusivo para o ator do evento. Restrições de tamanho: tamanho máximo de 1024.
• • detalhes	Objeto JSON	Opcional	Informações adicionais sobre a identidade.

Nome do campo	Tipo de entrada	Requisito	Descrição
• userAgent	string	Opcional	O agente por meio do qual a solicitação foi feita. Restrições de tamanho: tamanho máximo de 1024.
• eventSource	string	Obrigatório	Essa é a fonte do evento do parceiro, ou a aplicação personalizada da qual os eventos são registrados em log. Restrições de tamanho: tamanho máximo de 1024.
• eventName	string	Obrigatório	A ação solicitada, uma das ações na API do serviço ou aplicação de fonte. Restrições de tamanho: tamanho máximo de 1024.
• eventTime	string	Obrigatório	O carimbo de data e hora do evento, no formato `yyyy-MM-DDTHH:mm:ss`, em Universal Coordinated Time (UTC – Tempo universal coordenado).

Nome do campo	Tipo de entrada	Requisito	Descrição
• UID	string	Obrigatório	O valor do UID que identifica a solicitação. O serviço ou a aplicação chamada gera esse valor. Restrições de tamanho: tamanho máximo de 1024.
• requestParameters	Objeto JSON	Opcional	Os parâmetros, se houver, que foram enviados com a solicitação. Este campo tem um tamanho máximo de 100 KB, e o conteúdo que exceder esse limite será rejeitado.
• responseElements	Objeto JSON	Opcional	O elemento de resposta das ações que fazem alterações (criar, atualizar ou excluir ações). Este campo tem um tamanho máximo de 100 KB, e o conteúdo que exceder esse limite será rejeitado.

Nome do campo	Tipo de entrada	Requisito	Descrição
• errorCode	string	Opcional	Uma string represent ando um erro para o evento. Restrições de tamanho: tamanho máximo de 256.
• errorMessage	string	Opcional	A descrição do erro. Restrições de tamanho: tamanho máximo de 256.
• sourceIPAddress	string	Opcional	O endereço IP do qual a solicitação foi feita. Tanto endereços IPv4 quanto IPv6 são aceitos.
• recipientAccountId	string	Obrigatório	Representa o ID da conta que recebeu esse evento. O ID da conta deve ser igual ao ID da AWS conta proprietária do canal.

Nome do campo	Tipo de entrada	Requisito	Descrição
• additionalEventData	Objeto JSON	Opcional	Dados adicionais sobre o evento que não faziam parte da solicitação ou resposta. Este campo tem um tamanho máximo de 28 KB, e o conteúdo que exceder esse limite será rejeitado.

O exemplo a seguir mostra a hierarquia dos elementos do esquema que correspondem aos dos registros de CloudTrail eventos.

```
{
    "eventVersion": String,
    "eventCategory": String,
    "eventType": String,
    "eventID": String,
    "eventTime": String,
    "awsRegion": String,
    "recipientAccountId": String,
    "addendum": {
       "reason": String,
       "updatedFields": String,
       "originalUID": String,
       "originalEventID": String
    },
    "metadata" : {
       "ingestionTime": String,
       "channelARN": String
    },
    "eventData": {
        "version": String,
        "userIdentity": {
          "type": String,
          "principalId": String,
          "details": {
```

```
            JSON
          }
        },
        "userAgent": String,
        "eventSource": String,
        "eventName": String,
        "eventTime": String,
        "UID": String,
        "requestParameters": {
           JSON
        },
        "responseElements": {
           JSON
        },
        "errorCode": String,
        "errorMessage": String,
        "sourceIPAddress": String,
        "recipientAccountId": String,
        "additionalEventData": {
           JSON
        }
    }
}
```

Veja os painéis CloudTrail do Lake

Você pode usar os painéis do CloudTrail Lake para visualizar os eventos em um armazenamento de dados de eventos. Você pode selecionar entre vários tipos de painel diferentes. Os tipos de painéis disponíveis para um armazenamento de dados de eventos dependem da configuração dos seletores de eventos avançados do armazenamento de dados de eventos. Por exemplo, se um tipo de painel exibir informações sobre eventos CloudTrail de gerenciamento, você só poderá selecionar o painel se o armazenamento de dados de eventos atualmente selecionado coletar eventos CloudTrail de gerenciamento.

Cada tipo de painel consiste em vários widgets e cada widget representa uma consulta SQL. Para visualizar a consulta por um widget, escolha Visualizar e analisar no editor de consultas para abrir o editor de consultas. Não é possível modificar a consulta gerada pelo sistema que é usada para preencher o widget, mas você pode fazer edições na consulta e executá-la no editor de consultas para realizar uma análise mais detalhada.

Para preencher e atualizar um painel, escolha Executar consultas. Quando você escolhe Executar consultas, CloudTrail executa consultas geradas pelo sistema em seu nome. Como a execução de consultas gera custos, CloudTrail solicita que você reconheça os custos associados à execução de consultas. Essa confirmação é necessária apenas uma vez. Para obter mais informações sobre CloudTrail preços, consulte CloudTrail Preços.

Tópicos

Limitações

As limitações a seguir se aplicam à versão atual.

- A versão atual não oferece suporte a painéis, widgets ou consultas personalizados.
- A versão atual fornece apenas painéis para armazenamentos de dados de eventos que coletam CloudTrail eventos (eventos de dados, eventos de gerenciamento) e eventos do Insights.
- A versão atual não oferece suporte à edição das consultas geradas pelo sistema usadas para preencher o painel. É possível visualizar e editar a consulta subjacente de qualquer widget na guia Editor de consultas. No entanto, todas as alterações feitas na consulta são destinadas à análise complementar fora do painel.

Pré-requisitos

Os pré-requisitos a seguir se aplicam aos painéis do Lake.

- Para visualizar e usar os painéis do Lake, você deve criar pelo menos um armazenamento de dados de eventos do CloudTrail Lake. Você pode criar armazenamentos de dados de eventos usando o console ou SDKs. AWS CLI Para obter informações sobre a criação de armazenamentos de dados de eventos usando o console, consulte Crie um armazenamento de dados de CloudTrail eventos para eventos com o console. Para obter informações sobre como criar um armazenamento de dados de eventos usando o AWS CLI, consulteCrie, atualize e gerencie armazenamentos de dados de eventos com o AWS CLI.

- Para preencher o painel, CloudTrail executa consultas em seu nome. Na primeira vez que você visualiza a página Painéis, CloudTrail solicita que você reconheça os custos associados à execução de consultas. Escolha Eu concordo para confirmar que está ciente do custo da execução de consultas.

Escolher um painel

Use o procedimento a seguir para selecionar um armazenamento de dados de eventos e um tipo de painel para visualizar.

1. Faça login no AWS Management Console e abra o CloudTrail console em https://console.aws.amazon.com/cloudtrail/.
2. No painel de navegação, em Lake, escolha Painel.
3. Escolha o armazenamento de dados de eventos para o qual deseja visualizar os dados.
4. Escolha o tipo de painel que deseja visualizar. A lista de painéis é preenchida com base na configuração avançada dos seletores de eventos do armazenamento de dados de eventos selecionado.

   Os possíveis tipos de painel são apresentados a seguir.

   - Painel de visão geral - Mostra os usuários mais ativos e Serviços da AWS por contagem de eventos. Regiões da AWS Também é possível visualizar informações sobre atividades de eventos de gerenciamento de `read` e `write`, eventos com mais controle de utilização e os principais erros. Esse painel está disponível para armazenamentos de dados de eventos que coletam eventos de gerenciamento.
   - Painel Gerenciamento de eventos: mostra eventos de login do console, eventos de acesso negado, ações destrutivas e principais erros por usuário. Você também pode visualizar informações sobre versões do TLS e chamadas de TLS desatualizadas por usuário. Esse painel está disponível para armazenamentos de dados de eventos que coletam eventos de gerenciamento.
   - Painel Eventos de dados do S3: mostra a atividade da conta do S3, os objetos mais acessados do S3, os principais usuários do S3 e as principais ações do S3. Esse painel está disponível para armazenamentos de dados de eventos que coletam eventos de dados do Amazon S3.
   - Painel Eventos do Insights: mostra a proporção geral de eventos do Insights por tipo de Insights, a proporção de eventos do Insights por tipo de Insights para os principais usuários

e serviços e o número de eventos do Insights por dia. O painel também inclui um widget que lista até 30 dias de eventos do Insights. Esse painel está disponível somente para armazenamentos de dados de eventos que coletam eventos do Insights.

> **Note**
>
> - Depois de ativar o CloudTrail Insights pela primeira vez no armazenamento de dados do evento de origem, pode levar até 7 dias CloudTrail para entregar o primeiro evento do Insights, se uma atividade incomum for detectada. Para ter mais informações, consulte Entender a entrega de eventos do Insights.
> - O painel Eventos do Insights exibe apenas informações sobre os eventos do Insights coletados pelo armazenamento de dados de eventos selecionado, o qual é determinado pela configuração do armazenamento de dados do evento de origem. Por exemplo, se você configurar o armazenamento de dados de eventos de origem para ativar eventos do Insights em `ApiCallRateInsight` mas não `ApiErrorRateInsight`, você não verá informações sobre os eventos do Insights em `ApiErrorRateInsight`.

5. Escolha entre filtrar os dados do painel por um Intervalo absoluto ou um Intervalo relativo. Escolha Intervalo absoluto para selecionar um intervalo específico de data e hora. Escolha Intervalo relativo para selecionar um intervalo de tempo predefinido ou um intervalo personalizado. Por padrão, o painel exibe dados de eventos das últimas 24 horas.

> **Note**
>
> CloudTrail As consultas do Lake incorrem em custos com base na quantidade de dados digitalizados. Para ajudar a controlar os custos, é possível filtrar em um intervalo de tempo mais restrito. Para obter mais informações sobre CloudTrail preços, consulte AWS CloudTrail Preços.

6. Escolha Executar consultas para executar as consultas nos widgets do painel.

Filtrar um painel por um intervalo de data ou hora

Por padrão, o painel exibe dados das últimas 24 horas. É possível filtrar um painel por um Intervalo absoluto ou um Intervalo relativo.

Escolha Intervalo absoluto para selecionar um intervalo específico de data e hora.

Escolha Intervalo relativo para selecionar um intervalo de tempo predefinido ou um intervalo personalizado.

Após escolher o intervalo de tempo, escolha Executar consultas para atualizar o painel.

> **Note**
>
> CloudTrail As consultas do Lake incorrem em custos com base na quantidade de dados digitalizados. Para ajudar a controlar os custos, é possível filtrar em um intervalo de tempo mais restrito. Para obter mais informações sobre CloudTrail preços, consulte AWS CloudTrail Preços.

Visualizar a consulta para um widget de painel

Cada widget representa uma consulta SQL. Para visualizar a consulta por um widget, escolha Visualizar e analisar no editor de consultas para abrir o editor de consultas. Usando o editor de consultas, é possível refinar ainda mais a consulta fora do painel e executá-la para ver os resultados da consulta atualizada. Para obter mais informações sobre como trabalhar consultas, veja Criar ou editar uma consulta.

> **Note**
>
> Não é possível modificar a consulta gerada pelo sistema para um widget do painel. Todas as alterações feitas na consulta na guia Editor de consultas são destinadas exclusivamente a análises adicionais fora do painel.

CloudTrail Consultas sobre o lago

As consultas no CloudTrail Lake são criadas em SQL. Você pode criar uma consulta na guia CloudTrail Lake Editor escrevendo a consulta em SQL do zero ou abrindo uma consulta salva ou de amostra e editando-a. Você não pode sobrescrever uma consulta de exemplo incluída por suas alterações, mas você pode salvá-la como uma nova consulta. Para obter mais informações sobre a linguagem de consulta SQL permitida, consulte CloudTrail Restrições do Lake SQL.

Uma consulta ilimitada (como `SELECT * FROM edsID`) verifica todos os dados no armazenamento de dados do seu evento. Para ajudar a controlar os custos, recomendamos que você restrinja as consultas adicionando carimbos de data/hora `eventTime` de início e término nas consultas. Veja a seguir um exemplo que pesquisa todos os eventos em um armazenamento de dados de eventos especificado, onde a hora do evento é depois de (>) 5 de janeiro de 2023 às 13h51 e antes de (<) 19 de janeiro de 2023 às 13h51. Como um armazenamento de dados de eventos tem um período de retenção mínimo de sete dias, o intervalo de tempo mínimo entre valores `eventTime` de início e término também é de sete dias.

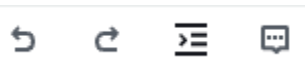
```
SELECT *
FROM eds-ID
WHERE
     eventtime >='2023-01-05 13:51:00' and eventtime < ='2023-01-19 13:51:00'
```

Tópicos

- Ferramentas do editor de consultas
- Veja exemplos de consultas no console CloudTrail
- Criar ou editar uma consulta
- Executar uma consulta e salvar os resultados de consulta
- Visualizar resultados da consulta
- Baixar resultados de consulta salvos
- Validar resultados de consulta salva
- Execute e gerencie consultas do CloudTrail Lake com o AWS CLI

Ferramentas do editor de consultas

Uma barra de ferramentas no canto superior direito do editor de consultas oferece comandos para ajudar a criar e formatar sua consulta de SQL.



As seções a seguir descreve os comandos da barra de ferramentas.

- Undo (Desfazer): reverte a última alteração de conteúdo feita no editor de consultas.
- Redo (Refazer): repete a última alteração de conteúdo feita no editor de consultas.

- Format selected (Formatar seleção): organiza o conteúdo do editor de consultas de acordo com as convenções de formatação e espaçamento de SQL.
- Comentar/descomentar seleção: comenta a parte selecionada da consulta, caso ela ainda não tenha sido comentada. Se a parte selecionada já estiver comentada, escolher essa opção removerá o comentário.

Veja exemplos de consultas no console CloudTrail

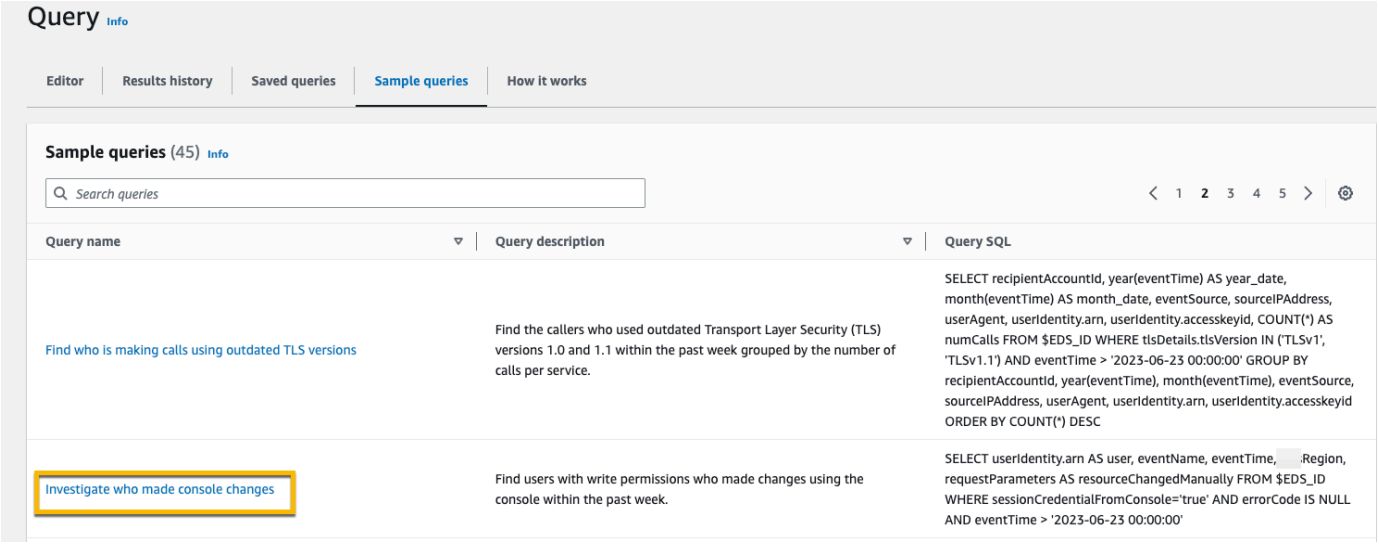
O CloudTrail console fornece vários exemplos de consultas que podem ajudar você a começar a escrever suas próprias consultas.

CloudTrail as consultas incorrem em cobranças com base na quantidade de dados digitalizados. Para ajudar a controlar os custos, recomendamos que você restrinja as consultas adicionando carimbos de data/hora `eventTime` de início e término nas consultas. Para obter mais informações sobre CloudTrail preços, consulte AWS CloudTrail Preços.

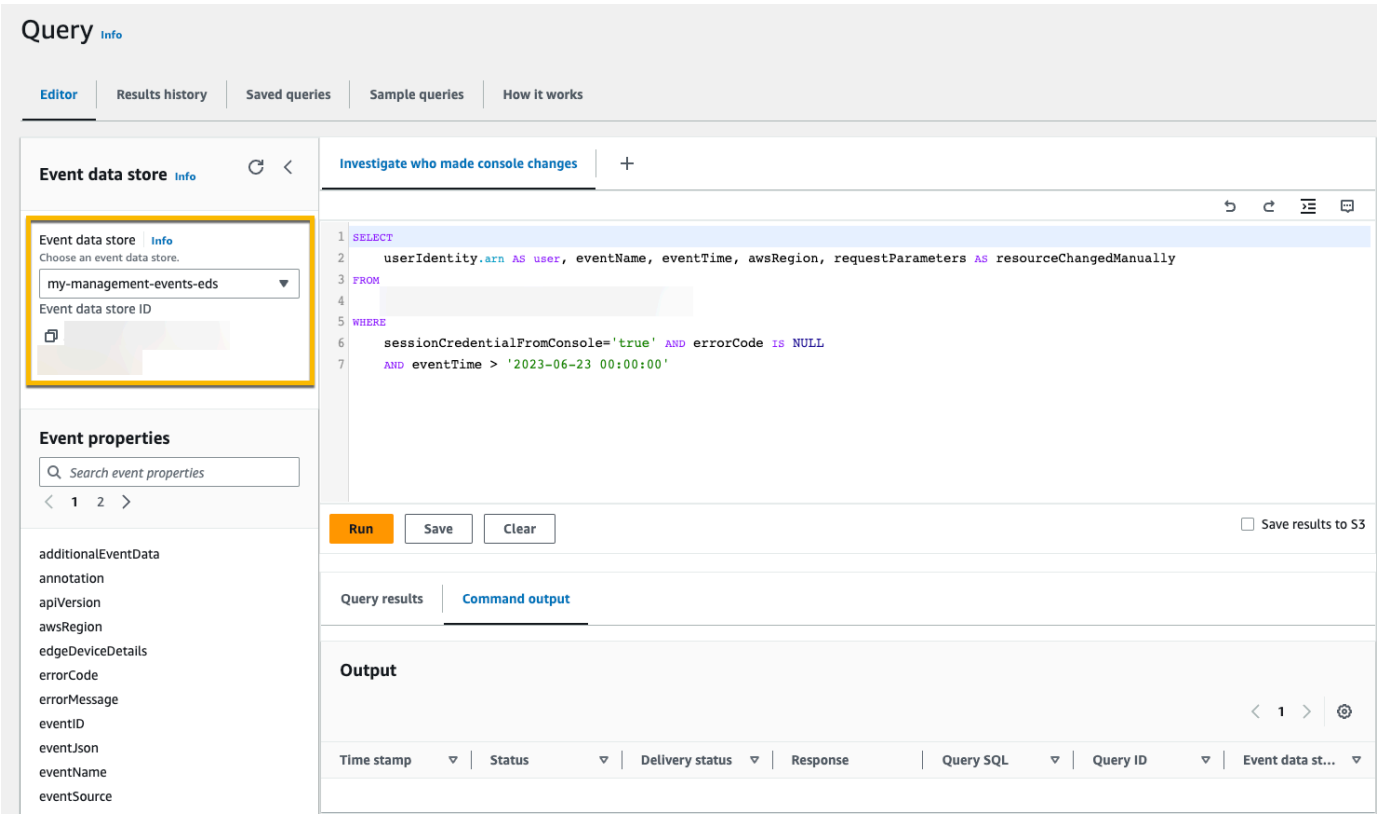
> **Note**
>
> Você também pode ver as consultas criadas pela GitHub comunidade. Para obter mais informações e ver esses exemplos de consultas, consulte Exemplos de consultas do CloudTrail Lake no GitHub site. AWS CloudTrail não avaliou as consultas em GitHub.

Para visualizar e executar uma consulta de exemplo

1. Faça login no AWS Management Console e abra o CloudTrail console em https://console.aws.amazon.com/cloudtrail/.
2. No painel de navegação, em Lake, escolha Consulta.
3. Na página Query (Consulta), escolha a guia Sample queries (Consultas de exemplo).
4. Escolha uma consulta de exemplo na lista ou pesquise pela consulta para filtrar a lista. Neste exemplo, abriremos a consulta Investigar quem fez alterações no console escolhendo o Nome da consulta. Isso abre a consulta na guia Editor.

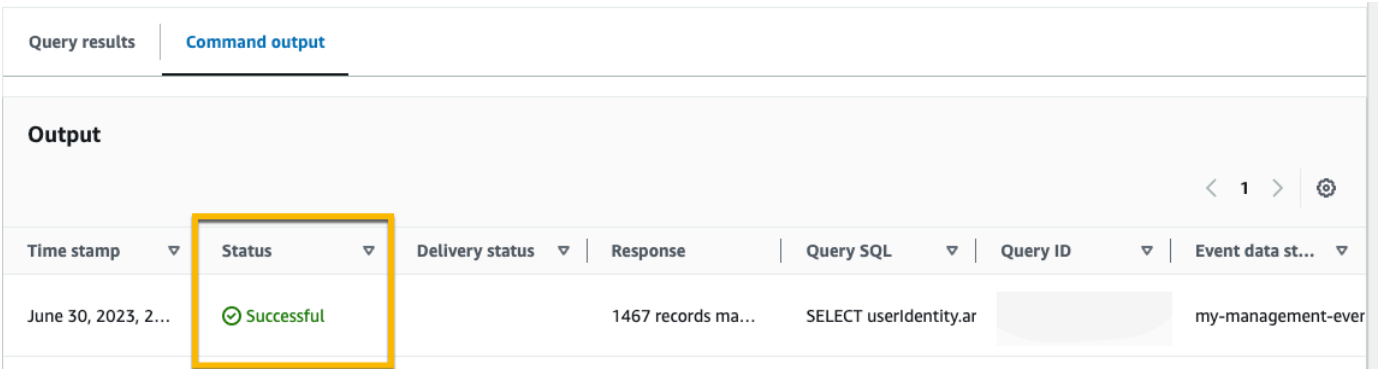


5. Na guia Editor, escolha o armazenamento de dados de eventos para o qual você deseja executar a consulta. Quando você escolhe o armazenamento de dados do evento na lista, preenche CloudTrail automaticamente o ID do armazenamento de dados do evento na `FROM` linha do editor de consultas.

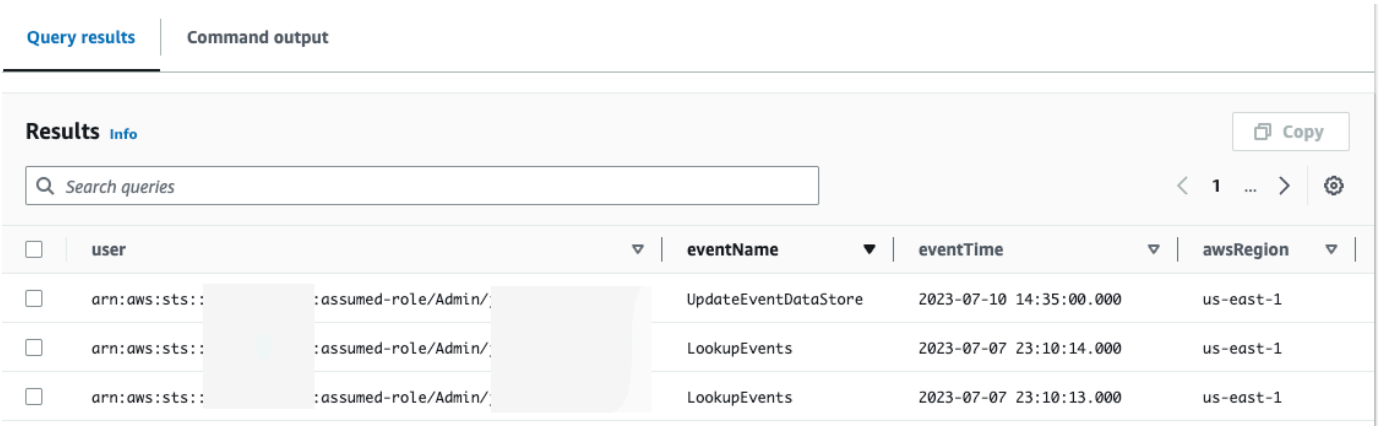


6. Para executar a consulta, escolha Executar.

A guia Saída do comando mostra metadados sobre a consulta, por exemplo, se a consulta foi bem-sucedida, o número de registros correspondentes e o tempo de execução da consulta.



A guia Resultados da consulta mostra os dados de eventos no armazenamento de dados de eventos selecionado que correspondem à sua consulta.



Para obter mais informações sobre a edição de uma consulta, veja Criar ou editar uma consulta. Para obter mais informações sobre como executar uma consulta e salvar seus resultados, consulte Executar uma consulta e salvar os resultados de consulta.

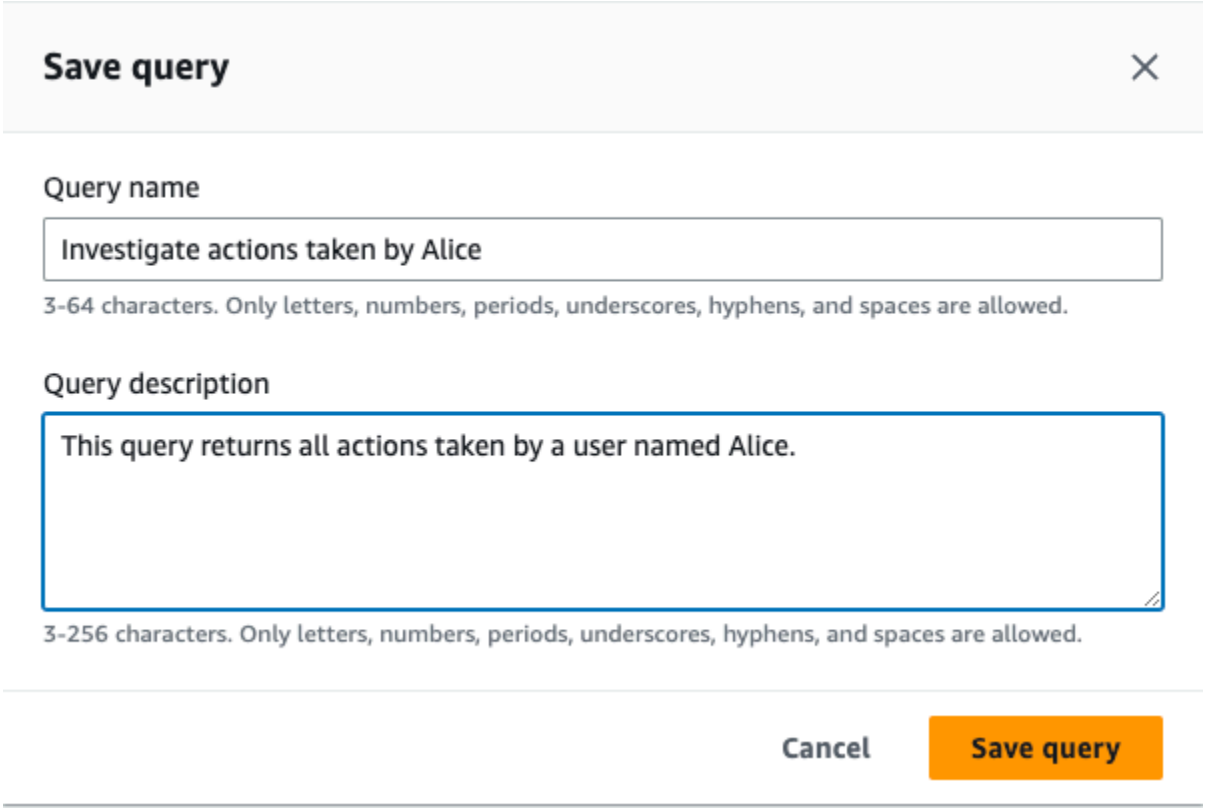
Criar ou editar uma consulta

Neste passo a passo, abrimos uma das consultas de exemplo, a editamos para encontrar ações realizadas por um usuário específico chamado `Alice` e a salvamos como uma nova consulta. Você também pode editar uma consulta salva na guia Saved queries (Consultas salvas), caso tenha consultas salvas. Para ajudar a controlar os custos, recomendamos que você restrinja as consultas adicionando carimbos de data/hora `eventTime` de início e término nas consultas.

1. Faça login no AWS Management Console e abra o CloudTrail console em https://console.aws.amazon.com/cloudtrail/.
2. No painel de navegação, em Lake, escolha Consulta.
3. Na página Query (Consulta), escolha a guia Sample queries (Consultas de exemplo).
4. Abra uma consulta de exemplo escolhendo o Nome da consulta. Isso abre a consulta na guia Editor. Neste exemplo, selecionaremos a consulta chamada Investigar ações do usuário e editaremos a consulta para encontrar as ações de um usuário específico chamado `Alice`.
5. Na guia Editor, edite a linha `WHERE` para especificar o usuário que você deseja investigar e atualize os `eventTime` valores conforme necessário. O valor de `FROM` é a parte da ID do ARN do armazenamento de dados do evento e é preenchido automaticamente CloudTrail quando você escolhe o armazenamento de dados do evento.

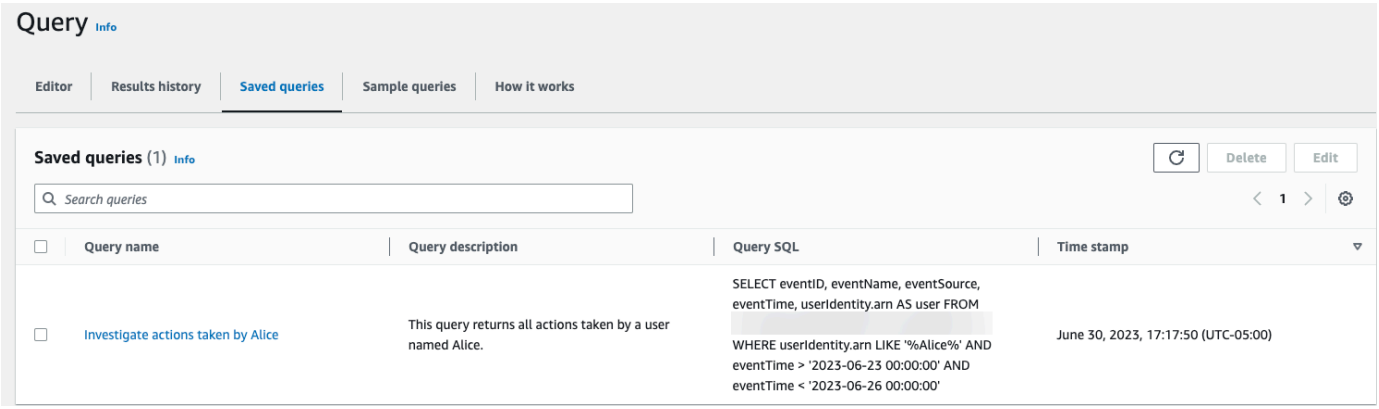
```
SELECT
    eventID, eventName, eventSource, eventTime, userIdentity.arn AS user
FROM
    event-data-store-id
WHERE
    userIdentity.arn LIKE '%Alice%'
    AND eventTime > '2023-06-23 00:00:00' AND eventTime < '2023-06-26 00:00:00'
```

6. Você pode executar uma consulta antes de salvá-la para verificar se a consulta funciona. Para executar uma consulta, escolha um armazenamento de dados de eventos na lista suspensa Event data store (Armazenamentos de dados de eventos) e, em seguida, escolha Run (Executar). Veja a coluna Status da guia Command output (Saída do comando) para a consulta ativa para verificar se uma consulta foi executada com êxito.
7. Depois de atualizar a consulta de exemplo, escolha Salvar.
8. Em Save query (Salvar consulta), insira um nome e uma descrição para a consulta. Escolha Save query (Salvar consulta) para salvar suas alterações como a nova consulta. Para descartar as alterações em uma consulta, escolha Cancel (Cancelar) ou feche a janela Save query (Salvar consulta).



> **Note**
>
> As consultas salvas estão vinculadas ao seu navegador; se você usar um navegador ou dispositivo diferente para acessar o CloudTrail console, as consultas salvas não estarão disponíveis.

9. Abra a guia Saved queries (Consultas salvas) para ver a nova consulta na tabela.



Executar uma consulta e salvar os resultados de consulta

Após escolher ou salvar uma consulta, você poderá executar uma consulta em um armazenamento de dados de eventos.

Ao executar uma consulta, você tem a opção de salvar os resultados de consulta em um bucket do Amazon S3. Ao executar consultas no CloudTrail Lake, você incorre em cobranças com base na quantidade de dados digitalizados pela consulta. Não há cobranças adicionais do CloudTrail Lake para salvar os resultados da consulta em um bucket do S3. No entanto, há cobranças de armazenamento do S3. Para obter mais informações sobre os preços, consulte Preços do Amazon S3.

Quando você salva os resultados da consulta, os resultados da consulta podem ser exibidos no CloudTrail console antes de serem visualizados no bucket do S3, pois CloudTrail entregam os resultados da consulta após a conclusão da verificação da consulta. Embora a maioria das consultas seja concluída em alguns minutos, dependendo do tamanho do seu armazenamento de dados de eventos, pode levar muito mais tempo para entregar os resultados da consulta CloudTrail ao seu bucket do S3. CloudTrail entrega os resultados da consulta ao bucket do S3 no formato gzip compactado. Em média, após a conclusão da análise da consulta, você pode esperar uma latência de 60 a 90 segundos para cada GB de dados entregue ao bucket do S3.

Para executar uma consulta usando o CloudTrail Lake

1. Faça login no AWS Management Console e abra o CloudTrail console em https://console.aws.amazon.com/cloudtrail/.
2. No painel de navegação, em Lake, escolha Consulta.
3. Nas guias Consultas de exemplo ou Consultas salvas, escolha uma consulta a ser executada escolhendo o valor na coluna Nome da consulta.
4. Na guia Editor, em Event data store (Armazenamento de dados de eventos), escolha um armazenamento de dados de eventos na lista suspensa.
5. (Opcional) Na guia Editor, escolha Save results to S3 (Salvar resultados no S3) para salvar os resultados de consulta em um bucket do S3. Quando você escolhe o bucket S3 padrão, CloudTrail cria e aplica as políticas de bucket necessárias. Se você escolher o bucket S3 padrão, sua política do IAM precisará incluir permissão para a `s3:PutEncryptionConfiguration` ação porque, por padrão, a criptografia do lado do servidor está habilitada para o bucket. Para obter mais informações sobre como salvar resultados de consulta, acesse Informações adicionais sobre resultados de consultas salvas.

> **Note**
>
> Para usar um bucket diferente, especifique um nome de bucket ou escolha Browse S3 (Procurar S3) para escolher um bucket. A política do bucket deve conceder CloudTrail permissão para entregar os resultados da consulta ao bucket. Para obter informações sobre como editar manualmente a política de bucket, consulte Política de bucket do Amazon S3 para resultados de consulta CloudTrail do Lake.

6. Na guia Editor, escolha Run (Executar).

   Dependendo do tamanho do armazenamento de dados do evento e do número de dias de dados que ele inclui, uma consulta pode levar vários minutos para ser executada. A guia Command output (Saída do comando) mostra o status de uma consulta e se uma consulta tem a execução concluída. Quando uma consulta terminar de ser executada, abra a guia Query results (Resultados da consulta) para ver uma tabela de resultados para a consulta ativa (a consulta atualmente mostrada no editor).

> **Note**
>
> Consultas que são executadas por mais de uma hora podem expirar. Você ainda pode obter resultados parciais que foram processados antes do tempo limite da consulta. CloudTrail não fornece resultados de consulta parciais para um bucket do S3. Para evitar atingir um tempo limite, você pode refinar sua consulta a fim de limitar a quantidade de dados digitalizados especificando um intervalo de tempo mais restrito.

Informações adicionais sobre resultados de consultas salvas

Após salvar os resultados de consulta, você pode baixar os resultados de consulta salvos diretamente do bucket do S3. Para obter mais informações sobre como localizar e baixar resultados de consultas salvas, acesse Baixar resultados de consulta salvos.

Você também pode validar os resultados da consulta salvos para determinar se os resultados da consulta foram modificados, excluídos ou inalterados após a CloudTrail entrega dos resultados da consulta. Para obter mais informações sobre validação de resultados de consultas salvas, acesse Validar resultados de consulta salva.

Exemplo: salvar os resultados da consulta em um bucket do Amazon S3

Este passo a passo mostra como você pode salvar os resultados da consulta em um bucket do S3 e, em seguida, fazer o download desses resultados.

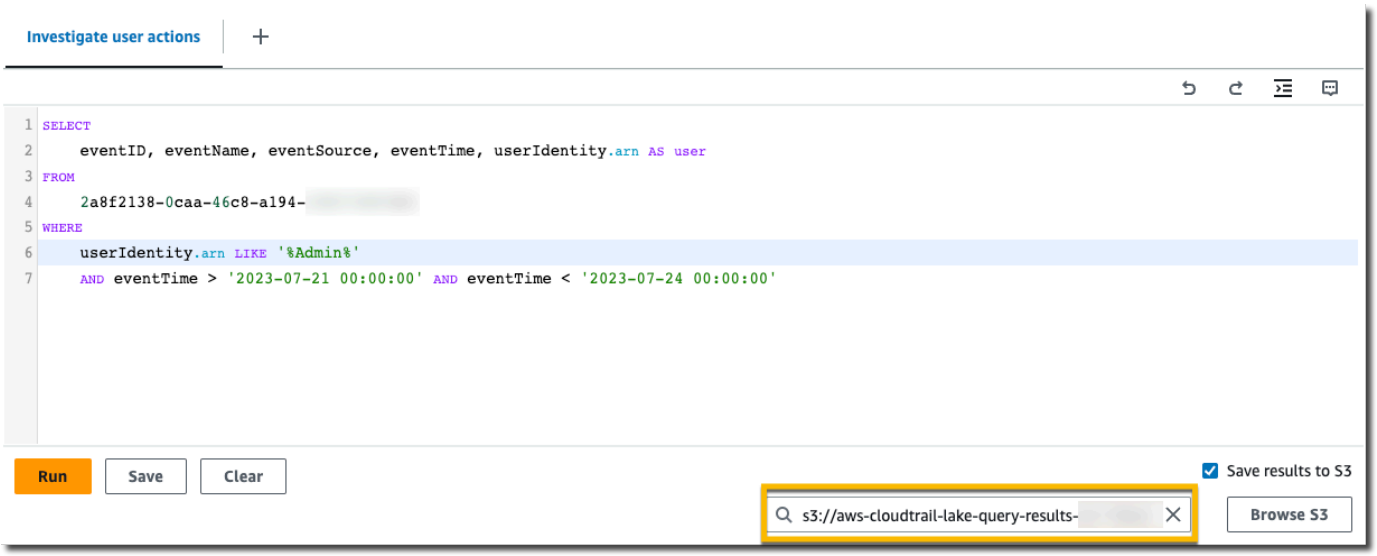
Para salvar resultados de consultas em um bucket do Amazon S3

1. Faça login no AWS Management Console e abra o CloudTrail console em https://console.aws.amazon.com/cloudtrail/.
2. No painel de navegação, em Lake, escolha Consulta.
3. Nas guias Consultas de exemplo ou Consultas salvas, escolha uma consulta a ser executada escolhendo o valor na coluna Nome da consulta. Neste exemplo, escolheremos a consulta de exemplo chamada Investigar ações do usuário.
4. Na guia Editor, em Event data store (Armazenamento de dados de eventos), escolha um armazenamento de dados de eventos na lista suspensa. Quando você escolhe o armazenamento de dados do evento na lista, preenche CloudTrail automaticamente o ID do armazenamento de dados do evento na `From` linha.
5. Nesta consulta de exemplo, editaremos o valor `userIdentity.ARN` para especificar um usuário chamado `Admin` e mantermos os valores padrão para `eventTime`. Ao executar uma consulta, você é cobrado pela quantidade de dados examinados. Para ajudar a controlar os custos, recomendamos que você restrinja as consultas adicionando carimbos de data/hora `eventTime` de início e término nas consultas.

6. Escolha Salvar resultados no S3 para salvar os resultados da consulta em um bucket do S3. Quando você escolhe o bucket S3 padrão, CloudTrail cria e aplica as políticas de bucket necessárias. Se você escolher o bucket S3 padrão, sua política do IAM precisará incluir permissão para a `s3:PutEncryptionConfiguration` ação porque, por padrão, a criptografia

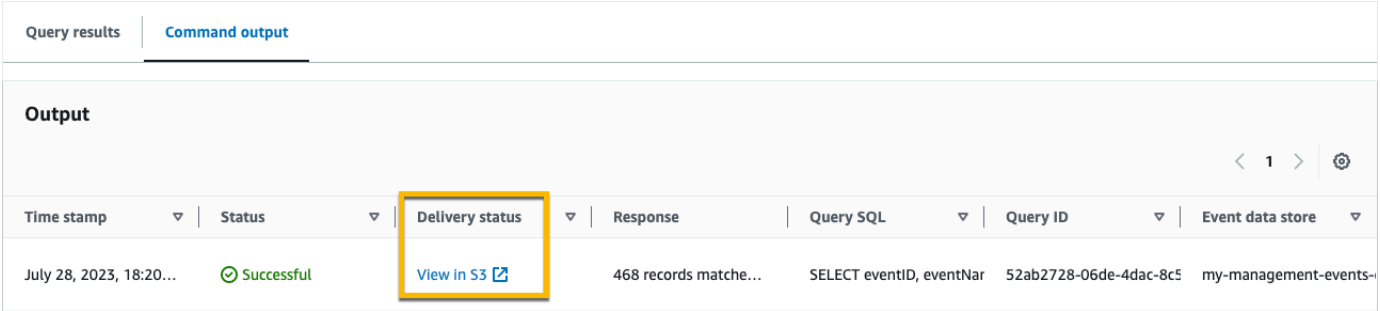
do lado do servidor está habilitada para o bucket. Neste exemplo, usaremos o bucket do S3 padrão.

> **Note**
>
> Para usar um bucket diferente, especifique um nome de bucket ou escolha Browse S3 (Procurar S3) para escolher um bucket. A política do bucket deve conceder CloudTrail permissão para entregar os resultados da consulta ao bucket. Para obter informações sobre como editar manualmente a política de bucket, consulte Política de bucket do Amazon S3 para resultados de consulta CloudTrail do Lake.

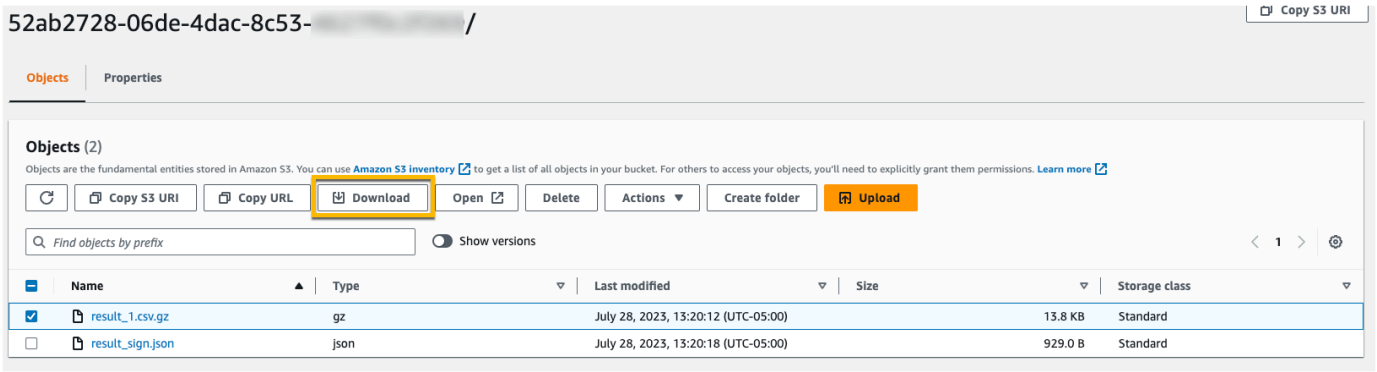


7. Escolha Executar. Dependendo do tamanho do armazenamento de dados do evento e do número de dias de dados que ele inclui, uma consulta pode levar vários minutos para ser executada. A guia Command output (Saída do comando) mostra o status de uma consulta e se uma consulta tem a execução concluída. Quando uma consulta terminar de ser executada, abra a guia Query results (Resultados da consulta) para ver uma tabela de resultados para a consulta ativa (a consulta atualmente mostrada no editor).
8. Ao CloudTrail concluir a entrega dos resultados da consulta salva no bucket do S3, a coluna Status da entrega fornece um link para o bucket do S3 que contém os arquivos de resultados da consulta salvos, bem como um arquivo de sinal que você pode usar para verificar os resultados da consulta salva. Escolha Visualizar no S3 para visualizar os arquivos de resultados da consulta e os arquivos de assinatura no bucket do S3.

> **Note**
>
> Quando você salva os resultados da consulta, os resultados da consulta podem ser exibidos no CloudTrail console antes de serem visualizados no bucket do S3, pois CloudTrail entregam os resultados da consulta após a conclusão da verificação da consulta. Embora a maioria das consultas seja concluída em alguns minutos, dependendo do tamanho do seu armazenamento de dados de eventos, pode levar muito mais tempo para entregar os resultados da consulta CloudTrail ao seu bucket do S3. CloudTrail entrega os resultados da consulta ao bucket do S3 no formato gzip compactado. Em média, após a conclusão da análise da consulta, você pode esperar uma latência de 60 a 90 segundos para cada GB de dados entregue ao bucket do S3.



9. Para baixar os resultados da consulta, escolha o arquivo de resultados da consulta (neste exemplo, `result_1.csv.gz`) e escolha Baixar.



Para obter mais informações sobre validação de resultados de consultas salvas, acesse [Validar resultados de consulta salva](#).

Visualizar resultados da consulta

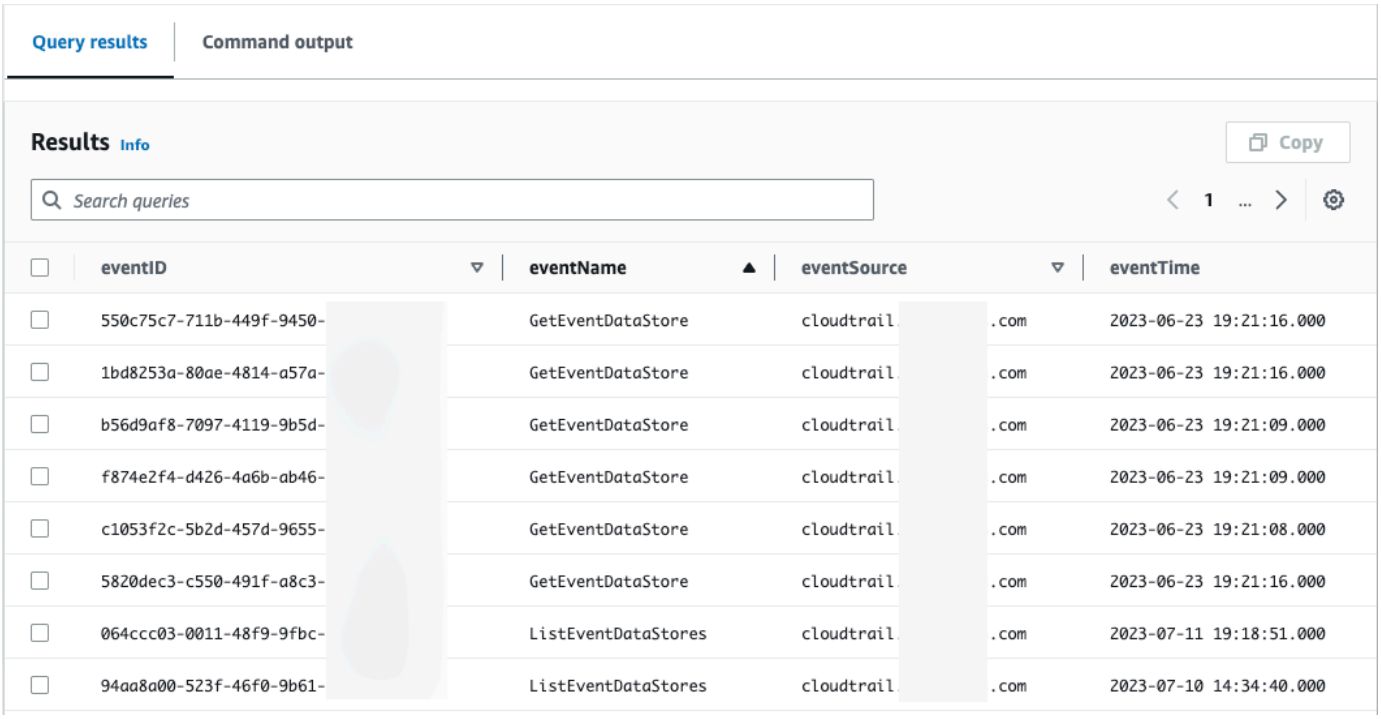
Após a conclusão da consulta, você poderá visualizar seus resultados. Os resultados de uma consulta ficam disponíveis por sete dias após a conclusão da consulta. É possível visualizar os resultados da consulta ativa na guia Query results (Resultados da consulta) ou acessar os resultados de todas as consultas recentes na guia Results history (Histórico de resultados), na página inicial do Lake.

Os resultados da consulta podem mudar de execuções mais antigas de uma consulta para as mais recentes, pois eventos posteriores no período de consulta podem ser registrados entre consultas.

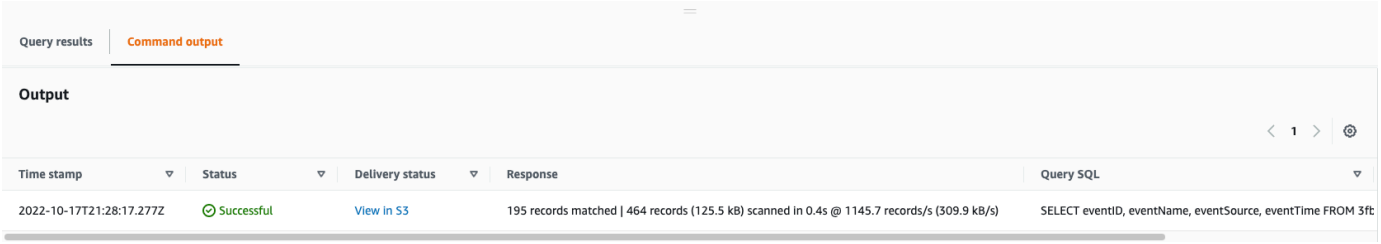
Quando você salva os resultados da consulta, os resultados da consulta podem ser exibidos no CloudTrail console antes de serem visualizados no bucket do S3, pois CloudTrail entregam os resultados da consulta após a conclusão da verificação da consulta. Embora a maioria das consultas seja concluída em alguns minutos, dependendo do tamanho do seu armazenamento de dados de eventos, pode levar muito mais tempo para entregar os resultados da consulta CloudTrail ao seu bucket do S3. CloudTrail entrega os resultados da consulta ao bucket do S3 no formato gzip compactado. Em média, após a conclusão da verificação da consulta, você pode esperar uma latência de 60 a 90 segundos para cada GB de dados entregue ao bucket do S3. Para obter mais informações sobre como localizar e baixar resultados de consultas salvas, acesse Baixar resultados de consulta salvos.

> **Note**
>
> Consultas executadas por mais de uma hora podem expirar. Você ainda pode obter resultados parciais que foram processados antes do tempo limite da consulta. CloudTrail não fornece resultados de consulta parciais para um bucket do S3. Para evitar atingir um tempo limite, você pode refinar sua consulta a fim de limitar a quantidade de dados digitalizados especificando um intervalo de tempo mais restrito.

1. Na guia Query results (Resultados da consulta) de uma consulta ativa, cada linha representa um resultado de evento que correspondeu à consulta. Filtre os resultados inserindo todo ou parte de um valor de campo de evento na barra de pesquisas. Para copiar um evento, escolha o evento que você deseja copiar e, em seguida, escolha Copiar.



2. Na guia Command output (Saída do comando) são exibidos metadados sobre a consulta que foi executada, como o ID do armazenamento de dados de eventos, o tempo de execução, o número de resultados verificados e se a consulta teve êxito ou não. Se você tiver salvado os resultados de consulta em um bucket do Amazon S3, os metadados também incluirão um link para o bucket do S3 que contém os resultados de consulta salvos.



Baixar resultados de consulta salvos

Depois de salvar os resultados da consulta, você precisa ser capaz de localizar o arquivo que contém os resultados da consulta. CloudTrail entrega os resultados da consulta para um bucket do Amazon S3 que você especifica ao salvar os resultados da consulta.

> **Note**
>
> Quando você salva os resultados da consulta, os resultados da consulta podem ser exibidos no console antes de serem visualizados no bucket do S3, pois CloudTrail entregam os

resultados da consulta após a conclusão da verificação da consulta. Embora a maioria das consultas seja concluída em alguns minutos, dependendo do tamanho do seu armazenamento de dados de eventos, pode levar muito mais tempo para entregar os resultados da consulta CloudTrail ao seu bucket do S3. CloudTrail entrega os resultados da consulta ao bucket do S3 no formato gzip compactado. Em média, após a conclusão da análise da consulta, você pode esperar uma latência de 60 a 90 segundos para cada GB de dados entregue ao bucket do S3.

Tópicos

Encontre os resultados de sua consulta salva no CloudTrail Lake

CloudTrail publica o resultado da consulta e assina arquivos no seu bucket do S3. O arquivo de resultado de consulta contém a saída da consulta salva e o arquivo de assinatura fornece a assinatura e o valor de hash para os resultados de consulta. Você pode usar o arquivo de assinatura para validar os resultados de consulta. Para obter mais informações sobre validação de resultados de consultas, acesse Validar resultados de consulta salva.

Para recuperar um arquivo de resultado de consulta ou de assinatura, é possível usar o console do Amazon S3, a interface de linha de comando (CLI) ou a API do Amazon S3.

Para localizar seus arquivos de resultados de consulta ou assinatura com o console do Amazon S3

1. Abra o console Amazon S3.
2. Escolha o bucket que você especificou.
3. Navegue pela hierarquia de objetos até encontrar os arquivos de resultado de consulta e assinatura. O arquivo de resultado de consulta tem uma extensão .csv.gz e o arquivo de assinatura tem uma extensão .json.

Você vai navegar por uma hierarquia de objetos semelhante ao exemplo a seguir, mas com nome de bucket, ID da conta, data e ID de consulta diferentes.

```
All Buckets
    Bucket_Name
        AWSLogs
            Account_ID;
                CloudTrail-Lake
                    Query
                        2022
                            06
                              20
                                Query_ID
```

Baixe os resultados de sua consulta salva no CloudTrail Lake

Quando você salva os resultados da consulta, CloudTrail entrega dois tipos de arquivos ao seu bucket do Amazon S3.

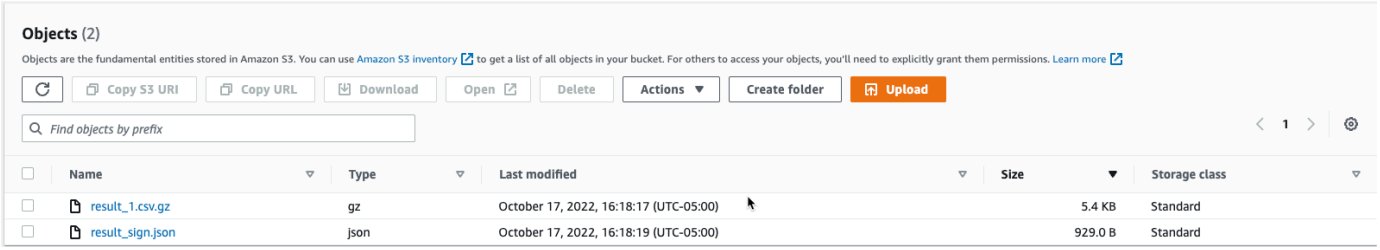
- Um arquivo de assinatura no formato JSON que você pode usar para validar os arquivos de resultados de consulta. O arquivo de assinatura é chamado result_sign.json. Para obter mais informações sobre o arquivo de assinatura, consulte CloudTrail estrutura de arquivo de assinatura.
- Um ou mais arquivos de resultados de consultas no formato CSV, que contêm os resultados de consulta. O número de arquivos de resultado de consulta entregue depende do tamanho total dos resultados de consulta. O tamanho máximo de arquivo de um resultado de consulta é de 1 TB. Cada arquivo de resultado de consulta é denominado result_ *número*.csv.gz. Por exemplo, se o tamanho total dos resultados de consulta for de 2 TB, você terá 2 arquivos de resultados de consulta, result_1.csv.gz e result_2.csv.gz.

CloudTrail o resultado da consulta e os arquivos de assinatura são objetos do Amazon S3. Você pode usar o console do S3, a AWS Command Line Interface (CLI) ou a API do S3 para recuperar o resultado da consulta e assinar arquivos.

O procedimento a seguir descreve como baixar os arquivos de resultado de consulta e assinatura com o console do Amazon S3.

Para baixar seu arquivo de resultado de consulta ou assinatura com o console do Amazon S3

1. Abra o console Amazon S3.
2. Escolha o bucket e o arquivo que você deseja baixar.



3. Escolha Download e siga as instruções na tela para salvar o arquivo.

> **Note**
>
> Alguns navegadores, como o Chrome, extraem automaticamente o arquivo de resultado de consulta para você. Se o navegador fizer isso, pule para a etapa 5.

4. Use um produto como o 7-Zip para extrair o arquivo de resultado de consulta.
5. Abra o arquivo de resultado de consulta ou de assinatura.

Validar resultados de consulta salva

Para determinar se os resultados da consulta foram modificados, excluídos ou inalterados após a CloudTrail entrega dos resultados da consulta, você pode usar a validação de integridade dos resultados da CloudTrail consulta. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computacionalmente inviável modificar, excluir ou falsificar arquivos de resultados de CloudTrail consultas sem detecção. Você pode usar a linha de comando para validar os arquivos de resultados de consulta.

Por que usá-la?

Os arquivos de resultado de consulta validados são valiosíssimos para segurança e investigações forenses. Por exemplo, um arquivo de resultado de consulta validado permite que você afirme positivamente que o arquivo de resultados da consulta em si não foi alterado. O processo de validação da integridade do arquivo de resultados da CloudTrail consulta também permite que você saiba se um arquivo de resultado da consulta foi excluído ou alterado.

Tópicos

- Valide os resultados da consulta salvos com o AWS CLI
- CloudTrail estrutura de arquivo de assinatura

- Implementações personalizadas da validação da integridade do arquivo de resultados da CloudTrail consulta

Valide os resultados da consulta salvos com o AWS CLI

É possível validar a integridade dos arquivos de resultado de consultas e do arquivo de assinatura com o comando aws cloudtrail verify-query-results.

Pré-requisitos

Para validar a integridade dos resultados de consulta com a linha de comando, é necessário satisfazer as seguintes condições:

- Você deve ter conectividade on-line com AWS.
- Você deve usar a AWS CLI versão 2.
- Para validar arquivos de resultados de consulta e o arquivo de assinatura localmente, as seguintes condições se aplicam:
  - É necessário colocar os arquivos de resultados de consulta e o arquivo de assinatura no caminho de arquivo especificado. Especifique o caminho do arquivo como o valor do parâmetro --local-export-path.
  - Você não deve renomear os arquivos de resultados de consulta e o arquivo de assinatura.
- Para validar os arquivos de resultados de consulta e o arquivo de assinatura no bucket do S3, as seguintes condições se aplicam:
  - Você não deve renomear os arquivos de resultados de consulta e o arquivo de assinatura.
  - É necessário ter acesso de leitura ao bucket do Amazon S3 que contém os arquivos de resultado de consultas e de assinatura.
  - O prefixo do S3 especificado deve conter os arquivos de resultados de consulta e o arquivo de assinatura. Especifique o prefixo do S3 como o valor do parâmetro --s3-prefix.

verify-query-results

O comando verify-query-results verifica o valor de hash de cada arquivo de resultado de consulta, comparando o valor com `fileHashValue` no arquivo de assinatura e, em seguida, validando o valor `hashSignature` no arquivo de assinatura.

Ao verificar os resultados da consulta, você pode usar as opções de linha de comando --s3-bucket e --s3-prefix para validar os arquivos de resultados de consulta e o arquivo de assinatura armazenados

em um bucket do S3 ou pode usar a opção de linha de comando --local-export-path para realizar uma validação local dos arquivos de resultados de consulta e do arquivo de assinatura baixados.

> **Note**
>
> O comando verify-query-results é específico da região. Você deve especificar a opção --region global para validar os resultados da consulta para uma específica Região da AWS.

Veja a seguir as opções para o comando verify-query-results.

--s3-bucket *<string>*

Especifica o nome do bucket do S3 que armazena os arquivos de resultados de consulta e o arquivo de assinatura. Não é possível usar esse parâmetro com --local-export-path.

--s3-prefix *<string>*

Especifica o caminho do S3 da pasta do S3 que contém os arquivos de resultados de consulta e o arquivo de assinatura (por exemplo, `s3/path/`). Não é possível usar esse parâmetro com --local-export-path. Esse parâmetro não precisará ser fornecido se os arquivos estiverem localizados no diretório raiz do bucket do S3.

--local-export-path *<string>*

Especifica o diretório local que contém os arquivos de resultados de consulta e o arquivo de assinatura (por exemplo, `/local/path/to/export/file/`). Não é possível usar esse parâmetro com --s3-bucket ou --s3-prefix.

Exemplos

O exemplo a seguir valida os resultados da consulta usando as opções de linha de comando --s3-bucket e --s3-prefix para especificar o nome e o prefixo do bucket do S3 que contém os arquivos de resultados de consulta e o arquivo de assinatura.

```
aws cloudtrail verify-query-results --s3-bucket bucket_name --s3-prefix prefix --
region region
```

O exemplo a seguir valida os resultados da consulta baixados usando a opção de linha de comando --local-export-path para especificar o caminho local para os arquivos de resultados de consulta e o arquivo de assinatura. Para obter mais informações sobre como baixar arquivos de resultados de consulta, verifique Baixe os resultados de sua consulta salva no CloudTrail Lake.

```
aws cloudtrail verify-query-results --local-export-path local_file_path --region region
```

Resultados da validação

A tabela a seguir descreve as possíveis mensagens de validação de arquivos de resultados de consulta e de assinatura.

Tipo de arquivo	Mensagem de validação	Descrição
`Sign file`	`Successfully validated sign and query result files`	A assinatura do arquivo de assinatura é válida. Os arquivos de resultados de consulta aos quais ele faz referência podem ser verificados.
`Query result file`	`ValidationError: "File file_name has inconsistent hash value with hash value recorded in sign file, hash value in sign file is expected_hash , but get computed_hash`	A validação falhou porque o valor de hash do arquivo de resultados de consulta não correspondia ao `fileHashValue` do arquivo de assinatura.
`Sign file`	`ValidationError: Invalid signature in sign file`	A validação do arquivo de assinatura falhou porque a assinatura não é válida.

CloudTrail estrutura de arquivo de assinatura

O arquivo de assinatura contém o nome de cada arquivo de resultado de consulta do S3 que foi entregue ao seu bucket do Amazon S3 quando você salvou os resultados de consulta, o valor de

hash de cada arquivo de resultado de consulta e a assinatura digital do arquivo. A assinatura digital e os valores de hash são usados para validar a integridade dos arquivos de resultado de consulta e do próprio arquivo de assinatura.

Local do arquivo de assinatura

O arquivo de assinatura é entregue a um local de bucket do Amazon S3 que segue essa sintaxe.

```
s3://s3-bucket-name/optional-prefix/AWSLogs/aws-account-ID/CloudTrail-Lake/
Query/year/month/date/query-ID/result_sign.json
```

Amostra de conteúdo do arquivo de assinatura

O exemplo de arquivo de sinal a seguir contém informações sobre os resultados da consulta CloudTrail Lake.

```
{
  "version": "1.0",
  "region": "us-east-1",
  "files": [
    {
      "fileHashValue" :
 "de85a48b8a363033c891abd723181243620a3af3b6505f0a44db77e147e9c188",
      "fileName" : "result_1.csv.gz"
    }
  ],
  "hashAlgorithm" : "SHA-256",
  "signatureAlgorithm" : "SHA256withRSA",
  "queryCompleteTime": "2022-05-10T22:06:30Z",
  "hashSignature" :
 "7664652aaf1d5a17a12ba50abe6aca77c0ec76264bdf7dce71ac6d1c7781117c2a412e5820bccf473b1361306dff6
  "publicKeyFingerprint" : "67b9fa73676d86966b449dd677850753"
}
```

Descrições dos campos do arquivo de assinatura

Veja a seguir as descrições de cada campo no arquivo de assinatura:

`version`

A versão do arquivo de assinatura.

`region`

A região da AWS conta usada para salvar os resultados da consulta.

`files.fileHashValue`

O valor de hash com codificação hexadecimal do conteúdo do arquivo de log não compactado.

`files.fileName`

O nome do arquivo de resultado de consulta.

`hashAlgorithm`

O algoritmo de hash usado para fazer hash do arquivo de resultado de consulta.

`signatureAlgorithm`

O algoritmo usado para assinar o arquivo.

`queryCompleteTime`

Indica quando os resultados da consulta foram CloudTrail entregues ao bucket do S3. Você pode usar esse valor para encontrar a chave pública.

`hashSignature`

A assinatura de hash do arquivo.

`publicKeyFingerprint`

A impressão digital com codificação hexadecimal da chave pública usada para assinar o arquivo.

Implementações personalizadas da validação da integridade do arquivo de resultados da CloudTrail consulta

Como CloudTrail usa algoritmos criptográficos e funções de hash padrão do setor e disponíveis abertamente, você pode criar suas próprias ferramentas para validar a integridade dos arquivos

de resultados da CloudTrail consulta. Quando você salva os resultados da consulta em um bucket do Amazon S3, CloudTrail entrega um arquivo de sinal para o seu bucket do S3. Você pode implementar sua própria solução de validação para validar os arquivos de resultados da assinatura e da consulta. Para obter mais informações sobre o arquivo de assinatura, consulte CloudTrail estrutura de arquivo de assinatura.

Este tópico descreve como o arquivo de assinatura é assinado e detalha as etapas que você precisará seguir para implementar uma solução que valide o arquivo de assinatura e os arquivos de resultado de consulta aos quais o arquivo de assinatura faz referência.

Entendendo como CloudTrail os arquivos de assinatura são assinados

CloudTrail os arquivos de assinatura são assinados com assinaturas digitais RSA. Para cada arquivo de sinal, CloudTrail faça o seguinte:

1. Cria uma lista de hash contendo o valor de hash para cada arquivo de resultado de consulta.
2. Obtém uma chave privada exclusiva para a região.
3. Transmite o hash SHA-256 da string e a chave privada ao algoritmo de assinatura RSA, que produz uma assinatura digital.
4. Codifica o código de byte da assinatura em formato hexadecimal.
5. Coloca a assinatura digital no arquivo de assinatura.

Conteúdo da string de assinatura de dados

A string de assinatura de dados consiste no valor de hash para cada arquivo de resultado de consulta separado por um espaço. O arquivo de assinatura lista o `fileHashValue` para cada arquivo de resultado de consulta.

Etapas da implementação da validação personalizada

Ao implementar uma solução personalizada de validação, você precisará validar o arquivo de assinatura e os arquivos de resultado de consulta aos quais ele faz referência.

Validar o arquivo de assinatura

Para validar um arquivo de assinatura, você precisa da assinatura dele, da chave pública cuja chave privada foi usada para assiná-lo e de uma string de assinatura de dados computada.

1. Obtenha o arquivo de assinatura.

2. Verifique se o arquivo de assinatura foi recuperado de seu local original.
3. Obtenha a assinatura com codificação hexadecimal do arquivo de assinatura.
4. Obtenha a impressão digital com codificação hexadecimal da chave pública cuja chave privada foi usada para assinar o arquivo de assinatura.
5. Recupere a chave pública do intervalo de tempo correspondente a `queryCompleteTime` no arquivo de assinatura. Para o intervalo de tempo, escolha um `StartTime` anterior a `queryCompleteTime` e um `EndTime` posterior a `queryCompleteTime`.
6. Entre as chaves públicas recuperadas, escolha aquela cuja impressão digital corresponda ao valor `publicKeyFingerprint` no arquivo de assinatura.
7. Usando uma lista de hash contendo o valor de hash para cada arquivo de resultado de consulta separado por um espaço, recrie a string de assinatura de dados usada para verificar a assinatura do arquivo de assinatura. O arquivo de assinatura lista o `fileHashValue` para cada arquivo de resultado de consulta.

   Por exemplo, se a matriz `files` do seu arquivo de assinatura contiver os três arquivos de resultados de consulta a seguir, sua lista de hash será “aaa bbb ccc”.

```
“files": [

   {

        "fileHashValue" : “aaa”,

        "fileName" : "result_1.csv.gz"

   },
   {

        "fileHashValue" : “bbb”,

        "fileName" : "result_2.csv.gz"

   },
   {

        "fileHashValue" : “ccc”,

        "fileName" : "result_3.csv.gz"

   }
```

```
],
```

8. Para validar a assinatura, transmita o hash SHA-256 da string, a chave pública e a assinatura como parâmetros ao algoritmo de verificação de assinatura RSA. Se o resultado for verdadeiro, o arquivo de assinatura será válido.

Validar os arquivos de resultados de consulta

Se o arquivo de assinatura for válido, valide os arquivos de resultados de consulta aos quais o arquivo de assinatura faz referência. Para validar a integridade de um arquivo de resultado de consulta, calcule seu valor de hash SHA-256 em seu conteúdo compactado e compare os resultados com o `fileHashValue` do arquivo de resultado de consulta registrado no arquivo de assinatura. Se os hashes forem correspondentes, o arquivo de resultado de consulta será válido.

As seções a seguir descrevem o processo de validação em detalhes.

A. Obter o arquivo de assinatura

Os primeiros passos são obter o arquivo de assinatura e obter a impressão digital da chave pública.

1. Obtenha o arquivo de assinatura do seu bucket do Amazon S3 para os resultados de consulta que deseja validar.
2. Em seguida, obtenha o valor `hashSignature` do arquivo de assinatura.
3. No arquivo de assinatura, obtenha a impressão digital da chave pública cuja chave privada foi usada para assinar o arquivo do campo `publicKeyFingerprint`.

B. Recuperar a chave pública para validar o arquivo de assinatura

Para obter a chave pública para validar o arquivo de assinatura, você pode usar a API AWS CLI ou a CloudTrail API. Em ambos os casos, você especifica um intervalo de tempo (ou seja, um horário de início e de término) para o arquivo de assinatura que você deseja validar. Use um intervalo de tempo correspondente a `queryCompleteTime` no arquivo de assinatura. Uma ou mais chaves públicas podem ser retornadas para o período que você especificar. As chaves retornadas podem ter períodos de validade que se sobrepõem.

> **Note**
>
> Como CloudTrail usa diferentes pares de chaves privadas/públicas por região, cada arquivo de sinal é assinado com uma chave privada exclusiva para sua região. Portanto, quando

você valida um arquivo de assinatura de uma região específica, precisa recuperar a chave pública da mesma região.

Use o AWS CLI para recuperar chaves públicas

Para recuperar uma chave pública para um arquivo de sinal usando o AWS CLI, use o `cloudtrail list-public-keys` comando. O comando tem o formato a seguir:

```
aws cloudtrail list-public-keys [--start-time <start-time>] [--end-time <end-time>]
```

Os parâmetros de horário de início e de término são carimbos de data e hora UTC opcionais. Se eles não forem especificados, a hora atual será usada, e a chave ou as chaves públicas atualmente ativas serão retornadas.

Exemplo de resposta

A resposta será uma lista de objetos JSON que representam a chave ou as chaves retornadas:

Use a CloudTrail API para recuperar chaves públicas

Para recuperar uma chave pública para um arquivo de assinatura usando a CloudTrail API, transmita os valores de hora de início e hora de término para a `ListPublicKeys` API. A API `ListPublicKeys` retorna as chaves públicas cujas chaves privadas foram usadas para assinar o arquivo dentro do período especificado. Para cada chave pública, a API também retorna a impressão digital correspondente.

`ListPublicKeys`

Esta seção descreve os parâmetros de solicitação e os elementos de resposta da API `ListPublicKeys`.

> **Note**
>
> A codificação dos campos binários de `ListPublicKeys` está sujeita a alterações.

Parâmetros de solicitação

Nome	Descrição
`StartTime`	Opcionalmente, especifica, em UTC, o início do intervalo de tempo para pesquisar a chave pública para o arquivo de assinatura. CloudTrail Se não StartTime for especificado, a hora atual será usada e a chave pública atual será retornada. Tipo: DateTime
`EndTime`	Opcionalmente, especifica, em UTC, o final do intervalo de tempo para pesquisar chaves públicas para arquivos de assinatura. CloudTrail Se não EndTime for especificado, a hora atual será usada. Tipo: DateTime

Elementos de resposta

`PublicKeyList`, um conjunto de `PublicKey` objetos que contém:

Name (Nome)	Descrição
`Value`	O valor de chave pública codificado DER no formato PKCS #1. Tipo: Blob
`ValidityStartTime`	O horário de início da validade da chave pública. Tipo: DateTime
`ValidityEndTime`	O horário de término da validade da chave pública. Tipo: DateTime
`Fingerprint`	A impressão digital da chave pública. A impressão digital pode ser usada para identificar a chave pública que você precisa usar para validar o arquivo de assinatura. Tipo: string

C. Escolha a chave pública a ser usada para a validação

Entre as chaves públicas recuperadas por `list-public-keys` ou `ListPublicKeys`, escolha a chave pública cuja impressão digital corresponde à impressão digital gravada no campo `publicKeyFingerprint` do arquivo de assinatura. Essa é a chave pública que você usará para validar o arquivo de assinatura.

D. Recrie a string de assinatura de dados

Agora que você tem a assinatura do arquivo de assinatura e a chave pública associada, precisa calcular a string de assinatura de dados. Depois que você calcular a string de assinatura de dados, terá o necessário para verificar a assinatura.

A string de assinatura de dados consiste no valor de hash para cada arquivo de resultado de consulta separado por um espaço. Depois que você recriar essa string, poderá validar o arquivo de assinatura.

E. Validar o arquivo de assinatura

Transmita a string de assinatura de dados recriada, a assinatura digital e a chave pública ao algoritmo de verificação de assinatura RSA. Se o resultado for verdadeiro, a assinatura do arquivo de assinatura será verificada, e o arquivo de assinatura será válido.

F. Validar os arquivos de resultados de consulta

Depois que você validar o arquivo de assinatura, poderá validar os arquivos de resultado de consulta aos quais ele faz referência. O arquivo de assinatura contém os hashes SHA-256 dos arquivos de resultado de consulta. Se um dos arquivos de resultados da consulta for modificado após a CloudTrail entrega, os hashes SHA-256 serão alterados e a assinatura do arquivo de assinatura não corresponderá.

Siga o procedimento abaixo para validar os arquivos de resultados de consulta listados na matriz `files` do arquivo de assinatura.

1. Recupere o hash original do arquivo no campo `files.fileHashValue` do arquivo de assinatura.
2. Faça o hash do conteúdo compactado do arquivo de resultado de consulta com o algoritmo de hashing especificado em `hashAlgorithm`.
3. Compare o valor de hash que você gerou para cada arquivo de resultado de consulta com o `files.fileHashValue` do arquivo de assinatura. Se os hashes forem correspondentes, os arquivos de resultado de consulta serão válidos.

Validação offline de arquivos de resultado de consulta e assinatura

Ao validar offline os arquivos de resultado de consulta e assinatura, você pode seguir os procedimentos descritos nas seções anteriores. No entanto, você deve levar em consideração as seguintes informações sobre chaves públicas.

Chaves públicas

Para fazer a validação offline, primeiramente é necessário obter online (p. ex., chamando `ListPublicKeys`) a chave pública de que você precisa para validar os arquivos de resultado de consulta em um determinado intervalo de tempo e, depois, armazená-la offline. Essa etapa precisará ser repetida sempre que você quiser validar arquivos adicionais fora do período inicial que especificou.

Exemplo de snippet de validação

O trecho de amostra a seguir fornece um código básico para validar arquivos de resultados de CloudTrail assinatura e consulta. O código esqueleto pode ser online ou offline, ou seja, você decide se o implementará com ou sem conectividade online na AWS. A implementação sugerida usa Java Cryptography Extension (JCE) e Bouncy Castle como um provedor de segurança.

O exemplo de snippet mostra:

- Como criar a string de assinatura de dados usada para validar a assinatura do arquivo de assinatura.
- Como verificar a assinatura do arquivo de assinatura.
- Como calcular o valor de hash para o arquivo de resultado de consulta e compará-lo com o `fileHashValue` listado no arquivo de assinatura para verificar a autenticidade do arquivo de resultado de consulta.

```
import org.apache.commons.codec.binary.Hex;
import org.bouncycastle.asn1.pkcs.PKCSObjectIdentifiers;
import org.bouncycastle.asn1.pkcs.RSAPublicKey;
import org.bouncycastle.asn1.x509.AlgorithmIdentifier;
import org.bouncycastle.asn1.x509.SubjectPublicKeyInfo;
import org.bouncycastle.jce.provider.BouncyCastleProvider;
import org.json.JSONArray;
import org.json.JSONObject;

import java.security.KeyFactory;
```

```
import java.security.MessageDigest;
import java.security.PublicKey;
import java.security.Security;
import java.security.Signature;
import java.security.spec.X509EncodedKeySpec;
import java.util.ArrayList;
import java.util.Arrays;
import java.util.List;
import java.util.stream.Collectors;


public class SignFileValidationSampleCode {

    public void validateSignFile(String s3Bucket, String s3PrefixPath) throws Exception
 {
        MessageDigest messageDigest = MessageDigest.getInstance("SHA-256");

        // Load the sign file from S3 (using Amazon S3 Client) or from your local copy
        JSONObject signFile = loadSignFileToMemory(s3Bucket, String.format("%s/%s",
 s3PrefixPath, "result_sign.json"));

        // Using the Bouncy Castle provider as a JCE security provider - http://
www.bouncycastle.org/
        Security.addProvider(new BouncyCastleProvider());

        List<String> hashList = new ArrayList<>();

        JSONArray jsonArray = signFile.getJSONArray("files");

        for (int i = 0; i < jsonArray.length(); i++) {
            JSONObject file = jsonArray.getJSONObject(i);
            String fileS3ObjectKey = String.format("%s/%s", s3PrefixPath,
 file.getString("fileName"));

            // Load the export file from S3 (using Amazon S3 Client) or from your local
 copy
            byte[] exportFileContent = loadCompressedExportFileInMemory(s3Bucket,
 fileS3ObjectKey);
            messageDigest.update(exportFileContent);
            byte[] exportFileHash = messageDigest.digest();
            messageDigest.reset();
            byte[] expectedHash = Hex.decodeHex(file.getString("fileHashValue"));

            boolean signaturesMatch = Arrays.equals(expectedHash, exportFileHash);
```

```
            if (!signaturesMatch) {
                System.err.println(String.format("Export file: %s/%s hash doesn't
match.\tExpected: %s Actual: %s",
                        s3Bucket, fileS3ObjectKey,
                        Hex.encodeHexString(expectedHash),
Hex.encodeHexString(exportFileHash)));
            } else {
                System.out.println(String.format("Export file: %s/%s hash match",
                        s3Bucket, fileS3ObjectKey));
            }

            hashList.add(file.getString("fileHashValue"));
        }
        String hashListString = hashList.stream().collect(Collectors.joining(" "));

        /*
            NOTE:
            To find the right public key to verify the signature, call CloudTrail
ListPublicKey API to get a list
            of public keys, then match by the publicKeyFingerprint in the sign file.
Also, the public key bytes
            returned from ListPublicKey API are DER encoded in PKCS#1 format:

            PublicKeyInfo ::= SEQUENCE {
                algorithm       AlgorithmIdentifier,
                PublicKey       BIT STRING
            }

            AlgorithmIdentifier ::= SEQUENCE {
                algorithm       OBJECT IDENTIFIER,
                parameters      ANY DEFINED BY algorithm OPTIONAL
            }
        */
        byte[] pkcs1PublicKeyBytes =
getPublicKey(signFile.getString("queryCompleteTime"),
                signFile.getString("publicKeyFingerprint"));
        byte[] signatureContent = Hex.decodeHex(signFile.getString("hashSignature"));

        // Transform the PKCS#1 formatted public key to x.509 format.
        RSAPublicKey rsaPublicKey = RSAPublicKey.getInstance(pkcs1PublicKeyBytes);
        AlgorithmIdentifier rsaEncryption = new
AlgorithmIdentifier(PKCSObjectIdentifiers.rsaEncryption, null);
        SubjectPublicKeyInfo publicKeyInfo = new SubjectPublicKeyInfo(rsaEncryption,
rsaPublicKey);
```

```
        // Create the PublicKey object needed for the signature validation
        PublicKey publicKey = KeyFactory.getInstance("RSA", "BC")
                .generatePublic(new X509EncodedKeySpec(publicKeyInfo.getEncoded()));

        // Verify signature
        Signature signature = Signature.getInstance("SHA256withRSA", "BC");
        signature.initVerify(publicKey);
        signature.update(hashListString.getBytes("UTF-8"));

        if (signature.verify(signatureContent)) {
            System.out.println("Sign file signature is valid.");
        } else {
            System.err.println("Sign file signature failed validation.");
        }

        System.out.println("Sign file validation completed.");
    }
}
```

Execute e gerencie consultas do CloudTrail Lake com o AWS CLI

Você pode usar o AWS CLI para executar e gerenciar suas consultas CloudTrail do Lake. Ao usar o AWS CLI, lembre-se de que seus comandos são Região da AWS executados no configurado para seu perfil. Se você deseja executar os comandos em uma região diferente, altere a região padrão para o seu perfil ou use o parâmetro --region com o comando.

Comandos disponíveis para consultas CloudTrail do Lake

Os comandos para executar e gerenciar consultas no CloudTrail Lake incluem:

- `start-query`para executar uma consulta.
- `describe-query`para retornar metadados sobre uma consulta.
- `get-query-results`para retornar os resultados da consulta para o ID de consulta especificado.
- `list-queries`para obter uma lista de consultas para o armazenamento de dados de eventos especificado.
- `cancel-query`para cancelar uma consulta em execução.

Para obter uma lista dos comandos disponíveis para armazenamentos de dados de eventos do CloudTrail Lake, consulteComandos disponíveis para armazenamentos de dados de eventos.

Para obter uma lista dos comandos disponíveis para integrações com o CloudTrail Lake, consulteComandos disponíveis para integrações com o CloudTrail Lake.

Inicie uma consulta com o AWS CLI

O AWS CLI start-query comando de exemplo a seguir executa uma consulta no armazenamento de dados de eventos especificado como um ID na instrução de consulta e entrega os resultados da consulta a um bucket do S3 especificado. O parâmetro `--query-statement` fornece uma consulta de SQL entre aspas simples. Os parâmetros opcionais incluem `--delivery-s3uri`, para entregar os resultados de consulta a um bucket especificado do S3. Para obter mais informações sobre a linguagem de consulta que você pode usar no CloudTrail Lake, consulteCloudTrail Restrições do Lake SQL.

```
aws cloudtrail start-query
--query-statement 'SELECT eventID, eventTime FROM EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
 LIMIT 10'
--delivery-s3uri "s3://aws-cloudtrail-lake-query-results-123456789012-us-east-1"
```

A resposta é uma string de `QueryId`. Para obter o status de uma consulta, execute describe-query usando o valor `QueryId` retornado por start-query. Se a consulta tiver êxito, você poderá executar get-query-results para obter os resultados.

Saída

```
{
    "QueryId": "EXAMPLE2-0add-4207-8135-2d8a4EXAMPLE"
}
```

> **Note**
>
> Consultas que são executadas por mais de uma hora podem expirar. No entanto, ainda é possível obter resultados parciais que foram processados antes do tempo limite da consulta esgotar.
>
> Se você estiver entregando os resultados da consulta para um bucket do S3 usando o `--delivery-s3uri` parâmetro opcional, a política do bucket deverá conceder CloudTrail permissão para entregar os resultados da consulta ao bucket. Para obter informações sobre como editar manualmente a política de bucket, consulte Política de bucket do Amazon S3 para resultados de consulta CloudTrail do Lake.

Obtenha metadados sobre uma consulta com o AWS CLI

O AWS CLI describe-query comando de exemplo a seguir obtém metadados sobre uma consulta, incluindo tempo de execução da consulta em milissegundos, número de eventos verificados e correspondidos, número total de bytes verificados e status da consulta. O valor `BytesScanned` corresponde ao número de bytes pelos quais sua conta é cobrada pela consulta, a menos que a consulta ainda esteja em execução. Se os resultados da consulta foram entregues em um bucket do S3, a resposta também fornecerá o URI do S3 e o status da entrega.

Você pode especificar um valor para o parâmetro `--query-id` ou `--query-alias`. A especificação do parâmetro `--query-alias` retorna informações sobre a última consulta executada para o alias.

```
aws cloudtrail describe-query --query-id EXAMPLEd-17a7-47c3-a9a1-eccf7EXAMPLE
```

A seguir, uma exemplo de resposta.

```
{
    "QueryId": "EXAMPLE2-0add-4207-8135-2d8a4EXAMPLE",
    "QueryString": "SELECT eventID, eventTime FROM EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
 LIMIT 10",
    "QueryStatus": "RUNNING",
    "QueryStatistics": {
        "EventsMatched": 10,
        "EventsScanned": 1000,
        "BytesScanned": 35059,
        "ExecutionTimeInMillis": 3821,
        "CreationTime": "1598911142"
    }
}
```

Obtenha os resultados da consulta com o AWS CLI

O comando da AWS CLI get-query-results do exemplo a seguir obtém resultados de dados de eventos de uma consulta. Você deve especificar o `--query-id` retornado pelo comando start-query. O valor `BytesScanned` corresponde ao número de bytes pelos quais sua conta é cobrada pela consulta, a menos que a consulta ainda esteja em execução. Parâmetros opcionais incluem `--max-query-results` para especificar um número máximo de resultados que você deseja que o comando retorne em uma única página. Se houver mais resultados do que o valor especificado

para `--max-query-results`, execute o comando novamente adicionando o valor retornado `NextToken` para obter a próxima página de resultados.

```
aws cloudtrail get-query-results
--query-id EXAMPLEd-17a7-47c3-a9a1-eccf7EXAMPLE
```

Saída

```
{
    "QueryStatus": "RUNNING",
    "QueryStatistics": {
        "ResultsCount": 244,
        "TotalResultsCount": 1582,
        "BytesScanned":27044
    },
    "QueryResults": [
      {
        "key": "eventName",
        "value": "StartQuery",
      }
   ],
    "QueryId": "EXAMPLE2-0add-4207-8135-2d8a4EXAMPLE",
    "QueryString": "SELECT eventID, eventTime FROM EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
 LIMIT 10",
    "NextToken": "20add42078135EXAMPLE"
}
```

Liste todas as consultas em um armazenamento de dados de eventos com a AWS CLI

O comando da AWS CLI list-queries do exemplo a seguir retorna uma lista de consultas e status de consulta em um armazenamento de dados de eventos especificado nos últimos sete dias. Você deve especificar um ARN ou o sufixo de ID de um valor de ARN para `--event-data-store`. Opcionalmente, para encurtar a lista de resultados, você pode especificar um intervalo de tempo, formatado como carimbos de data/hora, adicionando os parâmetros `--start-time` e `--end-time` e um valor `--query-status`. Os valores válidos para `QueryStatus` incluem `QUEUED`, `RUNNING`, `FINISHED`, `FAILED` ou `CANCELLED`.

list-queries também tem parâmetros de paginação opcionais. Use `--max-results` para especificar um número máximo de resultados que você deseja que o comando retorne em uma única página. Se houver mais resultados do que o valor especificado para `--max-results`, execute o comando novamente adicionando o valor retornado `NextToken` para obter a próxima página de resultados.

```
aws cloudtrail list-queries
--event-data-store EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
--query-status CANCELLED
--start-time 1598384589
--end-time 1598384602
--max-results 10
```

Saída

```
{
    "Queries": [
        {
          "QueryId": "EXAMPLE2-0add-4207-8135-2d8a4EXAMPLE",
          "QueryStatus": "CANCELLED",
          "CreationTime": 1598911142
        },
        {
          "QueryId": "EXAMPLE2-4e89-9230-2127-5dr3aEXAMPLE",
          "QueryStatus": "CANCELLED",
          "CreationTime": 1598296624
        }
     ],
    "NextToken": "20add42078135EXAMPLE"
}
```

Cancelar uma consulta em execução com o AWS CLI

O AWS CLI cancel-query comando de exemplo a seguir cancela uma consulta com um status de`RUNNING`. Especifique um valor para `--query-id`. Quando você executa cancel-query, o status da consulta pode ser exibido como `CANCELLED` mesmo que a operação cancel-query ainda não esteja concluída.

> **Note**
>
> Uma consulta cancelada pode incorrer em cobranças. Sua conta ainda é cobrada pela quantidade de dados que foram examinados antes de você cancelar a consulta.

Veja a seguir um exemplo da CLI.

```
aws cloudtrail cancel-query
```

```
--query-id EXAMPLEd-17a7-47c3-a9a1-eccf7EXAMPLE
```

Saída

```
QueryId -> (string)
QueryStatus -> (string)
```

CloudTrail Restrições do Lake SQL

CloudTrail As consultas Lake são cadeias de caracteres SQL. Esta seção fornece informações sobre funções, operadores e esquemas compatíveis.

Somente instruções `SELECT` são permitidas. Nenhuma string de consulta pode alterar ou modificar dados.

CloudTrail O Lake oferece suporte a todas as `SELECT` instruções, funções e operadores válidos do Presto SQL. Para obter mais informações sobre as funções e os operadores SQL compatíveis, consulte Funções e operadores no site de documentação do Presto.

O CloudTrail console fornece vários exemplos de consultas que podem ajudar você a começar a escrever suas próprias consultas. Para ter mais informações, consulte Veja exemplos de consultas no console CloudTrail .

Tópicos

- Funções, condições e operadores de junção compatíveis
- Compatibilidade avançada para consultas com várias tabelas

Funções, condições e operadores de junção compatíveis

Funções compatíveis

CloudTrail O Lake suporta todas as funções do Presto. Para obter mais informações sobre as funções compatíveis, consulte Funções e operadores no site de documentação do Presto.

CloudTrail Lake não suporta a `INTERVAL` palavra-chave.

Operadores de condição compatíveis

Os operadores de condição a seguir são compatíveis.

```
AND
OR
IN
NOT
IS (NOT) NULL
LIKE
BETWEEN
GREATEST
LEAST
IS DISTINCT FROM
IS NOT DISTINCT FROM
<
>
<=
>=
<>
!=
( conditions ) #parenthesised conditions
```

Operadores de junção compatíveis

Os operadores `JOIN` a seguir são compatíveis. Para obter mais informações sobre a execução de consultas em várias tabelas, veja Compatibilidade avançada para consultas com várias tabelas.

```
UNION
UNION ALL
EXCEPT
INTERSECT
LEFT JOIN
RIGHT JOIN
INNER JOIN
```

Compatibilidade avançada para consultas com várias tabelas

CloudTrail O Lake suporta linguagem de consulta avançada em vários armazenamentos de dados de eventos.

- `UNION|UNION ALL|EXCEPT|INTERSECT`
- `LEFT|RIGHT|INNER JOIN`

Para executar sua consulta, use o comando start-query na AWS CLI. Veja a seguir um exemplo que usa uma das amostras de consultas nesta seção.

```
aws cloudtrail start-query
--query-statement "Select eventId, eventName from EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE
 UNION Select eventId, eventName from EXAMPLEg741-6y1x-9p3v-bnh6iEXAMPLE UNION ALL
 Select eventId, eventName from EXAMPLEb529-4e8f9l3d-6m2z-lkp5sEXAMPLE ORDER BY eventId
 LIMIT 10;"
```

A resposta é uma string de `QueryId`. Para obter o status de uma consulta, execute `describe-query` usando o valor `QueryId` retornado por `start-query`. Se a consulta tiver êxito, você poderá executar `get-query-results` para obter os resultados.

UNION|UNION ALL|EXCEPT|INTERSECT

Veja a seguir um exemplo de consulta que usa `UNION` e `UNION ALL` para localizar eventos por ID e nome do evento em três armazenamentos de dados de eventos, EDS1, EDS2 e EDS3. Os resultados são selecionados primeiramente de cada armazenamento de dados de eventos e, em seguida, os resultados são concatenados, ordenados por ID do evento e limitados a dez eventos.

```
Select eventId, eventName from EDS1
UNION
Select eventId, eventName from EDS2
UNION ALL
Select eventId, eventName from EDS3
ORDER BY eventId LIMIT 10;
```

LEFT|RIGHT|INNER JOIN

Veja a seguir um exemplo de consulta que usa `LEFT JOIN` para encontrar todos os eventos de um armazenamento de dados de eventos chamado `eds2`, mapeado para `edsB`, que correspondam aos eventos de um armazenamento primário (à esquerda) de dados de eventos, `edsA`. Os eventos retornados ocorrem até 1.º de janeiro de 2020 e somente os nomes dos eventos são retornados.

```
SELECT edsA.eventName, edsB.eventName, element_at(edsA.map, 'test')
FROM eds1 as edsA
LEFT JOIN eds2 as edsB
ON edsA.eventId = edsB.eventId
WHERE edsA.eventtime <= '2020-01-01'
ORDER BY edsB.eventName;
```

Esquemas SQL compatíveis para armazenamentos de dados de eventos

As seções a seguir fornecem o esquema SQL compatível para cada tipo de armazenamento de dados de eventos.

Tópicos

Esquema compatível para campos de registro de CloudTrail eventos

A seguir está o esquema SQL válido para campos de registro de eventos de dados e CloudTrail gerenciamento. Para obter mais informações sobre campos de registro de CloudTrail eventos, consulteCloudTrail conteúdo do registro.

```
[
    {
        "Name": "eventversion",
        "Type": "string"
    },
    {
        "Name": "useridentity",
        "Type":
 "struct<type:string,principalid:string,arn:string,accountid:string,accesskeyid:string,

 username:string,sessioncontext:struct<attributes:struct<creationdate:timestamp,

 mfaauthenticated:string>,sessionissuer:struct<type:string,principalid:string,arn:string,

 accountid:string,username:string>,webidfederationdata:struct<federatedprovider:string,

 attributes:map<string,string>>,sourceidentity:string,ec2roledelivery:string,
                ec2issuedinvpc:string>,invokedby:string,identityprovider:string>"
    },
```

```
    {
        "Name": "eventtime",
        "Type": "timestamp"
    },
    {
        "Name": "eventsource",
        "Type": "string"
    },
    {
        "Name": "eventname",
        "Type": "string"
    },
    {
        "Name": "awsregion",
        "Type": "string"
    },
    {
        "Name": "sourceipaddress",
        "Type": "string"
    },
    {
        "Name": "useragent",
        "Type": "string"
    },
    {
        "Name": "errorcode",
        "Type": "string"
    },
    {
        "Name": "errormessage",
        "Type": "string"
    },
    {
        "Name": "requestparameters",
        "Type": "map<string,string>"
    },
    {
        "Name": "responseelements",
        "Type": "map<string,string>"
    },
    {
        "Name": "additionaleventdata",
        "Type": "map<string,string>"
    },
```

```
    {
        "Name": "requestid",
        "Type": "string"
    },
    {
        "Name": "eventid",
        "Type": "string"
    },
    {
        "Name": "readonly",
        "Type": "boolean"
    },
    {
        "Name": "resources",
        "Type":
 "array<struct<accountid:string,type:string,arn:string,arnprefix:string>>"
    },
    {
        "Name": "eventtype",
        "Type": "string"
    },
    {
        "Name": "apiversion",
        "Type": "string"
    },
    {
        "Name": "managementevent",
        "Type": "boolean"
    },
    {
        "Name": "recipientaccountid",
        "Type": "string"
    },
    {
        "Name": "sharedeventid",
        "Type": "string"
    },
    {
        "Name": "annotation",
        "Type": "string"
    },
    {
        "Name": "vpcendpointid",
        "Type": "string"
```

```
    },
    {
        "Name": "serviceeventdetails",
        "Type": "map<string,string>"
    },
    {
        "Name": "addendum",
        "Type": "map<string,string>"
    },
    {
        "Name": "edgedevicedetails",
        "Type": "map<string,string>"
    },
    {
        "Name": "insightdetails",
        "Type": "map<string,string>"
    },
    {
        "Name": "eventcategory",
        "Type": "string"
    },
    {
        "Name": "tlsdetails",
        "Type":
 "struct<tlsversion:string,ciphersuite:string,clientprovidedhostheader:string>"
    },
    {
        "Name": "sessioncredentialfromconsole",
        "Type": "string"
    },
    {
        "Name": "eventjson",
        "Type": "string"
    }
    {
        "Name": "eventjsonchecksum",
        "Type": "string"
    }
]
```

Esquema compatível para campos de registro de eventos do CloudTrail Insights

Veja a seguir o esquema de SQL válido para campos de registro de eventos do Insights.
Para eventos do Insights o valor de `eventcategory` é `Insight`, e o valor de `eventtype` é `AwsCloudTrailInsight`.

```
[
    {
        "Name": "eventversion",
        "Type": "string"
    },
    {
        "Name": "eventcategory",
        "Type": "string"
    },
    {
        "Name": "eventtype",
        "Type": "string"
    },
        "Name": "eventid",
        "Type": "string"
    },
    {
        "Name": "eventtime",
        "Type": "timestamp"
    },
    {
        "Name": "awsregion",
        "Type": "string"
    },
    {
        "Name": "recipientaccountid",
        "Type": "string"
    },
    {
        "Name": "sharedeventid",
        "Type": "string"
    },
    {
        "Name": "addendum",
        "Type": "map<string,string>"
```

```
    },
    {
        "Name": "insightsource",
        "Type": "string"
    },
    {
        "Name": "insightstate",
        "Type": "string"
    },
    {
        "Name": "insighteventsource",
        "Type": "string"
    },
    {
        "Name": "insighteventname",
        "Type": "string"
    },
    {
        "Name": "insighterrorcode",
        "Type": "string"
    },
    {
        "Name": "insighttype",
        "Type": "string"
    },
    {
        "Name": "insightContext",
        "Type":
 "struct<baselineaverage:double,insightaverage:double,baselineduration:integer,

 insightduration:integer,attributions:struct<attribute:string,insightvalue:string,
                insightaverage:double,baselinevalue:string,baselineaverage:double>>"
    }
]
```

Esquema compatível para campos de registro de itens de configuração do AWS Config

Veja a seguir o esquema válido de SQL para campos de registro de item de configuração. Para itens de configuração, o valor de `eventcategory` é `ConfigurationItem` e o valor de `eventtype` é `AwsConfigurationItem`.

```
[
    {
        "Name": "eventversion",
        "Type": "string"
    },
    {
        "Name": "eventcategory",
        "Type": "string"
    },
    {
        "Name": "eventtype",
        "Type": "string"
    },
        "Name": "eventid",
        "Type": "string"
    },
    {
        "Name": "eventtime",
        "Type": "timestamp"
    },
    {
        "Name": "awsregion",
        "Type": "string"
    },
    {
        "Name": "recipientaccountid",
        "Type": "string"
    },
    {
        "Name": "addendum",
        "Type": "map<string,string>"
    },
    {
        "Name": "eventdata",
        "Type": "struct<configurationitemversion:string,configurationitemcapturetime:

 string,configurationitemstatus:string,configurationitemstateid:string,accountid:string,

 resourcetype:string,resourceid:string,resourcename:string,arn:string,awsregion:string,

 availabilityzone:string,resourcecreationtime:string,configuration:map<string,string>,
                supplementaryconfiguration:map<string,string>,relatedevents:string,
```

```
 relationships:struct<name:string,resourcetype:string,resourceid:string,
                 resourcename:string>,tags:map<string,string>>"
    }
]
```

Esquema suportado para campos de registro de AWS Audit Manager evidências

Veja a seguir o esquema de SQL válido para campos de registro de evidência do Audit Manager. Para campos de registro de evidências do Audit Manager, o valor de `eventcategory` é `Evidence` e o valor de `eventtype` é `AwsAuditManagerEvidence`. Para obter mais informações sobre como agregar evidências no CloudTrail Lake usando o Audit Manager, consulte Localizador de evidências no Guia do AWS Audit Manager Usuário.

```
[
    {
        "Name": "eventversion",
        "Type": "string"
    },
    {
        "Name": "eventcategory",
        "Type": "string"
    },
    {
        "Name": "eventtype",
        "Type": "string"
    },
        "Name": "eventid",
        "Type": "string"
    },
    {
        "Name": "eventtime",
        "Type": "timestamp"
    },
    {
        "Name": "awsregion",
        "Type": "string"
    },
    {
        "Name": "recipientaccountid",
        "Type": "string"
```

```
    },
    {
        "Name": "addendum",
        "Type": "map<string,string>"
    },
    {
        "Name": "eventdata",
        "Type":
 "struct<attributes:map<string,string>,awsaccountid:string,awsorganization:string,

 compliancecheck:string,datasource:string,eventname:string,eventsource:string,

 evidenceawsaccountid:string,evidencebytype:string,iamid:string,evidenceid:string,

 time:timestamp,assessmentid:string,controlsetid:string,controlid:string,

 controlname:string,controldomainname:string,frameworkname:string,frameworkid:string,

 service:string,servicecategory:string,resourcearn:string,resourcetype:string,

 evidencefolderid:string,description:string,manualevidences3resourcepath:string,
                evidencefoldername:string,resourcecompliancecheck:string>"
    }
]
```

Esquema suportado para campos que não sejam de AWS eventos

A seguir está o esquema SQL válido para AWS não-eventos. Para AWS não-eventos, o valor de `eventcategory` é `ActivityAuditLog` e o valor de `eventtype` é`ActivityLog`.

```
[
    {
        "Name": "eventversion",
        "Type": "string"
    },
    {
        "Name": "eventcategory",
        "Type": "string"
    },
    {
        "Name": "eventtype",
        "Type": "string"
    },
```

```
        "Name": "eventid",
        "Type": "string"
    },
    {
        "Name": "eventtime",
        "Type": "timestamp"
    },
    {
        "Name": "awsregion",
        "Type": "string"
    },
    {
        "Name": "recipientaccountid",
        "Type": "string"
    },
    {
        "Name": "addendum",
        "Type":
 "struct<reason:string,updatedfields:string,originalUID:string,originaleventid:string>"
    },
    {
        "Name": "metadata",
        "Type": "struct<ingestiontime:string,channelarn:string>"
    },
    {
        "Name": "eventdata",
        "Type": "struct<version:string,useridentity:struct<type:string,

 principalid:string,details:map<string,string>>,useragent:string,eventsource:string,

 eventname:string,eventtime:string,uid:string,requestparameters:map<string,string>>,

 responseelements":map<string,string>>,errorcode:string,errormssage:string,sourceipaddress:stri
                recipientaccountid:string,additionaleventdata":map<string,string>>"
    }
]
```

Controle de permissões de usuário para o CloudTrail Lake

AWS CloudTrail se integra ao AWS Identity and Access Management (IAM) para ajudar você a controlar o acesso ao CloudTrail Lake e a outros AWS recursos CloudTrail necessários. Você pode usar o IAM para controlar quais AWS usuários podem criar, configurar ou excluir bancos de dados de

CloudTrail eventos ou canais, iniciar e interromper a ingestão de eventos e copiar eventos de trilha. Para saber mais, consulte Identity and Access Management para AWS CloudTrail.

Os tópicos a seguir ajudam você a entender as permissões, as políticas e a CloudTrail segurança:

- Concedendo permissões para administração CloudTrail
- Política de bucket do Amazon S3 para resultados de consulta CloudTrail do Lake
- Permissões necessárias para copiar eventos da trilha
- Permissões necessárias para federação
- Um exemplo de política que restringe o acesso a um armazenamento de dados de eventos com base em tags: Exemplos: negação de acesso para criar ou excluir armazenamentos de dados de eventos com base em tags
- AWS CloudTrail exemplos de políticas baseadas em recursos
- Permissões necessárias para atribuir um administrador delegado
- Política de chaves KMS padrão para armazenamentos de dados de eventos em CloudTrail Lake

Gerenciando os custos CloudTrail do Lake

AWS CloudTrail Os armazenamentos e consultas de dados de eventos em Lake incorrem em cobranças. Como prática recomendada, recomendamos o uso Serviços da AWS de ferramentas que possam ajudá-lo a gerenciar CloudTrail custos. Também é possível configurar armazenamentos de dados de eventos de formas que capturam os dados necessários e, ao mesmo tempo, permanecem econômicas. Para obter mais informações sobre a definição de preço do CloudTrail , consulte Definição de preço do AWS CloudTrail.

Tópicos

- Opções de preços do armazenamento de dados de eventos
- Entendendo as taxas CloudTrail do Lake
- Recomendações sobre como você pode reduzir custos
- Ferramentas para ajudar a gerenciar os custos
- Consulte também

Opções de preços do armazenamento de dados de eventos

Ao criar um armazenamento de dados de eventos, você escolhe a opção de preço que deseja usar para ele. A opção de preço determina o custo para a ingestão e para o armazenamento de eventos, e os períodos de retenção padrão e máximo para o armazenamento de dados de eventos.

A tabela a seguir descreve as opções de preços disponíveis. A tabela mostra a opção de preços no console e o valor do `BillingMode` correspondente para a API, além de listar o período de retenção padrão e máximo para cada opção.

Opção de preço (console)	BillingMode (API)	Descrição
Preço de retenção extensível de um ano	`EXTENDABLE_RETENTION_PRICING`	Recomendado se você espera ingerir menos de 25 TB de dados de eventos por mês e deseja um período de retenção flexível de até 10 anos. Essa opção também é recomendada se o armazenamento de dados de eventos coletar itens de configuração do AWS Config , evidências do Audit Manager e eventos de fora da AWS. Nos primeiros 366 dias (o período de retenção padrão), o armazenamento é incluído sem custo adicional no preço de ingestão. Depois de 366 dias, a retenção estendida está disponível pelo pay-as-you-go preço. Esta é a opção padrão. Período de retenção padrão: 366 dias Período máximo de retenção: 3.653 dias
Preços de retenção de sete anos	`FIXED_RETENTION_PRICING`	Recomendado se você espera ingerir mais de 25 TB de dados de eventos por mês e precisa de um período de retenção de até 7 anos.

Opção de preço (console)	BillingMode (API)	Descrição
		A retenção está incluída no preço de ingestão sem custo adicional. Período de retenção padrão: 2.557 dias Período máximo de retenção: 2.557 dias

Entendendo as taxas CloudTrail do Lake

As tabelas a seguir fornecem informações sobre como os armazenamentos e consultas de dados de eventos do CloudTrail Lake geram cobranças. Para obter mais informações sobre a definição de preço do CloudTrail , consulte Definição de preço do AWS CloudTrail.

Tipo de despesa	Como você incorre em cobranças
Ingestão de dados (dados não compactados)	Para o CloudTrail Lake, você paga com base nos dados não compactados ingeridos. A opção de preço do armazenamento de dados de eventos determina o custo da ingestão de eventos: • Preço de retenção extensível de um ano: oferece preços de ingestão com base no tipo de evento. • Preço de retenção de sete anos: oferece preços de ingestão com base no volume de dados ingeridos. A maior economia é obtida quando o volume de dados ingeridos mensalmente ultrapassa 25 TB. Copiar eventos de trilhas Quando você copia eventos de trilha para o CloudTrail Lake, CloudTrail descompacta os registros armazenados no formato gzip (compactado). Em seguida, CloudTrail copia os eventos contidos nos registros para seu armazenamento de dados de eventos. O tamanho dos dados não compactados pode ser

Tipo de despesa	Como você incorre em cobranças
	maior do que o tamanho real do armazenamento do Amazon S3. Para obter uma estimativa geral do tamanho dos dados não compactados, multiplique o tamanho dos registros no bucket do S3 por 10. **Note** CloudTrail não copiará um evento se o horário do evento for anterior ao período de retenção especific ado. Para determinar o período de retenção adequado, calcule a soma do evento mais antigo que você deseja copiar em dias e o número de dias em que deseja reter os eventos no armazenamento de dados de eventos, conforme demonstrado nesta equação: Período de retenção = *oldest-event-in-days* + *number-days-to-retain* Por exemplo, se o evento mais antigo que você está copiando tiver 45 dias e você quiser manter os eventos no armazenamento de dados de eventos por mais 45 dias, defina o período de retenção como 90 dias.

Tipo de despesa	Como você incorre em cobranças
Retenção de dados (dados otimizados e compactados)	CloudTrail O Lake converte eventos existentes no formato JSON baseado em linhas para o formato Apache ORC. O ORC é um formato colunar de armazenamento otimizado para recuperação rápida de dados compactados. O período de retenção de um armazenamento de dados de eventos determina por quanto tempo os dados de eventos são mantidos no armazenamento de dados de eventos. CloudTrai l Lake determina se um evento deve ser retido verificando se o horário do evento está dentro do período de retenção especific ado. Por exemplo, se você especificar um período de retenção de 90 dias, CloudTrail removerá eventos quando o horário do evento for superior a 90 dias. Para armazenamentos de dados de eventos que usam a opção de preço de retenção de sete anos, o armazenamento está incluído no preço de ingestão sem custo adicional. Para armazenamentos de dados de eventos que usam a opção de preço de retenção extensível de um ano, o armazenamento é incluído gratuitamente no preço de ingestão dos primeiros 366 dias (o período de retenção padrão). Após 366 dias, o armazenamento é oferecido pay-as-you-pricing e cobrado com base nos dados otimizados e compactados no armazenamento de dados do evento.
Executando consultas no CloudTrail Lake (dados otimizados e compactados)	Ao executar consultas no CloudTrail Lake, você paga com base na quantidade de dados otimizados e compactados digitaliz ados.

Recomendações sobre como você pode reduzir custos

Esta seção fornece recomendações sobre como você pode reduzir custos ao trabalhar com o CloudTrail Lake.

Escolha uma opção de preço com base no tipo de eventos que seu armazenamento de dados de eventos coletará e na ingestão mensal esperada

Ao criar um armazenamento de dados de eventos, escolha uma opção de preço com base no tipo de eventos que seu armazenamento de dados de eventos coletará e na ingestão mensal esperada.

Se você espera ingerir menos de 25 TB de dados de eventos por mês e deseja um período de retenção flexível de até 10 anos, escolha a opção de preço de retenção extensível de um ano. Geralmente, também recomendamos essa opção para armazenamentos de dados de eventos que coletam itens de AWS Config configuração, evidências do Audit Manager e eventos externos AWS.

Se você espera ingerir mais de 25 TB de dados de eventos mensalmente e precisa de um período de retenção de 7 anos, escolha a opção de preço de retenção de sete anos.

Avalie a ingestão mensal do seu armazenamento de dados de eventos ao longo do tempo

Avalie o histórico de ingestão mensal do seu armazenamento de dados de eventos para ver se há uma opção de preço mais adequada às suas necessidades.

Se você tem um armazenamento de dados de eventos existente que usa a opção de preço de retenção de sete anos e ingere menos de 25 TB de dados mensalmente, considere atualizar o armazenamento de dados de eventos para usar o preço de retenção extensível de um ano. Para armazenamentos de dados de eventos usando a opção de preço de retenção de sete anos, você pode alterar a opção de preço usando o CloudTrail console ou UpdateEventDataStorea operação da AWS CLIAPI.

Se você tem um armazenamento de dados de eventos existente que usa a opção de preço de retenção extensível de um ano e ingere mais de 25 TB de dados de eventos mensalmente, considere se o preço de retenção de sete anos seria mais adequado às suas necessidades. Para usar a nova opção de preço, interrompa a ingestão em seu armazenamento de dados de eventos e crie um novo armazenamento de dados de eventos com a opção de preço de retenção de sete anos.

Use seletores de eventos avançados para filtrar eventos que não são de interesse

Ao configurar um armazenamento de dados de eventos para CloudTrail gerenciamento ou eventos de dados, filtre os eventos que não são de interesse usando seletores de eventos avançados.

Se você estiver criando um armazenamento de dados de eventos para coletar eventos de gerenciamento, poderá filtrar AWS Key Management Service (AWS KMS) ou os eventos da API de dados do Amazon Relational Database Service (Amazon RDS). Normalmente, AWS KMS ações como `EncryptDecrypt`, e `GenerateDataKey` geram mais de 99% dos eventos.

Se você estiver criando um armazenamento de dados de eventos para coletar eventos de dados, poderá usar seletores de eventos avançados para filtrar os campos `eventName`, `resources.type`, `resources.ARN` e `readOnly`. Para ver um exemplo, consulte Exemplo: criar um armazenamento de dados de eventos para eventos de dados do S3.

Escolha um intervalo de tempo mais curto ao copiar eventos de trilha

Ao copiar eventos de trilha para o CloudTrail Lake, especifique um horário de início e um horário de término mais estreitos para reduzir a quantidade de dados ingeridos.

Se você estiver copiando eventos de trilha para o CloudTrail Lake para análise histórica e não quiser ingerir eventos futuros, desmarque a opção de ingerir eventos para não incorrer em cobranças pela ingestão de eventos adicionais.

Formatar consultas para usar um **`eventTime`** inicial e final

Ao executar consultas no Lake, você paga de acordo com a quantidade de dados examinados. Você pode restringir os custos especificando um `eventTime` inicial e final para a consulta.

Ferramentas para ajudar a gerenciar os custos

AWS Os orçamentos, um recurso do AWS Billing and Cost Management, permitem que você defina orçamentos personalizados que alertam você quando seus custos ou uso excedem (ou se prevê que excedam) o valor orçado.

Ao criar armazenamentos de dados de eventos, criar um AWS orçamento CloudTrail usando Orçamentos é uma prática recomendada e pode ajudá-lo a controlar seus CloudTrail gastos. Orçamentos baseados em custos ajudam a promover a conscientização de quanto você pode ser cobrado por seu uso. CloudTrail alertas de orçamento notificam você quando sua fatura atinge um limite definido por você. Quando receber um alerta de orçamento, você poderá fazer alterações antes do fim do ciclo de faturamento para gerenciar seus custos.

Depois de criar um orçamento, você pode usá-lo AWS Cost Explorer para ver como seus CloudTrail custos estão influenciando sua AWS fatura geral. No AWS Cost Explorer, depois de adicionar

CloudTrail ao filtro Serviço, você pode comparar seus CloudTrail gastos históricos com os gastos atuais month-to-date (MTD), por região e conta. Esse recurso ajuda você a monitorar e detectar custos inesperados em seus CloudTrail gastos mensais. Os recursos adicionais do Cost Explorer permitem comparar os CloudTrail gastos com os gastos mensais no nível de recurso específico, fornecendo informações sobre o que pode estar gerando aumentos ou reduções de custos em sua fatura.

Para começar a usar AWS Orçamentos AWS Billing and Cost Management, abra e escolha Orçamentos na barra de navegação à esquerda. Recomendamos configurar alertas de orçamento ao criar um orçamento para monitorar os CloudTrail gastos. Para obter mais informações sobre como usar AWS orçamentos, consulte Gerenciando seus custos com orçamentos AWS Budgets e melhores práticas para AWS orçamentos.

Criação de etiquetas de alocação de custos definidas pelo usuário para armazenamentos de dados de eventos do CloudTrail Lake

Você pode criar tags de alocação de custos definidas pelo usuário para rastrear os custos de consulta e ingestão dos seus armazenamentos de dados de eventos do CloudTrail Lake. Uma tag de alocação de custos definida pelo usuário é um par chave-valor que pode ser associado a um armazenamento de dados de eventos. Depois de ativar as tags de alocação de custos, AWS use as tags para organizar seus custos de recursos em seu relatório de alocação de custos.

- Para criar tags no console, consulte a etapa 9 do procedimento Para criar um armazenamento de dados de eventos para CloudTrail gerenciamento ou eventos de dados.
- Para criar tags usando a CloudTrail API, consulte CreateEventDataStoree AddTagsna Referência da AWS CloudTrail API.
- Para criar tags usando o AWS CLI, consulte create-event-data-storee adicione tags na Referência de AWS CLI Comandos.

Para obter mais informações sobre a ativação de tags, consulte Ativar tags de alocação de custos definidas pelo usuário.

Consulte também

- Definição de preço do AWS CloudTrail
- CloudWatch Métricas suportadas
- Gerenciando seus custos com AWS Budgets

- Conceitos básicos do Explorador de Custos

CloudWatch Métricas suportadas

CloudTrail O Lake oferece suporte às CloudWatch métricas da Amazon. CloudWatch é um serviço de monitoramento de AWS recursos. Você pode usar CloudWatch para coletar e monitorar métricas, definir alarmes e reagir automaticamente às mudanças em seus AWS recursos.

O `AWS/CloudTrail` namespace inclui as seguintes métricas para CloudTrail o Lake.

Métrica	Descrição	Unidades
`HourlyDataIngested`	A quantidade de dados ingeridos no armazenamento de dados de eventos durante a última hora. Esta métrica é atualizada a cada hora. Esta métrica está disponíve l para todos os tipos de armazenamento de dados de eventos.	Bytes
`TotalDataRetained`	A quantidade de dados retidos no armazenamento de dados de eventos durante todo o período de retenção. Esta métrica é atualizada todas as noites. Esta métrica está disponíve l para todos os tipos de armazenamento de dados de eventos.	Bytes
`TotalStorageBytes`	O total de bytes compactados no armazenamento de dados de eventos no dia atual.	Bytes

Métrica	Descrição	Unidades
	Esta métrica está disponíve l para todos os tipos de armazenamento de dados de eventos.	

Métrica	Descrição	Unidades
`TotalPaidStorageBytes`	Para armazenamentos de dados de eventos que usam a opção de preço de retenção extensível de um ano, esse é o total de bytes compactados após 366 dias até o período máximo de retenção configurado para o armazenamento de dados de eventos. Para armazenamentos de dados de eventos que usam a opção de preço de retenção extensível de um ano, o armazenamento é incluído sem custo adicional com preços de ingestão para os primeiros 366 dias, que é o período de retenção padrão para o armazenamento de dados de eventos. Após 366 dias, o armazenamento é pay-as-you-go. Para obter mais informações sobre definição de preços, consulte Definição de preço do AWS CloudTrail. Essa métrica está disponível somente para armazenamentos de dados de eventos que usam a opção de preço de retenção extensível de um ano.	Bytes

Métrica	Descrição	Unidades
`HourlyEventsAnalyzed`	O número total de eventos analisados pelo CloudTrail Insights no armazenamento de dados de eventos. Esta métrica é atualizada a cada hora. Essa métrica é para armazenamentos de dados de CloudTrail eventos que habilitam o CloudTrail Insights.	Contagem

Para obter mais informações sobre CloudWatch métricas, consulte os tópicos a seguir.

- Usando CloudWatch métricas da Amazon
- Usando CloudWatch alarmes da Amazon

Trabalhando com CloudTrail trilhas

As trilhas capturam um registro das AWS atividades, entregando e armazenando esses eventos em um bucket do Amazon S3, com entrega opcional para a CloudWatch Logs e a Amazon. EventBridge

Você pode entregar uma cópia dos seus eventos de gerenciamento contínuos para o bucket do S3 sem nenhum custo CloudTrail criando uma trilha. No entanto, há cobranças de armazenamento do Amazon S3. Para obter mais informações sobre CloudTrail preços, consulte AWS CloudTrail Preços. Para receber informações sobre a definição de preço do Amazon S3, consulte Definição de preço do Amazon S3.

Você pode criar dois tipos de trilhas para uma Conta da AWS: trilhas multirregionais e trilhas de região única.

Trilhas multirregionais

Quando você cria uma trilha multirregional, CloudTrail registra todos os eventos Regiões da AWS na AWS partição em que você está trabalhando e entrega os arquivos de log de CloudTrail eventos em um bucket do S3 que você especificar. Se uma Região da AWS for adicionada após a criação de uma trilha multirregional, essa nova região será incluída automaticamente e os eventos dessa região serão registrados. Criar uma trilha de várias regiões é uma prática recomendada, pois você captura atividades em todas as regiões da conta. Todas as trilhas que você cria usando o CloudTrail console são multirregionais. Você pode converter uma trilha de região única em uma trilha de várias regiões usando o. AWS CLI Para obter mais informações, consulte Criar uma trilha no console e Converter uma trilha que se aplica a uma região para que ela se aplique a todas as regiões.

Trilhas de uma única região

Ao criar uma trilha de região única, CloudTrail registra os eventos somente nessa região. Em seguida, ele entrega os arquivos de log de CloudTrail eventos para um bucket do Amazon S3 que você especificar. Só é possível criar uma trilha de região única usando a AWS CLI. Se você criar trilhas únicas adicionais, poderá fazer com que essas trilhas entreguem arquivos de log de CloudTrail eventos para o mesmo bucket do S3 ou para buckets separados. Essa é a opção padrão quando você cria uma trilha usando a AWS CLI ou a CloudTrail API. Para ter mais informações, consulte Criando, atualizando e gerenciando trilhas com o AWS CLI.

> **Note**
>
> Para os dois tipos de trilhas, é possível especificar um bucket do Amazon S3 de qualquer região.

Se você criou uma organização em AWS Organizations, você pode criar uma trilha da organização que registra todos os eventos de todas as AWS contas dessa organização. As trilhas da organização podem ser aplicadas a todas as AWS regiões ou à região atual. As trilhas da organização devem ser criadas com a conta de gerenciamento ou conta de administrador delegado e, quando especificadas como aplicáveis a uma organização, são aplicadas automaticamente a todas as contas-membro da respectiva organização. As contas dos membros podem ver a trilha da organização, mas não podem modificá-la ou excluí-la. Por padrão, as contas de membro não têm acesso aos arquivos de log de uma trilha da organização no bucket do Amazon S3. Para ter mais informações, consulte Criar uma trilha para uma organização.

Tópicos

Criando uma trilha para o seu Conta da AWS

Ao criar uma trilha, você habilita o fornecimento contínuo de eventos como arquivos de log para um bucket do Amazon S3 especificado. Há muitos benefícios na criação de uma trilha, incluindo:

- Um registro de eventos que abrange mais de 90 dias.

- A opção de monitorar e alertar automaticamente sobre eventos específicos enviando eventos de log para o Amazon CloudWatch Logs.
- A opção de consultar registros e analisar a atividade do AWS serviço com o Amazon Athena.

A partir de 12 de abril de 2019, você pode ver as trilhas somente nas AWS regiões em que elas registram eventos. Se você criar uma trilha que registre eventos em todas as AWS regiões, ela aparecerá no console em todas as regiões da AWS partição em que você está trabalhando. Se você criar uma trilha que registra eventos em log apenas em uma única região da , poderá visualizá-la e gerenciá-la apenas nessa região da . Criar uma trilha multirregional é a opção padrão se você criar uma trilha usando o AWS CloudTrail console, e é uma prática recomendada. Para criar uma trilha de região única, é necessário usar a AWS CLI.

Se você usar AWS Organizations, você pode criar uma trilha que registrará eventos para todas as AWS contas na organização. Uma trilha com o mesmo nome será criada em cada conta-membro, e eventos de cada trilha serão fornecidos ao bucket do Amazon S3 que você especificar.

> **Note**
>
> Somente a conta de gerenciamento ou conta de administrador delegado de uma organização pode criar uma trilha para a organização. Criar uma trilha para uma organização permite automaticamente a integração entre CloudTrail e Organizations. Para ter mais informações, consulte Criar uma trilha para uma organização.

Tópicos

Criar e atualizar uma trilha com o console

Você pode usar o CloudTrail console para criar, atualizar ou excluir suas trilhas. As trilhas criadas usando o console são de várias regiões. Para criar uma trilha que registre eventos em apenas uma Região da AWS, use AWS CLI o.

É possível criar até cinco trilhas para cada região. Depois de criar uma trilha, começa CloudTrail automaticamente a registrar chamadas de API e eventos relacionados em sua conta no bucket do

Amazon S3 que você especificar. Para interromper o registro, você pode desativá-lo para a trilha ou excluí-lo.

Usar o CloudTrail console para criar ou atualizar uma trilha oferece as seguintes vantagens.

- Se for a primeira vez que você cria uma trilha, o uso do CloudTrail console permite que você visualize os recursos e as opções disponíveis.
- Se você estiver configurando uma trilha para registrar eventos de dados, o uso do CloudTrail console permite visualizar os tipos de dados disponíveis. Para obter mais informações sobre log de eventos de dados, consulte Eventos de dados de log.

Para obter informações específicas sobre a criação de uma trilha para uma organização em AWS Organizations, consulteCriar uma trilha para uma organização.

Tópicos

- Criar uma trilha
- Atualizar uma trilha
- Excluir uma trilha
- Desativar o registro de uma trilha

Criar uma trilha

Como prática recomendada, crie uma trilha aplicável a todas as Regiões da AWS. Essa é a configuração padrão quando você cria uma trilha no CloudTrail console. Quando uma trilha se aplica a todas as regiões, CloudTrail entrega arquivos de log de todas as regiões na AWS partição em que você está trabalhando para um bucket do S3 especificado por você. Depois de criar a trilha, começa AWS CloudTrail automaticamente a registrar os eventos que você especificou.

> **Note**
>
> Depois de criar uma trilha, você pode configurar outra Serviços da AWS para analisar e agir com base nos dados do evento coletados nos CloudTrail registros. Para ter mais informações, consulte AWS integrações de serviços com registros CloudTrail .

Tópicos

Criar uma trilha no console

Use o procedimento a seguir para criar uma trilha que registre todos os eventos Regiões da AWS na AWS partição em que você está trabalhando. Essa é uma prática recomendada. Para registrar eventos em uma única região (não recomendado), use a AWS CLI.

Para criar uma CloudTrail trilha com o AWS Management Console

1. Faça login no AWS Management Console e abra o CloudTrail console em https://console.aws.amazon.com/cloudtrail/.
2. Na página inicial do CloudTrail serviço, na página Trilhas ou na seção Trilhas da página Painel, escolha Criar trilha.
3. Na página Create Trail (Criar trilha), em Trail name (Nome da trilha), digite um nome para a sua trilha. Para ter mais informações, consulte Requisitos de nomenclatura.
4. Se essa for uma trilha AWS Organizations da organização, você poderá habilitá-la para todas as contas da sua organização. Para ver essa opção, será necessário fazer login no console com um usuário ou perfil na conta de gerenciamento ou de administrador delegado. Para criar uma trilha da organização, verifique se o usuário ou a função tem permissões suficientes. Para ter mais informações, consulte Criar uma trilha para uma organização.
5. Em Storage location (Local de armazenamento), escolha Create a S3 bucket (Criar um bucket do S3) para criar um bucket. Quando você cria um bucket, CloudTrail cria e aplica as políticas de bucket necessárias. Se você optar por criar um novo bucket do S3, sua política do IAM precisará incluir permissão para a `s3:PutEncryptionConfiguration` ação porque, por padrão, a criptografia do lado do servidor está habilitada para o bucket.

> **Note**
>
> Se você escolheu Usar bucket do S3 existente, especifique um bucket em Nome do bucket de log da trilha, ou escolha Procurar para escolher um bucket em sua própria conta. Para usar um bucket em outra conta, é necessário especificar o nome do bucket. A política do bucket deve conceder CloudTrail permissão para gravar nela. Para obter informações sobre como editar manualmente a política de bucket, consulte Política de bucket do Amazon S3 para CloudTrail.

Para facilitar a localização de seus registros, crie uma nova pasta (também conhecida como prefixo) em um bucket existente para armazenar seus CloudTrail registros. Insira o prefixo em Prefix (Prefixo).

6. Em Log file SSE-KMS encryption (Criptografia de arquivo de log com SSE-KMS), escolha Enabled (Habilitado) se quiser criptografar os arquivos de log com criptografia SSE-KMS em vez de criptografia SSE-S3. O padrão é Enabled (Habilitado). Se você não habilitar a criptografia SSE-SKMS, seus registros serão criptografados usando a criptografia SSE-S3. Para obter mais informações sobre a criptografia SSE-KMS, consulte Usando a criptografia do lado do servidor com (SSE-KMS). AWS Key Management Service Para obter mais informações sobre a criptografia SSE-S3, consulte Using Server-Side Encryption with Amazon S3-Managed Encryption Keys (SSE-S3) (Uso de criptografia no lado do servidor com chaves de criptografia gerenciadas pelo Amazon S3 [SSE-S3]).

   Se você habilitar a criptografia SSE-KMS, escolha Nova ou Existente. AWS KMS key Em AWS KMS Alias, especifique um alias, no formato. `alias/ MyAliasName` Para ter mais informações, consulte Atualizar um recurso para usar sua chave do KMS. CloudTrail também oferece suporte a chaves AWS KMS multirregionais. Para obter mais informações sobre chaves de várias regiões, consulte Usar chaves de várias regiões no Manual do desenvolvedor do AWS Key Management Service .

   > **Note**
   >
   > Você também pode digitar o Nome de região da Amazon (ARN) de uma chave de outra conta. Para ter mais informações, consulte Atualizar um recurso para usar sua chave do KMS. A política de chaves deve permitir CloudTrail o uso da chave para criptografar seus arquivos de log e permitir que os usuários que você especificar leiam os arquivos de log em formato não criptografado. Para obter informações sobre como editar manualmente a política de chaves, consulte Configure as AWS KMS principais políticas para CloudTrail.

7. Em Additional settings (Configurações adicionais), configure as opções a seguir.

   a. Em Log file validation (Validação de arquivo de log), escolha Enabled (Habilitado) para receber resumos de log no seu bucket do S3. Você pode usar os arquivos de resumo para verificar se seus arquivos de log não foram alterados após CloudTrail serem entregues. Para ter mais informações, consulte Validando a integridade CloudTrail do arquivo de log.

b. Para entrega de notificações do SNS, escolha Ativado para ser notificado sempre que um registro for entregue ao seu bucket. CloudTrail armazena vários eventos em um arquivo de log. As notificações do SNS são enviadas para todos os arquivos de log, não para todos os eventos. Para ter mais informações, consulte Configurando notificações do Amazon SNS para CloudTrail.

   Se você habilitar notificações do SNS, para Create a new SNS topic (Criar um tópico do SNS), escolha New (Novo) para criar um tópico ou escolha Existing (Existente) para usar um tópico existente. Se criar uma trilha aplicável a todas as regiões, as notificações do SNS sobre a entrega de arquivos de log de todas as regiões serão enviadas ao único tópico do SNS que você criar.

   Se você escolher Novo, CloudTrail especifica um nome para o novo tópico para você ou pode digitar um nome. Se escolher Existing (Existente), escolha um tópico do SNS na lista suspensa. Você também pode inserir o Nome de região da Amazon (ARN) de um tópico de outra região ou de uma conta com permissões apropriadas. Para ter mais informações, consulte Política de tópicos do Amazon SNS para CloudTrail.

   Se você criar um tópico, precisará se inscrever nele para ser notificado sobre a entrega de arquivos de log. Você pode se inscrever no console do Amazon SNS. Devido à frequência das notificações, recomendamos que você configure a inscrição para usar uma fila do Amazon SQS para gerenciar as notificações de modo programático. Para obter mais informações, consulte Conceitos básicos do Amazon SNS no Guia do desenvolvedor do Amazon Simple Notification Service.

8. Opcionalmente, configure CloudTrail para enviar arquivos de log para o CloudWatch Logs escolhendo Habilitado em CloudWatch Registros. Para ter mais informações, consulte Envio de eventos para o CloudWatch Logs.

   a. Se você habilitar a integração com CloudWatch Logs, escolha Novo para criar um novo grupo de registros ou Existente para usar um existente. Se você escolher Novo, CloudTrail especifica um nome para o novo grupo de registros para você ou pode digitar um nome.

   b. Se escolher Existing (Existente), escolha um grupo de logs na lista suspensa.

   c. Escolha Novo para criar uma nova função do IAM para obter permissões para enviar registros para o CloudWatch Logs. Escolha Existing (Existente) para escolher uma função do IAM existente na lista suspensa. A declaração de política para a função nova ou existente é exibida quando você expande Policy document (Documento de política). Para

obter mais informações sobre essa função, consulte Documento de política de funções CloudTrail para usar CloudWatch registros para monitoramento.

> **Note**
>
> - Quando você configurar uma trilha, você pode escolher um bucket do S3 e um tópico do SNS que pertençam a outra conta. No entanto, se você quiser CloudTrail entregar eventos a um grupo de CloudWatch registros de registros, deverá escolher um grupo de registros que exista na sua conta atual.
> - Somente a conta de gerenciamento pode configurar um grupo de CloudWatch registros de registros para uma trilha da organização usando o console. O administrador delegado pode configurar um grupo de CloudWatch registros de registros usando as operações AWS CLI ou CloudTrail `CreateTrail` ou `UpdateTrail` da API.

9. Para Tags, adicione uma ou mais tags personalizadas (pares chave-valor) à sua trilha. As tags podem ajudá-lo a identificar suas CloudTrail trilhas e os buckets do Amazon S3 que contêm CloudTrail arquivos de log. Em seguida, você pode usar grupos de recursos para seus CloudTrail recursos. Para obter mais informações, consulte AWS Resource Groups e Tags.
10. Na página Choose log events (Escolher eventos de log), escolha os tipos de eventos que você deseja registrar. Em Management events (Eventos de gerenciamento), faça o indicado a seguir.

    a. Em API activity (Atividade da API), escolha se você deseja que sua trilha registre eventos Read (Leitura), Write (Gravação) ou ambos. Para ter mais informações, consulte Eventos de gerenciamento.

    b. Escolha Excluir AWS KMS eventos para filtrar AWS Key Management Service (AWS KMS) eventos da sua trilha. A configuração padrão é incluir todos os AWS KMS eventos.

    A opção de registrar ou excluir AWS KMS eventos está disponível somente se você registrar eventos de gerenciamento em sua trilha. Se você optar por não registrar eventos de gerenciamento, os AWS KMS eventos não serão registrados e você não poderá alterar as configurações do registro de AWS KMS eventos.

    AWS KMS ações como`Encrypt`,`Decrypt`, e `GenerateDataKey` normalmente geram um grande volume (mais de 99%) de eventos. Agora essas ações são registradas em log como eventos de Leitura. AWS KMS Ações relevantes de baixo volume, como **`DisableDelete`**,

e **`ScheduleKey`** (que normalmente representam menos de 0,5% do volume de AWS KMS eventos) são registradas como eventos de gravação.

Para excluir eventos de alto volume`Encrypt`, como`Decrypt`, e`GenerateDataKey`, mas ainda registrar eventos relevantes`Disable`, como `Delete` e`ScheduleKey`, escolha registrar eventos de gerenciamento de gravação e desmarque a caixa de seleção Excluir AWS KMS eventos.

c. Escolha Exclude Amazon RDS Data API events (Excluir eventos da API de dados do Amazon RDS) para filtrar eventos da API de dados do Amazon Relational Database Service fora da trilha. A configuração padrão é incluir todos os eventos da API de dados do Amazon RDS. Para obter mais informações sobre eventos da API de dados do Amazon RDS, consulte Registrar em log chamadas da API de dados com o AWS CloudTrail no Manual do usuário do Amazon RDS for Aurora.

11. Para registrar eventos de dados, escolha Data events (Eventos de dados). Há cobranças adicionais para o registro de eventos de dados. Para obter mais informações, consulte Preços do AWS CloudTrail.

12. **Important**

    As etapas 12 a 16 devem ser usadas para configurar eventos de dados usando seletores de eventos avançados, que é o padrão. Os seletores de eventos avançados permitem que você configure mais tipos de eventos de dados e oferecem um controle mais preciso sobre quais eventos de dados são capturados por sua trilha. Se você optou por usar seletores de eventos básicos, conclua as etapas em Configurar opções de eventos de dados utilizando seletores de eventos básicos e retorne à etapa 17 desse procedimento.

    Em Data event type (Tipo de evento de dados), escolha o tipo de recurso no qual você deseja registrar eventos de dados. Para obter mais informações sobre os tipos de eventos de dados disponíveis, consulte Eventos de dados.

    Note

    Para registrar eventos de dados para AWS Glue tabelas criadas pelo Lake Formation, escolha Lake Formation.

13. Escolha um modelo de seletor de registros. CloudTrail inclui modelos predefinidos que registram todos os eventos de dados do tipo de recurso. Para criar um modelo de seletor de log personalizado, escolha Custom (Personalizado).

> **Note**
>
> A escolha de um modelo predefinido para buckets do S3 permite o registro de eventos de dados de todos os buckets atualmente em sua AWS conta e de todos os buckets que você criar depois de concluir a criação da trilha. Ele também permite o registro da atividade de eventos de dados realizada por qualquer identidade do IAM em sua AWS conta, mesmo que essa atividade seja realizada em um bucket que pertença a outra AWS conta.
>
> Se a trilha se aplicar somente a uma região, a escolha da opção Select all S3 buckets in your account (Selecionar todos os buckets do S3 em sua conta) habilitará o registro de eventos de dados para todos os buckets do S3 na mesma região que a trilha e todos os buckets que você criar posteriormente nessa região. Ele não registrará eventos de dados para buckets do Amazon S3 em outras regiões da sua conta. AWS
>
> Se você estiver criando uma trilha para todas as regiões, a escolha de um modelo predefinido para as funções do Lambda permite o registro de eventos de dados para todas as funções atualmente em AWS sua conta e para quaisquer funções do Lambda que você possa criar em qualquer região depois de terminar de criar a trilha. Se você estiver criando uma trilha para uma única região (feita usando o AWS CLI), essa seleção habilita o registro de eventos de dados para todas as funções atualmente nessa região em sua AWS conta e quaisquer funções Lambda que você possa criar nessa região depois de terminar de criar a trilha. Essa opção não permite o registro de eventos de dados para funções do Lambda criadas em outras regiões.
>
> O registro de eventos de dados para todas as funções também permite o registro da atividade de eventos de dados realizada por qualquer identidade do IAM em sua AWS conta, mesmo que essa atividade seja realizada em uma função que pertence a outra AWS conta.

14. (Opcional) Em Nome do seletor, insira um nome para identificar o seletor. O nome do seletor é um nome descritivo para um seletor de eventos avançado, como "Registrar eventos de dados em log para apenas dois buckets do S3". O nome do seletor é listado como `Name` no seletor de eventos avançado e poderá ser visualizado se você expandir a visualização JSON.

15. Em Advanced event selectors (Seletores de eventos avançados), crie uma expressão para os recursos específicos nos quais você deseja registrar eventos de dados. Você poderá ignorar esta etapa se estiver usando um modelo de log predefinido.

    a. Escolha um dos seguintes campos:

    - **`readOnly`**- `readOnly` pode ser definido como igual a um valor de `true` ou. `false` Eventos de dados somente leitura são eventos que não alteram o estado de um recurso, como `Get*` ou `Describe*`. Eventos de gravação adicionam, alteram ou excluem recursos, atributos ou artefatos, como `Put*`, `Delete*` ou `Write*`. Para registrar os eventos `read` e `write`, não adicione um seletor `readOnly`.
    - **`eventName`** - `eventName` pode usar qualquer operador. Você pode usá-lo para incluir ou excluir qualquer evento de dados registrado CloudTrail, como `PutBucketPutItem`, ou`GetSnapshotBlock`.
    - **`resources.ARN`**- Você pode usar qualquer operador com`resources.ARN`, mas se usar igual ou diferente, o valor deverá corresponder exatamente ao ARN de um recurso válido do tipo que você especificou no modelo como valor de. `resources.type`

      A tabela a seguir mostra o formato de ARN válido para cada `resources.type`.

      > **Note**
      >
      > Você não pode usar o `resources.ARN` campo para filtrar tipos de recursos que não tenham ARNs.

resources.type	resources.ARN
`AWS::DynamoDB::Table` [1]	`arn:partition :dynamodb : region:account_ID :table/table_name`
`AWS::Lambda::Function`	`arn:partition :lambda:region:account_ID :function: function_name`

resources.type	resources.ARN
AWS::S3::Object [2]	arn:*partition* :s3:::*bucket_name* / arn:*partition* :s3:::*bucket_name* /*object_or_file_name* /
AWS::AppConfig::Configuration	arn:*partition* :appconfig: *region*:*account_ID* :application/ *application_ID* /environment/ *environment_ID* /configuration/ *configuration_profile_ID*
AWS::B2BI::Transformer	arn:*partition* :b2bi:*region*:*account_ID* :transformer/ *transformer_ID*
AWS::Bedrock::AgentAlias	arn:*partition* :bedrock: *region*:*account_ID* :agent-alias/ *agent_ID*/*alias_ID*
AWS::Bedrock::KnowledgeBase	arn:*partition* :bedrock: *region*:*account_ID* :knowledge-base/*knowledge_base_ID*
AWS::Cassandra::Table	arn:*partition* :cassandra: *region*:*account_ID* :keyspace/ *keyspace_name* /table/*table_name*
AWS::CloudFront::KeyValueStore	arn:*partition* :cloudfront: *region*:*account_ID* :key-value-store/*KVS_name*
AWS::CloudTrail::Channel	arn:*partition* :cloudtrail: *region*:*account_ID* :channel/ *channel_UUID*

resources.type	resources.ARN
AWS::CodeWhisperer::Customization	arn:*partition* :codewhisperer: *region*:*account_ID* :customization/ *customization_ID*
AWS::CodeWhisperer::Profile	arn:*partition* :codewhisperer: *region*:*account_ID* :profile/ *profile_ID*
AWS::Cognito::IdentityPool	arn:*partition* :cognito-identity: *region*:*account_ID* :identitypool/ *identity_pool_ID*
AWS::DynamoDB::Stream	arn:*partition* :dynamodb: *region*:*account_ID* :table/*table_name* /stream/*date_time*
AWS::EC2::Snapshot	arn:*partition* :ec2:*region*::snapshot/ *snapshot_ID*
AWS::EMRWAL::Workspace	arn:*partition* :emrwal:*region*:*account_ID* :workspace/ *workspace_name*
AWS::FinSpace::Environment	arn:*partition* :finspace: *region*:*account_ID* :environment/ *environment_ID*
AWS::Glue::Table	arn:*partition* :glue:*region*:*account_ID* :table/*database_name* /*table_name*
AWS::GreengrassV2::ComponentVersion	arn:*partition* :greengrass: *region*:*account_ID* :components/ *component_name*

resources.type	resources.ARN
AWS::GreengrassV2::Deployment	arn:*partition* :greengra ss: *region*:*account_ID* :deployme nts/ *deployment_ID*
AWS::GuardDuty::Detector	arn:*partition* :guarddut y: *region*:*account_ID* :detector / *detector_ID*
AWS::IoT::Certificate	arn:*partition* :iot:*region*:*account_I D* :cert/*certificate_ID*
AWS::IoT::Thing	arn:*partition* :iot:*region*:*account_I D* :thing/*thing_ID*
AWS::IoTSiteWise::Asset	arn:*partition* :iotsitew ise: *region*:*account_ID* :asset/*asset_ID*
AWS::IoTSiteWise::TimeSeries	arn:*partition* :iotsitew ise: *region*:*account_ID* :timeseri es/ *timeseries_ID*
AWS::IoTTwinMaker::Entity	arn:*partition* :iottwinm aker: *region*:*account_ID* :workspac e/ *workspace_ID* /entity/*entity_ID*
AWS::IoTTwinMaker::Workspace	arn:*partition* :iottwinm aker: *region*:*account_ID* :workspac e/ *workspace_ID*

resources.type	resources.ARN
AWS::KendraRanking::ExecutionPlan	arn:*partition* :kendra-ranking: *region*:*account_ID* :rescore-execution-plan/ *rescore_execution_plan_ID*
AWS::Kinesis::Stream	arn:*partition* :kinesis: *region*:*account_ID* :stream/*stream_name*
AWS::Kinesis::StreamConsumer	arn:*partition* :kinesis: *region*:*account_ID* :*stream_type* /*stream_name* /consumer/ *consumer_name* :*consumer_creation_timestamp*
AWS::KinesisVideo::Stream	arn:*partition* :kinesisvideo: *region*:*account_ID* :stream/*stream_name* /*creation_time*
AWS::ManagedBlockchain::Network	arn:*partition* :managedblockchain :::networks/ *network_name*
AWS::ManagedBlockchain::Node	arn:*partition* :managedblockchain : *region*:*account_ID* :nodes/*node_ID*
AWS::MedicalImaging::Datastore	arn:*partition* :medical-imaging: *region*:*account_ID* :datastore/ *data_store_ID*
AWS::NeptuneGraph::Graph	arn:*partition* :neptune-graph: *region*:*account_ID* :graph/*graph_ID*

resources.type	resources.ARN
AWS::PCAConnectorAD::Connector	arn:*partition* :pca-connector-ad: *region*:*account_ID* :connector/ *connector_ID*
AWS::QApps:QApp	arn:*partition* :qapps:*region*:*account_ID* :application/ *application_UUID* / qapp/*qapp_UUID*
AWS::QBusiness::Application	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID*
AWS::QBusiness::DataSource	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID* /index/*index_ID*/ data-source/ *datasource_ID*
AWS::QBusiness::Index	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID* /index/*index_ID*
AWS::QBusiness::WebExperience	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID* /web-experience/ *web_experienc_ID*
AWS::RDS::DBCluster	arn:*partition* :rds:*region*:*account_ID* :cluster/ *cluster_name*
AWS::S3::AccessPoint [3]	arn:*partition* :s3:*region*:*account_ID* :accesspoint/ *access_point_name*

resources.type	resources.ARN
AWS::S3ObjectLambda::AccessPoint	arn:*partition* :s3-object-lambda: *region*:*account_ID* :accesspoint/ *access_point_name*
AWS::S3Outposts::Object	arn:*partition* :s3-outposts: *region*:*account_ID* :*object_path*
AWS::SageMaker::Endpoint	arn:*partition* :sagemaker: *region*:*account_ID* :endpoint/ *endpoint_name*
AWS::SageMaker::ExperimentTrialComponent	arn:*partition* :sagemaker: *region*:*account_ID* :experiment-trial-component/ *experiment_trial_component_name*
AWS::SageMaker::FeatureGroup	arn:*partition* :sagemaker: *region*:*account_ID* :feature-group/ *feature_group_name*
AWS::SCN::Instance	arn:*partition* :scn:*region*:*account_ID* :instance/ *instance_ID*
AWS::ServiceDiscovery::Namespace	arn:*partition* :servicediscovery: *region*:*account_ID* :namespace/ *namespace_ID*
AWS::ServiceDiscovery::Service	arn:*partition* :servicediscovery: *region*:*account_ID* :service/ *service_ID*

resources.type	resources.ARN
AWS::SNS::PlatformEndpoint	arn:*partition* :sns:*region*:*account_ID* :endpoint/ *endpoint_type* /*endpoint_name* /*endpoint_ID*
AWS::SNS::Topic	arn:*partition* :sns:*region*:*account_ID* :*topic_name*
AWS::SQS::Queue	arn:*partition* :sqs:*region*:*account_ID* :*queue_name*
AWS::SSM::ManagedNode	O ARN deve estar em um dos seguintes formatos: • arn:*partition* :ssm:*region*:*account_ID* :managed-instance/ *instance_ID* • arn:*partition* :ec2:*region*:*account_ID* :instance/ *instance_ID*
AWS::SSMMessages::ControlChannel	arn:*partition* :ssmmessages: *region*:*account_ID* :control-channel/ *control_channel_ID*
AWS::StepFunctions::StateMachine	O ARN deve estar em um dos seguintes formatos: • arn:*partition* :states:*region*:*account_ID* :stateMachine: *stateMachine_name* • arn:*partition* :states:*region*:*account_ID* :stateMachine: *stateMachine_name* /*label_name*

resources.type	resources.ARN
AWS::SWF::Domain	arn:*partition* :swf:*region*:*account_ID* :/domain/ *domain_name*
AWS::ThinClient::Device	arn:*partition* :thinclient: *region*:*account_ID* :device/*device_ID*
AWS::ThinClient::Environment	arn:*partition* :thinclient: *region*:*account_ID* :environment/ *environment_ID*
AWS::Timestream::Database	arn:*partition* :timestream: *region*:*account_ID* :database/ *database_name*
AWS::Timestream::Table	arn:*partition* :timestream: *region*:*account_ID* :database/ *database_name* /table/*table_name*
AWS::VerifiedPermissions::PolicyStore	arn:*partition* :verifiedpermissions: *region*:*account_ID* :policy-store/ *policy_store_ID*

[1] Para tabelas com fluxos habilitados, o campo `resources` no evento de dados contém `AWS::DynamoDB::Stream` e `AWS::DynamoDB::Table`. Se você especificar `AWS::DynamoDB::Table` como `resources.type`, ele registrará os eventos da tabela do DynamoDB e dos fluxos do DynamoDB por padrão. Para excluir eventos de streams, adicione um filtro no `eventName` campo.

[2] Para registrar em log todos os eventos de dados de todos os objetos em um bucket do S3 específico, use o operador `StartsWith` e inclua apenas o ARN do bucket como o valor correspondente. A barra final é intencional; não a exclua.

[3] Para registrar em log eventos de todos os objetos em um ponto de acesso do S3, recomendamos usar somente o ARN do ponto de acesso, não incluir o caminho do objeto e usar os operadores `StartsWith` ou `NotStartsWith`.

Para obter mais informações sobre os formatos do ARN de recursos de evento de dados, consulte Ações, recursos e chaves de condição no Guia do usuário do AWS Identity and Access Management .

b. Para cada campo, escolha + Condição para adicionar quantas condições forem necessárias até o máximo de 500 valores especificados para todas as condições. Por exemplo, para excluir eventos de dados de dois buckets do S3 dos eventos de dados registrados em sua trilha, você pode definir o campo como Resources.arn, definir o operador para does not start with e, em seguida, colar o ARN de um bucket do S3 ou procurar os buckets do S3 nos quais você não deseja registrar eventos.

   Para adicionar o segundo bucket do S3, escolha + Condição e, em seguida, repita a instrução anterior, colando o ARN ou procurando um bucket diferente.

   > **Note**
   >
   > É possível ter, no máximo, 500 valores para todos os seletores em uma trilha. Isso inclui matrizes de vários valores para um seletor, como `eventName`. Se você tiver valores únicos para todos os seletores, poderá ter um máximo de 500 condições adicionadas a um seletor.
   > Se você tiver mais de 15.000 funções do Lambda em sua conta, não poderá visualizar ou selecionar todas as funções no console CloudTrail ao criar uma trilha. Ainda será possível registrar todas as funções com um modelo de seletor predefinido, mesmo se elas não forem exibidas. Se você desejar registrar eventos de dados para funções específicas, poderá adicionar manualmente uma função se você souber seu ARN. Você também pode concluir a criação da trilha no console e, em seguida, usar o put-event-selectors comando AWS CLI e o para configurar o registro de eventos de dados para funções específicas do Lambda. Para ter mais informações, consulte Gerenciando trilhas com o AWS CLI.

c. Selecione + Field (+ Campo) para adicionar outros campos, conforme necessário. Para evitar erros, não defina valores conflitantes ou duplicados para campos. Por exemplo, não

especifique um ARN em um seletor para ser igual a um valor e, em seguida, especifique que o ARN não seja igual ao mesmo valor em outro seletor.

16. Para adicionar outro tipo de dados no qual registrar eventos de dados, escolha Add data event type (Adicionar tipo de evento de dados). Repita as etapas de 12 até esta etapa para configurar seletores de eventos avançados para o tipo de evento de dados.
17. Escolha eventos do Insights se quiser que sua trilha registre eventos do CloudTrail Insights.

    Em Event type (Tipo de evento), selecione Insights events (Eventos do Insights). Você deve registrar eventos de gerenciamento de gravação para registrar em log eventos do Insights sobre a taxa de chamadas à API. É necessário registrar eventos de gerenciamento de leitura ou gravação para registrar em log eventos do Insights sobre a taxa de erros da API.

    CloudTrail O Insights analisa eventos de gerenciamento em busca de atividades incomuns e registra eventos quando anomalias são detectadas. Por padrão, as trilhas não registram em log eventos do Insights. Para obter mais informações sobre eventos do Insights, consulte Registrar eventos do Insights. Há cobranças adicionais para o registro em log de eventos do Insights. Para CloudTrail saber os preços, consulte AWS CloudTrail Preços.

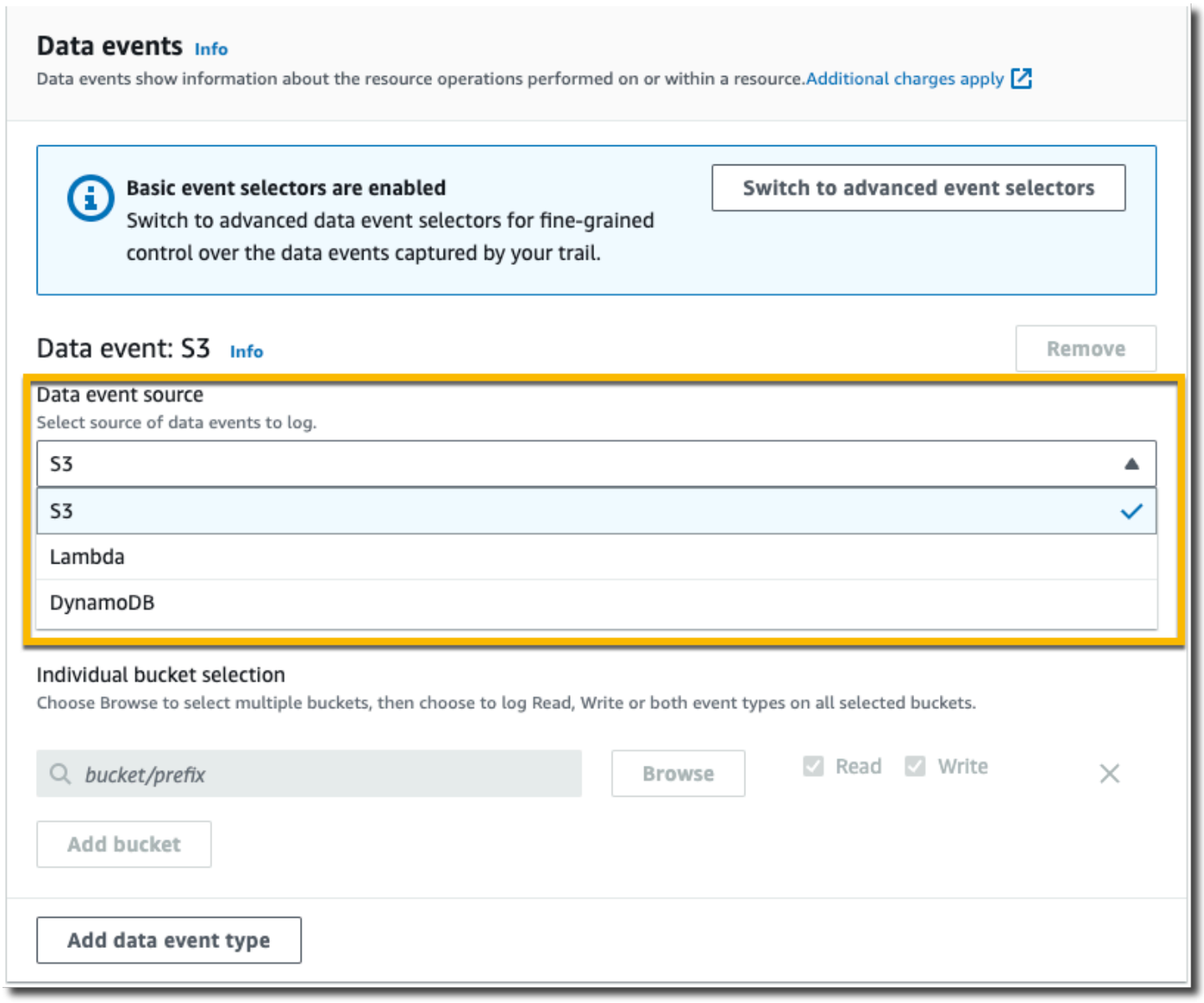
    Os eventos do Insights são entregues em uma pasta diferente chamada `/CloudTrail-Insight` do mesmo bucket do S3 que é especificado na área de localização de armazenamento da página de detalhes da trilha. CloudTrailcria o novo prefixo para você. Por exemplo, se o bucket de destino do S3 atual for chamado de `S3bucketName/AWSLogs/CloudTrail/`, o nome do bucket do S3 com um novo prefixo será chamado de `S3bucketName/AWSLogs/CloudTrail-Insight/`.
18. Quando terminar de escolher os tipos de eventos para registrar, escolhaNext (Próximo).
19. Na página Review and create (Revisar e criar), revise as suas escolhas. Escolha Edit (Editar) em uma seção para alterar as configurações de trilha mostradas nessa seção. Quando estiver pronto para criar a trilha, escolha Create trail (Criar trilha).
20. A nova trilha será exibida na página Trails (Trilhas). Em cerca de 5 minutos, CloudTrail publica arquivos de log que mostram as chamadas de AWS API feitas em sua conta. Você pode ver os arquivos de log no bucket do S3 que você especificou. Pode levar até 36 horas CloudTrail para entregar o primeiro evento do Insights, se você tiver ativado o registro de eventos do Insights e uma atividade incomum for detectada.

> **Note**
>
> CloudTrail normalmente entrega registros em uma média de cerca de 5 minutos após uma chamada de API. Desta vez não há garantias. Consulte o Acordo de Nível de Serviço do AWS CloudTrail para obter mais informações.
> Se você configurar incorretamente sua trilha (por exemplo, o bucket do S3 está inacessível), CloudTrail tentará reenviar os arquivos de log para o bucket do S3 por 30 dias, e esses attempted-to-deliver eventos estarão sujeitos às cobranças padrão. CloudTrail Para evitar cobranças em uma trilha mal configurada, você precisa excluir a trilha.

Configurar opções de eventos de dados utilizando seletores de eventos básicos

Você pode usar seletores de eventos avançados para configurar todos os tipos de eventos de dados. Os seletores de eventos avançados permitem criar seletores refinados para registrar somente os eventos de interesse.

Se você usa seletores de eventos básicos para registrar eventos de dados, você está limitado a registrar eventos de dados para buckets AWS Lambda , funções e tabelas do Amazon DynamoDB do Amazon S3. Você não pode filtrar no `eventName` campo usando seletores de eventos básicos.



Use o procedimento a seguir para configurar opções de eventos de dados utilizando seletores de eventos básicos.

Para configurar opções de eventos de dados utilizando seletores de eventos básicos

1. Em Eventos, escolha Eventos de dados para registrar eventos de dados. Há cobranças adicionais para o registro de eventos de dados. Para obter mais informações, consulte Preços do AWS CloudTrail.
2. Para Buckets do Amazon S3:

   a. Em Data event source (Fonte do eventos de dados), escolha S3.

b. Você pode escolher registrar All current and future S3 buckets (Todos os buckets do S3 atuais e futuros) ou pode especificar buckets ou funções individuais. Por padrão, os eventos de dados são registrados para todos os buckets do S3 atuais e futuros.

> **Note**
>
> Manter a opção padrão All current and future S3 buckets permite o registro de eventos de dados para todos os buckets atualmente em sua AWS conta e para todos os buckets que você criar depois de concluir a criação da trilha. Ele também permite o registro da atividade de eventos de dados realizada por qualquer identidade do IAM em sua AWS conta, mesmo que essa atividade seja realizada em um bucket que pertença a outra AWS conta.
> Se você estiver criando uma trilha para uma única região (usando o AWS CLI), escolher Todos os buckets atuais e futuros do S3 permite o registro de eventos de dados para todos os buckets na mesma região da sua trilha e para todos os buckets que você criar posteriormente nessa região. Ele não registrará eventos de dados para buckets do Amazon S3 em outras regiões da sua conta. AWS

c. Se você deixar a opção padrão All current and future S3 buckets (Todos os buckets do S3 atuais e futuros), escolha para registrar eventos Read (Leitura), Write (Gravação) ou ambos.

d. Para selecionar buckets individuais, desmarque as caixas de seleção Read (Leitura) e Write (Gravação) em All current and future S3 buckets (Todos os buckets do S3 atuais e futuros). Em Individual bucket selection (Seleção de bucket individual), procure por um bucket no qual registrar eventos de dados. Localize buckets específicos digitando um prefixo de bucket para o bucket desejado. É possível selecionar vários buckets nesta janela. Escolha Add bucket (Adicionar bucket) para registrar eventos de dados em mais buckets. Escolha se você deseja registrar eventos de Read (Leitura), como `GetObject`, Write (Gravação), como `PutObject`, ou ambos.

   Essa configuração tem precedência sobre configurações individuais que você configura para buckets individuais. Por exemplo, se você especificar o registro de eventos de Read (Leitura) para todos os buckets do S3 e escolher adicionar um bucket específico ao registro de eventos de dados, Read (Leitura) já estará selecionada para o bucket adicionado. Você não pode limpar a seleção. Você pode somente configurar a opção para Write (Gravação).

   Para remover um bucket do registro, escolha X.

3. Para adicionar outro tipo de dados no qual registrar eventos de dados, escolha Add data event type (Adicionar tipo de evento de dados).
4. Funções do Lambda:

   a. Em Data event source (Fonte do eventos de dados), escolha Lambda.

   b. Em Lambda function (Função do Lambda), escolha All regions (Todas as regiões) para registrar todas as funções do Lambda, ou Input function as ARN (Função de entrada como ARN) para registrar eventos de dados em uma função específica.

      Para registrar eventos de dados para todas as funções do Lambda em sua AWS conta, selecione Registrar todas as funções atuais e futuras. Essa configuração tem precedência sobre configurações individuais definidas para funções individuais. Todas as funções são registradas, mesmo se todas as funções não forem exibidas.

      > **Note**
      >
      > Se estiver criando uma trilha para todas as regiões, essa seleção habilitará o registro de eventos de dados para todas as funções atualmente em sua conta da AWS e qualquer função Lambda que você venha a criar em qualquer região depois de concluir a criação da trilha. Se você estiver criando uma trilha para uma única região (feita usando o AWS CLI), essa seleção habilita o registro de eventos de dados para todas as funções atualmente nessa região em sua AWS conta e quaisquer funções Lambda que você possa criar nessa região depois de terminar de criar a trilha. Essa opção não permite o registro de eventos de dados para funções do Lambda criadas em outras regiões.
      > O registro de eventos de dados para todas as funções também permite o registro da atividade de eventos de dados realizada por qualquer identidade do IAM em sua AWS conta, mesmo que essa atividade seja realizada em uma função que pertence a outra AWS conta.

   c. Se você escolher Input function as ARN (Função de entrada como ARN), insira o ARN de uma função do Lambda.

      > **Note**
      >
      > Se você tiver mais de 15.000 funções do Lambda em sua conta, não poderá visualizar ou selecionar todas as funções no console CloudTrail ao criar uma trilha. Você ainda poderá selecionar a opção de registrar todas as funções, mesmo se

elas não forem exibidas. Se você desejar registrar eventos de dados para funções específicas, poderá adicionar manualmente uma função se você souber seu ARN. Você também pode concluir a criação da trilha no console e, em seguida, usar o put-event-selectors comando AWS CLI e o para configurar o registro de eventos de dados para funções específicas do Lambda. Para ter mais informações, consulte Gerenciando trilhas com o AWS CLI.

5. Para tabelas do DynamoDB:

   a. Em Data event source (Fonte do eventos de dados), escolha DynamoDB.

   b. Em DynamoDB table selection (Seleção da tabela do DynamoDB), escolha Browse (Navegar) para selecionar uma tabela ou cole no ARN de uma tabela do DynamoDB à qual você tem acesso. Um ARN de tabela do DynamoDB utiliza o seguinte formato:

   ```
   arn:partition:dynamodb:region:account_ID:table/table_name
   ```

   Para adicionar outra tabela, escolha Add row (Adicionar linha) e procure uma tabela ou cole no ARN de uma tabela à qual você tem acesso.

6. Para configurar eventos do Insights e outras configurações para sua trilha, volte ao procedimento anterior neste tópico, ???.

Próximas etapas

Depois que você criar a trilha, poderá retornar a ela para fazer alterações:

- Se ainda não o fez, você pode configurar CloudTrail para enviar arquivos de log para o CloudWatch Logs. Para ter mais informações, consulte Envio de eventos para o CloudWatch Logs.
- Crie uma tabela e use-a para executar uma consulta no Amazon Athena para analisar sua atividade de serviço da AWS . Para obter mais informações, consulte Criação de uma tabela para CloudTrail registros no CloudTrail console no Guia do usuário do Amazon Athena.
- Adicione tags personalizadas (pares de chave-valor) à trilha.
- Para criar outra trilha, abra a página Trilhas e escolha Criar trilha.

Atualizar uma trilha

Esta seção descreve como alterar as configurações da trilha.

Para atualizar uma trilha de região única para registrar todos os eventos Regiões da AWS na AWS partição em que você está trabalhando, ou atualizar uma trilha multirregional para registrar eventos em apenas uma única região, você deve usar o. AWS CLI Para obter mais informações sobre como atualizar uma trilha de região única para registrar eventos em todas as regiões, consulte Converter uma trilha que se aplica a uma região para que ela se aplique a todas as regiões. Para obter mais informações sobre como atualizar uma trilha de váreias regiões para registrar eventos em uma região única, consulte Converter uma trilha de várias regiões em uma trilha de região única.

Se você habilitou eventos CloudTrail de gerenciamento no Amazon Security Lake, é necessário manter pelo menos uma trilha organizacional que seja multirregional e `read` registre os eventos `write` de gerenciamento. Você não pode atualizar uma trilha de qualificação de uma forma que não atenda aos requisitos do Security Lake. Por exemplo, alterando a trilha para região única ou desativando o registro em log de eventos de gerenciamento de `read` ou `write`.

> **Note**
>
> CloudTrail atualiza as trilhas da organização nas contas dos membros, mesmo que a validação do recurso falhe. Exemplos de falhas de validação incluem:
>
> - uma política incorreta de bucket do Amazon S3
> - uma política de tópicos incorreta do Amazon SNS
> - incapacidade de entregar para um grupo de CloudWatch registros de registros
> - permissão insuficiente para criptografar usando uma chave KMS
>
> Uma conta membro com CloudTrail permissões pode ver qualquer falha de validação de uma trilha da organização visualizando a página de detalhes da trilha no CloudTrail console ou executando o AWS CLI get-trail-statuscomando.

Para atualizar uma trilha com o AWS Management Console

1. Faça login no AWS Management Console e abra o CloudTrail console em https://console.aws.amazon.com/cloudtrail/.
2. No painel de navegação, escolha Trilhas e o nome da trilha.
3. Em General details (Detalhes gerais), escolha Edit (Editar) para alterar as configurações a seguir. Não é possível alterar o nome de uma trilha.

- Aplicar trilha à minha organização - altere se essa trilha é uma trilha AWS Organizations da organização.

  > **Note**
  >
  > Somente a conta de gerenciamento da organização pode converter uma trilha da organização em uma trilha não pertencente à organização ou converter uma trilha não pertencente à organização em uma trilha da organização.

- Trail log location (Localização do log de trilha) - Altere o nome do bucket do S3 ou prefixo no qual você está armazenando logs para essa trilha.
- Log file SSE-KMS encryption (Criptografia SSE-KMS do arquivo de log) - Escolha habilitar ou desabilitar a criptografia de arquivos de log com SSE-KMS em vez de SSE-S3.
- Log file validation (Validação do arquivo de log) - Escolha habilitar ou desabilitar a validação da integridade dos arquivos de log.
- SNS notification delivery (Entrega de notificações do SNS) - Escolha habilitar ou desabilitar as notificações de Amazon Simple Notification Service (Amazon SNS) de que os arquivos de logs foram entregues ao bucket especificado para a trilha.

a. Para alterar a trilha para uma trilha AWS Organizations da organização, você pode optar por habilitar a trilha para todas as contas da sua organização. Para ter mais informações, consulte Criar uma trilha para uma organização.

b. Para alterar o bucket especificado no Storage location (Local de armazenamento), escolha Create new S3 bucket (Criar novo bucket do S3) para criar um bucket. Quando você cria um bucket, CloudTrail cria e aplica as políticas de bucket necessárias. Se você optar por criar um novo bucket do S3, sua política do IAM precisará incluir permissão para a `s3:PutEncryptionConfiguration` ação porque, por padrão, a criptografia do lado do servidor está habilitada para o bucket.

   > **Note**
   >
   > Se você escolheu Use existing S3 bucket (Usar bucket do S3 existente), especifique um bucket em Trail log bucket name (Nome do bucket de log de trilha), ou escolha Browse (Procurar) para escolher um bucket. A política do bucket deve conceder CloudTrail permissão para gravar nela. Para obter informações sobre como editar

manualmente a política de bucket, consulte Política de bucket do Amazon S3 para CloudTrail.

Para facilitar a localização de seus registros, crie uma nova pasta (também conhecida como prefixo) em um bucket existente para armazenar seus CloudTrail registros. Insira o prefixo em Prefix (Prefixo).

c. Em Log file SSE-KMS encryption (Criptografia de arquivo de log com SSE-KMS), escolha Enabled (Habilitado) se quiser criptografar os arquivos de log com criptografia SSE-KMS em vez de criptografia SSE-S3. O padrão é Enabled (Habilitado). Se você não habilitar a criptografia SSE-SKMS, seus registros serão criptografados usando a criptografia SSE-S3. Para obter mais informações sobre a criptografia SSE-KMS, consulte Usando a criptografia do lado do servidor com (SSE-KMS). AWS Key Management Service Para obter mais informações sobre a criptografia SSE-S3, consulte Using Server-Side Encryption with Amazon S3-Managed Encryption Keys (SSE-S3) (Uso de criptografia no lado do servidor com chaves de criptografia gerenciadas pelo Amazon S3 [SSE-S3]).

   Se você habilitar a criptografia SSE-KMS, escolha Nova ou Existente. AWS KMS key Em AWS KMS Alias, especifique um alias, no formato. `alias/` *`MyAliasName`* Para ter mais informações, consulte Atualizar um recurso para usar sua chave do KMS. CloudTrail também oferece suporte a chaves AWS KMS multirregionais. Para obter mais informações sobre chaves de várias regiões, consulte Usar chaves de várias regiões no Manual do desenvolvedor do AWS Key Management Service .

   > **Note**
   >
   > Você também pode digitar o Nome de região da Amazon (ARN) de uma chave de outra conta. Para ter mais informações, consulte Atualizar um recurso para usar sua chave do KMS. A política de chaves deve permitir CloudTrail o uso da chave para criptografar seus arquivos de log e permitir que os usuários que você especificar leiam os arquivos de log em formato não criptografado. Para obter informações sobre como editar manualmente a política de chaves, consulte Configure as AWS KMS principais políticas para CloudTrail.

d. Em Log file validation (Validação de arquivo de log), escolha Enabled (Habilitado) para receber resumos de log no seu bucket do S3. Você pode usar os arquivos de resumo para

verificar se seus arquivos de log não foram alterados após CloudTrail serem entregues. Para ter mais informações, consulte Validando a integridade CloudTrail do arquivo de log.

e. Para entrega de notificações do SNS, escolha Ativado para ser notificado sempre que um registro for entregue ao seu bucket. CloudTrail armazena vários eventos em um arquivo de log. As notificações do SNS são enviadas para todos os arquivos de log, não para todos os eventos. Para ter mais informações, consulte Configurando notificações do Amazon SNS para CloudTrail.

   Se você habilitar notificações do SNS, para Create a new SNS topic (Criar um tópico do SNS), escolha New (Novo) para criar um tópico ou escolha Existing (Existente) para usar um tópico existente. Se criar uma trilha aplicável a todas as regiões, as notificações do SNS sobre a entrega de arquivos de log de todas as regiões serão enviadas ao único tópico do SNS que você criar.

   Se você escolher Novo, CloudTrail especifica um nome para o novo tópico para você ou pode digitar um nome. Se escolher Existing (Existente), escolha um tópico do SNS na lista suspensa. Você também pode inserir o Nome de região da Amazon (ARN) de um tópico de outra região ou de uma conta com permissões apropriadas. Para ter mais informações, consulte Política de tópicos do Amazon SNS para CloudTrail.

   Se você criar um tópico, precisará se inscrever nele para ser notificado sobre a entrega de arquivos de log. Você pode se inscrever no console do Amazon SNS. Devido à frequência das notificações, recomendamos que você configure a inscrição para usar uma fila do Amazon SQS para gerenciar as notificações de modo programático. Para obter mais informações, consulte Conceitos básicos do Amazon SNS no Guia do desenvolvedor do Amazon Simple Notification Service.

4. Em CloudWatch Registros, escolha Editar para alterar as configurações de envio de arquivos de CloudTrail registro para o CloudWatch Logs. Escolha Ativado em CloudWatch registros para ativar o envio de arquivos de log. Para ter mais informações, consulte Envio de eventos para o CloudWatch Logs.

   a. Se você habilitar a integração com CloudWatch Logs, escolha Novo para criar um novo grupo de registros ou Existente para usar um existente. Se você escolher Novo, CloudTrail especifica um nome para o novo grupo de registros para você ou pode digitar um nome.

   b. Se escolher Existing (Existente), escolha um grupo de logs na lista suspensa.

   c. Escolha Novo para criar uma nova função do IAM para obter permissões para enviar registros para o CloudWatch Logs. Escolha Existing (Existente) para escolher uma função

do IAM existente na lista suspensa. A declaração de política para a função nova ou existente é exibida quando você expande Policy document (Documento de política). Para obter mais informações sobre essa função, consulte Documento de política de funções CloudTrail para usar CloudWatch registros para monitoramento.

> **Note**
>
> - Quando você configurar uma trilha, você pode escolher um bucket do S3 e um tópico do SNS que pertençam a outra conta. No entanto, se você quiser CloudTrail entregar eventos a um grupo de CloudWatch registros de registros, deverá escolher um grupo de registros que exista na sua conta atual.
> - Somente a conta de gerenciamento pode configurar um grupo de CloudWatch registros de registros para uma trilha da organização usando o console. O administrador delegado pode configurar um grupo de CloudWatch registros de registros usando as operações AWS CLI ou CloudTrail `CreateTrail` ou `UpdateTrail` da API.

5. Em Tags, escolha Edit (Editar) para alterar, adicionar ou excluir tags na trilha. Adicione uma ou mais tags personalizadas (pares chave-valor) à sua trilha. As tags podem ajudá-lo a identificar suas CloudTrail trilhas e os buckets do Amazon S3 que contêm CloudTrail arquivos de log. Em seguida, você pode usar grupos de recursos para seus CloudTrail recursos. Para obter mais informações, consulte AWS Resource Groups e Tags.
6. Em Management events (Eventos de gerenciamento), escolha Edit (Editar) para alterar as configurações de log de eventos de gerenciamento.

   a. Em API activity (Atividade da API), escolha se você deseja que sua trilha registre eventos Read (Leitura), Write (Gravação) ou ambos. Para ter mais informações, consulte Eventos de gerenciamento.

   b. Escolha Excluir AWS KMS eventos para filtrar AWS Key Management Service (AWS KMS) eventos da sua trilha. A configuração padrão é incluir todos os eventos do AWS KMS .

      A opção de registrar ou excluir AWS KMS eventos está disponível somente se você registrar eventos de gerenciamento em sua trilha. Se você optar por não registrar eventos de gerenciamento, os AWS KMS eventos não serão registrados e você não poderá alterar as configurações do registro de AWS KMS eventos.

AWS KMS ações como`Encrypt`,`Decrypt`, e `GenerateDataKey` normalmente geram um grande volume (mais de 99%) de eventos. Agora essas ações são registradas em log como eventos de Leitura. AWS KMS Ações relevantes de baixo volume, como **`DisableDelete`**, e **`ScheduleKey`** (que normalmente representam menos de 0,5% do volume de AWS KMS eventos) são registradas como eventos de gravação.

Para excluir eventos de alto volume, como `Encrypt`, `Decrypt` e`GenerateDataKey`, mas ainda registra eventos relevantes como `Disable`, `Delete` e `ScheduleKey`, escolha para registrar Write (Gravação) e desmarque a caixa de seleção para Exclude AWS KMS events (Excluir eventos do KMS).

c. Escolha Exclude Amazon RDS Data API events (Excluir eventos da API de dados do Amazon RDS) para filtrar eventos da API de dados do Amazon Relational Database Service fora da trilha. A configuração padrão é incluir todos os eventos da API de dados do Amazon RDS. Para obter mais informações sobre eventos da API de dados do Amazon RDS, consulte Registrar em log chamadas da API de dados com o AWS CloudTrail no Manual do usuário do Amazon RDS for Aurora.

7.

> **Important**
>
> As etapas 7 a 11 devem ser usadas para configurar eventos de dados usando seletores de eventos avançados. Os seletores de eventos avançados permitem que você configure mais tipos de eventos de dados e oferecem um controle mais preciso sobre quais eventos de dados são capturados por sua trilha. Se você estiver usando seletores de eventos básicos, consulte Atualizar configurações de eventos de dados com seletores de eventos básicos e, em seguida, volte para a etapa 12 deste procedimento.

Em Data events (Eventos de dados), escolha Edit (Editar) para alterar as configurações de log dos eventos de dados. Por padrão, as trilhas não registram eventos de dados. Há cobranças adicionais para o registro de eventos de dados. Para obter a definição de preço do CloudTrail, consulte Definição de preço do AWS CloudTrail.

Em Data event type (Tipo de evento de dados), escolha o tipo de recurso no qual você deseja registrar eventos de dados. Para obter mais informações sobre os tipos de eventos de dados disponíveis, consulte Eventos de dados.

> **Note**
>
> Para registrar eventos de dados para AWS Glue tabelas criadas pelo Lake Formation, escolha Lake Formation.

8. Escolha um modelo de seletor de registros. CloudTrail inclui modelos predefinidos que registram todos os eventos de dados do tipo de recurso. Para criar um modelo de seletor de log personalizado, escolha Custom (Personalizado).

> **Note**
>
> A escolha de um modelo predefinido para buckets do S3 permite o registro de eventos de dados de todos os buckets atualmente em sua AWS conta e de todos os buckets que você criar depois de concluir a criação da trilha. Ele também permite o registro da atividade de eventos de dados realizada por qualquer usuário ou função em sua AWS conta, mesmo que essa atividade seja realizada em um bucket que pertença a outra AWS conta.
>
> Se a trilha se aplicar somente a uma região, a escolha da opção Select all S3 buckets in your account (Selecionar todos os buckets do S3 em sua conta) habilitará o registro de eventos de dados para todos os buckets do S3 na mesma região que a trilha e todos os buckets que você criar posteriormente nessa região. Os eventos de dados não serão registrados para os buckets do Amazon S3 em outras regiões em sua conta da AWS .
>
> Se você estiver criando uma trilha para todas as regiões, a escolha de um modelo predefinido para as funções do Lambda permite o registro de eventos de dados para todas as funções atualmente em AWS sua conta e para quaisquer funções do Lambda que você possa criar em qualquer região depois de terminar de criar a trilha. Se você estiver criando uma trilha para uma única região (feita usando o AWS CLI), essa seleção habilita o registro de eventos de dados para todas as funções atualmente nessa região em sua AWS conta e quaisquer funções Lambda que você possa criar nessa região depois de terminar de criar a trilha. Essa opção não permite o registro de eventos de dados para funções do Lambda criadas em outras regiões.
>
> O registro de eventos de dados para todas as funções também permite o registro da atividade de eventos de dados realizada por qualquer usuário ou função em sua AWS conta, mesmo que essa atividade seja realizada em uma função que pertença a outra AWS conta.

9. (Opcional) Em Nome do seletor, insira um nome para identificar o seletor. O nome do seletor é um nome descritivo para um seletor de eventos avançado, como "Registrar eventos de dados em log para apenas dois buckets do S3". O nome do seletor é listado como `Name` no seletor de eventos avançado e poderá ser visualizado se você expandir a visualização JSON.
10. Em Advanced event selectors (Seletores de eventos avançados), crie uma expressão para os recursos específicos nos quais você deseja coletar eventos de dados. Você poderá ignorar esta etapa se estiver usando um modelo de log predefinido.

    a. Escolha um dos seguintes campos:

    - **`readOnly`**- `readOnly` pode ser definido como igual a um valor de `true` ou. `false` Para registrar os eventos `read` e `write`, não adicione um seletor `readOnly`.
    - **`eventName`** - `eventName` pode usar qualquer operador. Você pode usá-lo para incluir ou excluir qualquer evento de dados registrado CloudTrail, como `PutBucket` ou`GetSnapshotBlock`.
    - **`resources.ARN`**- Você pode usar qualquer operador com`resources.`ARN, mas se usar igual ou diferente, o valor deverá corresponder exatamente ao ARN de um recurso válido do tipo que você especificou no modelo como valor de. `resources.type`

      A tabela a seguir mostra o formato de ARN válido para cada `resources.type`.

      > **Note**
      >
      > Você não pode usar o `resources.`ARN campo para filtrar tipos de recursos que não tenham ARNs.

resources.type	resources.ARN
`AWS::DynamoDB::Table` [1]	`arn:`*`partition`*` :dynamodb : `*`region`*`:`*`account_ID`*` :table/`*`table_name`*
`AWS::Lambda::Function`	`arn:`*`partition`*` :lambda:`*`region`*`:`*`account_ID`*` :function: `*`function_name`*
`AWS::S3::Object` [2]	`arn:`*`partition`*` :s3:::`*`bucket_name`*` /`

resources.type	resources.ARN
	arn:*partition* :s3:::*bucket_name* /*object_or_file_name* /
AWS::AppConfig::Configuration	arn:*partition* :appconfig: *region*:*account_ID* :application/ *application_ID* /environment/ *environment_ID* /configuration/ *configuration_profile_ID*
AWS::B2BI::Transformer	arn:*partition* :b2bi:*region*:*account_ID* :transformer/ *transformer_ID*
AWS::Bedrock::AgentAlias	arn:*partition* :bedrock: *region*:*account_ID* :agent-alias/ *agent_ID*/*alias_ID*
AWS::Bedrock::KnowledgeBase	arn:*partition* :bedrock: *region*:*account_ID* :knowledge-base/*knowledge_base_ID*
AWS::Cassandra::Table	arn:*partition* :cassandra: *region*:*account_ID* :keyspace/ *keyspace_name* /table/*table_name*
AWS::CloudFront::KeyValueStore	arn:*partition* :cloudfront: *region*:*account_ID* :key-value-store/*KVS_name*
AWS::CloudTrail::Channel	arn:*partition* :cloudtrail: *region*:*account_ID* :channel/ *channel_UUID*

resources.type	resources.ARN
AWS::CodeWhisperer::Customization	arn:*partition* :codewhisperer: *region*:*account_ID* :customization/ *customization_ID*
AWS::CodeWhisperer::Profile	arn:*partition* :codewhisperer: *region*:*account_ID* :profile/ *profile_ID*
AWS::Cognito::IdentityPool	arn:*partition* :cognito-identity: *region*:*account_ID* :identitypool/ *identity_pool_ID*
AWS::DynamoDB::Stream	arn:*partition* :dynamodb: *region*:*account_ID* :table/*table_name* /stream/*date_time*
AWS::EC2::Snapshot	arn:*partition* :ec2:*region*::snapshot/ *snapshot_ID*
AWS::EMRWAL::Workspace	arn:*partition* :emrwal:*region*:*account_ID* :workspace/ *workspace_name*
AWS::FinSpace::Environment	arn:*partition* :finspace: *region*:*account_ID* :environment/ *environment_ID*
AWS::Glue::Table	arn:*partition* :glue:*region*:*account_ID* :table/*database_name* /*table_name*
AWS::GreengrassV2::ComponentVersion	arn:*partition* :greengrass: *region*:*account_ID* :components/ *component_name*

resources.type	resources.ARN
AWS::GreengrassV2::Deployment	arn:*partition* :greengra ss: *region*:*account_ID* :deployme nts/ *deployment_ID*
AWS::GuardDuty::Detector	arn:*partition* :guarddut y: *region*:*account_ID* :detector / *detector_ID*
AWS::IoT::Certificate	arn:*partition* :iot:*region*:*account_I D* :cert/*certificate_ID*
AWS::IoT::Thing	arn:*partition* :iot:*region*:*account_I D* :thing/*thing_ID*
AWS::IoTSiteWise::Asset	arn:*partition* :iotsitew ise: *region*:*account_ID* :asset/*asset_ID*
AWS::IoTSiteWise::TimeSeries	arn:*partition* :iotsitew ise: *region*:*account_ID* :timeseri es/ *timeseries_ID*
AWS::IoTTwinMaker::Entity	arn:*partition* :iottwinm aker: *region*:*account_ID* :workspac e/ *workspace_ID* /entity/*entity_ID*
AWS::IoTTwinMaker::Workspace	arn:*partition* :iottwinm aker: *region*:*account_ID* :workspac e/ *workspace_ID*

resources.type	resources.ARN
AWS::KendraRanking::ExecutionPlan	arn:*partition* :kendra-ranking: *region*:*account_ID* :rescore-execution-plan/ *rescore_execution_plan_ID*
AWS::Kinesis::Stream	arn:*partition* :kinesis: *region*:*account_ID* :stream/*stream_name*
AWS::Kinesis::StreamConsumer	arn:*partition* :kinesis: *region*:*account_ID* :*stream_type* /*stream_name* /consumer/ *consumer_name* :*consumer_creation_timestamp*
AWS::KinesisVideo::Stream	arn:*partition* :kinesisvideo: *region*:*account_ID* :stream/*stream_name* /*creation_time*
AWS::ManagedBlockchain::Network	arn:*partition* :managedblockchain :::networks/ *network_name*
AWS::ManagedBlockchain::Node	arn:*partition* :managedblockchain : *region*:*account_ID* :nodes/*node_ID*
AWS::MedicalImaging::Datastore	arn:*partition* :medical-imaging: *region*:*account_ID* :datastore/ *data_store_ID*
AWS::NeptuneGraph::Graph	arn:*partition* :neptune-graph: *region*:*account_ID* :graph/*graph_ID*

resources.type	resources.ARN
AWS::PCAConnectorAD::Connector	arn:*partition* :pca-connector-ad: *region*:*account_ID* :connector/ *connector_ID*
AWS::QApps:QApp	arn:*partition* :qapps:*region*:*account_ID* :application/ *application_UUID* / qapp/*qapp_UUID*
AWS::QBusiness::Application	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID*
AWS::QBusiness::DataSource	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID* /index/*index_ID*/ data-source/ *datasource_ID*
AWS::QBusiness::Index	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID* /index/*index_ID*
AWS::QBusiness::WebExperience	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID* /web-experience/ *web_experienc_ID*
AWS::RDS::DBCluster	arn:*partition* :rds:*region*:*account_ID* :cluster/ *cluster_name*
AWS::S3::AccessPoint [3]	arn:*partition* :s3:*region*:*account_ID* :accesspoint/ *access_point_name*

resources.type	resources.ARN
AWS::S3ObjectLambda::AccessPoint	arn:*partition* :s3-object-lambda: *region*:*account_ID* :accesspoint/ *access_point_name*
AWS::S3Outposts::Object	arn:*partition* :s3-outposts: *region*:*account_ID* :*object_path*
AWS::SageMaker::Endpoint	arn:*partition* :sagemaker: *region*:*account_ID* :endpoint/ *endpoint_name*
AWS::SageMaker::ExperimentTrialComponent	arn:*partition* :sagemaker: *region*:*account_ID* :experiment-trial-component/ *experiment_trial_component_name*
AWS::SageMaker::FeatureGroup	arn:*partition* :sagemaker: *region*:*account_ID* :feature-group/ *feature_group_name*
AWS::SCN::Instance	arn:*partition* :scn:*region*:*account_ID* :instance/ *instance_ID*
AWS::ServiceDiscovery::Namespace	arn:*partition* :servicediscovery: *region*:*account_ID* :namespace/ *namespace_ID*
AWS::ServiceDiscovery::Service	arn:*partition* :servicediscovery: *region*:*account_ID* :service/ *service_ID*

resources.type	resources.ARN
AWS::SNS::PlatformEndpoint	arn:*partition* :sns:*region*:*account_ID* :endpoint/ *endpoint_type* /*endpoint_name* /*endpoint_ID*
AWS::SNS::Topic	arn:*partition* :sns:*region*:*account_ID* :*topic_name*
AWS::SQS::Queue	arn:*partition* :sqs:*region*:*account_ID* :*queue_name*
AWS::SSM::ManagedNode	O ARN deve estar em um dos seguintes formatos: • arn:*partition* :ssm:*region*:*account_ID* :managed-instance/ *instance_ID* • arn:*partition* :ec2:*region*:*account_ID* :instance/ *instance_ID*
AWS::SSMMessages::ControlChannel	arn:*partition* :ssmmessages: *region*:*account_ID* :control-channel/ *control_channel_ID*
AWS::StepFunctions::StateMachine	O ARN deve estar em um dos seguintes formatos: • arn:*partition* :states:*region*:*account_ID* :stateMachine: *stateMachine_name* • arn:*partition* :states:*region*:*account_ID* :stateMachine: *stateMachine_name* /*label_name*

resources.type	resources.ARN
AWS::SWF::Domain	arn:*partition* :swf:*region*:*account_ID* :/domain/ *domain_name*
AWS::ThinClient::Device	arn:*partition* :thinclient: *region*:*account_ID* :device/*device_ID*
AWS::ThinClient::Environment	arn:*partition* :thinclient: *region*:*account_ID* :environment/ *environment_ID*
AWS::Timestream::Database	arn:*partition* :timestream: *region*:*account_ID* :database/ *database_name*
AWS::Timestream::Table	arn:*partition* :timestream: *region*:*account_ID* :database/ *database_name* /table/*table_name*
AWS::VerifiedPermissions::PolicyStore	arn:*partition* :verifiedpermissions: *region*:*account_ID* :policy-store/ *policy_store_ID*

[1] Para tabelas com fluxos habilitados, o campo `resources` no evento de dados contém `AWS::DynamoDB::Stream` e `AWS::DynamoDB::Table`. Se você especificar `AWS::DynamoDB::Table` como `resources.type`, ele registrará os eventos da tabela do DynamoDB e dos fluxos do DynamoDB por padrão. Para excluir eventos de streams, adicione um filtro no `eventName` campo.

[2] Para registrar em log todos os eventos de dados de todos os objetos em um bucket do S3 específico, use o operador `StartsWith` e inclua apenas o ARN do bucket como o valor correspondente. A barra final é intencional; não a exclua.

[3] Para registrar em log eventos de todos os objetos em um ponto de acesso do S3, recomendamos usar somente o ARN do ponto de acesso, não incluir o caminho do objeto e usar os operadores `StartsWith` ou `NotStartsWith`.

Para obter mais informações sobre os formatos do ARN de recursos de evento de dados, consulte Ações, recursos e chaves de condição no Guia do usuário do AWS Identity and Access Management .

b. Para cada campo, escolha + Condição para adicionar quantas condições forem necessárias até o máximo de 500 valores especificados para todas as condições. Por exemplo, para excluir eventos de dados de dois buckets do S3 dos eventos de dados registrados em sua trilha, você pode definir o campo como Resources.arn, definir o operador para does not start with e, em seguida, colar o ARN de um bucket do S3 ou procurar os buckets do S3 nos quais você não deseja registrar eventos.

   Para adicionar o segundo bucket do S3, escolha + Condição e, em seguida, repita a instrução anterior, colando o ARN ou procurando um bucket diferente.

   > **Note**
   >
   > É possível ter, no máximo, 500 valores para todos os seletores em uma trilha. Isso inclui matrizes de vários valores para um seletor, como `eventName`. Se você tiver valores únicos para todos os seletores, poderá ter um máximo de 500 condições adicionadas a um seletor.
   > Se você tiver mais de 15.000 funções do Lambda em sua conta, não poderá visualizar ou selecionar todas as funções no console CloudTrail ao criar uma trilha. Ainda será possível registrar todas as funções com um modelo de seletor predefinido, mesmo se elas não forem exibidas. Se você desejar registrar eventos de dados para funções específicas, poderá adicionar manualmente uma função se você souber seu ARN. Você também pode concluir a criação da trilha no console e, em seguida, usar o put-event-selectors comando AWS CLI e o para configurar o registro de eventos de dados para funções específicas do Lambda. Para ter mais informações, consulte Gerenciando trilhas com o AWS CLI.

c. Selecione + Field (+ Campo) para adicionar outros campos, conforme necessário. Para evitar erros, não defina valores conflitantes ou duplicados para campos. Por exemplo, não

especifique um ARN em um seletor para ser igual a um valor e, em seguida, especifique que o ARN não seja igual ao mesmo valor em outro seletor.

11. Para adicionar outro tipo de dados no qual registrar eventos de dados, escolha Add data event type (Adicionar tipo de evento de dados). Repita as etapas de 3 até esta etapa para configurar seletores de eventos avançados para o tipo de evento de dados.
12. Em Eventos do Insights, escolha Editar se quiser que sua trilha registre eventos do CloudTrail Insights.

    Em Event type (Tipo de evento), selecione Insights events (Eventos do Insights).

    Em Eventos do Insights, escolha Taxa de chamada da API, Taxa de erro da API ou ambos. Você deve registrar eventos de gerenciamento de gravação para registrar em log eventos do Insights sobre a taxa de chamadas à API. É necessário registrar eventos de gerenciamento de leitura ou gravação para registrar em log eventos do Insights sobre a taxa de erros da API.

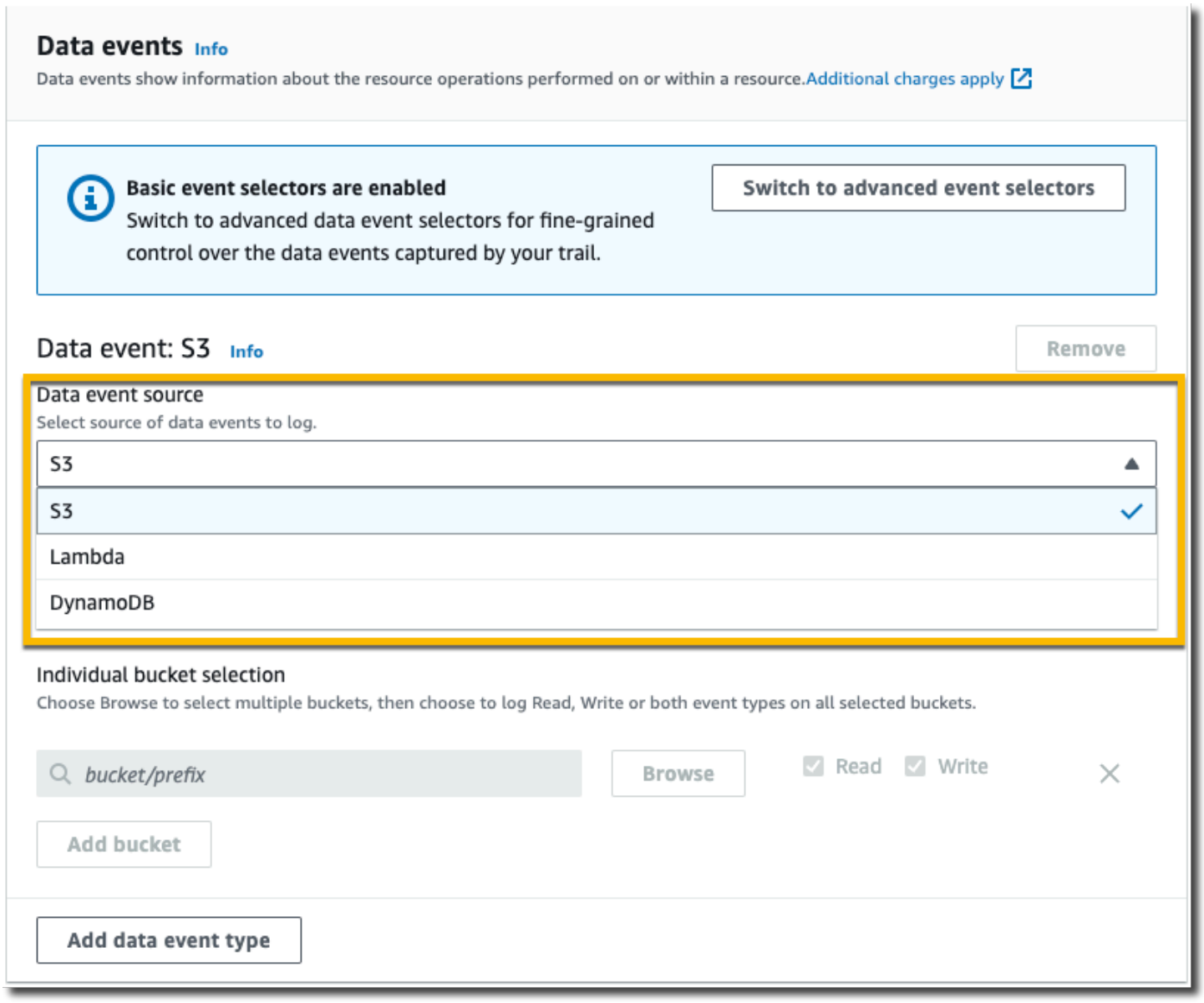
    CloudTrail O Insights analisa eventos de gerenciamento em busca de atividades incomuns e registra eventos quando anomalias são detectadas. Por padrão, as trilhas não registram em log eventos do Insights. Para obter mais informações sobre eventos do Insights, consulte Registrar eventos do Insights. Há cobranças adicionais para o registro em log de eventos do Insights. Para CloudTrail saber os preços, consulte AWS CloudTrail Preços.

    Os eventos do Insights são entregues em uma pasta diferente chamada `/CloudTrail-Insight` do mesmo bucket do S3 que é especificado na área de localização de armazenamento da página de detalhes da trilha. CloudTrailcria o novo prefixo para você. Por exemplo, se o bucket de destino do S3 atual for chamado de `S3bucketName/AWSLogs/CloudTrail/`, o nome do bucket do S3 com um novo prefixo será chamado de `S3bucketName/AWSLogs/CloudTrail-Insight/`.
13. Quando você terminar de alterar configurações da trilha, escolha Update trail (Atualizar trilha).

Atualizar configurações de eventos de dados com seletores de eventos básicos

Você pode usar seletores de eventos avançados para configurar todos os tipos de eventos de dados. Os seletores de eventos avançados permitem criar seletores refinados para registrar somente os eventos de interesse.

Se você usa seletores de eventos básicos para registrar eventos de dados, você está limitado a registrar eventos de dados para buckets AWS Lambda , funções e tabelas do Amazon DynamoDB do Amazon S3. Você não pode filtrar no `eventName` campo usando seletores de eventos básicos.



Use o procedimento a seguir para configurar opções de eventos de dados utilizando seletores de eventos básicos.

1. Em Data events (Eventos de dados), escolha Edit (Editar) para alterar as configurações de log dos eventos de dados. Com seletores de eventos básicos, você pode especificar eventos de dados de registro para buckets AWS Lambda , funções, DynamoDBtables do Amazon S3 ou uma combinação desses recursos. Tipos de eventos de dados adicionais têm suporte dos seletores de eventos avançados. Por padrão, as trilhas não registram eventos de dados. Há cobranças adicionais para o registro de eventos de dados. Para ter mais informações, consulte Eventos de dados. Para obter a definição de preço do CloudTrail, consulte Definição de preço do AWS CloudTrail.

Para Buckets do Amazon S3:

a. Em Data event source (Fonte do eventos de dados), escolha S3.

b. Você pode escolher registrar All current and future S3 buckets (Todos os buckets do S3 atuais e futuros) ou pode especificar buckets ou funções individuais. Por padrão, os eventos de dados são registrados para todos os buckets do S3 atuais e futuros.

> **Note**
>
> Manter a opção padrão All current and future S3 buckets permite o registro de eventos de dados para todos os buckets atualmente em sua AWS conta e para todos os buckets que você criar depois de concluir a criação da trilha. Ele também permite o registro da atividade de eventos de dados realizada por qualquer usuário ou função em sua AWS conta, mesmo que essa atividade seja realizada em um bucket que pertença a outra AWS conta.
> Se a trilha se aplicar somente a uma região, selecionar All current and future S3 buckets (Todos os buckets do S3 atuais ou futuros) habilitará o registro de eventos de dados para todos os buckets na mesma região que a trilha e todos os buckets que você criar posteriormente nessa região. Ele não registrará eventos de dados para buckets do Amazon S3 em outras regiões da sua conta. AWS

c. Se você deixar a opção padrão All current and future S3 buckets (Todos os buckets do S3 atuais e futuros), escolha para registrar eventos Read (Leitura), Write (Gravação) ou ambos.

d. Para selecionar buckets individuais, desmarque as caixas de seleção Read (Leitura) e Write (Gravação) em All current and future S3 buckets (Todos os buckets do S3 atuais e futuros). Em Individual bucket selection (Seleção de bucket individual), procure por um bucket no qual registrar eventos de dados. Para localizar períodos específicos, digite um prefixo de bucket para o bucket desejado. É possível selecionar vários buckets nesta janela. Escolha Add bucket (Adicionar bucket) para registrar eventos de dados em mais buckets. Escolha se você deseja registrar eventos de Read (Leitura), como `GetObject`, Write (Gravação), como `PutObject`, ou ambos.

   Essa configuração tem precedência sobre configurações individuais que você configura para buckets individuais. Por exemplo, se você especificar o registro de eventos de Read (Leitura) para todos os buckets do S3 e escolher adicionar um bucket específico ao registro de eventos de dados, Read (Leitura) já estará selecionada para o bucket adicionado. Você não pode limpar a seleção. Você pode somente configurar a opção para Write (Gravação).

Para remover um bucket do registro, escolha X.

2. Para adicionar outro tipo de dados no qual registrar eventos de dados, escolha Add data event type (Adicionar tipo de evento de dados).
3. Funções do Lambda:

   a. Em Data event source (Fonte do eventos de dados), escolha Lambda.

   b. Em Lambda function (Função do Lambda), escolha All regions (Todas as regiões) para registrar todas as funções do Lambda, ou Input function as ARN (Função de entrada como ARN) para registrar eventos de dados em uma função específica.

      Para registrar eventos de dados para todas as funções do Lambda em sua AWS conta, selecione Registrar todas as funções atuais e futuras. Essa configuração tem precedência sobre configurações individuais definidas para funções individuais. Todas as funções são registradas, mesmo se todas as funções não forem exibidas.

      > **Note**
      >
      > Se você estiver criando uma trilha para todas as regiões, essa seleção habilita o registro de eventos de dados para todas as funções atualmente em sua AWS conta e quaisquer funções Lambda que você possa criar em qualquer região depois de terminar de criar a trilha. Se você estiver criando uma trilha para uma única região (feita usando o AWS CLI), essa seleção habilita o registro de eventos de dados para todas as funções atualmente nessa região em sua AWS conta e quaisquer funções Lambda que você possa criar nessa região depois de terminar de criar a trilha. Essa opção não permite o registro de eventos de dados para funções do Lambda criadas em outras regiões.
      > O registro de eventos de dados para todas as funções também permite o registro da atividade de eventos de dados realizada por qualquer usuário ou função em sua AWS conta, mesmo que essa atividade seja realizada em uma função que pertença a outra AWS conta.

   c. Se você escolher Input function as ARN (Função de entrada como ARN), insira o ARN de uma função do Lambda.

> **Note**
>
> Se você tiver mais de 15.000 funções do Lambda em sua conta, não poderá visualizar ou selecionar todas as funções no console CloudTrail ao criar uma trilha. Você ainda poderá selecionar a opção de registrar todas as funções, mesmo se elas não forem exibidas. Se você desejar registrar eventos de dados para funções específicas, poderá adicionar manualmente uma função se você souber seu ARN. Também é possível criar da trilha no console e usar o AWS CLI e o comando put-event-selectors para configurar o registro de eventos de dados para funções do Lambda específicas. Para ter mais informações, consulte Gerenciando trilhas com o AWS CLI.

4. Para adicionar outro tipo de dados no qual registrar eventos de dados, escolha Add data event type (Adicionar tipo de evento de dados).
5. Para tabelas do DynamoDB:

   a. Em Data event source (Fonte do eventos de dados), escolha DynamoDB.

   b. Em DynamoDB table selection (Seleção da tabela do DynamoDB), escolha Browse (Navegar) para selecionar uma tabela ou cole no ARN de uma tabela do DynamoDB à qual você tem acesso. Um ARN de tabela do DynamoDB tem o seguinte formato:

   ```
   arn:partition:dynamodb:region:account_ID:table/table_name
   ```

   Para adicionar outra tabela, escolha Add row (Adicionar linha) e procure uma tabela ou cole no ARN de uma tabela à qual você tem acesso.
6. Para configurar eventos do Insights e outras configurações para sua trilha, volte ao procedimento anterior neste tópico, Atualizar uma trilha.

Excluir uma trilha

Você pode excluir trilhas com o CloudTrail console. Se a conta de gerenciamento ou conta de administrador delegado de uma organização excluir uma trilha da organização, a trilha será removida de todas as contas-membro da organização.

Se você habilitou eventos CloudTrail de gerenciamento no Amazon Security Lake, é necessário manter pelo menos uma trilha organizacional que seja multirregional e `read` registre os eventos

`write` de gerenciamento. Você não pode excluir uma trilha se ela for a única trilha que atenda a esse requisito, a menos que você desative os eventos CloudTrail de gerenciamento no Security Lake.

Para excluir uma trilha com o CloudTrail console

1. Faça login no AWS Management Console e abra o CloudTrail console em https://console.aws.amazon.com/cloudtrail/.
2. Abra a página Trilhas do CloudTrail console.
3. Escolha o nome da trilha.
4. Na parte superior da página de detalhes da trilha, escolha Delete (Excluir).
5. Quando solicitado a confirmar a exclusão, escolha Delete (Excluir). A trilha é removida da lista de trilhas. Os arquivos de log que já foram entregues ao bucket do Amazon S3 não serão excluídos.

> **Note**
>
> O conteúdo entregue aos buckets do Amazon S3 pode conter conteúdo do cliente. Para obter mais informações sobre a remoção de dados confidenciais, consulte Como esvaziar um bucket e Excluir um bucket no Guia do usuário do Amazon S3.

Desativar o registro de uma trilha

Quando você cria uma trilha, o registro é ativado automaticamente. Você pode desativar o registro de uma trilha.

Quando você desativa o registro em log, os logs existentes permanecem armazenados no bucket do Amazon S3 da trilha e continuam incorrendo em cobranças do S3.

Para desativar o registro de uma trilha com o CloudTrail console

1. Faça login no AWS Management Console e abra o CloudTrail console em https://console.aws.amazon.com/cloudtrail/.
2. No painel de navegação, escolha Trails (Trilhas) e o nome da trilha.
3. Na parte superior da página de detalhes da trilha, escolha Stop Logging (Parar o registro) para desativar o registro da trilha.

4. Quando você for solicitado a confirmar, escolha Parar de registrar. CloudTrailinterrompe a atividade de registro dessa trilha.
5. Para retomar o registro dessa trilha, escolha Start logging (Iniciar o registro em log) na página de configuração da trilha.

Criando, atualizando e gerenciando trilhas com o AWS CLI

Você pode usar o AWS CLI para criar, atualizar e gerenciar suas trilhas. Ao usar o AWS CLI, lembre-se de que seus comandos são executados na AWS região configurada para seu perfil. Se você deseja executar os comandos em uma região diferente, altere a região padrão para o seu perfil ou use o parâmetro --region com o comando.

> **Note**
>
> Você precisa das ferramentas de linha de AWS comando para executar os comandos AWS Command Line Interface (AWS CLI) neste tópico. Verifique se você tem uma versão recente do AWS CLI instalado. Para mais informações, consulte o Guia do usuário do AWS Command Line Interface. Para obter ajuda com CloudTrail os comandos na linha de AWS CLI comando, digite`aws cloudtrail help`.

Comandos normalmente usados para criação, gerenciamento e status de trilhas

Alguns dos comandos mais usados para criar e atualizar trilhas CloudTrail incluem:

- create-trail para criar uma trilha.
- update-trail para alterar a configuração de uma trilha existente.
- add-tags para adicionar uma ou mais tags (pares de chave-valor) a uma trilha existente.
- remove-tags para remover uma ou mais tags de uma trilha.
- list-tags para retornar uma lista de tags associadas a uma trilha.
- put-event-selectors para adicionar ou modificar seletores de evento a uma trilha.
- put-insight-selectors para adicionar ou modificar seletores de eventos do Insights para uma trilha existente e ativar ou desativar eventos do Insights.
- start-logging para iniciar eventos de log com sua trilha.
- stop-logging para pausar eventos de log com sua trilha.

- delete-trail para excluir uma trilha. Esse comando não exclui o bucket do Amazon S3 que contém os arquivos de log dessa trilha, se houver.
- describe-trailspara retornar informações sobre trilhas em uma AWS região.
- get-trail para retornar informações de configurações de uma trilha.
- get-trail-status para retornar informações sobre o status atual de uma trilha.
- get-event-selectors para retornar informações sobre seletores de evento configurados para uma trilha.
- get-insight-selectors para retornar informações sobre seletores de eventos do Insights configurados para uma trilha.

Os comandos com suporte para criar e atualizar trilhas: create-trail e update-trail

Os comandos `update-trail` e `create-trail` oferecem uma variedade de funcionalidades para criar e gerenciar trilhas, incluindo:

- Criar uma trilha que recebe logs entre regiões ou atualizar uma trilha com a opção `--is-multi-region-trail`. Na maioria das circunstâncias, você deve criar trilhas que registrem eventos em todas as AWS regiões.
- Criar uma trilha que receba registros de todas as AWS contas em uma organização com a --is-organization-trail opção.
- Converter uma trilha de várias regiões em uma trilha de região única com a opção `--no-is-multi-region-trail`.
- Ativar ou desativar a criptografia de arquivos de log com a opção `--kms-key-id`. A opção especifica uma AWS KMS chave que você já criou e à qual anexou uma política que permite CloudTrail criptografar seus registros. Para ter mais informações, consulte Ativando e desativando a criptografia do arquivo de CloudTrail log com o AWS CLI.
- Ativar ou desativar a validação do arquivo de log com as opções `--no-enable-log-file-validation` e `--enable-log-file-validation`. Para ter mais informações, consulte Validando a integridade CloudTrail do arquivo de log.
- Especificar um grupo e uma função de CloudWatch registros de registros para que CloudTrail possa entregar eventos a um grupo de CloudWatch registros de registros de registros. Para ter mais informações, consulte Monitoramento CloudTrail de arquivos de log com o Amazon CloudWatch Logs.

Comandos suspensos: create-subscription e update-subscription

> **Important**
>
> Os comandos `create-subscription` e `update-subscription` foram usados para criar e atualizar trilhas, mas estão defasados. Não use esses comandos. Eles não fornecem funcionalidade completa para criar e gerenciar as trilhas.
> Se você configurou automação que usa um ou ambos os comandos, recomendamos que atualize seu código ou scripts para usar comandos suportados como create-trail.

Usar create-trail

Você pode usar o comando `create-trail` para criar trilhas que são especificamente configuradas para atender às suas necessidades de negócios. Ao usar o AWS CLI, lembre-se de que seus comandos são executados na AWS região configurada para seu perfil. Se você deseja executar os comandos em uma região diferente, altere a região padrão para o seu perfil ou use o parâmetro --region com o comando.

Criar uma trilha que se aplica a todas as regiões

Para criar uma trilha que se aplica a todas as regiões, use a opção `--is-multi-region-trail`. Por padrão, o comando `create-trail` cria uma trilha que registra eventos apenas na região da AWS em que a trilha foi criada. Para garantir que você registre eventos de serviços globais e capture todas as atividades de gerenciamento de eventos em sua AWS conta, crie trilhas que registrem eventos em todas as AWS regiões.

> **Note**
>
> Ao criar uma trilha, se você especificar um bucket do Amazon S3 que não foi criado com CloudTrail, você precisa anexar a política apropriada. Consulte Política de bucket do Amazon S3 para CloudTrail.

O exemplo a seguir cria uma trilha com o nome *`my-trail`* e uma tag com uma chave denominada *`Group`* com um valor de *`Marketing`* que fornece logs de todas as regiões a um bucket existente chamado *`my-bucket`*.

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name my-bucket --is-multi-
region-trail --tags-list [key=Group,value=Marketing]
```

Para confirmar se sua trilha existe em todas as regiões, o elemento `IsMultiRegionTrail` no resultado mostra `true`:

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": false,
    "S3BucketName": "my-bucket"
}
```

> **Note**
>
> Use o comando `start-logging` para iniciar o registro da sua trilha.

Inicie o registro da trilha

Depois que o comando `create-trail` for concluído, execute o comando `start-logging` para iniciar o registro dessa trilha.

> **Note**
>
> Quando você cria uma trilha com o CloudTrail console, o registro é ativado automaticamente.

O exemplo a seguir inicia o registro de uma trilha.

```
aws cloudtrail start-logging --name my-trail
```

Esse comando não retorna uma saída, mas você pode usar o comando `get-trail-status` para verificar se o registro foi iniciado.

```
aws cloudtrail get-trail-status --name my-trail
```

Para confirmar se a trilha está sendo registrada, o elemento `IsLogging` no resultado mostra `true`.

```
{
    "LatestDeliveryTime": 1441139757.497,
    "LatestDeliveryAttemptTime": "2015-09-01T20:35:57Z",
    "LatestNotificationAttemptSucceeded": "2015-09-01T20:35:57Z",
    "LatestDeliveryAttemptSucceeded": "2015-09-01T20:35:57Z",
    "IsLogging": true,
    "TimeLoggingStarted": "2015-09-01T00:54:02Z",
    "StartLoggingTime": 1441068842.76,
    "LatestDigestDeliveryTime": 1441140723.629,
    "LatestNotificationAttemptTime": "2015-09-01T20:35:57Z",
    "TimeLoggingStopped": ""
}
```

Criar uma trilha de região única

O comando a seguir cria uma trilha de região única. O bucket especificado do Amazon S3 já deve existir e ter as CloudTrail permissões apropriadas aplicadas. Para ter mais informações, consulte Política de bucket do Amazon S3 para CloudTrail.

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name my-bucket
```

Para ter mais informações, consulte Requisitos de nomenclatura.

A seguir, um exemplo de saída.

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": false,
    "IsOrganizationTrail": false,
    "S3BucketName": "my-bucket"
}
```

Criar uma trilha que se aplica a todas as regiões e que tem a validação do arquivo de log ativada

Para ativar a validação do arquivo de log ao usar `create-trail`, use a opção `--enable-log-file-validation`.

Para obter informações sobre a validação do arquivo de log, consulte Validando a integridade CloudTrail do arquivo de log.

O exemplo a seguir cria uma trilha que fornece logs de todas as regiões ao bucket especificado. O comando usa a opção `--enable-log-file-validation`.

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name my-bucket --is-multi-region-trail --enable-log-file-validation
```

Para confirmar se a validação do arquivo de log está ativada, o elemento `LogFileValidationEnabled` no resultado mostra `true`.

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": true,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": false,
    "S3BucketName": "my-bucket"
}
```

Usar update-trail

> **Important**
>
> Em 22 de novembro de 2021, AWS CloudTrail mudou a forma como as trilhas capturam eventos de serviços globais. Agora, os eventos criados pela Amazon CloudFront AWS Identity and Access Management, e AWS STS são registrados na região em que foram criados, a região Leste dos EUA (Norte da Virgínia), us-east-1. Isso faz com que a forma como CloudTrail trata esses serviços seja consistente com a de outros serviços AWS globais. Para continuar recebendo eventos de serviços globais fora do Leste dos EUA (Norte da Virgínia), certifique-se de converter as trilhas de região única que usam eventos de serviços globais fora do Leste dos EUA (Norte da Virgínia) para trilhas de várias regiões. Para obter mais informações sobre como capturar eventos de serviços globais, consulte Como habilitar e desabilitar o registro de eventos de serviços globais que aparece adiante nesta seção. Por outro lado, o histórico de eventos no CloudTrail console e o aws cloudtrail lookup-events comando mostrarão esses eventos no Região da AWS local em que eles ocorreram.

Você pode usar o comando `update-trail` para alterar as definições de configuração de uma trilha. Você também pode usar os comandos remove-tags e add-tags para adicionar e remover tags de uma trilha. Você só pode atualizar trilhas da AWS região em que a trilha foi criada (sua região de origem). Ao usar o AWS CLI, lembre-se de que seus comandos são executados na AWS região configurada para seu perfil. Se você deseja executar os comandos em uma região diferente, altere a região padrão para o seu perfil ou use o parâmetro --region com o comando.

Se você habilitou eventos CloudTrail de gerenciamento no Amazon Security Lake, é necessário manter pelo menos uma trilha organizacional que seja multirregional e `read` registre os eventos `write` de gerenciamento. Você não pode atualizar uma trilha de qualificação de uma forma que não atenda aos requisitos do Security Lake. Por exemplo, alterando a trilha para região única ou desativando o registro em log de eventos de gerenciamento de `read` ou `write`.

> **Note**
>
> Se você usar o AWS CLI ou um dos AWS SDKs para modificar uma trilha, verifique se a política de bucket da trilha é up-to-date. Para que seu bucket receba automaticamente eventos de um novo Região da AWS, a política deve conter o nome completo do serviço,`cloudtrail.amazonaws.com`. Para ter mais informações, consulte Política de bucket do Amazon S3 para CloudTrail.

Tópicos

- Converter uma trilha que se aplica a uma região para que ela se aplique a todas as regiões
- Converter uma trilha de várias regiões em uma trilha de região única
- Como habilitar e desabilitar o registro de eventos de serviços globais
- Ativar a validação do arquivo de log
- Desativar a validação do arquivo de log

Converter uma trilha que se aplica a uma região para que ela se aplique a todas as regiões

Para alterar uma trilha existente para que ela se aplique a todas as regiões, use a opção `--is-multi-region-trail`.

```
aws cloudtrail update-trail --name my-trail --is-multi-region-trail
```

Para confirmar se a trilha agora se aplica a todas as regiões, o elemento `IsMultiRegionTrail` no resultado mostra `true`.

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": false,
    "S3BucketName": "my-bucket"
}
```

Converter uma trilha de várias regiões em uma trilha de região única

Para alterar uma trilha de várias regiões existente de modo que ela se aplique somente à região na qual foi criada, use a opção `--no-is-multi-region-trail`.

```
aws cloudtrail update-trail --name my-trail --no-is-multi-region-trail
```

Para confirmar se a trilha agora se aplica a uma única região, o elemento `IsMultiRegionTrail` no resultado mostra `false`.

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": false,
    "IsOrganizationTrail": false,
    "S3BucketName": "my-bucket"
}
```

Como habilitar e desabilitar o registro de eventos de serviços globais

Para alterar uma trilha para que ela não registre eventos de serviços globais, use a opção `--no-include-global-service-events`.

```
aws cloudtrail update-trail --name my-trail --no-include-global-service-events
```

Para confirmar se a trilha não deve registrar eventos de serviços globais, o elemento `IncludeGlobalServiceEvents` no resultado deve mostrar `false`.

```
{
    "IncludeGlobalServiceEvents": false,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": false,
    "IsOrganizationTrail": false,
    "S3BucketName": "my-bucket"
}
```

Para alterar uma trilha para que ela registre eventos de serviços globais, use a opção `--include-global-service-events`.

As trilhas de região única não receberão mais eventos de serviços globais a partir de 22 de novembro de 2021, a menos que uma trilha já apareça na região Leste dos EUA (Norte da Virgínia), us-east-1. Para continuar capturando eventos de serviços globais, atualize a configuração da trilha para trilha de várias regiões. Por exemplo, esse comando atualiza uma trilha de região única na região Leste dos EUA (Ohio), us-east-2, para uma trilha de várias regiões. Substitua o *myExistingSingleRegionTrailWithGSE* pelo nome da trilha apropriada para sua configuração.

```
aws cloudtrail --region us-east-2 update-trail --
name myExistingSingleRegionTrailWithGSE --is-multi-region-trail
```

Como os eventos de serviços globais só estarão disponíveis no Leste dos EUA (Norte da Virgínia) a partir de 22 de novembro de 2021, você também pode criar uma trilha de região única para assinar eventos de serviços globais na região Leste dos EUA (Norte da Virgínia), us-east-1. O comando a seguir cria uma trilha de região única em us-east-1 para CloudFront receber, IAM e eventos: AWS STS

```
aws cloudtrail --region us-east-1 create-trail --include-global-service-events --
name myTrail --s3-bucket-name DOC-EXAMPLE-BUCKET
```

Ativar a validação do arquivo de log

Para ativar a validação do arquivo de log em uma trilha, use a opção `--enable-log-file-validation`. Os arquivos de resumo são fornecidos ao bucket do Amazon S3 dessa trilha.

```
aws cloudtrail update-trail --name my-trail --enable-log-file-validation
```

Para confirmar se a validação do arquivo de log está ativada, o elemento `LogFileValidationEnabled` no resultado mostra `true`.

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": true,
    "IsMultiRegionTrail": false,
    "IsOrganizationTrail": false,
    "S3BucketName": "my-bucket"
}
```

Desativar a validação do arquivo de log

Para desativar a validação do arquivo de log em uma trilha, use a opção `--no-enable-log-file-validation`.

```
aws cloudtrail update-trail --name my-trail-name --no-enable-log-file-validation
```

Para confirmar se a validação do arquivo de log está desativada, o elemento `LogFileValidationEnabled` no resultado mostra `false`.

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": false,
    "IsOrganizationTrail": false,
    "S3BucketName": "my-bucket"
}
```

Para validar arquivos de log com o AWS CLI, consulteValidando a integridade do arquivo de CloudTrail log com o AWS CLI.

Gerenciando trilhas com o AWS CLI

AWS CLI Isso inclui vários outros comandos que ajudam você a gerenciar suas trilhas. Esses comandos adicionam tags a trilhas, obtêm o status da trilha, iniciam e interrompem o registro de trilhas e excluem uma trilha. Você deve executar esses comandos na mesma AWS região em que a trilha foi criada (sua região de origem). Ao usar o AWS CLI, lembre-se de que seus comandos são executados na AWS região configurada para seu perfil. Se você deseja executar os comandos em uma região diferente, altere a região padrão para o seu perfil ou use o parâmetro --region com o comando.

Tópicos

Adicionar uma ou mais tags a uma trilha

Para adicionar uma ou mais tags a uma trilha existente, execute o comando add-tags.

O exemplo a seguir adiciona uma tag com o nome *Owner* (Proprietário) e o valor de *Mary* a uma trilha com o ARN *arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail* na região Leste dos EUA (Ohio).

```
aws cloudtrail add-tags --resource-id arn:aws:cloudtrail:us-
east-2:123456789012:trail/my-trail --tags-list Key=Owner,Value=Mary --region us-east-2
```

Se houver êxito, o comando não retornará nada.

Listar tags para uma ou mais trilhas

Para visualizar as tags associadas a uma ou mais trilhas existentes, use o comando list-tags.

O exemplo a seguir lista as tags de *Trail1* e *Trail2*.

```
aws cloudtrail list-tags --resource-id-list arn:aws:cloudtrail:us-
east-2:123456789012:trail/Trail1 arn:aws:cloudtrail:us-east-2:123456789012:trail/Trail2
```

Se houver êxito, o comando gerará uma saída semelhante à seguinte.

```
{
 "ResourceTagList": [
     {
         "ResourceId": "arn:aws:cloudtrail:us-east-2:123456789012:trail/Trail1",
         "TagsList": [
             {
                 "Value": "Alice",
                 "Key": "Name"
             },
             {
                 "Value": "Ohio",
                 "Key": "Location"
             }
         ]
     },
     {
         "ResourceId": "arn:aws:cloudtrail:us-east-2:123456789012:trail/Trail2",
         "TagsList": [
             {
                 "Value": "Bob",
                 "Key": "Name"
             }
         ]
     }
  ]
}
```

Remover uma ou mais tags de uma trilha

Para remover uma ou mais tags de uma trilha existente, execute o comando remove-tags.

O exemplo a seguir remove tags com os nomes *Location* (Localização) e *Name* (Nome) de uma trilha com o ARN *arn:aws:cloudtrail:us-east-2:123456789012:trail/Trail1* na região Leste dos EUA (Ohio).

```
aws cloudtrail remove-tags --resource-id arn:aws:cloudtrail:us-
east-2:123456789012:trail/Trail1 --tags-list Key=Name Key=Location --region us-east-2
```

Se houver êxito, o comando não retornará nada.

Recuperar as configurações de trilha e o status de uma trilha

Execute o `describe-trails` comando para recuperar informações sobre trilhas em uma AWS região. O exemplo a seguir retorna informações sobre as trilhas configuradas na região Leste dos EUA (Ohio).

```
aws cloudtrail describe-trails --region us-east-2
```

Se o comando for bem-sucedido, você verá um resultado semelhante a este.

```
{
  "trailList": [
    {
      "Name": "my-trail",
      "S3BucketName": "my-bucket",
      "S3KeyPrefix": "my-prefix",
      "IncludeGlobalServiceEvents": true,
      "IsMultiRegionTrail": true,
      "HomeRegion": "us-east-2"
      "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
      "LogFileValidationEnabled": false,
      "HasCustomEventSelectors": false,
      "SnsTopicName": "my-topic",
      "IsOrganizationTrail": false,
    },
    {
      "Name": "my-special-trail",
      "S3BucketName": "another-bucket",
      "S3KeyPrefix": "example-prefix",
      "IncludeGlobalServiceEvents": false,
      "IsMultiRegionTrail": false,
      "HomeRegion": "us-east-2",
      "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-special-trail",
      "LogFileValidationEnabled": false,
      "HasCustomEventSelectors": true,
      "IsOrganizationTrail": false
```

```
    },
    {
      "Name": "my-org-trail",
      "S3BucketName": "my-bucket",
      "S3KeyPrefix": "my-prefix",
      "IncludeGlobalServiceEvents": true,
      "IsMultiRegionTrail": true,
      "HomeRegion": "us-east-1"
      "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-org-trail",
      "LogFileValidationEnabled": false,
      "HasCustomEventSelectors": false,
      "SnsTopicName": "my-topic",
      "IsOrganizationTrail": true
    }
  ]
}
```

Execute o comando `get-trail` para recuperar informações de configurações sobre uma trilha específica. O exemplo a seguir retorna informações de configurações para uma trilha chamada *my-trail*.

```
aws cloudtrail get-trail - -name my-trail
```

Se houver êxito, o comando gerará uma saída semelhante à seguinte.

```
{
   "Trail": {
      "Name": "my-trail",
      "S3BucketName": "my-bucket",
      "S3KeyPrefix": "my-prefix",
      "IncludeGlobalServiceEvents": true,
      "IsMultiRegionTrail": true,
      "HomeRegion": "us-east-2"
      "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
      "LogFileValidationEnabled": false,
      "HasCustomEventSelectors": false,
      "SnsTopicName": "my-topic",
      "IsOrganizationTrail": false,
   }
}
```

Execute o comando `get-trail-status` para recuperar o status de uma trilha. Você deve executar esse comando na AWS região em que ele foi criado (a região de origem) ou especificar essa região adicionando o --region parâmetro.

> **Note**
>
> Se a trilha for uma trilha da organização e você for uma conta membro da organização em AWS Organizations, deverá fornecer o ARN completo dessa trilha, e não apenas o nome.

```
aws cloudtrail get-trail-status --name my-trail
```

Se o comando for bem-sucedido, você verá um resultado semelhante a este.

```
{
    "LatestDeliveryTime": 1441139757.497,
    "LatestDeliveryAttemptTime": "2015-09-01T20:35:57Z",
    "LatestNotificationAttemptSucceeded": "2015-09-01T20:35:57Z",
    "LatestDeliveryAttemptSucceeded": "2015-09-01T20:35:57Z",
    "IsLogging": true,
    "TimeLoggingStarted": "2015-09-01T00:54:02Z",
    "StartLoggingTime": 1441068842.76,
    "LatestDigestDeliveryTime": 1441140723.629,
    "LatestNotificationAttemptTime": "2015-09-01T20:35:57Z",
    "TimeLoggingStopped": ""
}
```

Além dos campos exibidos no código JSON anterior, o status conterá os seguintes campos, se houver erros do Amazon SNS ou do Amazon S3:

- `LatestNotificationError`. Contém o erro emitido pelo Amazon SNS se uma inscrição em um tópico falhar.
- `LatestDeliveryError`. Contém o erro emitido pelo Amazon S3 CloudTrail se não puder entregar um arquivo de log para um bucket.

Configurando seletores de eventos do CloudTrail Insights

Habilite eventos do Insights em uma trilha executando o put-insight-selectors, e especificando `ApiCallRateInsight`, `ApiErrorRateInsight` ou ambos como o valor do atributo

`InsightType`. Para visualizar as configurações do seletor do Insights para uma trilha, execute o comando `get-insight-selectors`. Você deve executar esse comando na AWS região em que a trilha foi criada (a região de origem) ou especificar essa região adicionando o --region parâmetro ao comando.

> **Note**
>
> Para registrar em log eventos do Insights para `ApiCallRateInsight`, a trilha deve registrar em log os eventos de gerenciamento de `write`. Para registrar em log eventos do Insights para `ApiErrorRateInsight`, a trilha deve registrar em log os eventos de gerenciamento de `read` ou `write`.

Exemplo: trilha que registra em log eventos do Insights

O exemplo a seguir é usado put-insight-selectors para criar um seletor de eventos do Insights para uma trilha chamada *`TrailName3`*. Isso permite a coleta de eventos do Insights para a trilha *`TrailName3`*. O seletor de eventos do Insights registra ambos`ApiErrorRateInsight` e `ApiCallRateInsight`Tipos de eventos do Insights.

```
aws cloudtrail put-insight-selectors --trail-name TrailName3 --insight-selectors
 '[{"InsightType": "ApiCallRateInsight"},{"InsightType": "ApiErrorRateInsight"}]'
```

O exemplo retorna o seletor de eventos do Insights que está configurado para a trilha.

```
{
   "InsightSelectors":
      [
         {
            "InsightType": "ApiErrorRateInsight"
         },
         {
            "InsightType": "ApiCallRateInsight"
         }
      ],
   "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName3"
}
```

Exemplo: desative a coleção de eventos do Insights

O exemplo a seguir é usado put-insight-selectors para remover o seletor de eventos do Insights para uma trilha chamada *TrailName3*. *Limpar a string JSON dos seletores do Insights desativa a coleta de eventos do Insights para a trilha 3. TrailName*

```
aws cloudtrail put-insight-selectors --trail-name TrailName3 --insight-selectors '[]'
```

O exemplo retorna o seletor de eventos do Insights que ficou vazio configurado para a trilha.

```
{
   "InsightSelectors": [ ],
   "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName3"
}
```

Configurar seletores de eventos

Para visualizar as configurações do seletor de eventos de uma trilha, execute o comando `get-event-selectors`. Você deve executar esse comando na AWS região em que ele foi criado (a região de origem) ou especificar essa região usando o --region parâmetro.

```
aws cloudtrail get-event-selectors --trail-name TrailName
```

> **Note**
>
> Se a trilha for uma trilha da organização e você for uma conta membro da organização em AWS Organizations, deverá fornecer o ARN completo dessa trilha, e não apenas o nome.

O exemplo a seguir retorna as configurações padrão de um seletor de eventos de uma trilha.

```
{
    "EventSelectors": [
        {
            "ExcludeManagementEventSources": [],
            "IncludeManagementEvents": true,
            "DataResources": [],
            "ReadWriteType": "All"
        }
    ],
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
```

```
}
```

Para criar um seletor de eventos, execute o comando `put-event-selectors`. Se você quiser registrar eventos do Insights na trilha, certifique-se de que o seletor de eventos habilite o registro dos tipos de Insights que você deseja configurar em sua trilha. Para obter mais informações sobre registrar eventos do Insights, consulte Registrar eventos do Insights.

Quando ocorre um evento em sua conta, CloudTrail avalia a configuração de suas trilhas. Se o evento corresponder a qualquer seletor de evento de uma trilha, ela processará e registrará o evento. Você pode configurar até 5 seletores de eventos para uma trilha e até 250 recursos de dados para uma trilha. Para ter mais informações, consulte Eventos de dados de log.

Tópicos

- Exemplo: trilha com seletores de eventos específicos
- Exemplo: trilha que registra em log todos os eventos de dados e de gerenciamento
- Exemplo de trilha que não registra AWS Key Management Service eventos
- Exemplo de trilha que registra eventos relevantes de baixo volume AWS Key Management Service
- Exemplo de trilha que não registra eventos de API de dados do Amazon RDS

Exemplo: trilha com seletores de eventos específicos

O exemplo a seguir cria um seletor de eventos para uma trilha nomeada *`TrailName`*para incluir eventos de gerenciamento somente para leitura e somente gravação, eventos de dados para duas combinações de bucket/prefixo do Amazon S3 e eventos de dados para uma única função chamada. AWS Lambda *`hello-world-python-function`*

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-selectors
 '[{"ReadWriteType": "All","IncludeManagementEvents": true,"DataResources":
 [{"Type":"AWS::S3::Object", "Values": ["arn:aws:s3:::mybucket/
prefix","arn:aws:s3:::mybucket2/prefix2"]},{"Type": "AWS::Lambda::Function","Values":
 ["arn:aws:lambda:us-west-2:999999999999:function:hello-world-python-function"]}]}]'
```

O exemplo a seguir retorna o seletor de eventos configurado para a trilha:

```
{
    "EventSelectors": [
        {
            "ExcludeManagementEventSources": [],
```

```
            "IncludeManagementEvents": true,
            "DataResources": [
                {
                    "Values": [
                        "arn:aws:s3:::mybucket/prefix",
                        "arn:aws:s3:::mybucket2/prefix2"
                    ],
                    "Type": "AWS::S3::Object"
                },
                {
                    "Values": [
                        "arn:aws:lambda:us-west-2:123456789012:function:hello-world-
python-function"
                    ],
                    "Type": "AWS::Lambda::Function"
                },
            ],
            "ReadWriteType": "All"
        }
    ],
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Exemplo: trilha que registra em log todos os eventos de dados e de gerenciamento

O exemplo a seguir cria um seletor de eventos para uma trilha chamada *TrailName2* que inclui todos os eventos, incluindo eventos de gerenciamento somente para leitura e somente gravação, e todos os eventos de dados para todos os buckets AWS Lambda , funções e tabelas do Amazon DynamoDB do Amazon S3 na conta. AWS Como esse exemplo usa seletores de eventos básicos, ele não pode configurar o registro de eventos do S3 em AWS Outposts, chamadas JSON-RPC do Amazon Managed Blockchain em nós Ethereum ou outros tipos de recursos de seletores de eventos avançados. Você deve usar seletores de eventos avançados para registrar eventos de dados para esses recursos. Para ter mais informações, consulte Configurar seletores de eventos avançados.

> **Note**
>
> Se a trilha se aplicar somente a uma região, somente eventos nessa região serão registrados, mesmo que os parâmetros do seletor de eventos especificarem todos os buckets do Amazon S3 e funções do Lambda. Os seletores de eventos se aplicam somente às regiões em que a trilha é criada.

```
aws cloudtrail put-event-selectors --trail-name TrailName2 --event-selectors
 '[{"ReadWriteType": "All","IncludeManagementEvents": true,"DataResources":
 [{"Type":"AWS::S3::Object", "Values": ["arn:aws:s3:::"]},{"Type":
 "AWS::Lambda::Function","Values": ["arn:aws:lambda"]},{"Type":
 "AWS::DynamoDB::Table","Values": ["arn:aws:dynamodb"]}]}]'
```

O exemplo a seguir retorna os seletores de eventos configurados para a trilha:

```
{
    "EventSelectors": [
        {
            "ExcludeManagementEventSources": [],
            "IncludeManagementEvents": true,
            "DataResources": [
                {
                    "Values": [
                        "arn:aws:s3:::"
                    ],
                    "Type": "AWS::S3::Object"
                },
                {
                    "Values": [
                        "arn:aws:lambda"
                    ],
                    "Type": "AWS::Lambda::Function"
                },
{
                    "Values": [
                        "arn:aws:dynamodb"
                    ],
                    "Type": "AWS::DynamoDB::Table"
                }
            ],
            "ReadWriteType": "All"
        }
    ],
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName2"
}
```

Exemplo de trilha que não registra AWS Key Management Service eventos

O exemplo a seguir cria um seletor de eventos para uma trilha chamada *TrailName* para incluir eventos de gerenciamento somente para leitura e somente gravação, mas para excluir eventos (). AWS Key Management Service AWS KMS Como AWS KMS os eventos são tratados como eventos de gerenciamento e podem haver um grande volume deles, eles podem ter um impacto substancial em sua CloudTrail fatura se você tiver mais de uma trilha que capture eventos de gerenciamento. O usuário neste exemplo optou por excluir eventos do AWS KMS de todas as trilhas, exceto uma. Para excluir uma origem de evento, adicione `ExcludeManagementEventSources` ao seletor de eventos e especifique uma origem de evento no valor da string.

Se você optar por não registrar eventos de gerenciamento, os AWS KMS eventos não serão registrados e você não poderá alterar as configurações do registro de AWS KMS eventos.

Para começar a registrar AWS KMS eventos em uma trilha novamente, passe uma matriz vazia como o valor de`ExcludeManagementEventSources`.

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "All","ExcludeManagementEventSources":
 ["kms.amazonaws.com"],"IncludeManagementEvents": true]}]'
```

O exemplo retorna o seletor de eventos configurado para a trilha.

```
{
    "EventSelectors": [
        {
            "ExcludeManagementEventSources": [ "kms.amazonaws.com" ],
            "IncludeManagementEvents": true,
            "DataResources": [],
            "ReadWriteType": "All"
        }
    ],
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Para começar a registrar AWS KMS eventos em uma trilha novamente, passe uma matriz vazia como o valor de`ExcludeManagementEventSources`, conforme mostrado no comando a seguir.

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "All","ExcludeManagementEventSources":
 [],"IncludeManagementEvents": true]}]'
```

Exemplo de trilha que registra eventos relevantes de baixo volume AWS Key Management Service

O exemplo a seguir cria um seletor de eventos para uma trilha chamada *TrailName* para incluir eventos e eventos de gerenciamento somente para gravação. AWS KMS Como AWS KMS os eventos são tratados como eventos de gerenciamento e podem haver um grande volume deles, eles podem ter um impacto substancial em sua CloudTrail fatura se você tiver mais de uma trilha que capture eventos de gerenciamento. O usuário neste exemplo optou por incluir eventos de AWS KMS gravação, que incluirão `Disable`, `Delete` e `ScheduleKey`, mas não incluirão mais ações de alto volume `Encrypt`, como `Decrypt`, e `GenerateDataKey` (agora são tratados como eventos de leitura).

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "WriteOnly","ExcludeManagementEventSources":
 [],"IncludeManagementEvents": true]}]'
```

O exemplo retorna o seletor de eventos configurado para a trilha. Isso registra eventos de gerenciamento somente para gravação, incluindo AWS KMS eventos.

```
{
    "EventSelectors": [
        {
            "ExcludeManagementEventSources": [],
            "IncludeManagementEvents": true,
            "DataResources": [],
            "ReadWriteType": "WriteOnly"
        }
    ],
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Exemplo de trilha que não registra eventos de API de dados do Amazon RDS

O exemplo a seguir cria um seletor de eventos para uma trilha nomeada *TrailName* para incluir eventos de gerenciamento somente para leitura e somente gravação, mas para excluir eventos da API de dados do Amazon RDS. Como os eventos da API de dados do Amazon RDS são tratados como eventos de gerenciamento e pode haver um grande volume deles, eles podem ter um impacto substancial em sua CloudTrail fatura se você tiver mais de uma trilha que capture eventos de gerenciamento. O usuário neste exemplo optou por excluir eventos do Amazon RDS Data API de todas as trilhas, exceto uma. Para excluir uma origem de evento, adicione

`ExcludeManagementEventSources` ao seletor de eventos e especifique uma fonte de evento do Amazon RDS Data API no valor da string: `rdsdata.amazonaws.com`.

Se você optar por não registrar eventos de gerenciamento, os eventos do Amazon RDS Data API não serão registrados e você não pode alterar as configurações de log de eventos.

Para começar a registrar novamente os eventos de gerenciamento da API de dados do Amazon RDS em uma trilha, passe uma matriz vazia como o valor de`ExcludeManagementEventSources`.

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "All","ExcludeManagementEventSources":
 ["rdsdata.amazonaws.com"],"IncludeManagementEvents": true]}]'
```

O exemplo retorna o seletor de eventos configurado para a trilha.

```
{
    "EventSelectors": [
        {
            "ExcludeManagementEventSources": [ "rdsdata.amazonaws.com" ],
            "IncludeManagementEvents": true,
            "DataResources": [],
            "ReadWriteType": "All"
        }
    ],
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Para começar a registrar novamente os eventos de gerenciamento da API de dados do Amazon RDS em uma trilha, passe uma matriz vazia como o valor de`ExcludeManagementEventSources`, conforme mostrado no comando a seguir.

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "All","ExcludeManagementEventSources":
 [],"IncludeManagementEvents": true]}]'
```

Configurar seletores de eventos avançados

Para usar seletores de evento avançado para incluir ou excluir eventos de dados em vez de seletores de eventos básicos, opte por usar seletores de eventos avançados na página de detalhes de uma trilha. Os seletores de eventos avançados permitem registrar eventos de dados em mais

tipos de recursos do que os seletores de eventos básicos. Os seletores básicos registram a atividade de objetos do S3, a atividade de execução da função do AWS Lambda e tabelas do DynamoDB.

Nos seletores de eventos avançados, crie uma expressão para coletar eventos de dados em tipos de recursos específicos, como buckets do S3, funções, tabelas do DynamoDB AWS Lambda , pontos de acesso do S3 Object Lambda, APIs diretas do Amazon EBS em snapshots do EBS, pontos de acesso do S3, fluxos do DynamoDB, tabelas criadas pelo Lake Formation e muito mais. AWS Glue

Para obter mais informações sobre seletores de eventos avançados, consulte Configurar seletores de eventos avançados.

Para visualizar as configurações do seletor de eventos avançados de uma trilha, execute o comando `get-event-selectors` a seguir. Você deve executar esse comando na AWS região em que a trilha foi criada (a região de origem) ou especificar essa região adicionando o --region parâmetro.

```
aws cloudtrail get-event-selectors --trail-name TrailName
```

> **Note**
>
> Se a trilha for uma trilha da organização e você estiver conectado com uma conta de membro na organização em AWS Organizations, deverá fornecer o ARN completo da trilha, e não apenas o nome.

O exemplo a seguir retorna as configurações padrão de um seletor de eventos avançado de uma trilha. Por padrão, nenhum seletor de evento avançado está configurado para uma trilha.

```
{
    "AdvancedEventSelectors": [],
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Para criar um seletor de eventos avançado, execute o comando `put-event-selectors`. Quando ocorre um evento de dados em sua conta, CloudTrail avalia a configuração de suas trilhas. Se o evento corresponder a qualquer seletor de evento avançado de uma trilha, ela processará e registrará o evento. Você pode configurar até 500 condições em uma trilha, incluindo todos os valores especificados para todos os seletores de eventos avançados em sua trilha. Para ter mais informações, consulte Eventos de dados de log.

Tópicos

- Exemplo de trilha com seletores de eventos avançados específicos
- Exemplo de trilha que usa seletores de eventos avançados personalizados para registrar o Amazon S3 AWS Outposts em eventos de dados
- Exemplo de trilha que usa seletores de eventos avançados para excluir AWS Key Management Service eventos
- Exemplo de trilha que usa seletores de eventos avançados para excluir eventos de gerenciamento da API de dados do Amazon RDS

Exemplo de trilha com seletores de eventos avançados específicos

O exemplo a seguir cria seletores de eventos avançados personalizados para uma trilha nomeada *TrailName* para incluir eventos de gerenciamento de leitura e gravação (omitindo o `readOnly` seletor) `PutObject` e eventos de `DeleteObject` dados para todas as combinações de bucket/prefixo do Amazon S3, exceto para um bucket chamado e eventos de dados para uma função chamada. `sample_bucket_name` AWS Lambda `MyLambdaFunction` Como estes são seletores de eventos avançados personalizados, cada conjunto de seletores tem um nome descritivo. Observe que uma barra à direita faz parte do valor ARN para buckets do S3.

```
aws cloudtrail put-event-selectors --trail-name TrailName --advanced-event-selectors
'[
  {
    "Name": "Log readOnly and writeOnly management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] }
    ]
  },
  {
    "Name": "Log PutObject and DeleteObject events for all but one bucket",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
      { "Field": "eventName", "Equals": ["PutObject","DeleteObject"] },
      { "Field": "resources.ARN", "NotStartsWith":
 ["arn:aws:s3:::sample_bucket_name/"] }
    ]
  },
  {
    "Name": "Log data plane actions on MyLambdaFunction",
```

```
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::Lambda::Function"] },
      { "Field": "resources.ARN", "Equals": ["arn:aws:lambda:us-
east-2:111122223333:function/MyLambdaFunction"] }
    ]
  }
]'
```

O exemplo retorna os seletores de eventos avançados configurados para a trilha.

```
{
  "AdvancedEventSelectors": [
    {
      "Name": "Log readOnly and writeOnly management events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Management" ]
        }
      ]
    },
    {
      "Name": "Log PutObject and DeleteObject events for all but one bucket",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Data" ]
        },
        {
          "Field": "resources.type",
          "Equals": [ "AWS::S3::Object" ]
        },
        {
          "Field": "resources.ARN",
          "NotStartsWith": [ "arn:aws:s3:::sample_bucket_name/" ]
        },
      ]
    },
{
      "Name": "Log data plane actions on MyLambdaFunction",
      "FieldSelectors": [
        {
```

```
          "Field": "eventCategory",
          "Equals": [ "Data" ]
        },
        {
          "Field": "resources.type",
          "Equals": [ "AWS::Lambda::Function" ]
        },
        {
          "Field": "eventName",
          "Equals": [ "Invoke" ]
        },
        {
          "Field": "resources.ARN",
          "Equals": [ "arn:aws:lambda:us-east-2:111122223333:function/
MyLambdaFunction" ]
        }
      ]
    }
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Exemplo de trilha que usa seletores de eventos avançados personalizados para registrar o Amazon S3 AWS Outposts em eventos de dados

O exemplo a seguir mostra como configurar sua trilha para incluir todos os eventos de dados de todo o Amazon S3 em AWS Outposts objetos em seu posto avançado. Nesta versão, o valor suportado para S3 em AWS Outposts eventos para o `resources.type` campo é`AWS::S3Outposts::Object`.

```
aws cloudtrail put-event-selectors --trail-name TrailName --region region \
--advanced-event-selectors \
'[
    {
            "Name": "OutpostsEventSelector",
            "FieldSelectors": [
                { "Field": "eventCategory", "Equals": ["Data"] },
                { "Field": "resources.type", "Equals": ["AWS::S3Outposts::Object"] }
            ]
        }
]'
```

Este comando retorna a saída de exemplo a seguir.

```
{
    "AdvancedEventSelectors": [
        {
            "Name": "OutpostsEventSelector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3Outposts::Object"
                    ]
                }
            ]
        }
    ],
  "TrailARN": "arn:aws:cloudtrail:region:123456789012:trail/TrailName"
}
```

Exemplo de trilha que usa seletores de eventos avançados para excluir AWS Key Management Service eventos

O exemplo a seguir cria um seletor de eventos avançado para uma trilha chamada *TrailName* para incluir eventos de gerenciamento somente para leitura e somente gravação (omitindo o `readOnly` seletor), mas para excluir eventos (). AWS Key Management Service AWS KMS Como AWS KMS os eventos são tratados como eventos de gerenciamento e podem haver um grande volume deles, eles podem ter um impacto substancial em sua CloudTrail fatura se você tiver mais de uma trilha que capture eventos de gerenciamento.

Se você optar por não registrar eventos de gerenciamento, os AWS KMS eventos não serão registrados e você não poderá alterar as configurações do registro de AWS KMS eventos.

Para começar a registrar AWS KMS eventos em uma trilha novamente, remova o `eventSource` seletor e execute o comando novamente.

```
aws cloudtrail put-event-selectors --trail-name TrailName \
```

```
--advanced-event-selectors '
[
  {
    "Name": "Log all management events except KMS events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] },
      { "Field": "eventSource", "NotEquals": ["kms.amazonaws.com"] }
    ]
  }
]'
```

O exemplo retorna os seletores de eventos avançados configurados para a trilha.

```
{
  "AdvancedEventSelectors": [
    {
      "Name": "Log all management events except KMS events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Management" ]
        },
        {
          "Field": "eventSource",
          "NotEquals": [ "kms.amazonaws.com" ]
        }
      ]
    }
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Para começar a registrar eventos excluídos para uma trilha novamente, remova o seletor `eventSource` e execute o comando novamente.

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] }
    ]
```

```
  }
]'
```

Exemplo de trilha que usa seletores de eventos avançados para excluir eventos de gerenciamento da API de dados do Amazon RDS

O exemplo a seguir cria um seletor de eventos avançado para uma trilha nomeada *TrailName* para incluir eventos de gerenciamento somente para leitura e somente gravação (omitindo o `readOnly` seletor), mas para excluir eventos de gerenciamento da API de dados do Amazon RDS. Para excluir eventos de gerenciamento da API de dados do Amazon RDS, especifique a origem do evento da API de dados do Amazon RDS no valor da string para o `eventSource` campo:. `rdsdata.amazonaws.com`

Se você optar por não registrar eventos de gerenciamento, os eventos de gerenciamento da API de dados do Amazon RDS não serão registrados e você não poderá alterar as configurações de registro de eventos da API de dados do Amazon RDS.

Para começar a registrar novamente os eventos de gerenciamento da API de dados do Amazon RDS em uma trilha, remova o `eventSource` seletor e execute o comando novamente.

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events except Amazon RDS Data API management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] },
      { "Field": "eventSource", "NotEquals": ["rdsdata.amazonaws.com"] }
    ]
  }
]'
```

O exemplo retorna os seletores de eventos avançados configurados para a trilha.

```
{
  "AdvancedEventSelectors": [
    {
      "Name": "Log all management events except Amazon RDS Data API management events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
```

```
          "Equals": [ "Management" ]
        },
        {
          "Field": "eventSource",
          "NotEquals": [ "rdsdata.amazonaws.com" ]
        }
      ]
    }
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Para começar a registrar eventos excluídos para uma trilha novamente, remova o seletor `eventSource` e execute o comando novamente.

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] }
    ]
  }
]'
```

Interromper e iniciar o registro de uma trilha

Os comandos a seguir iniciam e interrompem o CloudTrail registro.

```
aws cloudtrail start-logging --name awscloudtrail-example
```

```
aws cloudtrail stop-logging --name awscloudtrail-example
```

> **Note**
>
> Antes de excluir um bucket, execute o comando `stop-logging` para interromper o fornecimento de eventos ao bucket. Se você não parar de registrar, CloudTrail tentará entregar os arquivos de log em um bucket com o mesmo nome por um período limitado de tempo.

Se você parar de registrar ou excluir uma trilha, o CloudTrail Insights será desativado nessa trilha.

Excluir uma trilha

Se você habilitou eventos CloudTrail de gerenciamento no Amazon Security Lake, é necessário manter pelo menos uma trilha organizacional que seja multirregional e `read` registre os eventos `write` de gerenciamento. Você não pode excluir uma trilha se ela for a única trilha que atenda a esse requisito, a menos que você desative os eventos CloudTrail de gerenciamento no Security Lake.

Você pode excluir uma trilha com o comando a seguir. Só é possível excluir uma trilha na região em que ela foi criada (a região inicial).

```
aws cloudtrail delete-trail --name awscloudtrail-example
```

Ao excluir uma trilha, você não exclui o bucket do Amazon S3 ou o tópico do Amazon SNS associado a ela. Use a API de serviço AWS Management Console AWS CLI, ou para excluir esses recursos separadamente.

Criar uma trilha para uma organização

Se você criou uma organização em AWS Organizations, você pode criar uma trilha que registra todos os eventos de todos Contas da AWS nessa organização. Algumas vezes, ela é chamada de trilha da organização.

A conta de gerenciamento da organização pode atribuir um administrador delegado para criar novas ou gerenciar trilhas da organização existentes. Para obter mais informações sobre como adicionar um administrador delegado, consulte Adicionar um administrador CloudTrail delegado.

A conta de gerenciamento da organização pode editar uma trilha existente na conta e aplicá-la a uma organização, fazendo dela uma trilha da organização. As trilhas registram eventos para a conta de gerenciamento e todas as contas-membro da organização. Para obter mais informações sobre AWS Organizations, consulte Organizations Terminology and Concepts.

> **Note**
>
> Para criar uma trilha da organização, é necessário estar conectado com a conta de gerenciamento ou de administrador associada à organização. Você também deve ter permissões suficientes para que o usuário ou a função na conta gerencial ou de administrador delegado crie a trilha. Se não tiver permissões suficientes, você não terá a opção de aplicar a trilha a uma organização.

Todas as trilhas da organização criadas usando o console são trilhas da organização em várias regiões que registram eventos da conta habilitada Regiões da AWS em cada membro da organização. Para registrar eventos em todas as AWS partições da sua organização, crie uma trilha organizacional multirregional em cada partição. Você pode criar uma trilha organizacional de uma única região ou de várias regiões usando o. AWS CLI Se você criar uma trilha de região única, registrará atividades somente na trilha Região da AWS (também conhecida como Região de origem).

Embora a maioria Regiões da AWS esteja ativada por padrão para você Conta da AWS, você deve ativar manualmente determinadas regiões (também chamadas de regiões opcionais). Para obter informações sobre quais regiões estão habilitadas por padrão, consulte Considerações antes de ativar e desativar regiões no Guia de AWS Account Management referência. Para ver a lista de regiões CloudTrail compatíveis, consulteCloudTrail Regiões suportadas.

Quando você cria uma trilha da organização, uma cópia da trilha com o nome que você dá a ela é criada nas contas dos membros que pertencem à sua organização.

- Se a trilha da organização for para uma única região e a região de origem da trilha não for uma região OPT, uma cópia da trilha será criada na região de origem da trilha da organização na conta de cada membro.
- Se a trilha da organização for para uma única região e a região de origem da trilha for uma região OPT, uma cópia da trilha será criada na região de origem da trilha da organização nas contas dos membros que habilitaram essa região.
- Se a trilha da organização for multirregional e a região de origem da trilha não for uma região opcional, uma cópia da trilha será criada em cada uma habilitada Região da AWS na conta de cada membro. Quando uma conta de membro ativa uma região de adesão, uma cópia da trilha multirregional é criada na região recém-selecionada para a conta membro após a conclusão da ativação dessa região.

- Se a trilha da organização for multirregional e a região de origem for uma região opcional, as contas dos membros não enviarão atividades para a trilha da organização, a menos que optem pela trilha multirregional em Região da AWS que a trilha multirregional foi criada. Por exemplo, se você criar uma trilha multirregional e escolher a região da Europa (Espanha) como a região de origem da trilha, somente as contas dos membros que habilitaram a região da Europa (Espanha) para sua conta enviarão a atividade da conta para a trilha da organização.

> **Note**
>
> CloudTrail cria trilhas organizacionais nas contas dos membros, mesmo que a validação de um recurso falhe. Exemplos de falhas de validação incluem:
>
> - uma política incorreta de bucket do Amazon S3
> - uma política de tópicos incorreta do Amazon SNS
> - incapacidade de entregar para um grupo de CloudWatch registros de registros
> - permissão insuficiente para criptografar usando uma chave KMS
>
> Uma conta membro com CloudTrail permissões pode ver qualquer falha de validação de uma trilha da organização visualizando a página de detalhes da trilha no CloudTrail console ou executando o AWS CLI get-trail-statuscomando.

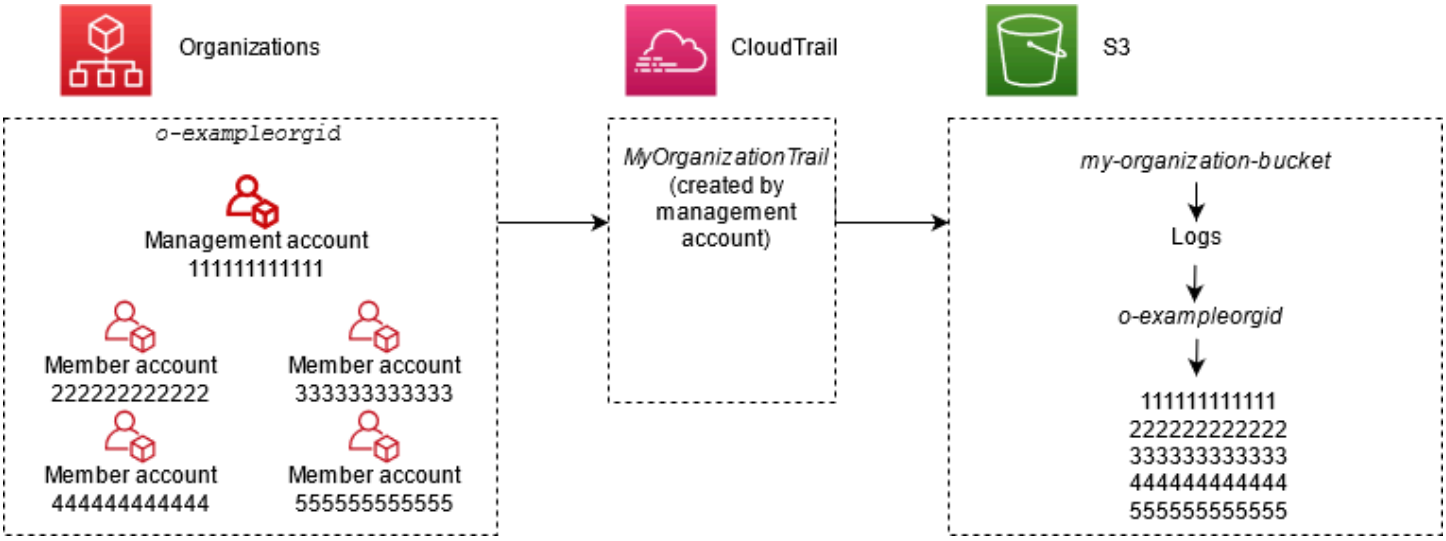
Os usuários com CloudTrail permissões nas contas dos membros podem ver as trilhas da organização quando fazem login no AWS CloudTrail console a partir de suas Contas da AWS contas ou quando executam AWS CLI comandos como`describe-trails`. No entanto, os usuários nas contas dos membros não têm permissões suficientes para excluir trilhas da organização, ativar ou desativar o login, alterar os tipos de eventos registrados ou alterar de alguma forma uma trilha da organização.

Quando você cria uma trilha da organização no console ou quando habilita CloudTrail como um serviço confiável no Organizations, isso cria uma função vinculada ao serviço para realizar tarefas de registro nas contas dos membros da sua organização. Essa função é AWSServiceRoleForCloudTrailnomeada e é necessária CloudTrail para registrar eventos de uma organização. Se um Conta da AWS for adicionado a uma organização, a trilha da organização e a função vinculada ao serviço serão adicionadas a ela Conta da AWS, e o registro dessa conta será iniciado automaticamente na trilha da organização. Se um Conta da AWS for removido de uma

organização, a trilha da organização e a função vinculada ao serviço serão excluídas da Conta da AWS que não faz mais parte da organização. No entanto, os arquivos de log da conta removida que foram criados antes da remoção da conta continuarão no bucket do Amazon S3, onde os arquivos de log são armazenados para a trilha.

Se a conta de gerenciamento de uma AWS Organizations organização criar uma trilha da organização, mas depois for removida como conta de gerenciamento da organização, qualquer trilha da organização criada usando sua conta se tornará uma trilha não organizacional.

No exemplo a seguir, a conta de gerenciamento da organização 111111111111 cria uma trilha chamada MyOrganizationTrailpara a organização o-example.orgid. A trilha registra a atividade de todas as contas da organização no mesmo bucket do Amazon S3. Todas as contas da organização podem ser vistas *MyOrganizationTrail*em sua lista de trilhas, mas as contas dos membros não podem remover ou modificar a trilha da organização. Somente a conta de gerenciamento ou a conta de administrador delegado pode alterar ou excluir a trilha para a organização. Somente a conta de gerenciamento pode remover uma conta-membro de uma organização. Da mesma forma, por padrão, somente a conta de gerenciamento tem acesso ao bucket do Amazon S3 *my-organization-bucket*para a trilha e aos registros contidos nela. A estrutura de bucket de alto nível para arquivos de log contém uma pasta com o nome do ID da organização e subpastas com os nomes dos IDs de cada conta da organização. Os eventos de cada conta-membro são registrados na pasta que corresponde ao ID da conta-membro. Se a conta do membro 444444444444 for removida da organização *MyOrganizationTrail*e a função vinculada ao serviço não aparecer mais na AWS conta 444444444444, e nenhum outro evento for registrado para essa conta pela trilha da organização. No entanto, a pasta 444444444444 permanece no bucket do Amazon S3, com todos os logs criados antes da remoção da conta da organização.



Neste exemplo, o ARN da trilha criada na conta de gerenciamento é `aws:cloudtrail:us-east-2:111111111111:trail/MyOrganizationTrail`. Esse também é o ARN da trilha em todas as contas-membro.

As trilhas da organização são semelhantes a trilhas regulares de muitas maneiras. É possível criar várias trilhas para a sua organização e optar por criar uma em todas as regiões ou em uma única região. Também é possível escolher quais tipos de eventos você deseja registrar na sua trilha da organização, assim como em qualquer outra trilha. No entanto, há algumas diferenças. Por exemplo, quando você cria uma trilha no console e escolhe se deseja registrar eventos de dados para buckets ou AWS Lambda funções do Amazon S3, os únicos recursos listados no CloudTrail console são aqueles da conta de gerenciamento, mas você pode adicionar os ARNs dos recursos nas contas dos membros. Os eventos de dados para recursos da conta-membro especificada são registrados sem a necessidade de configurar manualmente o acesso entre contas a esses recursos. Para obter mais informações sobre eventos de gerenciamento de registros, eventos do Insights e eventos de dados Log de eventos de gerenciamentoEventos de dados de log, consulte, Registrar eventos do Insights e.

> **Note**
>
> No console, você cria uma trilha multirregional. Essa é uma prática recomendada; registrar atividades em todas as suas regiões Conta da AWS ajuda a manter seu AWS ambiente mais seguro. Para criar uma trilha de região única, use a AWS CLI.

Ao visualizar eventos no Histórico de eventos de uma organização em AWS Organizations, você pode ver os eventos somente daquela Conta da AWS com a qual você está conectado. Por exemplo, se você estiver conectado à conta de gerenciamento da organização, Event history (Histórico de eventos) mostrará os últimos 90 dias de eventos de gerenciamento da conta de gerenciamento. Os eventos da conta-membro da organização não são mostrados emEvent history (Histórico de eventos) para a conta de gerenciamento. Para visualizar eventos de conta de membro em Event history (Histórico de eventos), inicie a sessão com a conta de membro.

Você pode configurar outros AWS serviços para analisar e agir com base nos dados de eventos coletados nos CloudTrail registros de uma trilha da organização da mesma forma que faria com qualquer outra trilha. Por exemplo, você pode analisar os dados em uma trilha da organização usando o Amazon Athena. Para ter mais informações, consulte AWS integrações de serviços com registros CloudTrail .

Tópicos

Passando das trilhas da conta de membro para as trilhas da organização

Se você já tem CloudTrail trilhas configuradas para contas de membros individuais, mas deseja ir para uma trilha da organização para registrar eventos em todas as contas, não quer perder eventos excluindo trilhas de contas de membros individuais antes de criar uma trilha da organização. No entanto, quando você tem duas trilhas, são gerados custos mais altos por conta da cópia adicional de eventos entregues à trilha da organização.

Para ajudar a gerenciar os custos, mas evitar a perda de eventos antes que a entrega de logs seja iniciada na trilha da organização, considere manter as trilhas de contas-membro individuais e a trilha da organização por até um dia. Isso garante que a trilha da organização registre em log todos os eventos, mas serão gerados custos de eventos duplicados apenas por um dia. Após o primeiro dia, é possível interromper o registro em log (ou excluir) qualquer trilha de conta-membro individual.

Preparar a criação de uma trilha para sua organização

Antes de criar uma trilha para sua organização, verifique se a conta de gerenciamento ou conta de administrador delegado está configurada corretamente para a criação de trilha.

- Sua organização deve ter todos os recursos habilitados antes de você criar uma trilha para ela. Para obter mais informações, consulte Habilitar todos os recursos na sua organização.
- A conta de gerenciamento deve ter a função do AWSServiceRoleForOrganizations. Essa função é criada automaticamente pelo Organizations quando você cria sua organização e é necessária CloudTrail para registrar eventos de uma organização. Para obter mais informações, consulte Organizations e funções vinculadas ao serviço.
- O perfil ou usuário do IAM que cria a trilha da organização na conta de gerenciamento ou de administrador delegado deve ter permissões suficientes para criar uma trilha da organização. É necessário pelo menos aplicar a política AWSCloudTrail_FullAccess ou uma política equivalente a esse perfil ou usuário. Você também deve ter permissões suficientes no IAM e no Organizations para criar a função vinculada ao serviço e habilitar o acesso confiável. Se você optar por criar

um novo bucket do S3 para uma trilha da organização usando o CloudTrail console, sua política também precisa incluir o `s3:PutEncryptionConfiguration` ação porque, por padrão, a criptografia do lado do servidor está habilitada para o bucket. A política de exemplo a seguir mostra as permissões mínimas necessárias.

> **Note**
>
> Você não deve compartilhar a AWSCloudTrail_FullAccesspolítica de forma ampla com todos os seus Conta da AWS. Em vez disso, você deve restringi-lo Conta da AWS aos administradores devido à natureza altamente confidencial das informações coletadas pelo CloudTrail. Os usuários com esse perfil têm a capacidade de desabilitar ou reconfigurar as funções de auditoria mais confidenciais e importantes em suas Contas da AWS. Por esse motivo, é necessário controlar e monitorar de perto o acesso a essa política.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iam:GetRole",
                "organizations:EnableAWSServiceAccess",
                "organizations:ListAccounts",
                "iam:CreateServiceLinkedRole",
                "organizations:DisableAWSServiceAccess",
                "organizations:DescribeOrganization",
                "organizations:ListAWSServiceAccessForOrganization",
                "s3:PutEncryptionConfiguration"
            ],
            "Resource": "*"
        }
    ]
}
```

- Para usar as APIs AWS CLI ou as CloudTrail APIs para criar uma trilha organizacional, você deve habilitar o acesso confiável para CloudTrail in Organizations e criar manualmente um bucket do Amazon S3 com uma política que permita o registro de uma trilha organizacional. Para ter mais informações, consulte Criando uma trilha para uma organização com o AWS Command Line Interface.

- Para usar uma função do IAM existente para adicionar monitoramento de uma trilha da organização ao Amazon CloudWatch Logs, você deve modificar manualmente a função do IAM para permitir a entrega de CloudWatch registros das contas membros ao grupo CloudWatch Logs da conta de gerenciamento, conforme mostrado no exemplo a seguir.

> **Note**
>
> Você deve usar uma função do IAM e um grupo de CloudWatch registros de registros que exista em sua própria conta. Você não pode usar uma função do IAM ou um grupo de CloudWatch registros de registros de propriedade de uma conta diferente.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailCreateLogStream20141101",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream"
            ],
            "Resource": [
                "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:111111111111_CloudTrail_us-east-2*",
                "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:o-exampleorgid_*"
            ]
        },
        {
            "Sid": "AWSCloudTrailPutLogEvents20141101",
            "Effect": "Allow",
            "Action": [
                "logs:PutLogEvents"
            ],
            "Resource": [
                "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:111111111111_CloudTrail_us-east-2*",
                "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:o-exampleorgid_*"
            ]
        }
```

```
    ]
}
```

Você pode aprender mais sobre o CloudTrail Amazon CloudWatch Logs inMonitoramento CloudTrail de arquivos de log com o Amazon CloudWatch Logs. Além disso, considere os limites dos CloudWatch registros e as considerações de preço do serviço antes de decidir habilitar a experiência para uma trilha organizacional. Para obter mais informações, consulte Limites de CloudWatch registros e CloudWatchpreços da Amazon.

- Para registrar eventos de dados na trilha da organização para recursos em contas-membro, tenha pronta uma lista de nomes de recurso da Amazon (ARN) para cada um desses recursos. Os recursos da conta do membro não são exibidos no CloudTrail console quando você cria uma trilha; você pode procurar recursos na conta de gerenciamento na qual a coleta de eventos de dados é suportada, como buckets do S3. Da mesma forma, se você quiser adicionar recursos de membro específicos ao criar ou atualizar uma trilha da organização na linha de comando, precisará dos ARNs desses recursos.

> **Note**
>
> Há cobranças adicionais para o registro de eventos de dados. Para CloudTrail saber os preços, consulte AWS CloudTrail Preços.

Você também deve analisar quantas trilhas já existem na conta de gerenciamento e nas contas dos membros antes de criar uma trilha da organização. CloudTrail limita o número de trilhas que podem ser criadas em cada região. Você não pode exceder esse limite na região em que cria a trilha da organização na conta de gerenciamento. No entanto, ela será criada nas contas-membro mesmo que elas tenham atingido o limite de trilhas em uma região. Embora a primeira trilha de eventos de gerenciamento em qualquer região seja gratuita, as trilhas adicionais são cobradas. Para reduzir o possível custo de uma trilha da organização, considere excluir qualquer trilha desnecessária nas contas de gerenciamento e membro. Para obter mais informações sobre CloudTrail preços, consulte AWS CloudTrail Preços.

Práticas recomendadas de segurança nas trilhas da organização

Como uma prática recomendada de segurança, sugerimos adicionar a `aws:SourceArn` chave de condição para políticas de recursos (como aquelas para buckets do S3, chaves KMS ou tópicos do SNS) que você usa com uma trilha da organização. O valor de `aws:SourceArn` é o ARN da trilha da organização (ou ARNs, se você estiver usando o mesmo recurso para mais de uma trilha, como o

mesmo bucket do S3 para armazenar logs de mais de uma trilha). Isso garante que o recurso, como um bucket do S3, aceite somente dados associados à trilha específica. O ARN de trilha deve usar a ID da conta da conta de gerenciamento. O trecho de política a seguir mostra um exemplo em que mais de uma trilha está usando o recurso.

```
"Condition": {
    "StringEquals": {
      "aws:SourceArn": ["Trail_ARN_1",..., "Trail_ARN_n"]
    }
}
```

Para obter informações sobre como adicionar chaves de condição às políticas de recursos, consulte o seguinte:

- Política de bucket do Amazon S3 para CloudTrail
- Configure as AWS KMS principais políticas para CloudTrail
- Política de tópicos do Amazon SNS para CloudTrail

Criar uma trilha para sua organização no console

Para criar uma trilha da organização a partir do CloudTrail console, você deve entrar no console como usuário ou função na conta de gerenciamento ou de administrador delegado que tenha permissões suficientes. Se você não entrar com a conta de gerenciamento ou de administrador delegado, não verá a opção de aplicar uma trilha a uma organização ao criar ou editar uma trilha no CloudTrail console.

Você pode configurar uma trilha da organização de várias maneiras. Por exemplo, é possível configurar os seguintes detalhes para sua trilha da organização:

- Por padrão, quando você cria uma trilha no console, a trilha registra em log todas as Regiões da AWS na partição da AWS na qual você está trabalhando. Como prática recomendada, é altamente recomendável registrar eventos em todas as regiões do seu Conta da AWS. Para criar uma trilha para uma região única, use a AWS CLI.
- Especifique se deseja aplicar a trilha à sua organização. Por padrão, as trilhas não são aplicadas a organizações. É necessário escolher essa opção para criar uma trilha da organização.
- Especifique qual bucket do Amazon S3 recebe arquivos de log para a trilha da organização. Você pode escolher um bucket existente do Amazon S3 ou criar um especificamente para a trilha da organização.

- Para o gerenciamento e os eventos de dados, especifique se você deseja registrar eventos Read (Leitura), Write (Gravação) ou ambos. CloudTrailOs eventos do Insights são registrados somente em eventos de gerenciamento. Você pode especificar o registro de eventos de dados para a conta de gerenciamento escolhendo-os nas listas do console e nas contas-membro, se você especificar os ARNs de cada recurso para o qual deseja habilitar o registro de eventos de dados. Para ter mais informações, consulte Eventos de dados.

Para criar uma trilha organizacional com o AWS Management Console

1. Faça login no AWS Management Console e abra o CloudTrail console em https://console.aws.amazon.com/cloudtrail/.

   É necessário estar conectado como uma identidade do IAM na conta de gerenciamento ou de administrador delegado com permissões suficientes para criar uma trilha da organização.
2. Escolha Trails (Trilhas) e, depois Create trail (Criar trilha).
3. Na página Create Trail (Criar trilha), em Trail name (Nome da trilha), digite um nome para a sua trilha. Para ter mais informações, consulte Requisitos de nomenclatura.
4. Selecione Enable for all accounts in my organization (Habilitar para todas as contas na minha organização). Você só verá essa opção se estiver conectado ao console com um perfil ou um usuário na conta de gerenciamento ou de administrador delegado. Para criar uma trilha da organização, verifique se o usuário ou a função tem permissões suficientes.
5. Em Storage location (Local de armazenamento), escolha Create a S3 bucket (Criar um bucket do S3) para criar um bucket. Quando você cria um bucket, CloudTrail cria e aplica as políticas de bucket necessárias.

   > **Note**
   >
   > Se você escolheu Use existing S3 bucket (Usar bucket do S3 existente), especifique um bucket em Trail log bucket name (Nome do bucket de log de trilha), ou escolha Browse (Procurar) para escolher um bucket. Você pode escolher um bucket pertencente a qualquer conta, no entanto, a política do bucket deve conceder CloudTrail permissão para gravar nele. Para obter informações sobre como editar manualmente a política de bucket, consulte Política de bucket do Amazon S3 para CloudTrail.

Para facilitar a localização de seus registros, crie uma nova pasta (também conhecida como prefixo) em um bucket existente para armazenar seus CloudTrail registros. Insira o prefixo em Prefix (Prefixo).

6. Em Log file SSE-KMS encryption (Criptografia de arquivo de log com SSE-KMS), escolha Enabled (Habilitado) se quiser criptografar os arquivos de log com criptografia SSE-KMS em vez de criptografia SSE-S3. O padrão é Enabled (Habilitado). Se você não habilitar a criptografia SSE-SKMS, seus registros serão criptografados usando a criptografia SSE-S3. Para obter mais informações sobre a criptografia SSE-KMS, consulte Uso de criptografia no lado do servidor com o AWS Key Management Service [SSE-KMS]. Para obter mais informações sobre a criptografia SSE-S3, consulte Using Server-Side Encryption with Amazon S3-Managed Encryption Keys (SSE-S3) (Uso de criptografia no lado do servidor com chaves de criptografia gerenciadas pelo Amazon S3 [SSE-S3]).

   Se você habilitar a criptografia SSE-KMS, escolha Nova ou Existente. AWS KMS key Em AWS KMS Alias, especifique um alias, no formato. `alias/` *`MyAliasName`* Para ter mais informações, consulte Atualizar um recurso para usar sua chave do KMS.

   > **Note**
   >
   > Você também pode digitar o Nome de região da Amazon (ARN) de uma chave de outra conta. Para ter mais informações, consulte Atualizar um recurso para usar sua chave do KMS. A política de chaves deve permitir CloudTrail o uso da chave para criptografar seus arquivos de log e permitir que os usuários que você especificar leiam os arquivos de log em formato não criptografado. Para obter informações sobre como editar manualmente a política de chaves, consulte Configure as AWS KMS principais políticas para CloudTrail.

7. Em Additional settings (Configurações adicionais), configure as opções a seguir.

   a. Em Log file validation (Validação de arquivo de log), escolha Enabled (Habilitado) para receber resumos de log no seu bucket do S3. Você pode usar os arquivos de resumo para verificar se seus arquivos de log não foram alterados após CloudTrail serem entregues. Para ter mais informações, consulte Validando a integridade CloudTrail do arquivo de log.

   b. Para entrega de notificações do SNS, escolha Ativado para ser notificado sempre que um registro for entregue ao seu bucket. CloudTrail armazena vários eventos em um arquivo de log. As notificações do SNS são enviadas para todos os arquivos de log, não para todos os

eventos. Para ter mais informações, consulte Configurando notificações do Amazon SNS para CloudTrail.

Se você habilitar notificações do SNS, para Create a new SNS topic (Criar um tópico do SNS), escolha New (Novo) para criar um tópico ou escolha Existing (Existente) para usar um tópico existente. Se criar uma trilha aplicável a todas as regiões, as notificações do SNS sobre a entrega de arquivos de log de todas as regiões serão enviadas ao único tópico do SNS que você criar.

Se você escolher Novo, CloudTrail especifica um nome para o novo tópico para você ou pode digitar um nome. Se escolher Existing (Existente), escolha um tópico do SNS na lista suspensa. Você também pode inserir o Nome de região da Amazon (ARN) de um tópico de outra região ou de uma conta com permissões apropriadas. Para ter mais informações, consulte Política de tópicos do Amazon SNS para CloudTrail.

Se você criar um tópico, precisará se inscrever nele para ser notificado sobre a entrega de arquivos de log. Você pode se inscrever no console do Amazon SNS. Devido à frequência das notificações, recomendamos que você configure a inscrição para usar uma fila do Amazon SQS para gerenciar as notificações de modo programático. Para obter mais informações, consulte Conceitos básicos do Amazon SNS no Guia do desenvolvedor do Amazon Simple Notification Service.

8. Opcionalmente, configure CloudTrail para enviar arquivos de log para o CloudWatch Logs escolhendo Habilitado em CloudWatch Registros. Para ter mais informações, consulte Envio de eventos para o CloudWatch Logs.

> **Note**
>
> Somente a conta de gerenciamento pode configurar um grupo de CloudWatch registros de registros para uma trilha da organização usando o console. O administrador delegado pode configurar um grupo de CloudWatch registros de registros usando as operações AWS CLI ou CloudTrail `CreateTrail` ou `UpdateTrail` da API.

   a. Se você habilitar a integração com CloudWatch Logs, escolha Novo para criar um novo grupo de registros ou Existente para usar um existente. Se você escolher Novo, CloudTrail especifica um nome para o novo grupo de registros para você ou pode digitar um nome.

   b. Se escolher Existing (Existente), escolha um grupo de logs na lista suspensa.

c. Escolha Novo para criar uma nova função do IAM para obter permissões para enviar registros para o CloudWatch Logs. Escolha Existing (Existente) para escolher uma função do IAM existente na lista suspensa. A declaração de política para a função nova ou existente é exibida quando você expande Policy document (Documento de política). Para obter mais informações sobre essa função, consulte Documento de política de funções CloudTrail para usar CloudWatch registros para monitoramento.

> **Note**
>
> Quando você configura uma trilha, é possível escolher um bucket do S3 e um tópico do Amazon SNS que pertençam a outra conta. No entanto, se você quiser CloudTrail entregar eventos a um grupo de CloudWatch registros de registros, deverá escolher um grupo de registros que exista na sua conta atual.

9. Para Tags, adicione uma ou mais tags personalizadas (pares chave-valor) à sua trilha. As tags podem ajudá-lo a identificar suas CloudTrail trilhas e os buckets do Amazon S3 que contêm CloudTrail arquivos de log. Em seguida, você pode usar grupos de recursos para seus CloudTrail recursos. Para obter mais informações, consulte AWS Resource Groups e Tags.
10. Na página Choose log events (Escolher eventos de log), escolha os tipos de eventos que você deseja registrar. Em Management events (Eventos de gerenciamento), faça o indicado a seguir.

    a. Em API activity (Atividade da API), escolha se você deseja que sua trilha registre eventos Read (Leitura), Write (Gravação) ou ambos. Para ter mais informações, consulte Eventos de gerenciamento.

    b. Escolha Excluir AWS KMS eventos para filtrar AWS Key Management Service (AWS KMS) eventos da sua trilha. A configuração padrão é incluir todos os eventos do AWS KMS .

    A opção de registrar ou excluir AWS KMS eventos está disponível somente se você registrar eventos de gerenciamento em sua trilha. Se você optar por não registrar eventos de gerenciamento, os AWS KMS eventos não serão registrados e você não poderá alterar as configurações do registro de AWS KMS eventos.

    AWS KMS ações como`Encrypt`,`Decrypt`, e `GenerateDataKey` normalmente geram um grande volume (mais de 99%) de eventos. Agora essas ações são registradas em log como eventos de Leitura. AWS KMS Ações relevantes de baixo volume, como **`DisableDelete`**, e **`ScheduleKey`** (que normalmente representam menos de 0,5% do volume de AWS KMS eventos) são registradas como eventos de gravação.

Para excluir eventos de alto volume, como `Encrypt`, `Decrypt` e `GenerateDataKey`, mas ainda registra eventos relevantes como `Disable`, `Delete` e `ScheduleKey`, escolha para registrar Write (Gravação) e desmarque a caixa de seleção para Exclude AWS KMS events (Excluir eventos do KMS).

c. Escolha Exclude Amazon RDS Data API events (Excluir eventos da API de dados do Amazon RDS) para filtrar eventos da API de dados do Amazon Relational Database Service fora da trilha. A configuração padrão é incluir todos os eventos da API de dados do Amazon RDS. Para obter mais informações sobre eventos da API de dados do Amazon RDS, consulte Registrar em log chamadas da API de dados com o AWS CloudTrail no Manual do usuário do Amazon RDS for Aurora.

11. Para registrar eventos de dados, escolha Data events (Eventos de dados). Há cobranças adicionais para o registro de eventos de dados. Para obter mais informações, consulte Preços do AWS CloudTrail.

12.

> **Important**
>
> As etapas 12 a 16 devem ser usadas para configurar eventos de dados usando seletores de eventos avançados, que é o padrão. Os seletores de eventos avançados permitem que você configure mais tipos de eventos de dados e oferecem um controle mais preciso sobre quais eventos de dados são capturados por sua trilha. Se você optou por usar seletores de eventos básicos, conclua as etapas em Configurar opções de eventos de dados utilizando seletores de eventos básicos e retorne à etapa 17 desse procedimento.

Em Data event type (Tipo de evento de dados), escolha o tipo de recurso no qual você deseja registrar eventos de dados. Para obter mais informações sobre os tipos de eventos de dados disponíveis, consulte Eventos de dados.

> **Note**
>
> Para registrar eventos de dados para AWS Glue tabelas criadas pelo Lake Formation, escolha Lake Formation.

13. Escolha um modelo de seletor de registros. CloudTrail inclui modelos predefinidos que registram todos os eventos de dados do tipo de recurso. Para criar um modelo de seletor de log personalizado, escolha Custom (Personalizado).

> **Note**
>
> A escolha de um modelo predefinido para buckets do S3 permite o registro de eventos de dados de todos os buckets atualmente em sua AWS conta e de todos os buckets que você criar depois de concluir a criação da trilha. Ele também permite o registro da atividade de eventos de dados realizada por qualquer identidade do IAM em sua AWS conta, mesmo que essa atividade seja realizada em um bucket que pertença a outra AWS conta.
>
> Se a trilha se aplicar somente a uma região, a escolha da opção Select all S3 buckets in your account (Selecionar todos os buckets do S3 em sua conta) habilitará o registro de eventos de dados para todos os buckets do S3 na mesma região que a trilha e todos os buckets que você criar posteriormente nessa região. Os eventos de dados não serão registrados para os buckets do Amazon S3 em outras regiões em sua conta da AWS .
>
> Se você estiver criando uma trilha para todas as regiões, a escolha de um modelo predefinido para as funções do Lambda permite o registro de eventos de dados para todas as funções atualmente em AWS sua conta e para quaisquer funções do Lambda que você possa criar em qualquer região depois de terminar de criar a trilha. Se você estiver criando uma trilha para uma única região (feita usando o AWS CLI), essa seleção habilita o registro de eventos de dados para todas as funções atualmente nessa região em sua AWS conta e quaisquer funções Lambda que você possa criar nessa região depois de terminar de criar a trilha. Essa opção não permite o registro de eventos de dados para funções do Lambda criadas em outras regiões.
>
> O registro de eventos de dados para todas as funções também permite o registro da atividade de eventos de dados realizada por qualquer identidade do IAM em sua AWS conta, mesmo que essa atividade seja realizada em uma função que pertence a outra AWS conta.

14. (Opcional) Em Nome do seletor, insira um nome para identificar o seletor. O nome do seletor é um nome descritivo para um seletor de eventos avançado, como "Registrar eventos de dados em log para apenas dois buckets do S3". O nome do seletor é listado como `Name` no seletor de eventos avançado e poderá ser visualizado se você expandir a visualização JSON.
15. Em Advanced event selectors (Seletores de eventos avançados), crie uma expressão para os recursos específicos nos quais você deseja registrar eventos de dados. Você poderá ignorar esta etapa se estiver usando um modelo de log predefinido.

    a. Escolha um dos seguintes campos:

- **`readOnly`**- `readOnly` pode ser definido como igual a um valor de `true` ou. `false` Eventos de dados somente leitura são eventos que não alteram o estado de um recurso, como `Get*` ou `Describe*`. Eventos de gravação adicionam, alteram ou excluem recursos, atributos ou artefatos, como `Put*`, `Delete*` ou `Write*`. Para registrar os eventos `read` e `write`, não adicione um seletor `readOnly`.
- **`eventName`** - `eventName` pode usar qualquer operador. Você pode usá-lo para incluir ou excluir qualquer evento de dados registrado CloudTrail, como `PutBucketPutItem`, ou`GetSnapshotBlock`.
- **`resources.ARN`**- Você pode usar qualquer operador com`resources.ARN`, mas se usar igual ou diferente, o valor deverá corresponder exatamente ao ARN de um recurso válido do tipo que você especificou no modelo como valor de. `resources.type`

  A tabela a seguir mostra o formato de ARN válido para cada `resources.type`.

  > **Note**
  >
  > Você não pode usar o `resources.ARN` campo para filtrar tipos de recursos que não tenham ARNs.

resources.type	resources.ARN
`AWS::DynamoDB::Table` [1]	`arn:partition :dynamodb : region:account_ID :table/table_name`
`AWS::Lambda::Function`	`arn:partition :lambda:region:account_ID :function: function_name`
`AWS::S3::Object` [2]	`arn:partition :s3:::bucket_name / arn:partition :s3:::bucket_name /object_or_file_name /`

resources.type	resources.ARN
AWS::AppConfig::Configuration	arn:*partition* :appconfig: *region*:*account_ID* :application/ *application_ID* /environment/ *environment_ID* /configuration/ *configuration_profile_ID*
AWS::B2BI::Transformer	arn:*partition* :b2bi:*region*:*account_ID* :transformer/ *transformer_ID*
AWS::Bedrock::AgentAlias	arn:*partition* :bedrock: *region*:*account_ID* :agent-alias/ *agent_ID*/*alias_ID*
AWS::Bedrock::KnowledgeBase	arn:*partition* :bedrock: *region*:*account_ID* :knowledge-base/*knowledge_base_ID*
AWS::Cassandra::Table	arn:*partition* :cassandra: *region*:*account_ID* :keyspace/ *keyspace_name* /table/*table_name*
AWS::CloudFront::KeyValueStore	arn:*partition* :cloudfront: *region*:*account_ID* :key-value-store/*KVS_name*
AWS::CloudTrail::Channel	arn:*partition* :cloudtrail: *region*:*account_ID* :channel/ *channel_UUID*
AWS::CodeWhisperer::Customization	arn:*partition* :codewhisperer: *region*:*account_ID* :customization/ *customization_ID*

resources.type	resources.ARN
AWS::CodeWhisperer::Profile	arn:*partition* :codewhis perer: *region*:*account_ID* :profile/ *profile_ID*
AWS::Cognito::IdentityPool	arn:*partition* :cognito-identity: *region*:*account_ID* :identity pool/ *identity_pool_ID*
AWS::DynamoDB::Stream	arn:*partition* :dynamodb : *region*:*account_ID* :table/*table_name* / stream/*date_time*
AWS::EC2::Snapshot	arn:*partition* :ec2:*region*::snapsho t/ *snapshot_ID*
AWS::EMRWAL::Workspace	arn:*partition* :emrwal:*region*:*account_I D* :workspace/ *workspace_name*
AWS::FinSpace::Environment	arn:*partition* :finspace : *region*:*account_ID* :environm ent/ *environment_ID*
AWS::Glue::Table	arn:*partition* :glue:*region*:*account_I D* :table/*database_name* /*table_name*
AWS::GreengrassV2::Componen tVersion	arn:*partition* :greengra ss: *region*:*account_ID* :componen ts/ *component_name*
AWS::GreengrassV2::Deployment	arn:*partition* :greengra ss: *region*:*account_ID* :deployme nts/ *deployment_ID*

resources.type	resources.ARN
AWS::GuardDuty::Detector	arn:*partition* :guarddut y: *region*:*account_ID* :detector / *detector_ID*
AWS::IoT::Certificate	arn:*partition* :iot:*region*:*account_I D* :cert/*certificate_ID*
AWS::IoT::Thing	arn:*partition* :iot:*region*:*account_I D* :thing/*thing_ID*
AWS::IoTSiteWise::Asset	arn:*partition* :iotsitew ise: *region*:*account_ID* :asset/*asset_ID*
AWS::IoTSiteWise::TimeSeries	arn:*partition* :iotsitew ise: *region*:*account_ID* :timeseri es/ *timeseries_ID*
AWS::IoTTwinMaker::Entity	arn:*partition* :iottwinm aker: *region*:*account_ID* :workspac e/ *workspace_ID* /entity/*entity_ID*
AWS::IoTTwinMaker::Workspace	arn:*partition* :iottwinm aker: *region*:*account_ID* :workspac e/ *workspace_ID*
AWS::KendraRanking::Executi onPlan	arn:*partition* :kendra-r anking: *region*:*account_ID* :rescore- execution-plan/ *rescore_execution_ plan_ID*
AWS::Kinesis::Stream	arn:*partition* :kinesis: *region*:*account_ID* :stream/*stream_name*

resources.type	resources.ARN
AWS::Kinesis::StreamConsumer	arn:*partition* :kinesis: *region*:*account_ID* :*stream_type* /*stream_name* /consumer/ *consumer_name* :*consumer_creation_timestamp*
AWS::KinesisVideo::Stream	arn:*partition* :kinesisvideo: *region*:*account_ID* :stream/*stream_name* /*creation_time*
AWS::ManagedBlockchain::Network	arn:*partition* :managedblockchain:::networks/ *network_name*
AWS::ManagedBlockchain::Node	arn:*partition* :managedblockchain: *region*:*account_ID* :nodes/*node_ID*
AWS::MedicalImaging::Datastore	arn:*partition* :medical-imaging: *region*:*account_ID* :datastore/ *data_store_ID*
AWS::NeptuneGraph::Graph	arn:*partition* :neptune-graph: *region*:*account_ID* :graph/*graph_ID*
AWS::PCAConnectorAD::Connector	arn:*partition* :pca-connector-ad: *region*:*account_ID* :connector/ *connector_ID*
AWS::QApps:QApp	arn:*partition* :qapps:*region*:*account_ID* :application/ *application_UUID* / qapp/*qapp_UUID*

resources.type	resources.ARN
AWS::QBusiness::Application	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID*
AWS::QBusiness::DataSource	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID* /index/*index_ID*/ data-source/ *datasource_ID*
AWS::QBusiness::Index	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID* /index/*index_ID*
AWS::QBusiness::WebExperience	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID* /web-expe rience/ *web_experienc_ID*
AWS::RDS::DBCluster	arn:*partition* :rds:*region*:*account_I D* :cluster/ *cluster_name*
AWS::S3::AccessPoint [3]	arn:*partition* :s3:*region*:*account_I D* :accesspoint/ *access_point_name*
AWS::S3ObjectLambda::AccessPoint	arn:*partition* :s3-object-lambda: *region*:*account_ID* :accesspo int/ *access_point_name*
AWS::S3Outposts::Object	arn:*partition* :s3-outpo sts: *region*:*account_ID* :*object_path*

resources.type	resources.ARN
AWS::SageMaker::Endpoint	arn:*partition* :sagemaker: *region*:*account_ID* :endpoint/ *endpoint_name*
AWS::SageMaker::ExperimentTrialComponent	arn:*partition* :sagemaker: *region*:*account_ID* :experiment-trial-component/ *experiment_trial_component_name*
AWS::SageMaker::FeatureGroup	arn:*partition* :sagemaker: *region*:*account_ID* :feature-group/ *feature_group_name*
AWS::SCN::Instance	arn:*partition* :scn:*region*:*account_ID* :instance/ *instance_ID*
AWS::ServiceDiscovery::Namespace	arn:*partition* :servicediscovery: *region*:*account_ID* :namespace/ *namespace_ID*
AWS::ServiceDiscovery::Service	arn:*partition* :servicediscovery: *region*:*account_ID* :service/ *service_ID*
AWS::SNS::PlatformEndpoint	arn:*partition* :sns:*region*:*account_ID* :endpoint/ *endpoint_type* /*endpoint_name* /*endpoint_ID*
AWS::SNS::Topic	arn:*partition* :sns:*region*:*account_ID* :*topic_name*

resources.type	resources.ARN
AWS::SQS::Queue	arn:*partition* :sqs:*region*:*account_ID* :*queue_name*
AWS::SSM::ManagedNode	O ARN deve estar em um dos seguintes formatos: • arn:*partition* :ssm:*region*:*account_ID* :managed-instance/ *instance_ID* • arn:*partition* :ec2:*region*:*account_ID* :instance/ *instance_ID*
AWS::SSMMessages::ControlChannel	arn:*partition* :ssmmessages: *region*:*account_ID* :control-channel/ *control_channel_ID*
AWS::StepFunctions::StateMachine	O ARN deve estar em um dos seguintes formatos: • arn:*partition* :states:*region*:*account_ID* :stateMachine: *stateMachine_name* • arn:*partition* :states:*region*:*account_ID* :stateMachine: *stateMachine_name* /*label_name*
AWS::SWF::Domain	arn:*partition* :swf:*region*:*account_ID* :/domain/ *domain_name*
AWS::ThinClient::Device	arn:*partition* :thinclient: *region*:*account_ID* :device/*device_ID*

resources.type	resources.ARN
`AWS::ThinClient::Environment`	`arn:partition :thinclient: region:account_ID :environment/ environment_ID`
`AWS::Timestream::Database`	`arn:partition :timestream: region:account_ID :database/ database_name`
`AWS::Timestream::Table`	`arn:partition :timestream: region:account_ID :database/ database_name /table/table_name`
`AWS::VerifiedPermissions::PolicyStore`	`arn:partition :verifiedpermissions: region:account_ID :policy-store/ policy_store_ID`

[1] Para tabelas com fluxos habilitados, o campo `resources` no evento de dados contém `AWS::DynamoDB::Stream` e `AWS::DynamoDB::Table`. Se você especificar `AWS::DynamoDB::Table` como `resources.type`, ele registrará os eventos da tabela do DynamoDB e dos fluxos do DynamoDB por padrão. Para excluir eventos de streams, adicione um filtro no `eventName` campo.

[2] Para registrar em log todos os eventos de dados de todos os objetos em um bucket do S3 específico, use o operador `StartsWith` e inclua apenas o ARN do bucket como o valor correspondente. A barra final é intencional; não a exclua.

[3] Para registrar em log eventos de todos os objetos em um ponto de acesso do S3, recomendamos usar somente o ARN do ponto de acesso, não incluir o caminho do objeto e usar os operadores `StartsWith` ou `NotStartsWith`.

Para obter mais informações sobre os formatos do ARN de recursos de evento de dados, consulte Ações, recursos e chaves de condição no Guia do usuário do AWS Identity and Access Management .

b. Para cada campo, escolha + Condição para adicionar quantas condições forem necessárias até o máximo de 500 valores especificados para todas as condições. Por exemplo, para excluir eventos de dados de dois buckets do S3 dos eventos de dados registrados em sua trilha, você pode definir o campo como Resources.arn, definir o operador para does not start with e, em seguida, colar o ARN de um bucket do S3 ou procurar os buckets do S3 nos quais você não deseja registrar eventos.

   Para adicionar o segundo bucket do S3, escolha + Condição e, em seguida, repita a instrução anterior, colando o ARN ou procurando um bucket diferente.

   > **Note**
   >
   > É possível ter, no máximo, 500 valores para todos os seletores em uma trilha. Isso inclui matrizes de vários valores para um seletor, como `eventName`. Se você tiver valores únicos para todos os seletores, poderá ter um máximo de 500 condições adicionadas a um seletor.
   > Se você tiver mais de 15.000 funções do Lambda em sua conta, não poderá visualizar ou selecionar todas as funções no console CloudTrail ao criar uma trilha. Ainda será possível registrar todas as funções com um modelo de seletor predefinido, mesmo se elas não forem exibidas. Se você desejar registrar eventos de dados para funções específicas, poderá adicionar manualmente uma função se você souber seu ARN. Você também pode concluir a criação da trilha no console e, em seguida, usar o put-event-selectors comando AWS CLI e o para configurar o registro de eventos de dados para funções específicas do Lambda. Para ter mais informações, consulte Gerenciando trilhas com o AWS CLI.

c. Selecione + Field (+ Campo) para adicionar outros campos, conforme necessário. Para evitar erros, não defina valores conflitantes ou duplicados para campos. Por exemplo, não especifique um ARN em um seletor para ser igual a um valor e, em seguida, especifique que o ARN não seja igual ao mesmo valor em outro seletor.

16. Para adicionar outro tipo de dados no qual registrar eventos de dados, escolha Add data event type (Adicionar tipo de evento de dados). Repita as etapas de 12 até esta etapa para configurar seletores de eventos avançados para o tipo de evento de dados.
17. Escolha eventos do Insights se quiser que sua trilha registre eventos do CloudTrail Insights.

    Em Event type (Tipo de evento), selecione Insights events (Eventos do Insights). Em Eventos do Insights, escolha Taxa de chamada da API, Taxa de erro da API ou ambos. Você deve registrar

eventos de gerenciamento de gravação para registrar em log eventos do Insights sobre a taxa de chamadas à API. É necessário registrar eventos de gerenciamento de leitura ou gravação para registrar em log eventos do Insights sobre a taxa de erros da API.

CloudTrail O Insights analisa eventos de gerenciamento em busca de atividades incomuns e registra eventos quando anomalias são detectadas. Por padrão, as trilhas não registram em log eventos do Insights. Para obter mais informações sobre eventos do Insights, consulte Registrar eventos do Insights. Há cobranças adicionais para o registro em log de eventos do Insights. Para CloudTrail saber os preços, consulte AWS CloudTrail Preços.

Os eventos do Insights são entregues em uma pasta diferente chamada `/CloudTrail-Insight` do mesmo bucket do S3 que é especificado na área de localização de armazenamento da página de detalhes da trilha. CloudTrailcria o novo prefixo para você. Por exemplo, se o bucket de destino do S3 atual for chamado de `S3bucketName/AWSLogs/CloudTrail/`, o nome do bucket do S3 com um novo prefixo será chamado de `S3bucketName/AWSLogs/CloudTrail-Insight/`.

18. Quando terminar de escolher os tipos de eventos para registrar, escolhaNext (Próximo).
19. Na página Review and create (Revisar e criar), revise as suas escolhas. Escolha Edit (Editar) em uma seção para alterar as configurações de trilha mostradas nessa seção. Quando estiver pronto para criar a trilha, escolha Create trail (Criar trilha).
20. A nova trilha será exibida na página Trails (Trilhas). Até 24 horas podem ser necessárias para uma trilha da organização ser criada em todas as regiões em todas as contas-membro. A página Trails (Trilhas) mostra as trilhas de todas as regiões na sua conta. Em cerca de 5 minutos, CloudTrail publica arquivos de log que mostram as chamadas de AWS API feitas em sua organização. Você pode ver os arquivos de log no bucket do Amazon S3 que você especificou.

> **Note**
>
> Não é possível renomear uma trilha após sua criação. Em vez disso, você pode excluir a trilha e criar uma nova.

Próximas etapas

Depois que você criar a trilha, poderá retornar a ela para fazer alterações:

- Edite sua trilha para alterar a configuração dela. Para ter mais informações, consulte Atualizar uma trilha.
- Se necessário, configure o bucket do Amazon S3 para permitir que usuários específicos em contas-membro leiam os arquivos de log da organização. Para ter mais informações, consulte Compartilhamento CloudTrail de arquivos de log entre AWS contas.
- Configure CloudTrail para enviar arquivos de log para o CloudWatch Logs. Para obter mais informações, consulte Envio de eventos para o CloudWatch Logs e o item CloudWatch Logs inPreparar a criação de uma trilha para sua organização.

> **Note**
>
> Somente a conta de gerenciamento pode configurar um grupo de CloudWatch registros de registros para uma trilha da organização.

- Crie uma tabela e use-a para executar uma consulta no Amazon Athena para analisar sua atividade de serviço da AWS . Para obter mais informações, consulte Criação de uma tabela para CloudTrail registros no CloudTrail console no Guia do usuário do Amazon Athena.
- Adicione tags personalizadas (pares de chave-valor) à trilha.
- Para criar outra trilha da organização, volte para a página Trails (Trilhas) e escolha Create trail (Criar trilha).

> **Note**
>
> Quando você configura uma trilha, é possível escolher um bucket do Amazon S3 e um tópico do SNS que pertençam a outra conta. No entanto, se você quiser CloudTrail entregar eventos a um grupo de CloudWatch registros de registros, deverá escolher um grupo de registros que exista na sua conta atual.

Criando uma trilha para uma organização com o AWS Command Line Interface

Você pode criar uma trilha da organização usando a AWS CLI. AWS CLI É atualizado regularmente com funcionalidades e comandos adicionais. Para ajudar a garantir o sucesso, certifique-se de ter instalado ou atualizado para uma AWS CLI versão recente antes de começar.

> **Note**
>
> Os exemplos nesta seção são específicos para a criação e atualização de trilhas da organização. Para exemplos de uso do AWS CLI para gerenciar trilhas, consulte Gerenciando trilhas com o AWS CLI Configurando o monitoramento CloudWatch de registros com o AWS CLI e. Ao criar ou atualizar uma trilha da organização com o AWS CLI, você deve usar um AWS CLI perfil na conta de gerenciamento ou na conta de administrador delegado com permissões suficientes. Se estiver convertendo uma trilha da organização em uma trilha não pertencente à organização, será necessário usar a conta de gerenciamento da respectiva organização.
> Você deve configurar o bucket do Amazon S3 usado para uma trilha de organização com permissões suficientes.

Criar ou atualizar um bucket do Amazon S3 a ser usado para armazenar os arquivos de log de uma trilha da organização

Você deve especificar um bucket do Amazon S3 para receber os arquivos de log para uma trilha de organização. Esse bucket deve ter uma política que CloudTrail permita colocar os arquivos de log da organização no bucket.

Veja a seguir um exemplo de política para um bucket do Amazon S3 chamado *myOrganizationBucket*, que pertence à conta de gerenciamento da organização. Substitua *myOrganizationBucket*, *region*, *managementAccountID*, *trailName* e *o-organizationID pelos valores da sua organização*

Essa política de bucket consiste em três instruções.

- A primeira declaração permite chamar CloudTrail a `GetBucketAcl` ação do Amazon S3 no bucket do Amazon S3.
- A segunda permite o registro em log caso a trilha seja alterada de uma trilha da organização para uma trilha somente dessa conta.
- A terceira instrução permite o registro em log para uma trilha da organização.

O exemplo de política inclui uma chave de condição `aws:SourceArn` para a política de bucket do Amazon S3. A chave de condição global do IAM `aws:SourceArn` ajuda a garantir que as CloudTrail gravações no bucket do S3 sejam gravadas somente para uma trilha ou trilhas específicas. Em uma

trilha da organização, o valor de `aws:SourceArn` deve ser um ARN de trilha que pertença à conta de gerenciamento e use a ID da conta de gerenciamento.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailAclCheck20150319",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "cloudtrail.amazonaws.com"
                ]
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::myOrganizationBucket",
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:managementAccountID:trail/trailName"
                }
            }
        },
        {
            "Sid": "AWSCloudTrailWrite20150319",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "cloudtrail.amazonaws.com"
                ]
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::myOrganizationBucket/AWSLogs/managementAccountID/
*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:managementAccountID:trail/trailName"
                }
            }
        },
        {
```

```
            "Sid": "AWSCloudTrailOrganizationWrite20150319",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "cloudtrail.amazonaws.com"
                ]
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::myOrganizationBucket/AWSLogs/o-organizationID/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:managementAccountID:trail/trailName"
                }
            }
        }
    ]
}
```

Essa política de exemplo não permite que usuários de contas-membro acessem os arquivos de log criados para a organização. Por padrão, os arquivos de log da organização poderão ser acessados somente pela conta de gerenciamento. Para obter informações sobre como conceder acesso de leitura ao bucket do Amazon S3 para usuários do IAM nas contas-membro, consulte Compartilhamento CloudTrail de arquivos de log entre AWS contas.

Habilitando CloudTrail como um serviço confiável em AWS Organizations

Antes de criar uma trilha da organização, primeiro é necessário habilitar todos os recursos no Organizations. Para obter mais informações, consulte Habilitar todos os recursos na sua organização ou execute o seguinte comando usando um perfil com permissões suficientes na conta de gerenciamento:

```
aws organizations enable-all-features
```

Depois de habilitar todos os recursos, você deve configurar o Organizations to trust CloudTrail como um serviço confiável.

Para criar a relação de serviço confiável entre AWS Organizations e CloudTrail, abra um terminal ou linha de comando e use um perfil na conta de gerenciamento. Execute o comando `aws organizations enable-aws-service-access`, conforme demonstrado no exemplo a seguir.

```
aws organizations enable-aws-service-access --service-principal
 cloudtrail.amazonaws.com
```

Usar create-trail

Criar uma trilha da organização que se aplica a todas as regiões

Para criar uma trilha da organização que se aplica a todas as regiões, adicione as opções `--is-organization-trail` e `--is-multi-region-trail`.

> **Note**
>
> Ao criar uma trilha da organização com o AWS CLI, você deve usar um AWS CLI perfil na conta de gerenciamento ou na conta de administrador delegado com permissões suficientes.

O exemplo a seguir cria uma trilha da organização que fornece logs de todas as regiões a um bucket existente chamado *my-bucket*:

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name my-bucket --is-
organization-trail --is-multi-region-trail
```

Para confirmar se a trilha existe em todas as regiões, os parâmetros `IsOrganizationTrail` e `IsMultiRegionTrail` no resultado estão configurados como `true`:

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": true,
    "S3BucketName": "my-bucket"
}
```

> **Note**
>
> Execute o comando `start-logging` para iniciar o registro da sua trilha. Para ter mais informações, consulte Interromper e iniciar o registro de uma trilha.

Criar uma trilha da organização como uma trilha de região única

O comando a seguir cria uma trilha organizacional que registra somente eventos em uma única trilha Região da AWS, também conhecida como trilha de região única. A AWS região em que os eventos são registrados é a região especificada no perfil de configuração do AWS CLI.

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name my-bucket --is-
organization-trail
```

Para ter mais informações, consulte Requisitos de nomenclatura.

Exemplo de resultado:

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": false,
    "IsOrganizationTrail": true,
    "S3BucketName": "my-bucket"
}
```

Por padrão, o comando `create-trail` cria uma trilha de região única que não habilita a validação do arquivo de log.

> **Note**
>
> Execute o comando `start-logging` para iniciar o registro da sua trilha.

Executar update-trail para atualizar uma trilha da organização

Você pode executar o comando `update-trail` para alterar as definições de configuração de uma trilha da organização ou aplicar uma trilha existente de uma única conta da AWS a toda a organização. Lembre-se de que só é possível executar o comando `update-trail` na região em que a trilha foi criada.

> **Note**
>
> Se você usa o AWS CLI ou um dos AWS SDKs para atualizar uma trilha, verifique se a política de bucket da trilha é up-to-date. Para ter mais informações, consulte Criando uma trilha para uma organização com o AWS Command Line Interface.
> Ao atualizar uma trilha da organização com o AWS CLI, você deve usar um AWS CLI perfil na conta de gerenciamento ou na conta de administrador delegado com permissões suficientes. Se você quiser converter uma trilha da organização em uma trilha não pertencente à organização, deverá usar a conta de gerenciamento da organização, porque a conta de gerenciamento é a proprietária de todos os recursos da organização.
> CloudTrail atualiza as trilhas da organização nas contas dos membros, mesmo que a validação do recurso falhe. Exemplos de falhas de validação incluem:
>
> - uma política incorreta de bucket do Amazon S3
> - uma política de tópicos incorreta do Amazon SNS
> - incapacidade de entregar para um grupo de CloudWatch registros de registros
> - permissão insuficiente para criptografar usando uma chave KMS
>
> Uma conta membro com CloudTrail permissões pode ver qualquer falha de validação de uma trilha da organização visualizando a página de detalhes da trilha no CloudTrail console ou executando o AWS CLI get-trail-statuscomando.

Aplicar uma trilha existente a uma organização

Para alterar uma trilha existente para que ela também se aplique a uma organização em vez de a uma única AWS conta, adicione a `--is-organization-trail` opção, conforme mostrado no exemplo a seguir.

> **Note**
>
> Use a conta de gerenciamento para transformar uma trilha existente não pertencente à organização em uma trilha da organização.

```
aws cloudtrail update-trail --name my-trail --is-organization-trail
```

Para confirmar se a trilha agora se aplica à organização, o parâmetro `IsOrganizationTrail` no resultado mostra um valor de `true`.

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": true,
    "S3BucketName": "my-bucket"
}
```

No exemplo anterior, a trilha foi configurada para ser aplicada a todas as regiões (`"IsMultiRegionTrail": true`). Uma trilha aplicada somente a uma única região mostraria o resultado `"IsMultiRegionTrail": false` na saída.

Converter uma trilha da organização que se aplica a uma única região para que ela se aplique a todas as regiões

Para alterar uma trilha da organização existente para que ela também se aplique a todas as regiões, adicione a opção `--is-multi-region-trail`, conforme mostrado no exemplo a seguir.

```
aws cloudtrail update-trail --name my-trail --is-multi-region-trail
```

Para confirmar se a trilha agora se aplica a todas as regiões, o parâmetro `IsMultiRegionTrail` no resultado mostra um valor de `true`.

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": true,
    "S3BucketName": "my-bucket"
}
```

Solução de problemas

Esta seção fornece informações sobre como solucionar problemas com uma trilha organizacional.

Tópicos

CloudTrail não está entregando eventos

Se não CloudTrail estiver entregando arquivos de CloudTrail log para o bucket do Amazon S3

Verifique se há algum problema com o bucket do S3.

- No CloudTrail console, confira a página de detalhes da trilha. Se houver um problema com o bucket do S3, a página de detalhes incluirá um aviso de que a entrega para o bucket do S3 falhou.
- A partir do AWS CLI, execute o get-trail-statuscomando. Se houver uma falha, a saída do comando inclui o `LatestDeliveryError` campo, que exibe qualquer erro do Amazon S3 CloudTrail encontrado ao tentar entregar arquivos de log para o bucket designado. Esse erro ocorre somente quando há um problema com o bucket S3 de destino e não ocorre para solicitações que atingem o tempo limite. Para resolver o problema, corrija a política do bucket para que ele CloudTrail possa gravar no bucket; ou crie um novo bucket e, em seguida, chame `update-trail` para especificar o novo bucket. Para obter informações sobre a política de bucket da organização, consulte Criar ou atualizar um bucket do Amazon S3 para usar para armazenar os arquivos de log de uma trilha da organização.

Se não CloudTrail estiver entregando registros para o CloudWatch Logs

Verifique se há algum problema com a configuração da política de função de CloudWatch registros.

- No CloudTrail console, confira a página de detalhes da trilha. Se houver um problema com CloudWatch os registros, a página de detalhes incluirá um aviso indicando que a entrega CloudWatch dos registros falhou.
- A partir do AWS CLI, execute o get-trail-statuscomando. Se houver uma falha, a saída do comando inclui o `LatestCloudWatchLogsDeliveryError` campo, que exibe qualquer erro de CloudWatch registros CloudTrail encontrado ao tentar entregar CloudWatch registros ao Logs. Para resolver o problema, corrija a política de função de CloudWatch registros. Para obter informações sobre a política de função de CloudWatch registros, consulteDocumento de política de funções CloudTrail para usar CloudWatch registros para monitoramento.

Se você não estiver vendo a atividade de uma conta de membro em uma trilha da organização

Se você não estiver vendo a atividade de uma conta de membro em uma trilha da organização, verifique o seguinte:

- Verifique a região de origem da trilha para ver se é uma região opcional

  Embora a maioria Regiões da AWS esteja ativada por padrão para você Conta da AWS, você deve ativar manualmente determinadas regiões (também chamadas de regiões opcionais). Para obter informações sobre quais regiões estão habilitadas por padrão, consulte Considerações antes de ativar e desativar regiões no Guia de AWS Account Management referência. Para ver a lista de regiões CloudTrail compatíveis, consulteCloudTrail Regiões suportadas.

  Se a trilha da organização for multirregional e a região de origem for uma região opcional, as contas dos membros não enviarão atividades para a trilha da organização, a menos que optem pela trilha multirregional em Região da AWS que a trilha multirregional foi criada. Por exemplo, se você criar uma trilha multirregional e escolher a região da Europa (Espanha) como a região de origem da trilha, somente as contas dos membros que habilitaram a região da Europa (Espanha) para sua conta enviarão a atividade da conta para a trilha da organização. Para resolver o problema, habilite a região de aceitação em cada conta membro em sua organização. Para obter informações sobre como ativar uma região opcional, consulte Ativar ou desativar uma região em sua organização no Guia de AWS Account Management referência.
- Verifique se a política baseada em recursos da organização está em conflito com a política de função vinculada ao CloudTrail serviço

  CloudTrail usa a função vinculada ao serviço nomeada `AWSServiceRoleForCloudTrail`para apoiar as trilhas da organização. Essa função vinculada ao serviço permite CloudTrail realizar ações nos recursos da organização, como. `organizations:DescribeOrganization` Se a política baseada em recursos da organização negar uma ação permitida na política de função vinculada ao serviço, não CloudTrail poderá realizar a ação, mesmo que ela seja permitida na política de função vinculada ao serviço. Para resolver o problema, corrija a política baseada em recursos da organização para que ela não negue ações permitidas na política de função vinculada ao serviço.

CloudTrail não está enviando notificações do Amazon SNS para uma conta membro em uma organização

Quando uma conta membro com uma trilha AWS Organizations organizacional não está enviando notificações do Amazon SNS, pode haver um problema com a configuração da política de tópicos do SNS. CloudTrail cria trilhas da organização nas contas dos membros mesmo se a validação do recurso falhar, por exemplo, o tópico do SNS da trilha da organização não inclui todas as IDs das contas dos membros. Se a política de tópicos do SNS estiver incorreta, ocorrerá uma falha na autorização.

Para verificar se a política de tópicos do SNS de uma trilha tem uma falha de autorização:

- No CloudTrail console, confira a página de detalhes da trilha. Se houver uma falha na autorização, a página de detalhes inclui um aviso `SNS authorization failed` e indica a correção da política de tópicos do SNS.
- A partir do AWS CLI, execute o get-trail-statuscomando. Se houver uma falha na autorização, a saída do comando incluirá o `LastNotificationError` campo com um valor de`AuthorizationError`. Para resolver o problema, corrija a política de tópicos do Amazon SNS. Para obter informações sobre a política de tópicos do Amazon SNS, consulte. Política de tópicos do Amazon SNS para CloudTrail

Para obter mais informações sobre tópicos do SNS e como se inscrever neles, consulte Introdução ao Amazon SNS no Guia do desenvolvedor do Amazon Simple Notification Service.

Visualizando eventos do CloudTrail Insights para trilhas

Depois de habilitar o CloudTrail Insights em uma trilha, você pode visualizar até 90 dias de eventos do Insights usando o CloudTrail console ou AWS CLI o. Esta seção descreve como exibir, pesquisar e baixar um arquivo de eventos do Insights. Para obter informações sobre como usar a `LookupEvents` API para recuperar informações de CloudTrail eventos, consulte a Referência da AWS CloudTrail API. Para obter mais informações sobre o CloudTrail Insights, consulte Registrar eventos do Insights este guia.

Para obter mais informações sobre como criar e gerenciar uma trilha, consulte Criar uma trilha e Obtendo e visualizando seus arquivos de CloudTrail log.

> **Note**
>
> Para registrar em log eventos do Insights sobre o volume de chamadas à API, a trilha deve registrar em log os eventos de gerenciamento de `write`. Para registrar em log eventos do Insights sobre a taxa de erros da API, a trilha deve registrar em log os eventos de gerenciamento de `read` ou `write`.

Tópicos

Visualizando eventos do CloudTrail Insights para trilhas no CloudTrail console

Depois de ativar os eventos do CloudTrail Insights em uma trilha, quando CloudTrail detecta atividades incomuns na API ou na taxa de erro, CloudTrail gera eventos do Insights e os exibe nas páginas do Painel e do Insights no AWS Management Console. É possível visualizar os eventos do Insights no console e solucionar problemas da atividade incomum. Os últimos 90 dias dos eventos dos Insights são mostrados no console. Você também pode baixar eventos do Insights usando o AWS CloudTrail console. Você pode pesquisar eventos de forma programática usando os AWS SDKs ou. AWS Command Line Interface Para obter mais informações sobre os eventos do CloudTrail Insights, consulte Registrar eventos do Insights este guia.

> **Note**
>
> Para registrar em log eventos do Insights sobre o volume de chamadas à API, a trilha deve registrar em log os eventos de gerenciamento de `write`. Para registrar em log eventos do Insights sobre a taxa de erros da API, a trilha deve registrar em log os eventos de gerenciamento de `read` ou `write`.

Depois que os eventos do Insights forem registrados em log, eles serão exibidos na página Insights por 90 dias. Não é possível excluir manualmente os eventos na página Insights. Como você deve criar uma trilha antes de habilitar o CloudTrail Insights, você pode visualizar os eventos do

Insights que estão registrados na sua trilha enquanto você os armazena no bucket do S3 que está configurado nas configurações da trilha.

Monitore seus registros de trilhas e seja notificado quando ocorrerem atividades específicas de eventos do Insights com o Amazon CloudWatch Logs. Para ter mais informações, consulte Monitoramento CloudTrail de arquivos de log com o Amazon CloudWatch Logs.

Para visualizar eventos do Insights

CloudTrail Os eventos do Insights devem estar habilitados em sua trilha para ver os eventos do Insights no console. Aguarde até 36 horas CloudTrail para entregar os primeiros eventos do Insights, se uma atividade incomum for detectada.

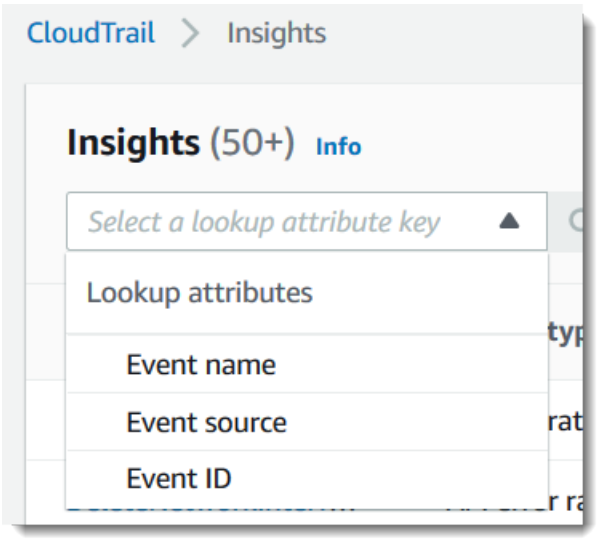
1. Faça login no AWS Management Console e abra o CloudTrail console em https://console.aws.amazon.com/cloudtrail/home/.
2. No painel de navegação, escolha Dashboard (Painel) para ver os cinco últimos eventos do Insights ou Insights para ver todos os eventos do Insights registrados em log na conta nos últimos 90 dias.

   Na página Insights, é possível filtrar eventos do Insights por critérios, incluindo a origem da API do evento, o nome do evento e o ID do evento, além de limitar os eventos exibidos aos que ocorrem em um intervalo de tempo específico. Para obter mais informações sobre a filtragem de eventos do Insights, consulte Filtrar eventos do Insights.

Sumário

Filtrar eventos do Insights

A exibição padrão de eventos em Insights mostra eventos em ordem cronológica inversa. Os eventos dos Insights mais recentes, classificados por hora de início do evento, estão no topo. A lista a seguir descreve os atributos disponíveis. Você pode filtrar os três primeiros atributos: Event name (Nome do evento), Fonte do evento, e ID do evento.



Nome do evento

O nome do evento, normalmente a AWS API na qual níveis incomuns de atividade foram registrados.

Tipo de insight

O tipo de evento do CloudTrail Insights, que é a taxa de chamadas da API ou a taxa de erro da API. O tipo de insight Taxa de chamadas à API analisa as chamadas à API de gerenciamento somente de gravação que são agregadas por minuto em relação a um volume de chamadas à API de linha de base. O tipo de insight Taxa de erros da API analisa as chamadas à API de gerenciamento que resultam em códigos de erro. O erro será exibido se a chamada à API não for bem-sucedida.

Origem do evento.

O AWS serviço para o qual a solicitação foi feita, como `iam.amazonaws.com` ou `s3.amazonaws.com`. Você pode percorrer uma lista de fontes de eventos depois que selecionar o filtro Origem do evento.

ID do evento

O ID de evento do Insights. Os IDs de evento não são mostrados na tabela da página Insights, mas estão em um atributo no qual é possível filtrar eventos do Insights. Os IDs de eventos de gerenciamento que são analisados para gerar eventos do Insights são diferente dos IDs de eventos do Insights.

Hora de início do evento

A hora de início do evento do Insights, medida como o primeiro minuto em que a atividade de API incomum foi registrada. Este atributo é mostrado na tabela do Insights, mas não é possível filtrar a hora de início do evento no console.

Linha de base

O padrão normal de taxa de chamada de API ou atividade de taxa de erro. A linha de base é calculada ao longo dos sete dias anteriores ao início de um evento do Insights. Embora o valor da duração da linha de base — o período que CloudTrail analisa a atividade normal nas APIs — seja de aproximadamente sete dias, CloudTrail arredonda a duração da linha de base para um dia inteiro inteiro, de modo que a duração exata da linha de base possa variar.

Média do Insight

O número médio de chamadas para uma API ou o número médio de um erro específico que foi retornado em chamadas para uma API, que acionou o evento Insights. A média do CloudTrail Insights para o evento inicial é a taxa de ocorrências que acionaram o evento do Insights. Normalmente, esse é o primeiro minuto de atividade incomum. A média do Insights para o evento de término é a taxa de chamadas de API por minuto sobre a duração da atividade incomum, entre o evento do Insights de início e o evento do Insights de término.

Mudança de taxa

A diferença entre o valor de Linha de base e média do Insight, medido em porcentagem. Por exemplo, se a média da linha de base de um `AccessDenied` erro ocorrido é 1,0, e a média do Insight é 3,0, a variação da taxa é de 300%. Uma mudança de taxa para uma média do Insight que excede uma média de linha de base mostra uma seta para cima ao lado do valor. Se o evento Insights foi registrado porque a atividade está abaixo da média da linha de base, Mudança de taxa mostra uma seta para baixo ao lado da porcentagem.

Se não houver eventos registrados para o atributo ou o tempo que você escolher, a lista de resultados estará vazia. Você pode aplicar apenas um filtro de atributo, além do período. Se você escolher um filtro de atributo diferente, o intervalo de tempo especificado será preservado.

As etapas a seguir descrevem como filtrar por atributo.

Para filtrar por atributo

1. Para filtrar os resultados por um atributo, escolha um atributo de pesquisa do menu suspenso e digite ou escolha um valor na caixa Enter a lookup value (Inserir um valor de pesquisa).

2. Para remover um filtro de atributo, selecione o X à direita da caixa de filtros de atributos.

As etapas a seguir descrevem como filtrar por data e hora de início e de término.

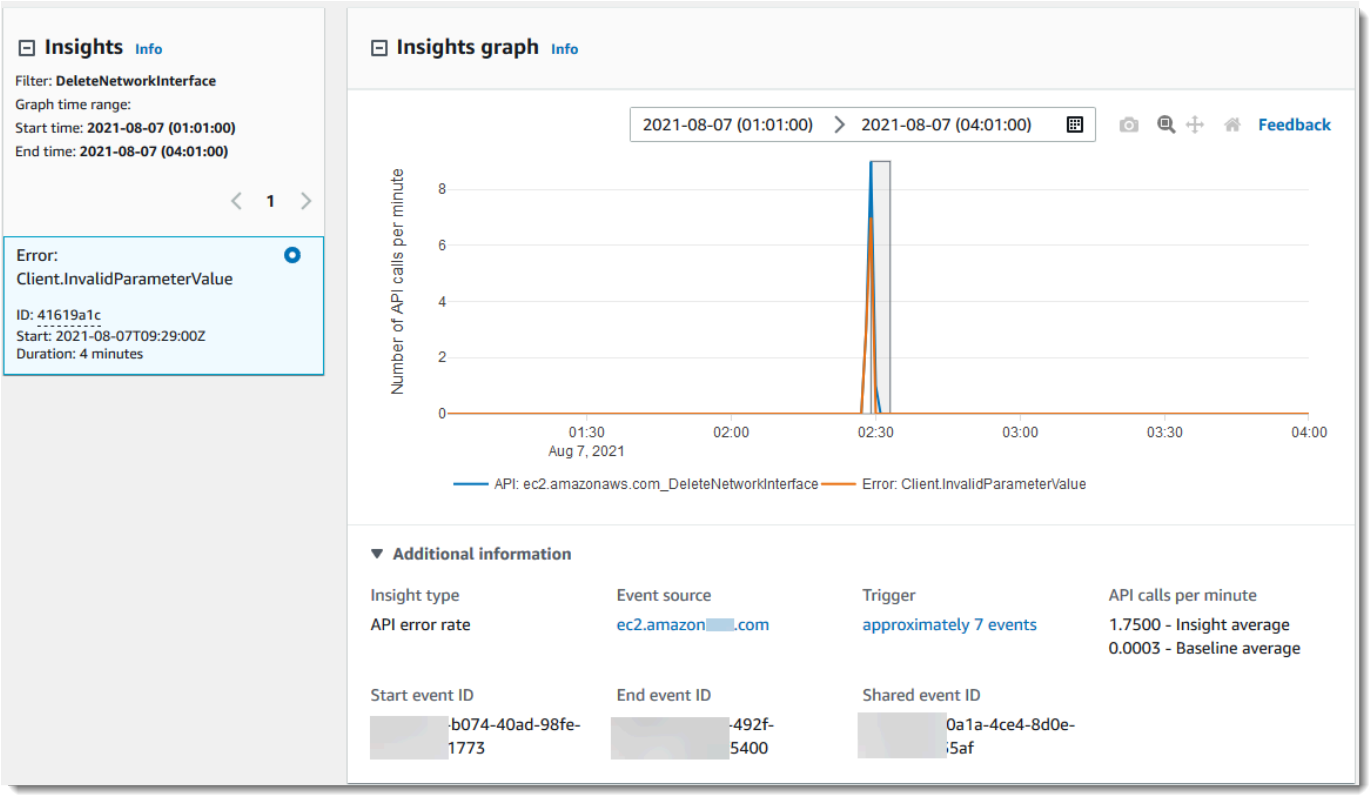
Para filtrar por data e hora de início e de término

1. Para limitar o período dos eventos que você deseja ver, escolha um período na barra de períodos na parte superior da tabela. Os intervalos de tempo predefinidos incluem 30 minutos, 1 hora, 3 horas ou 12 horas. Para especificar um período personalizado, escolha Custom (Personalizado).
2. Escolha uma das guias a seguir.
   - Absolute (Absoluto): permite-lhe escolher um horário específico. Prossiga para a próxima etapa.
   - Relative to selected event (Relativo ao evento selecionado): selecionado por padrão. Permite escolher um período relativo à hora de início de um evento do Insights. Prossiga para a etapa 4.
3. Para definir um intervalo Absolute (Absoluto), faça o seguinte.
   a. Na guia Absolute (Absoluto), escolha o dia em que você deseja que o intervalo de tempo comece. Insira uma hora de início no dia selecionado. Para inserir uma data manualmente, digite a data no formato `yyyy/mm/dd`. As horas de início e término usam um relógio de 24 horas e os valores devem estar no formato `hh:mm:ss`. Por exemplo, para indicar uma hora de início de 18h30, digite **`18:30:00`**.
   b. Escolha uma data de término para o intervalo no calendário ou especifique uma data e hora finais abaixo do calendário. Escolha Aplicar.
4. Para definir um período Relative to selected event (Relativo ao evento selecionado), faça o seguinte.
   a. Escolha um período predefinido relativo à hora de início dos eventos do Insights. Os valores predefinidos estão disponíveis em minutos, horas, dias ou semanas. O período relativo máximo é de 12 semanas.
   b. Se necessário, personalize o valor predefinido nas caixas abaixo das predefinições. Escolha Clear (Limpar) para redefinir as alterações, se necessário. Quando definir a hora relativa que você deseja, escolha Apply (Aplicar).

5. Em To (Até), escolha o dia e especifique a hora que deseja ser o fim do intervalo de tempo. Escolha Aplicar.
6. Para remover um filtro de período, selecione o ícone de calendário à direita da caixa Time range (Período) e escolha Remove (Remover).

Visualizar detalhes de eventos do Insights

1. Escolha um evento do Insights na lista de resultados para mostrar os detalhes dele. A página de detalhes de um evento do Insights mostra um gráfico da linha do tempo da atividade incomum.



2. Passe o mouse sobre as faixas destacadas para mostrar a hora inicial e a duração de cada evento do Insights no gráfico.

As informações a seguir são mostradas na área do gráfico Informações adicionais:

- Insight type (Tipo de insight). Isso pode ser taxa de chamada de API ou taxa de erros da API.

- Acionador. Este é um link para a guia Cloudtrail events (Eventos do Cloudtrail), que lista os eventos de gerenciamento que foram analisados para determinar se ocorreu atividade incomum.
- Chamadas à API por minuto
  - Baseline average (Média da linha de base) – A taxa típica de chamadas por minuto para essa API, conforme medida aproximadamente nos sete dias anteriores em uma região específica da sua conta.
  - Média do Insights – a taxa de chamadas por minuto para essa API que acionou o evento do Insights. A média do CloudTrail Insights para o evento inicial é a taxa de chamadas ou erros por minuto na API que acionou o evento do Insights. Normalmente, esse é o primeiro minuto de atividade incomum. A média do Insights para o evento de término é a taxa de chamadas de API por minuto sobre a duração da atividade incomum, entre o evento do Insights de início e o evento do Insights de término.
- Event source (Fonte do evento). O endpoint do AWS serviço no qual o número incomum de chamadas ou erros de API foram registrados. Na imagem anterior, a fonte é `ec2.amazonaws.com`, que é o endpoint de serviço do Amazon EC2.
- IDs de evento.
  - ID do evento de início - O ID do evento do Insights que foi registrado em log no início da atividade incomum.
  - ID do evento do fim - O ID do evento Insights que foi registrado no final de uma atividade incomum.
  - ID de evento compartilhado - Em eventos do Insights, o ID do evento compartilhado é um GUID gerado pelo CloudTrail Insights para identificar de forma exclusiva um par inicial e final de eventos do Insights. ID do evento compartilhado é comum entre o evento do Insights de início e de término e ajuda a criar uma correlação entre ambos os eventos para identificar exclusivamente a atividade incomum.

3. Selecione a guia Attributions (Atribuições) para exibir informações sobre as identidades de usuário, agentes de usuário e em eventos de inishgts de taxa de chamada de API, os códigos de erro são correlacionados com atividade incomum e base de referência. Um máximo de cinco identidades de usuário, cinco agentes de usuário e cinco códigos de erro são mostrados nas tabelas da guia Attributions (Atribuições), ordenadas por uma média da contagem de atividade, em ordem decrescente da mais alta para a mais baixa. Para obter mais informações sobre a guia Attributions (Atribuições), consulte Guia Attibutions (Atribuições) e CloudTrail `insightDetails`Elemento Insights neste guia.

4. Na guia CloudTrail Eventos, visualize os eventos relacionados que CloudTrail foram analisados para determinar a ocorrência de uma atividade incomum. Por padrão, um filtro já está aplicado ao nome do evento do Insights, que também é o nome da API relacionada. A guia de CloudTrail eventos mostra os eventos CloudTrail de gerenciamento relacionados à API do assunto que ocorreram entre a hora de início (menos um minuto) e a hora de término (mais um minuto) do evento do Insights.

   Conforme você seleciona outros eventos do Insights no gráfico, os eventos mostrados na tabela de CloudTrail eventos mudam. Esses eventos ajudam a executar uma análise mais profunda para determinar a provável causa de um evento do Insights e os motivos da atividade de API incomum.

   Para mostrar todos os CloudTrail eventos que foram registrados durante a duração do evento do Insights, e não apenas aqueles da API relacionada, desative o filtro.
5. Selecione a guia Insights event record (Registro de eventos do Insights) para exibir os eventos de início e término do Insights no formato JSON.
6. No painel da esquerda da página de detalhes, selecionar a Event source (Fonte do evento) vinculada retorna à página do Insights filtrada por essa fonte do evento.

Aproximar, inclinar e baixar o gráfico

É possível aplicar zoom, panorâmica e reiniciar os eixos do gráfico na página de detalhes do evento do Insights usando uma barra de ferramentas no canto direito superior.

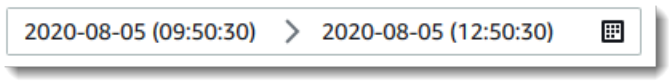
Da esquerda para a direita, os botões de comando na barra de ferramentas do gráfico fazem o seguinte:

- Download plot as a PNG (Fazer download do gráfico como PNG) – faça download da imagem do gráfico mostrada na página de detalhes, e salve-a no formato PNG.
- Zoom – arraste para selecionar uma área no gráfico que você deseja ampliar e ver com mais detalhes.
- Pan (Panorâmica) – desloque o gráfico para ver datas ou horas adjacentes.

- Reset axes (Redefinir eixos) – altere os eixos do gráfico de volta aos originais, limpando as configurações de zoom e panorâmica.

Alterar as configurações de intervalo de tempo do gráfico

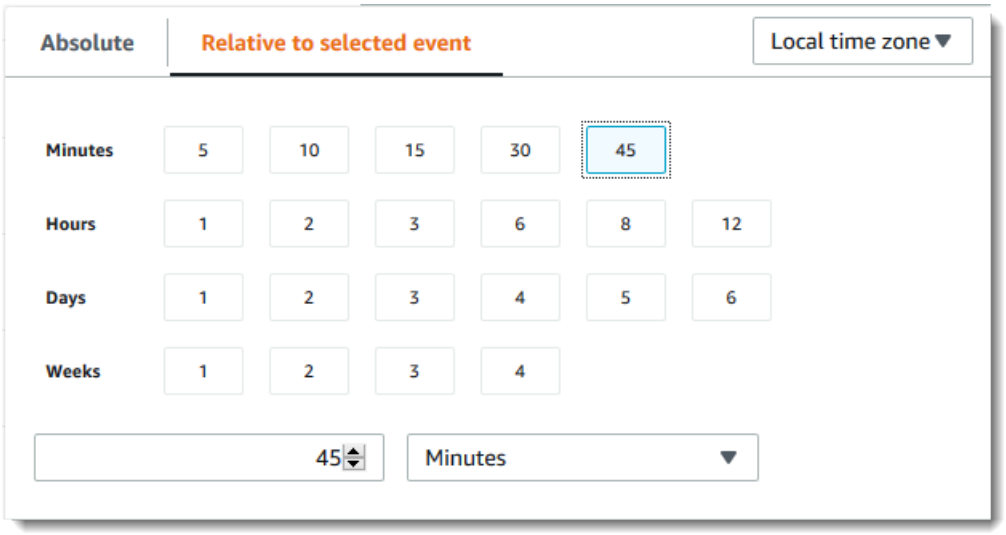
É possível alterar o intervalo de tempo (a duração selecionada dos eventos mostrada no eixo x) que é exibido no gráfico escolhendo uma configuração no canto superior direito do gráfico.



O intervalo de tempo padrão mostrado no gráfico depende da duração do evento do Insights selecionado.

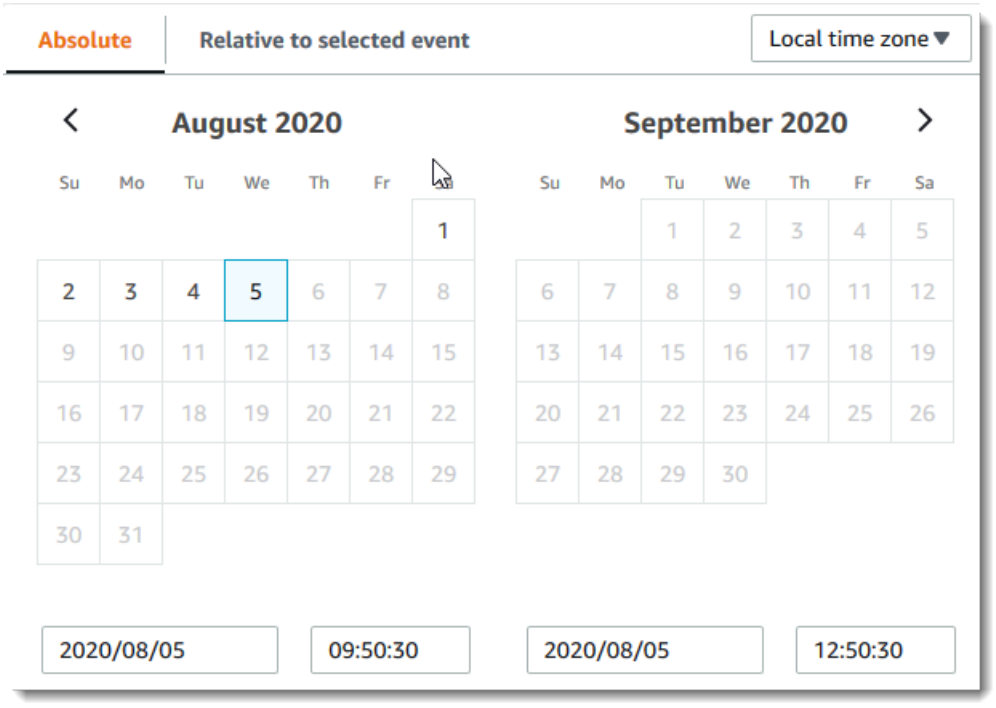
Duração do evento do Insights	Intervalo de tempo padrão
Menos de 4 horas	3h (três horas)
Entre 4 e 12 horas	12h(12 horas)
Entre 12 e 24 horas	1d (um dia)
Entre 24 e 72 horas	3d (três dias)
Mais de 72 horas	1w (uma semana)

Você pode escolher predefinições de 5 minutos, 30 minutos, 1 hora, 3 horas, 12 horas ou Custom (Personalizadas). A imagem a seguir mostra períodos de Relative to selected event (Relativo ao evento selecionado) que podem ser escolhidos nas configurações Custom (Personalizadas). Períodos relativos são períodos aproximados do início e do término do evento do Insights selecionado exibido em uma página de detalhes do evento do Insights.



Para personalizar uma predefinição selecionada, especifique um número e uma unidade de tempo nas caixas abaixo das predefinições.

Para especificar um intervalo de tempo e uma data exatos, selecione a guia Absolute (Absoluto). Se você definir um intervalo absoluto de data e hora, as horas inicial e final serão necessárias. Para obter informações sobre como definir a hora, consulte the section called “Filtrar eventos do Insights” neste tópico.



Fazer download de eventos do Insights

É possível fazer download do histórico de eventos registrados do Insights como um arquivo no formato CSV ou JSON. Use filtros e intervalos de tempo para reduzir o tamanho do arquivo que você fizer download.

> **Note**
>
> CloudTrail arquivos de histórico de eventos são arquivos de dados que contêm informações (como nomes de recursos) que podem ser configuradas por usuários individuais. Alguns dados podem ser interpretados como comandos em programas usados para ler e analisar esses dados (injeção de CSV). Por exemplo, quando CloudTrail os eventos são exportados para CSV e importados para um programa de planilhas, esse programa pode alertá-lo sobre questões de segurança. Como melhor prática de segurança, desative links ou macros de arquivos do histórico de eventos obtidos por download.

1. Especifique o filtro e o intervalo de tempo para os eventos dos quais você deseja fazer download. Por exemplo, você pode especificar o nome do evento, `StartInstances`, e um período relativo aos últimos três dias de atividade.
2. Escolha Download events (Baixar eventos) e, em seguida, Download CSV (Baixar CSV) ou Download JSON (Baixar JSON). Você será solicitado a escolher um local para salvar o arquivo.

   > **Note**
   >
   > O download pode levar algum tempo para ser concluído. Para obter resultados mais rápidos, antes de iniciar o processo de download, use um filtro específico ou um período mais curto para restringir os resultados.

3. Quando o download for concluído, abra o arquivo para visualizar os eventos que você especificou.
4. Para cancelar o download, escolha Cancel download (Cancelar download). Se você cancelar um download antes que ele seja concluído, um arquivo CSV ou JSON em seu computador local pode conter apenas parte de seus eventos.

Visualizando eventos do CloudTrail Insights para trilhas com o AWS CLI

Você pode pesquisar os eventos do CloudTrail Insights dos últimos 90 dias executando o aws cloudtrail lookup-events comando. O comando `lookup-events` apresenta as seguintes opções:

- `--end-time`
- `--event-category`
- `--max-results`
- `--start-time`
- `--lookup-attributes`
- `--next-token`
- `--generate-cli-skeleton`
- `--cli-input-json`

Para obter informações gerais sobre como usar o AWS Command Line Interface, consulte o Guia AWS Command Line Interface do usuário.

Sumário

Pré-requisitos

- Para executar AWS CLI comandos, você deve instalar AWS CLI o. Para obter mais informações, consulte Começar com AWS CLI o.

- Certifique-se de que sua AWS CLI versão seja maior que 1.6.6. Para verificar a versão da CLI, execute aws --version na linha de comando.
- Para definir a conta, a região e o formato de saída padrão para uma AWS CLI sessão, use o aws configure comando. Para obter mais informações, consulte Configurar a interface de linha de comando da AWS.
- Para registrar em log eventos do Insights sobre o volume de chamadas à API, a trilha deve registrar em log os eventos de gerenciamento de `write`. Para registrar em log eventos do Insights sobre a taxa de erros da API, a trilha deve registrar em log os eventos de gerenciamento de `read` ou `write`.

> **Note**
>
> Os CloudTrail AWS CLI comandos diferenciam maiúsculas de minúsculas.

Receber ajuda da linha de comando

Para ver a ajuda da linha de comando para `lookup-events`, digite o comando a seguir.

```
aws cloudtrail lookup-events help
```

Pesquisar eventos do Insights

Para ver os dez eventos do Insights mais recentes, digite o comando a seguir.

```
aws cloudtrail lookup-events --event-category insight
```

Um evento retornado tem aparência semelhante ao seguinte exemplo:

```
{
    "NextToken": "kbOt5LlZe+
+mErCebpy2TgaMgmDvF1kYGFcH64JSjIbZFjsuvrSqg66b5YGssKutDYIyII4lrP4IDbeQdiObkp9YAlju3oXd12juEXAMP
    "Events": [
        {
            "eventVersion": "1.07",
            "eventTime": "2019-10-15T21:13:00Z",
            "awsRegion": "us-east-1",
            "eventID": "EXAMPLE-9b6f-45f8-bc6b-9b41c052ebc7",
            "eventType": "AwsCloudTrailInsight",
```

```
            "recipientAccountId": "123456789012",
            "sharedEventID": "EXAMPLE8-02b2-4e93-9aab-08ed47ea5fd3",
            "insightDetails": {
            "state": "Start",
            "eventSource": "autoscaling.amazonaws.com",
            "eventName": "CompleteLifecycleAction",
            "insightType": "ApiCallRateInsight",
            "insightContext": {
              "statistics": {
                "baseline": {
                  "average": 0.0000882145
                },
                "insight": {
                  "average": 0.6
                },
                "insightDuration": 5,
                "baselineDuration": 11336
              },
              "attributions": [
                {
                  "attribute": "userIdentityArn",
                  "insight": [
                    {
                      "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole1",
                      "average": 0.2
                    },
                    {
                      "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole2",
                      "average": 0.2
                    },
                    {
                      "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole3",
                      "average": 0.2
                    }
                  ],
                  "baseline": [
                    {
                      "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole1",
                      "average": 0.0000882145
                    }
```

```
                ]
              },
              {
                "attribute": "userAgent",
                "insight": [
                  {
                    "value": "codedeploy.amazonaws.com",
                    "average": 0.6
                  }
                ],
                "baseline": [
                  {
                    "value": "codedeploy.amazonaws.com",
                    "average": 0.0000882145
                  }
                ]
              },
              {
                "attribute": "errorCode",
                "insight": [
                  {
                    "value": "null",
                    "average": 0.6
                  }
                ],
                "baseline": [
                  {
                    "value": "null",
                    "average": 0.0000882145
                  }
                ]
              }
            ]
          }
        },
          "eventCategory": "Insight"
      },
      {
          "eventVersion": "1.07",
          "eventTime": "2019-10-15T21:14:00Z",
          "awsRegion": "us-east-1",
          "eventID": "EXAMPLEc-9eac-4af6-8e07-26a5ae8786a5",
          "eventType": "AwsCloudTrailInsight",
          "recipientAccountId": "123456789012",
```

```
            "sharedEventID": "EXAMPLE8-02b2-4e93-9aab-08ed47ea5fd3",
            "insightDetails": {
            "state": "End",
            "eventSource": "autoscaling.amazonaws.com",
            "eventName": "CompleteLifecycleAction",
            "insightType": "ApiCallRateInsight",
            "insightContext": {
              "statistics": {
                "baseline": {
                  "average": 0.0000882145
                },
                "insight": {
                  "average": 0.6
                },
                "insightDuration": 5,
                "baselineDuration": 11336
              },
              "attributions": [
                {
                  "attribute": "userIdentityArn",
                  "insight": [
                    {
                      "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole1",
                      "average": 0.2
                    },
                    {
                      "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole2",
                      "average": 0.2
                    },
                    {
                      "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole3",
                      "average": 0.2
                    }
                  ],
                  "baseline": [
                    {
                      "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole1",
                      "average": 0.0000882145
                    }
                  ]
```

```
                },
                {
                  "attribute": "userAgent",
                  "insight": [
                    {
                      "value": "codedeploy.amazonaws.com",
                      "average": 0.6
                    }
                  ],
                  "baseline": [
                    {
                      "value": "codedeploy.amazonaws.com",
                      "average": 0.0000882145
                    }
                  ]
                },
                {
                  "attribute": "errorCode",
                  "insight": [
                    {
                      "value": "null",
                      "average": 0.6
                    }
                  ],
                  "baseline": [
                    {
                      "value": "null",
                      "average": 0.0000882145
                    }
                  ]
                }
              ]
            }
          },
            "eventCategory": "Insight"
        }
    ]
}
```

Para ver uma explicação dos campos relacionados à pesquisa nos resultados, consulte Pesquisar campos de resultados neste tópico. Para ver uma explicação sobre os eventos do Insights, consulte CloudTrail conteúdo do registro.

Especificar o número de eventos do Insights que devem ser retornados

Para especificar o número de eventos que devem ser retornados, digite o comando a seguir.

```
aws cloudtrail lookup-events --event-category insight --max-results <integer>
```

O valor padrão para *<integer>*, se ele não for especificado, será 10. Os valores possíveis são de 1 a 50. O exemplo a seguir retorna um resultado.

```
aws cloudtrail lookup-events --event-category insight --max-results 1
```

Pesquisar eventos do Insights por intervalo de tempo

Os eventos do Insights dos últimos 90 dias estão disponíveis para pesquisa. Para especificar um intervalo de tempo, digite o comando a seguir.

```
aws cloudtrail lookup-events --event-category insight --start-time <timestamp> --end-
time <timestamp>
```

`--start-time` *<timestamp>* especifica, em UTC, que apenas os eventos do Insights ocorridos no horário especificado ou depois dele são retornados. Se o horário de início especificado for posterior ao de término, um erro será retornado.

`--end-time` *<timestamp>* especifica, em UTC, que apenas os eventos do Insights ocorridos no horário especificado ou antes dele são retornados. Se o horário de término especificado for anterior ao de início, um erro será retornado.

O horário de início padrão é a primeira data em que os dados foram disponibilizados nos últimos 90 dias. O horário de término padrão é o horário de ocorrência de evento mais próximo do momento.

Todos os carimbos de data/hora são exibidos em UTC.

Pesquisar eventos do Insights por atributo

Para filtrar por um atributo, digite o comando a seguir.

```
aws cloudtrail lookup-events --event-category insight --lookup-attributes
 AttributeKey=<attribute>,AttributeValue=<string>
```

É possível especificar somente um par de chave-valor do atributo para cada comando lookup-events. Veja a seguir os valores de evento do Insights válidos para `AttributeKey`. Os nomes dos valores diferenciam maiúsculas de minúsculas.

- `EventId`
- `EventName`
- `EventSource`

O tamanho máximo para o `AttributeValue` é de 2.000 caracteres. Os caracteres a seguir (_", ' ', ',', '\\n') contam como dois caracteres até o limite de 2.000 caracteres.

Exemplos de consulta de atributo

O exemplo de comando a seguir retorna os eventos do Insights nos quais o valor de `EventName` é `PutRule`.

```
aws cloudtrail lookup-events --event-category insight --lookup-attributes
 AttributeKey=EventName, AttributeValue=PutRule
```

O exemplo de comando a seguir retorna os eventos do Insights nos quais o valor de `EventId` é `b5cc8c40-12ba-4d08-a8d9-2bceb9a3e002`.

```
aws cloudtrail lookup-events --event-category insight --lookup-attributes
 AttributeKey=EventId, AttributeValue=b5cc8c40-12ba-4d08-a8d9-2bceb9a3e002
```

O exemplo de comando a seguir retorna os eventos do Insights nos quais o valor de `EventSource` é `iam.amazonaws.com`.

```
aws cloudtrail lookup-events --event-category insight --lookup-attributes
 AttributeKey=EventSource, AttributeValue=iam.amazonaws.com
```

Especificar a próxima página de resultados

Para obter a próxima página de resultados de um comando `lookup-events`, digite o comando a seguir.

```
aws cloudtrail lookup-events --event-category insight <same parameters as previous
 command> --next-token=<token>
```

Neste comando, o valor de *<token>* é obtido do primeiro campo da saída do comando anterior.

Quando você usa `--next-token` em um comando, precisa usar os mesmos parâmetros do comando anterior. Por exemplo, suponha que você tenha executado o comando a seguir.

```
aws cloudtrail lookup-events --event-category insight --lookup-attributes
 AttributeKey=EventName, AttributeValue=PutRule
```

Para obter a próxima página de resultados, seu próximo comando pareceria com o indicado a seguir.

```
aws cloudtrail lookup-events --event-category insight --lookup-attributes
 AttributeKey=EventName,AttributeValue=PutRule --next-token=EXAMPLEZe+
+mErCebpy2TgaMgmDvF1kYGFcH64JSjIbZFjsuvrSqg66b5YGssKutDYIyII4lrP4IDbeQdiObkp9YAlju3oXd12juEXAMP
```

Obter entrada JSON de um arquivo

O AWS CLI para alguns AWS serviços tem dois parâmetros `--generate-cli-skeleton` e`--cli-input-json`, que você pode usar para gerar um modelo JSON, que você pode modificar e usar como entrada para o `--cli-input-json` parâmetro. Esta seção descreve como usar esses parâmetros com `aws cloudtrail lookup-events`. Para obter mais informações, consulte AWS CLI esqueletos e arquivos de entrada.

Para pesquisar os eventos do Insights obtendo a entrada JSON de um arquivo

1. Crie um modelo de entrada para uso com `lookup-events` redirecionando os resultados `--generate-cli-skeleton` para um arquivo, como no exemplo a seguir.

   ```
   aws cloudtrail lookup-events --event-category insight --generate-cli-skeleton >
    LookupEvents.txt
   ```

   O arquivo de modelo gerado (nesse caso, LookupEvents .txt) tem a seguinte aparência.

   ```
   {
       "LookupAttributes": [
           {
               "AttributeKey": "",
               "AttributeValue": ""
           }
       ],
   ```

```
    "StartTime": null,
    "EndTime": null,
    "MaxResults": 0,
    "NextToken": ""
}
```

2. Use um editor de texto para modificar o JSON conforme necessário. A entrada do JSON precisa conter apenas os valores especificados.

> **Important**
>
> Todos os valores nulos ou vazios precisam ser removidos do modelo antes que ele seja usado.

O exemplo a seguir especifica um período e o número máximo de resultados a serem retornados.

```
{
    "StartTime": "2023-11-01",
    "EndTime": "2023-12-12",
    "MaxResults": 10
}
```

3. Para usar o arquivo editado como entrada, use a sintaxe `--cli-input-json file://<filename>`, como no exemplo a seguir.

```
aws cloudtrail lookup-events --event-category insight --cli-input-json file://
LookupEvents.txt
```

> **Note**
>
> É possível usar outros argumentos na mesma linha de comando como `--cli-input-json`.

Pesquisar campos de resultados

Eventos

Uma lista de eventos de pesquisa com base no atributo de pesquisa e no período que foram especificados. A lista de eventos é classificada por tempo, com o último evento listado primeiro. Cada entrada contém informações sobre a solicitação de pesquisa e inclui uma representação em cadeia de caracteres do CloudTrail evento que foi recuperado.

As seguintes entradas descrevem os campos de cada evento de pesquisa.

CloudTrailEvent

Uma string JSON que contém uma representação do objeto do evento retornado. Para obter informações sobre cada um dos elementos retornados, consulte Conteúdo do corpo do registro.

EventId

Uma string que contém a GUID do evento retornado.

EventName

Uma string que contém o nome do evento retornado.

EventSource

O AWS serviço para o qual a solicitação foi feita.

EventTime

A data e a hora, em formato de horário do UNIX, do evento.

Recursos

Uma lista de recursos referenciados pelo evento que foi retornado. Cada entrada de recurso especifica um tipo e um nome do recurso.

ResourceName

Uma string que contém o nome do recurso referenciado pelo evento.

ResourceType

Uma string que contém o tipo de um recurso referenciado pelo evento. Quando o tipo de recurso não pode ser determinado, null é retornado.

Username

Uma string que contém o nome do usuário da conta do evento retornado.

NextToken

Uma string para obter a próxima página de resultados de um comando `lookup-events` anterior. Para usar o token, os parâmetros precisam ser os mesmos do comando original. Se nenhuma entrada `NextToken` aparecer nos resultados, significa que não há mais resultados a serem retornados.

Para obter mais informações sobre os eventos do CloudTrail Insights, consulte Registrar eventos do Insights este guia.

Copiando eventos da trilha para o CloudTrail lago

Você pode copiar eventos de trilha existentes para um armazenamento de dados de eventos do CloudTrail Lake para criar um point-in-time instantâneo dos eventos registrados na trilha. Copiar eventos da trilha não interfere na capacidade da trilha de registrar eventos e não modifica a trilha de nenhuma forma.

Você pode copiar eventos de trilha para um armazenamento de dados de eventos existente configurado para CloudTrail eventos ou pode criar um novo armazenamento de dados de CloudTrail eventos e escolher a opção Copiar eventos de trilha como parte da criação do armazenamento de dados de eventos. Para obter mais informações sobre cópia de eventos de trilhas para um armazenamento de dados de eventos existente, consulte Copie eventos de trilha para um armazenamento de dados de eventos existente usando o CloudTrail console. Para obter mais informações sobre como criar um armazenamento de dados de eventos, consulte Crie um armazenamento de dados de CloudTrail eventos para eventos com o console.

Copiar eventos de trilha para um armazenamento de dados de eventos do CloudTrail Lake permite que você execute consultas sobre os eventos copiados. CloudTrail As consultas do Lake oferecem uma visão mais profunda e personalizável dos eventos do que pesquisas simples de chaves e valores no histórico de eventos ou em execução. `LookupEvents` Para obter mais informações sobre CloudTrail Lake, consulteTrabalhando com AWS CloudTrail Lake.

Se estiver copiando eventos de trilha para um armazenamento de dados de eventos da organização, você deve usar a conta de gerenciamento da respectiva organização. Não é possível copiar eventos de trilha usando uma conta de administrador delegado para uma organização.

CloudTrail Os armazenamentos de dados de eventos em Lake incorrem em cobranças. Ao criar um armazenamento de dados de eventos, você escolhe a opção de preço que deseja usar para ele. A opção de preço determina o custo para a ingestão e para o armazenamento de eventos, e

o período de retenção padrão e máximo para o armazenamento de dados de eventos. Para obter informações sobre CloudTrail preços e gerenciamento de custos do Lake, consulte AWS CloudTrail Preços Gerenciando os custos CloudTrail do Lake e.

Ao copiar eventos de trilha para um armazenamento de dados de eventos do CloudTrail Lake, você incorre em cobranças com base na quantidade de dados não compactados que o armazenamento de dados de eventos ingere.

Ao copiar eventos de trilha para o CloudTrail Lake, CloudTrail descompacta os registros armazenados no formato gzip (compactado) e, em seguida, copia os eventos contidos nos registros para seu armazenamento de dados de eventos. O tamanho dos dados não compactados pode ser maior do que o tamanho real do armazenamento do S3. Para obter uma estimativa geral do tamanho dos dados não compactados, é possível multiplicar o tamanho dos registros no bucket do S3 por 10.

É possível pode reduzir os custos especificando um intervalo de tempo mais restrito para os eventos copiados. Se você planeja usar apenas o armazenamento de dados de eventos para consultar seus eventos copiados, poderá desativar a ingestão de eventos para evitar cobranças em eventos futuros. Para obter mais informações, consulte Preços do AWS CloudTrail e Gerenciando os custos CloudTrail do Lake.

Cenários

A tabela a seguir descreve alguns cenários comuns para copiar eventos de trilha e como você realiza cada cenário usando o console.

Cenário	Como faço isso no console?
Analise e consulte eventos históricos de trilhas em CloudTrail Lake sem ingerir novos eventos	Crie um novo armazenamento de dados de eventos e escolha a opção Copiar eventos da trilha como parte da criação do armazenamento de dados de eventos. Ao criar o armazenam ento de dados de eventos, desmarque a opção Ingerir eventos (etapa 15 do procedimento) para garantir que o armazenamento de dados de eventos contenha somente os eventos históricos da sua trilha e nenhum evento futuro.
Substitua sua trilha existente por um armazenamento de dados de eventos do CloudTrail Lake	Crie um armazenamento de dados de eventos com os mesmos seletores de eventos que sua trilha para garantir que o armazenamento de dados de eventos tenha a mesma cobertura da trilha.

Cenário	Como faço isso no console?
	Para evitar a duplicação de eventos entre a trilha de origem e o armazenamento de dados de eventos de destino, escolha um intervalo de datas para os eventos copiados que seja anterior à criação do armazenamento de dados de eventos. Após a criação do armazenamento de dados de eventos, você poderá desativar o registro em log da trilha para evitar cobranças adicionais.

Tópicos

Considerações para copiar eventos de trilhas

Considere os seguintes fatores ao copiar eventos de trilhas.

- Ao copiar eventos de trilha, CloudTrail usa a operação da `GetObject`API do S3 para recuperar os eventos de trilha no bucket do S3 de origem. Há algumas classes de armazenamento arquivadas no S3, como os níveis de S3 Glacier Flexible Retrieval, S3 Glacier Deep Archive, S3 Outposts e S3 Intelligent-Tiering Deep Archive que não são acessíveis via `GetObject`. Para copiar eventos de trilhas armazenados nessas classes de armazenamento arquivadas, primeiro é necessário restaurar uma cópia usando a operação `RestoreObject` do S3. Para obter informações sobre como restaurar objetos arquivados, consulte Restaurar objetos arquivados no Guia do usuário do Amazon S3.
- Quando você copia eventos de trilha para um armazenamento de dados de eventos, CloudTrail copia todos os eventos de trilha, independentemente da configuração dos tipos de eventos do armazenamento de dados de eventos de destino, seletores de eventos avançados ou Região da AWS.
- Antes de copiar eventos de trilha para um armazenamento de dados de eventos existente, certifique-se de que a opção de preço e o período de retenção do armazenamento de dados de eventos estejam configurados adequadamente para seu caso de uso.

  - Opção de preço: a opção de preço determina o custo de ingestão e armazenamento de eventos. Para obter mais informações sobre opções de preço, consulte Preço do AWS CloudTrail e Opções de preços do armazenamento de dados de eventos.
  - Período de retenção: o período de retenção determina por quanto tempo os dados do evento são mantidos no armazenamento de dados do evento. CloudTrail copia somente eventos de trilha que tenham um período de retenção `eventTime` dentro do armazenamento de dados de eventos. Para determinar o período de retenção adequado, calcule a soma do evento mais antigo que você deseja copiar em dias e o número de dias em que deseja reter os eventos no armazenamento de dados do evento (período de retenção = *`oldest-event-in-days`*+ *`number-days-to-retain`*). Por exemplo, se o evento mais antigo que você está copiando tiver 45 dias e você quiser manter os eventos no armazenamento de dados de eventos por mais 45 dias, defina o período de retenção como 90 dias.
- Se você estiver copiando eventos de trilha para um armazenamento de dados de eventos para investigação e não quiser ingerir nenhum evento futuro, poderá interromper a ingestão no armazenamento de dados de eventos. Ao criar o armazenamento de dados de eventos, desmarque a opção Ingerir eventos (etapa 15 do procedimento) para garantir que o armazenamento de dados de eventos contenha somente os eventos históricos da sua trilha e nenhum evento futuro.
- Antes de copiar os eventos da trilha, desative todas as listas de controle de acesso (ACLs) anexadas ao bucket do S3 de origem e atualize a política do bucket do S3 para o armazenamento de dados de eventos de destino. Para obter mais informações sobre a atualização da política de bucket do S3, consulte Política de buckets do Amazon S3 para copiar eventos da trilha. Para obter mais informações sobre a desabilitação de ACLs, consulte Controlar a propriedade de objetos e desabilitar ACLs para seu bucket.
- CloudTrail copia somente eventos de trilha de arquivos de log compactados Gzip que estão no bucket S3 de origem. CloudTrail não copia eventos de trilha de arquivos de log não compactados ou arquivos de log que foram compactados usando um formato diferente de Gzip.
- Para evitar a duplicação de eventos entre a trilha de origem e o armazenamento de dados de eventos de destino, escolha um intervalo de tempo para os eventos copiados que seja anterior à criação do armazenamento de dados de eventos.
- Por padrão, copia CloudTrail somente CloudTrail os eventos contidos no prefixo do bucket do S3 e os `CloudTrail` prefixos dentro do `CloudTrail` prefixo, e não verifica os prefixos de outros serviços. AWS Se quiser copiar CloudTrail eventos contidos em outro prefixo, você deve escolher o prefixo ao copiar eventos de trilha.

- Para copiar eventos de trilha para um armazenamento de dados de eventos da organização, você deve usar a conta de gerenciamento da organização. Não é possível usar a conta de administrador delegado para copiar eventos de trilhas para um armazenamento de dados de eventos da organização.

Permissões necessárias para copiar eventos da trilha

Antes de copiar os eventos da trilha, verifique se você tem todas as permissões necessárias para sua função do IAM. Se você escolher um perfil do IAM existente para copiar os eventos da trilha, atualizar as permissões do perfil do IAM será o suficiente. Se você optar por criar uma nova função do IAM, CloudTrail forneça todas as permissões necessárias para a função.

Se o bucket do S3 de origem usar uma chave KMS para criptografia de dados, certifique-se de que a política de chaves do KMS permita CloudTrail descriptografar dados no bucket. Se o bucket do S3 de origem usar várias chaves KMS, você deverá atualizar a política de cada chave CloudTrail para permitir a descriptografia dos dados no bucket.

Tópicos

Permissões do IAM para copiar eventos da trilha

Ao copiar os eventos da trilha, você tem a opção de criar um perfil do IAM ou usar um perfil do IAM existente. Quando você escolhe uma nova função do IAM, CloudTrail cria uma função do IAM com as permissões necessárias e nenhuma ação adicional é necessária de sua parte.

Se você escolher uma função existente, certifique-se de que as políticas da função do IAM CloudTrail permitam copiar eventos de trilha do bucket S3 de origem. Esta seção fornece exemplos das políticas de confiança e permissões do perfil do IAM necessárias.

O exemplo a seguir fornece a política de permissões, que CloudTrail permite copiar eventos de trilha do bucket S3 de origem. Substitua *myBucketNamemyAccountId*, *region*, *prefix* e *eventDataStoreId* pelos valores apropriados para sua configuração. O *myAccountID* é o ID da AWS conta usado para o CloudTrail Lake, que pode não ser o mesmo que o ID da AWS conta para o bucket do S3.

Substitua *key-region*, *keyAccountID* e *keyID* pelos valores da chave do KMS usada para criptografar o bucket do S3 de origem. Você poderá omitir a instrução `AWSCloudTrailImportKeyAccess` se o bucket do S3 de origem não usar uma chave KMS para criptografia.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSCloudTrailImportBucketAccess",
      "Effect": "Allow",
      "Action": ["s3:ListBucket", "s3:GetBucketAcl"],
      "Resource": [
        "arn:aws:s3:::myBucketName"
      ],
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "myAccountID",
          "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdataStore/eventDataStoreId"
        }
       }
    },
    {
      "Sid": "AWSCloudTrailImportObjectAccess",
      "Effect": "Allow",
      "Action": ["s3:GetObject"],
      "Resource": [
        "arn:aws:s3:::myBucketName/prefix",
        "arn:aws:s3:::myBucketName/prefix/*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "myAccountID",
          "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdataStore/eventDataStoreId"
        }
       }
    },
    {
      "Sid": "AWSCloudTrailImportKeyAccess",
      "Effect": "Allow",
      "Action": ["kms:GenerateDataKey","kms:Decrypt"],
```

```
      "Resource": [
        "arn:aws:kms:key-region:keyAccountID:key/keyID"
      ]
    }
  ]
}
```

O exemplo a seguir fornece a política de confiança do IAM, que CloudTrail permite assumir uma função do IAM para copiar eventos de trilha do bucket S3 de origem. Substitua *myAccountId*, *region* e *eventDataStoreId* pelos valores apropriados para sua configuração. O *myAccountID* é o ID da AWS conta usado para o CloudTrail Lake, que pode não ser o mesmo que o ID da AWS conta para o bucket do S3.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "myAccountID",
          "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdataStore/eventDataStoreId"
        }
      }
    }
  ]
}
```

Política de buckets do Amazon S3 para copiar eventos da trilha

Por padrão, os buckets e objetos do Amazon S3 são privados. Somente o proprietário do recurso (a conta da AWS que criou o bucket) pode acessar o bucket e os objetos que ele contém. O proprietário do recurso pode conceder permissões de acesso a outros recursos e usuários ao criar uma política de acesso padrão.

Antes de copiar eventos de trilha, você deve atualizar a política de bucket do S3 para permitir CloudTrail a cópia de eventos de trilha do bucket.

Você pode adicionar a seguinte declaração à política de bucket do S3 para conceder essas permissões. Substitua *roLearn* e *myBucketName*pelos valores apropriados para sua configuração.

```
{
  "Sid": "AWSCloudTrailImportBucketAccess",
  "Effect": "Allow",
  "Action": [
    "s3:ListBucket",
    "s3:GetBucketAcl",
    "s3:GetObject"
  ],
  "Principal": {
    "AWS": "roleArn"
  },
  "Resource": [
    "arn:aws:s3:::myBucketName",
    "arn:aws:s3:::myBucketName/*"
  ]
},
```

Política de chaves do KMS para descriptografar dados no bucket do S3 de origem

Se o bucket do S3 de origem usar uma chave KMS para criptografia de dados, certifique-se de que a política de chaves do KMS forneça CloudTrail `kms:GenerateDataKey` as permissões `kms:Decrypt` e as permissões necessárias para copiar eventos de trilha de um bucket do S3 com a criptografia SSE-KMS ativada. Se o bucket do S3 de origem usar várias chaves do KMS, será necessário atualizar a política de cada chave. A atualização da política de chaves do KMS permite CloudTrail descriptografar dados no bucket S3 de origem, executar verificações de validação para garantir que os eventos estejam em conformidade com os CloudTrail padrões e copiar eventos para o armazenamento de dados de eventos do Lake. CloudTrail

O exemplo a seguir fornece a política de chaves do KMS, que permite CloudTrail descriptografar os dados no bucket S3 de origem. Substitua *roLearn myBucketName*, *myAccountId*, *region* e *eventDataStoreId* pelos valores apropriados para sua configuração. O *myAccountID* é o ID da AWS conta usado para o CloudTrail Lake, que pode não ser o mesmo que o ID da AWS conta para o bucket do S3.

```
{
  "Sid": "AWSCloudTrailImportDecrypt",
  "Effect": "Allow",
  "Action": [
          "kms:Decrypt",
          "kms:GenerateDataKey"
  ],
  "Principal": {
    "AWS": "roleArn"
  },
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::myBucketName/*"
    },
    "StringEquals": {
      "aws:SourceAccount": "myAccountID",
      "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdataStore/eventDataStoreId"
    }
  }
}
```

Copie eventos de trilha para um armazenamento de dados de eventos existente usando o CloudTrail console

Use o procedimento a seguir para copiar eventos de trilha para um armazenamento de dados de eventos existentes. Para obter informações sobre como criar um armazenamento de dados de eventos, consulte Crie um armazenamento de dados de CloudTrail eventos para eventos com o console.

> **Note**
>
> Antes de copiar eventos de trilha para um armazenamento de dados de eventos existente, certifique-se de que a opção de preço e o período de retenção do armazenamento de dados de eventos estejam configurados adequadamente para seu caso de uso.
>
> - Opção de preço: a opção de preço determina o custo de ingestão e armazenamento de eventos. Para obter mais informações sobre opções de preço, consulte Preço do AWS CloudTrail e Opções de preços do armazenamento de dados de eventos.

- Período de retenção: o período de retenção determina por quanto tempo os dados do evento são mantidos no armazenamento de dados do evento. CloudTrail copia somente eventos de trilha que tenham um período de retenção `eventTime` dentro do armazenamento de dados de eventos. Para determinar o período de retenção adequado, calcule a soma do evento mais antigo que você deseja copiar em dias e o número de dias em que deseja reter os eventos no armazenamento de dados do evento (período de retenção = *`oldest-event-in-days`*+ *`number-days-to-retain`*). Por exemplo, se o evento mais antigo que você está copiando tiver 45 dias e você quiser manter os eventos no armazenamento de dados de eventos por mais 45 dias, defina o período de retenção como 90 dias.

Para copiar eventos de trilhas para um armazenamento de dados de eventos

1. Faça login no AWS Management Console e abra o CloudTrail console em https://console.aws.amazon.com/cloudtrail/.
2. Escolha Trilhas no painel de navegação esquerdo do CloudTrail console.
3. Na página Trails (Trilhas), escolha a trilha e, em seguida, escolha Copy events to Lake (Copiar eventos para o Lake). Se o bucket S3 de origem da trilha usar uma chave KMS para criptografia de dados, certifique-se de que a política de chaves do KMS permita CloudTrail descriptografar dados no bucket. Se o bucket do S3 de origem usar várias chaves KMS, você deverá atualizar a política de cada chave CloudTrail para permitir a descriptografia de dados no bucket. Para obter mais informações sobre a atualização da política de chaves do KMS, consulte Política de chaves do KMS para descriptografar dados no bucket do S3 de origem.
4. (Opcional) Por padrão, copia CloudTrail somente CloudTrail os eventos contidos no prefixo do bucket do S3 e os `CloudTrail` prefixos dentro do `CloudTrail` prefixo, e não verifica os prefixos de outros serviços. AWS Se você quiser copiar CloudTrail eventos contidos em outro prefixo, escolha Inserir URI do S3 e, em seguida, escolha Procurar no S3 para navegar até o prefixo.

   A política de bucket do S3 deve conceder CloudTrail acesso a eventos de trilha de cópia. Para obter mais informações sobre a atualização da política de bucket do S3, consulte Política de buckets do Amazon S3 para copiar eventos da trilha.
5. Em Especificar um intervalo de tempo de eventos, escolha o intervalo de tempo para copiar os eventos. CloudTrail verifica o prefixo e o nome do arquivo de log para verificar se o nome contém uma data entre as datas de início e término escolhidas antes de tentar copiar os eventos

da trilha. É possível escolher entre Relative range (Intervalo relativo) e Absolute range (Intervalo absoluto). Para evitar a duplicação de eventos entre a trilha de origem e o armazenamento de dados de eventos de destino, escolha um intervalo de tempo que seja anterior à criação do armazenamento de dados de eventos.

> **Note**
>
> CloudTrail copia somente eventos de trilha que tenham um período de retenção `eventTime` dentro do armazenamento de dados de eventos. Por exemplo, se o período de retenção de um armazenamento de dados de eventos for de 90 dias, não CloudTrail copiará nenhum evento de trilha com `eventTime` mais de 90 dias.

- Se você escolher Intervalo relativo, poderá optar por copiar eventos registrados nos últimos 6 meses, 1 ano, 2 anos, 7 anos ou um intervalo personalizado. CloudTrail copia os eventos registrados dentro do período de tempo escolhido.
- Se você escolher Intervalo absoluto, poderá escolher uma data específica de início e término. CloudTrail copia os eventos que ocorreram entre as datas de início e término escolhidas.

6. Em Delivery location (Local de entrega), escolha o armazenamento de dados de eventos de destino na lista suspensa.
7. Em Permissions (Permissões), escolha uma das opções de perfil do IAM a seguir. Ao escolher um perfil do IAM existente, verifique se a política de perfil do IAM fornece as permissões necessárias. Para obter mais informações sobre como atualizar as permissões do perfil do IAM, consulte Permissões do IAM para copiar eventos da trilha.

   - Escolha Create a new role (recommended) (Criar uma nova função [recomendado]) para criar um novo perfil do IAM. Em Enter IAM role name (Inserir nome do perfil do IAM), insira um nome exclusivo para o perfil. CloudTrail cria automaticamente as permissões necessárias para essa nova função.
   - Escolha Usar um ARN de função personalizada do IAM para usar uma função personalizada do IAM que não esteja listada. Em Enter IAM role ARN (Inserir ARN do perfil do IAM), insira o ARN do perfil.
   - Escolha uma função do IAM existente na lista suspensa.
8. Escolha Copy events (Copiar eventos).

9. Será necessário confirmar a cópia. Quando estiver pronto para confirmar, escolha Copy trail events to Lake (Copiar eventos da trilha para o Lake) e, em seguida, escolha Copy events (Copiar eventos).
10. Na página Copy details (Copiar detalhes), é possível ver o status da cópia e revisar quaisquer falhas. Quando uma cópia de evento de trilha é concluída, seu Copy status (Status de cópia) é definido como Completed (Concluída) se não houve erros ou como Failed (Falha) se houve algum erro.

    > **Note**
    >
    > Os detalhes apresentados na página de detalhes da cópia do evento não estão em tempo real. Os valores reais dos detalhes, como Prefixes copied (prefixos copiados), podem ser maiores do que os apresentados na página. CloudTrail atualiza os detalhes de forma incremental ao longo da cópia do evento.

11. Se o Copy status (Status da cópia) for Failed (Falha), corrija os erros mostrados em Copy failures (Falhas ao copiar) e, em seguida, escolha Retry copy (Tentar cópia novamente). Quando você tenta fazer uma cópia novamente, CloudTrail retoma a cópia no local em que a falha ocorreu.

Para obter mais informações sobre como visualizar os detalhes de uma cópia de evento de trilha, consulte Detalhes da cópia de um evento.

Obtendo e visualizando seus arquivos de CloudTrail log

Depois que você criar uma trilha e configurá-la para capturar os arquivos de log desejados, será necessário encontrá-los e interpretar as informações que eles contêm.

CloudTrail entrega seus arquivos de log para um bucket do Amazon S3 que você especifica ao criar a trilha. CloudTrail normalmente entrega registros em uma média de cerca de 5 minutos após uma chamada de API. Desta vez não há garantias. Consulte o Acordo de Nível de Serviço do AWS CloudTrail para obter mais informações. Os eventos do Insights normalmente são entregues ao bucket em até 30 minutos da atividade incomum. Após habilitar o Insights pela primeira vez, aguarde até 36 horas para ver os primeiros eventos do Insights caso seja detectada atividade incomum.

> **Note**
>
> Se você configurar incorretamente sua trilha (por exemplo, o bucket do S3 está inacessível), CloudTrail tentará reenviar os arquivos de log para o bucket do S3 por 30 dias, e esses attempted-to-deliver eventos estarão sujeitos às cobranças padrão. CloudTrail Para evitar cobranças em uma trilha mal configurada, você precisa excluir a trilha.

Tópicos

Encontrando seus arquivos CloudTrail de log

CloudTrail publica arquivos de log no seu bucket do S3 em um arquivo gzip. No bucket do S3, o arquivo de log tem um nome formatado que inclui os seguintes elementos:

- O nome do bucket que você especificou ao criar a trilha (encontrado na página Trilhas do CloudTrail console)
- O prefixo (opcional) que você especificou quando criou sua trilha
- A string "AWSLogs”
- O número da conta
- A string "CloudTrail”
- Um identificador de região, como us-west-1
- O ano em que o arquivo de log foi publicado no formato YYYY
- O mês em que o arquivo de log foi publicado no formato MM
- O dia em que o arquivo de log foi publicado no formato DD
- Uma string alfanumérica que distingue o arquivo dos demais que cobrem o mesmo período

O exemplo a seguir mostra o nome completo de um objeto do arquivo de log:

```
bucket_name/prefix_name/AWSLogs/Account ID/
CloudTrail/region/YYYY/MM/DD/file_name.json.gz
```

> **Note**
>
> Para trilhas organizacionais, o nome do objeto do arquivo de log no bucket do S3 inclui o ID da unidade organizacional no caminho, da seguinte forma:
>
> ```
> bucket_name/prefix_name/AWSLogs/O-ID/Account ID/
> CloudTrail/Region/YYYY/MM/DD/file_name.json.gz
> ```

Para recuperar um arquivo de log, é possível usar o console do Amazon S3, a interface de linha de comando (CLI) ou a API do Amazon S3.

Para localizar seus arquivos de log com o console do Amazon S3

1. Abra o console Amazon S3.
2. Escolha o bucket que você especificou.
3. Navegue pela hierarquia de objetos até encontrar o arquivo de log desejado.

   Todos os arquivos de log têm uma extensão .gz.

Você navegará por uma hierarquia de objetos semelhante ao exemplo a seguir, mas com nome de bucket, ID da conta, região e data diferentes.

```
All Buckets
    Bucket_Name
        AWSLogs
            123456789012
                CloudTrail
                    us-west-1
                        2014
                            06
                                20
```

Um arquivo de log para a hierarquia de objetos anterior terá a seguinte aparência:

```
123456789012_CloudTrail_us-west-1_20140620T1255ZHdkvFTXOA3Vnhbc.json.gz
```

> **Note**
>
> Você pode receber arquivos de log que contêm um ou mais eventos duplicados, embora isso seja incomum. Na maioria dos casos, eventos duplicados terão o mesmo `eventID`. Para obter mais informações sobre o campo `eventID`, consulte CloudTrail conteúdo do registro.

Baixando seus arquivos CloudTrail de log

Os arquivos de log estão em formato JSON. Se você tiver um complemento de visualizador de JSON instalado, poderá visualizar os arquivos diretamente no navegador. Clique duas vezes no nome do arquivo de log no bucket para abrir uma janela ou guia do navegador. O JSON é exibido em formato de leitura.

CloudTrail arquivos de log são objetos do Amazon S3. Você pode usar o console do Amazon S3, a (AWS Command Line Interface CLI) ou a API do Amazon S3 para recuperar arquivos de log.

Para obter mais informações, consulte a visão geral dos objetos do Amazon S3 no Guia do usuário do Amazon Simple Storage Service.

O procedimento a seguir descreve como fazer download de um arquivo de log com o AWS Management Console.

Para fazer download e ler um arquivo de log

1. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Escolha o bucket e o arquivo de log que você deseja fazer download.
3. Escolha Download ou Download as e siga as instruções na tela para salvar o arquivo. Essa ação salva o arquivo no formato compactado.

   > **Note**
   >
   > Alguns navegadores, como o Chrome, extraem automaticamente o arquivo de log para você. Se o navegador fizer isso, pule para a etapa 5.

4. Use um produto como o 7-Zip para extrair o arquivo de log.
5. Abra o arquivo de log em um editor de texto, como o Notepad++.

Para obter mais informações sobre os campos de eventos que podem aparecer na entrada de um arquivo de log, consulte CloudTrail conteúdo do registro.

AWS faz parceria com especialistas terceirizados em registro e análise para fornecer soluções que usam CloudTrail resultados. Para obter mais informações, consulte AWS CloudTrail parceiros.

> **Note**
>
> Você também pode usar o recurso de Histórico de eventos para procurar eventos de criação, atualização e exclusão de atividades de APIs nos últimos 90 dias.
> Para ter mais informações, consulte Trabalhando com o histórico de CloudTrail eventos.

Configurando notificações do Amazon SNS para CloudTrail

Você pode ser notificado quando CloudTrail publicar novos arquivos de log em seu bucket do Amazon S3. Gerencie notificações usando o Amazon Simple Notification Service (Amazon SNS).

As notificações são opcionais. Se você quiser notificações, configure CloudTrail para enviar informações de atualização para um tópico do Amazon SNS sempre que um novo arquivo de log for enviado. Para receber essas notificações, é possível usar o Amazon SNS para se inscrever no tópico. Como assinante, você pode receber atualizações enviadas a uma fila do Amazon Simple Queue Service (Amazon SQS), que permite processar essas notificações de modo programático.

Tópicos

- Configurando CloudTrail para enviar notificações

Configurando CloudTrail para enviar notificações

É possível configurar uma trilha para usar um tópico do Amazon SNS. Você pode usar o CloudTrail console ou o comando aws cloudtrail create-trailCLI para criar o tópico. CloudTrail cria o tópico do Amazon SNS para você e anexa uma política apropriada, para que CloudTrail tenha permissão para publicar nesse tópico.

Quando você cria o nome de um tópico do SNS, ele deve atender aos seguintes requisitos:

- Ter entre 1 e 256 caracteres
- Conter letras maiúsculas e minúsculas ASCIIs, números, sublinhados ou hífens

Quando você configura as notificações de uma trilha que se aplica a todas as regiões, as notificações de todas as regiões serão enviadas ao tópico do Amazon SNS que você especificar. Se você tem uma ou mais trilhas específicas da região, deve criar um tópico separado para cada região e se inscrever em cada um deles individualmente.

Para receber notificações, assine o tópico ou tópicos do Amazon SNS que CloudTrail usa. Isso é feito com o console ou com os comandos CLI do Amazon SNS. Para obter instruções, consulte Assinatura de um tópico do Amazon SNS no Guia do desenvolvedor do Amazon Simple Notification Service.

> **Note**
>
> CloudTrail envia uma notificação quando os arquivos de log são gravados no bucket do Amazon S3. Uma conta ativa pode gerar um grande número de notificações. Se você se inscrever para receber e-mails ou mensagens SMS, poderá receber um grande volume de mensagens. Recomendamos que você se inscreva usando o Amazon Simple Queue Service (Amazon SQS), que permite controlar as notificações de maneira programática. Para obter mais informações,consulte Subscribing an Amazon SQS queue to an Amazon SNS topic (console) no Guia do desenvolvedor do Amazon Simple Queue Service.

A notificação do Amazon SNS consiste em um objeto JSON que inclui um campo `Message`. O campo `Message` lista o caminho completo para o arquivo de log, como mostrado no exemplo a seguir:

```
{
    "s3Bucket": "your-bucket-name","s3ObjectKey": ["AWSLogs/123456789012/
CloudTrail/us-east-2/2013/12/13/123456789012_CloudTrail_us-
west-2_20131213T1920Z_LnPgDQnpkSKEsppV.json.gz"]
}
```

Se vários arquivos de log forem fornecidos ao bucket do Amazon S3, uma notificação poderá conter vários logs, conforme mostrado no seguinte exemplo:

```
{
    "s3Bucket": "your-bucket-name",
    "s3ObjectKey": [
        "AWSLogs/123456789012/CloudTrail/us-
east-2/2016/08/11/123456789012_CloudTrail_us-
east-2_20160811T2215Z_kpaMYavMQA9Ahp7L.json.gz",
```

```
        "AWSLogs/123456789012/CloudTrail/us-
east-2/2016/08/11/123456789012_CloudTrail_us-
east-2_20160811T2210Z_zqDkyQv3TK8ZdLr0.json.gz",
        "AWSLogs/123456789012/CloudTrail/us-
east-2/2016/08/11/123456789012_CloudTrail_us-
east-2_20160811T2205Z_jaMVRa6JfdLCJYHP.json.gz"
    ]
}
```

Se você optar por receber notificações por e-mail, o corpo do e-mail consistirá no conteúdo do campo `Message`. Para obter informações sobre a estrutura JSON, consulte Fanout para filas do Amazon SQS no Guia do desenvolvedor do Amazon Simple Notification Service. Somente o `Message` campo mostra CloudTrail informações. Os outros campos contêm informações do serviço do Amazon SNS.

Se você criar uma trilha com a CloudTrail API, poderá especificar um tópico existente do Amazon SNS para o qual CloudTrail deseja enviar notificações com as operações `CreateTrail`ou `UpdateTrail`. Você deve garantir que o tópico exista e tenha permissões que permitam CloudTrail enviar notificações a ele. Consulte Política de tópicos do Amazon SNS para CloudTrail.

Recursos adicionais do

Para obter mais informações sobre tópicos do Amazon SNS e como assiná-los, consulte o Guia do desenvolvedor do Amazon Simple Notification Service.

Dicas para gerenciar trilhas

- A partir de 12 de abril de 2019, as trilhas só podem ser visualizadas no Regiões da AWS local onde registram eventos. Se você criar uma trilha que registre todos os eventos Regiões da AWS, ela aparecerá no console em todas as partes Regiões da AWS da AWS partição em que você está trabalhando. Se você criar uma trilha que registra apenas eventos em uma única trilha Região da AWS, poderá visualizá-la e gerenciá-la somente nessa trilha Região da AWS.
- Para editar uma trilha na lista, escolha o nome dela.
- Configure pelo menos uma trilha que se aplique a todas as regiões para que você receba arquivos de log de todas as regiões na AWS partição em que você está trabalhando.
- Para registrar eventos de uma região específica e fornecer arquivos de log a um bucket do S3 na mesma região, é possível atualizar a trilha para aplicá-la a uma única região. Isso é útil se você deseja manter seus arquivos de log separados. Por exemplo, talvez você queira que os usuários

gerenciem seus próprios registros em regiões específicas ou separe CloudWatch os alarmes de registros por região.

- Para registrar eventos de várias AWS contas em uma trilha, considere criar uma organização AWS Organizations e, em seguida, criar uma trilha organizacional.
- Criar várias trilhas implicará custos adicionais. Para obter mais informações sobre preços, consulte Definição de preço do AWS CloudTrail.

Gerenciando os custos das CloudTrail trilhas

Como prática recomendada, recomendamos o uso de AWS serviços e ferramentas que possam ajudá-lo a gerenciar CloudTrail custos. Você também pode configurar e gerenciar CloudTrail trilhas de forma a capturar os dados de que precisa e, ao mesmo tempo, permanecer econômico. Para obter mais informações sobre CloudTrail preços, consulte AWS CloudTrail Preços.

Ferramentas para ajudar a gerenciar os custos

AWS Os orçamentos, um recurso do AWS Billing and Cost Management, permitem que você defina orçamentos personalizados que alertam você quando seus custos ou uso excedem (ou se prevê que excedam) o valor orçado.

Ao criar várias trilhas, criar um orçamento CloudTrail usando AWS Orçamentos é uma prática recomendada e pode ajudá-lo a controlar seus CloudTrail gastos. Orçamentos baseados em custos ajudam a promover a conscientização de quanto você pode ser cobrado por seu uso. CloudTrail alertas de orçamento notificam você quando sua fatura atinge um limite definido por você. Quando receber um alerta de orçamento, você poderá fazer alterações antes do fim do ciclo de faturamento para gerenciar seus custos.

Depois de criar um orçamento, você pode usá-lo AWS Cost Explorer para ver como seus CloudTrail custos estão influenciando sua AWS fatura geral. No AWS Cost Explorer, depois de adicionar CloudTrail ao filtro Serviço, você pode comparar seus CloudTrail gastos históricos com os gastos atuais month-to-date (MTD), por região e conta. Esse recurso ajuda você a monitorar e detectar custos inesperados em seus CloudTrail gastos mensais. Os recursos adicionais do Cost Explorer permitem comparar os CloudTrail gastos com os gastos mensais no nível de recurso específico, fornecendo informações sobre o que pode estar gerando aumentos ou reduções de custos em sua fatura.

> **Note**
>
> Embora você possa aplicar tags a CloudTrail trilhas, atualmente AWS Billing não é possível usar tags aplicadas a trilhas para alocação de custos. O Cost Explorer pode mostrar os custos dos armazenamentos de dados de eventos do CloudTrail Lake e do CloudTrail serviço como um todo.

Para começar a usar AWS Orçamentos AWS Billing and Cost Management, abra e escolha Orçamentos na barra de navegação à esquerda. Recomendamos configurar alertas de orçamento ao criar um orçamento para monitorar os CloudTrail gastos. Para obter mais informações sobre como usar AWS orçamentos, consulte Gerenciando seus custos com AWS Budgets e Melhores práticas para. AWS Budgets

Configuração da trilha

CloudTrail oferece flexibilidade na forma como você configura trilhas em sua conta. Algumas decisões que você toma durante o processo de configuração exigem que você entenda os impactos em sua CloudTrail fatura. Veja a seguir exemplos de como as configurações de trilhas podem influenciar sua CloudTrail fatura.

Criação de várias trilhas

A primeira cópia dos eventos de gerenciamento em cada região é entregue gratuitamente. Por exemplo, se sua conta tiver duas trilhas em uma única região, uma trilha de `us-east-1` entrada e outra de entrada`us-west-2`, não haverá CloudTrail cobranças porque há apenas um evento de registro de trilhas em cada região respectiva. No entanto, se sua conta tiver uma trilha multirregional e uma trilha adicional para uma única região, a trilha para uma única região incorrerá em cobranças porque a trilha multirregional já está registrando eventos em cada região.

Se você criar mais trilhas que entregam os mesmos eventos de gerenciamento para outros destinos, essas entregas subsequentes CloudTrail incorrerão em custos. Você pode fazer isso para permitir que diferentes grupos de usuários (como desenvolvedores, pessoal de segurança e auditores de TI) recebam suas próprias cópias dos arquivos de log. Para eventos de dados, todas as entregas incorrem em CloudTrail custos, incluindo a primeira.

Conforme você cria mais trilhas, é especialmente importante estar familiarizado com seus logs e compreender os tipos e os volumes de eventos que são gerados pelos recursos em sua conta. Isso ajuda você a prever o volume de eventos associados a uma conta e planejar os custos de

trilha. Por exemplo, usar criptografia AWS KMS gerenciada do lado do servidor (SSE-KMS) em seus buckets do S3 pode resultar em um grande número de eventos de gerenciamento em. AWS KMS CloudTrail Volumes maiores de eventos em várias trilhas também podem influenciar os custos.

Para ajudar a limitar o número de eventos registrados em sua trilha, você pode AWS KMS filtrar nossos eventos da API de dados do Amazon RDS escolhendo Excluir eventos ou Excluir AWS KMS eventos da API de dados do Amazon RDS nas páginas Criar trilha ou Atualizar trilha. Ao usar seletores de eventos básicos, você só pode filtrar eventos de gerenciamento. No entanto, é possível usar seletores de eventos avançados para filtrar eventos de gerenciamento e dados. Você pode usar seletores de eventos avançados para incluir ou excluir eventos de dados com base nos campos `resources.type`, `eventName`, `resources.ARN` e `readOnly`, permitindo que você registre somente os eventos de dados de interesse. Para obter mais informações sobre como configurar esses campos, consulte AdvancedFieldSelector. Para obter mais informações sobre como criar e atualizar uma trilha, consulte Criar uma trilha ou Atualizar uma trilha neste guia.

AWS Organizations

Quando você configura uma trilha de Organizations com CloudTrail, CloudTrail replica a trilha para cada conta de membro em sua organização. A nova trilha é criada além de quaisquer trilhas existentes nas contas-membro. Certifique-se de que a configuração da trilha da organização corresponda à forma como você deseja que as trilhas sejam configuradas para todas as contas em uma organização, pois a configuração da trilha da organização é propagada para todas as contas.

Como o Organizations cria uma trilha em cada conta-membro, uma conta-membro individual que crie uma trilha adicional para coletar os mesmos eventos de gerenciamento que a trilha do Organizations estará coletando uma segunda cópia dos eventos. A conta será cobrada pela segunda cópia. Da mesma forma, se uma conta tiver uma trilha de várias regiões e criar uma segunda trilha em uma região única para coletar os mesmos eventos de gerenciamento que a trilha de várias regiões, a trilha na região única estará fornecendo uma segunda cópia dos eventos. A segunda cópia gerará cobranças.

Consulte também

- Definição de preço do AWS CloudTrail
- Gerenciando seus custos com AWS Budgets

- Conceitos básicos do Explorador de Custos
- Preparar a criação de uma trilha para sua organização

Requisitos de nomenclatura

Esta seção fornece informações sobre os requisitos de nomenclatura para CloudTrail recursos, buckets do Amazon S3 e chaves KMS.

Tópicos

- CloudTrail requisitos de nomenclatura de recursos
- Requisitos de nomenclatura de buckets do Amazon S3
- AWS KMS requisitos de nomenclatura de aliases

CloudTrail requisitos de nomenclatura de recursos

CloudTrail os nomes dos recursos devem atender aos seguintes requisitos:

- Conter apenas letras (a-z, A-Z), números (0 – 9), pontos (.), sublinhados (_) ou traços (-) ASCII.
- Começar com uma letra ou um número e terminar com uma letra ou um número.
- Ter entre 3 e 128 caracteres.
- Não ter pontos, sublinhados ou traços adjacentes. Nomes como meu-_namespace e meu-\-namespace são inválidos.
- Não estar no formato de endereço IP (por exemplo, `192.168.5.4`).

Requisitos de nomenclatura de buckets do Amazon S3

O bucket do Amazon S3 que você usa para armazenar arquivos de CloudTrail log deve ter um nome que esteja em conformidade com os requisitos de nomenclatura para regiões fora do padrão dos EUA. O Amazon S3 define um nome de bucket como uma série de um ou mais rótulos, separados por pontos. Para obter uma lista completa das regras de nomenclatura, consulte as Regras de nomenclatura de buckets no Guia do usuário do Amazon Simple Storage Service.

Algumas das regras são:

- O nome do bucket pode ter entre 3 e 63 caracteres e conter apenas caracteres minúsculos, números, pontos e traços.

- Cada rótulo no nome do bucket deve começar com um número ou letra minúscula.
- O nome do bucket não pode conter sublinhados, terminar com um traço, ter pontos consecutivos ou usar traços adjacentes aos pontos.
- O nome do bucket não pode ser formatado como um endereço IP (198.51.100.24).

> **Warning**
>
> Como o S3 permite que seu bucket seja usado como um URL que pode ser acessado publicamente, o nome do bucket que você escolher deverá ser globalmente exclusivo. Se alguma outra conta já criou um bucket com o nome que você escolheu, será necessário usar outro nome. Para obter mais informações, consulte Restrições e limitações de bucket no Manual do usuário do Amazon Simple Storage Service.

AWS KMS requisitos de nomenclatura de aliases

Ao criar um AWS KMS key, você pode escolher um alias para identificá-lo. Por exemplo, você pode escolher o alias “KMS- CloudTrail -us-west-2" para criptografar os registros de uma trilha específica.

O alias deve atender aos seguintes requisitos:

- Ter entre 1 e 256 caracteres, inclusive
- Conter caracteres alfanuméricos (A-Z, a-z, 0-9), hífens (-), barras (/) e sublinhados (_)
- Não é permitido começar com aws

Para obter mais informações, consulte Criação de chaves no Guia do desenvolvedor AWS Key Management Service .

Criar várias trilhas

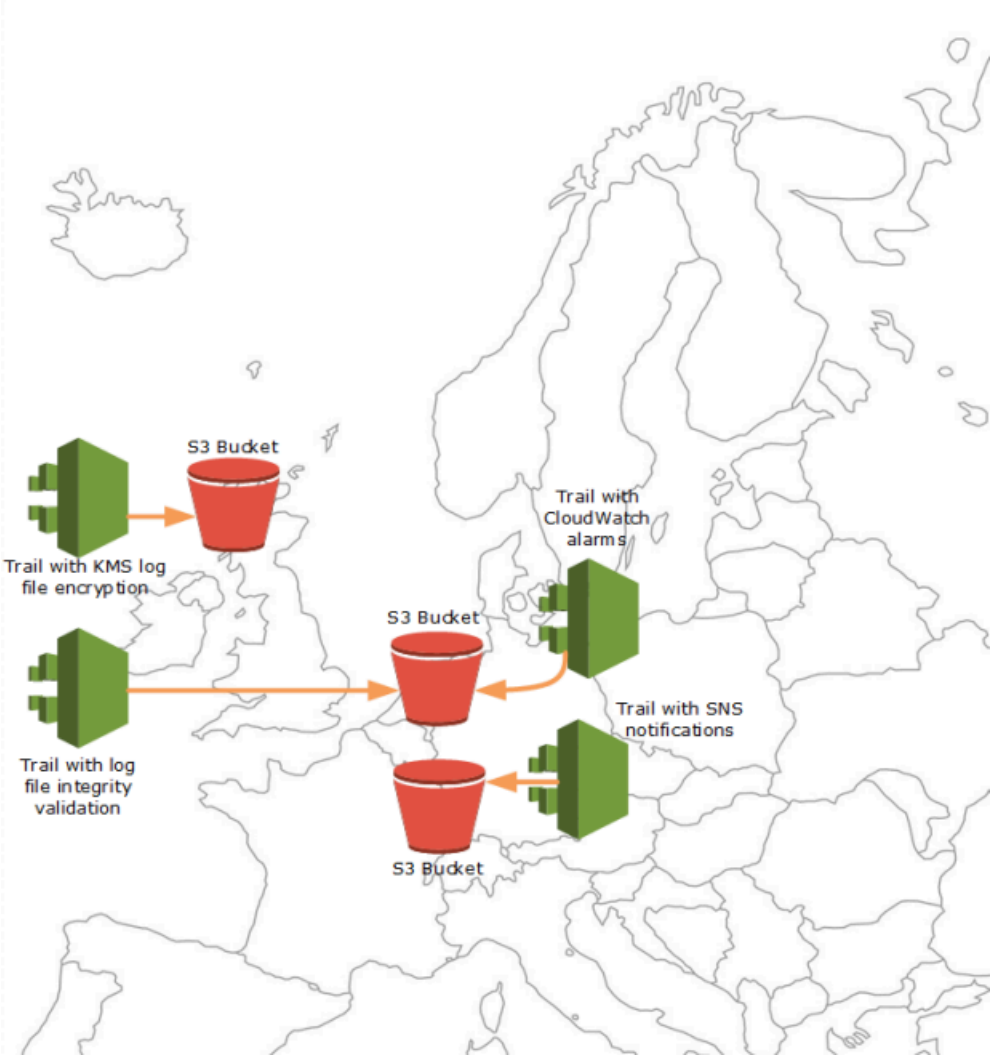
Você pode usar arquivos de CloudTrail log para solucionar problemas operacionais ou de segurança em sua AWS conta. Você pode criar trilhas para usuários diferentes, quem pode criar e gerenciar suas próprias trilhas. Você pode configurar as trilhas para fornecer arquivos de log a buckets do S3 separados ou compartilhados.

> **Note**
>
> A primeira cópia dos eventos de gerenciamento Região da AWS de cada conta é gratuita. Se você criar mais trilhas que entregam os mesmos eventos de gerenciamento para outros destinos, essas entregas subsequentes CloudTrail incorrerão em custos. Para obter mais informações sobre CloudTrail custos, consulte AWS CloudTrail Preços Gerenciando os custos das CloudTrail trilhas e.

Por exemplo, você pode ter os seguintes usuários:

- Um administrador de segurança cria uma trilha na região da Europa (Irlanda) e configura a criptografia de arquivos de log do KMS. A trilha fornece os arquivos de log a um bucket do S3 na região da Europa (Irlanda).
- Um auditor de TI cria uma trilha na região da Europa (Irlanda) e configura a validação da integridade do arquivo de log para garantir que os arquivos de log não tenham sido alterados desde que foram CloudTrail entregues. A trilha é configurada para fornecer arquivos de log a um bucket do S3 na região da Europa (Frankfurt)
- Um desenvolvedor cria uma trilha na região da Europa (Frankfurt) e configura CloudWatch alarmes para receber notificações sobre atividades específicas da API. A trilha compartilha o mesmo bucket do S3 que configurou para a integridade dos arquivos de log.
- Outro desenvolvedor cria uma trilha na região da Europa (Frankfurt) e configura o SNS. Os arquivos de log são fornecidos a um bucket do S3 separado na região da Europa (Frankfurt).

A imagem a seguir ilustra esse exemplo.



> **Note**
>
> Você pode criar até cinco trilhas por Região da AWS. Uma trilha multirregional conta como uma trilha por região.

Você pode usar permissões em nível de recurso para gerenciar a capacidade de um usuário de realizar operações específicas no. CloudTrail

Por exemplo, você pode conceder a um usuário permissão para visualizar as atividades de uma trilha, mas impedir que ele inicie ou interrompa o registro dela. Você pode conceder a outro usuário permissão total para criar e excluir trilhas. Desse modo, você tem o controle granular sobre as trilhas e o acesso do usuário.

Para obter mais informações sobre as permissões no nível do recurso, consulte Exemplos: criação e aplicação de políticas para ações em trilhas específicas.

Para obter mais informações sobre várias trilhas, consulte as CloudTrail perguntas frequentes.

Controle das permissões do usuário para CloudTrail trilhas

AWS CloudTrail se integra ao AWS Identity and Access Management (IAM) para ajudar você a controlar o acesso CloudTrail e outros AWS recursos CloudTrail necessários. Exemplos desses recursos incluem buckets do Amazon S3 e tópicos do Amazon Simple Notification Service (Amazon SNS). Você pode usar o IAM para controlar quais AWS usuários podem criar, configurar ou excluir CloudTrail trilhas, iniciar e interromper o registro e acessar os buckets que contêm informações de registro. Para saber mais, consulte Identity and Access Management para AWS CloudTrail.

Os tópicos a seguir ajudam você a entender as permissões, as políticas e a CloudTrail segurança:

- Concedendo permissões para administração CloudTrail
- Regras de nomenclatura de buckets do Amazon S3
- Política de bucket do Amazon S3 para CloudTrail
- Um exemplo de uma política de bucket para uma trilha de organização em Criando uma trilha para uma organização com o AWS Command Line Interface.
- Política de tópicos do Amazon SNS para CloudTrail
- Criptografando arquivos de CloudTrail log com AWS KMS chaves (SSE-KMS)
- Permissões necessárias para copiar eventos da trilha
- Permissões necessárias para atribuir um administrador delegado
- Política de chave KMS padrão criada no console CloudTrail
- Concedendo permissão para visualizar AWS Config informações no console CloudTrail
- Compartilhamento CloudTrail de arquivos de log entre AWS contas
- Permissões necessárias para criar uma trilha da organização
- Usando uma função do IAM existente anteriormente para adicionar monitoramento de uma trilha organizacional ao Amazon Logs CloudWatch

Usando AWS CloudTrail com interface VPC endpoints

Se você usa a Amazon Virtual Private Cloud (Amazon VPC) para hospedar seus AWS recursos, você pode estabelecer uma conexão privada entre sua VPC e. AWS CloudTrail Você pode usar essa conexão para permitir CloudTrail a comunicação com seus recursos em sua VPC sem passar pela Internet pública.

O Amazon VPC é um AWS serviço que você pode usar para lançar AWS recursos em uma rede virtual que você define. Com a VPC, você tem controle sobre as configurações de rede, como o intervalo de endereços IP, sub-redes, tabelas de rotas e gateways de rede. Com os VPC endpoints, o roteamento entre a VPC e os AWS serviços é gerenciado pela AWS rede, e você pode usar políticas do IAM para controlar o acesso aos recursos do serviço.

Para conectar sua VPC a CloudTrail, você define uma interface para a qual VPC endpoint. CloudTrail Um endpoint de interface é uma interface de rede elástica com um endereço IP privado que serve como ponto de entrada para o tráfego destinado a um serviço compatível AWS . O endpoint fornece conectividade confiável e escalável CloudTrail sem a necessidade de um gateway de internet, instância de tradução de endereços de rede (NAT) ou conexão VPN. Para obter mais informações, consulte O que é a Amazon VPC? no Manual do usuário da Amazon VPC.

Os endpoints VPC da Interface são alimentados por AWS PrivateLink uma AWS tecnologia que permite a comunicação privada entre AWS serviços usando uma interface de rede elástica com endereços IP privados. Para obter mais informações, consulte AWS PrivateLink.

As etapas a seguir são para usuários da Amazon VPC. Para obter mais informações, consulte Conceitos básicos da Amazon VPC no Manual do usuário da Amazon VPC.

Disponibilidade

CloudTrail atualmente oferece suporte a VPC endpoints nas seguintes regiões: AWS

- Leste dos EUA (Ohio)
- Leste dos EUA (N. da Virgínia)
- Oeste dos EUA (N. da Califórnia)
- Oeste dos EUA (Oregon)
- África (Cidade do Cabo)
- Ásia-Pacífico (Hong Kong)

- Ásia-Pacífico (Hyderabad)
- Ásia-Pacífico (Jacarta)
- Ásia-Pacífico (Melbourne)
- Ásia-Pacífico (Mumbai)
- Ásia-Pacífico (Osaka)
- Ásia-Pacífico (Seul)
- Ásia-Pacífico (Singapura)
- Ásia-Pacífico (Sydney)
- Ásia-Pacífico (Tóquio)
- Canadá (Central)
- Oeste do Canadá (Calgary)
- Europa (Frankfurt)
- Europa (Irlanda)
- Europa (Londres)
- Europa (Milão)
- Europe (Paris)
- Europa (Espanha)
- Europa (Estocolmo)
- Europa (Zurique)
- Israel (Tel Aviv)
- Oriente Médio (Barém)
- Oriente Médio (Emirados Árabes Unidos)
- América do Sul (São Paulo)
- AWS GovCloud (Leste dos EUA)
- AWS GovCloud (Oeste dos EUA)

Crie um VPC endpoint para CloudTrail

Para começar a usar CloudTrail com sua VPC, crie uma interface VPC endpoint para. CloudTrail Para obter mais informações, consulte Acessar e AWS service (Serviço da AWS) usar uma interface VPC endpoint no Guia do usuário da Amazon VPC.

Você não precisa alterar as configurações do CloudTrail. CloudTrail chama outros Serviços da AWS usando endpoints públicos ou endpoints VPC de interface privada, os que estiverem em uso.

Sub-redes compartilhadas

Um CloudTrail VPC endpoint, como qualquer outro VPC endpoint, só pode ser criado por uma conta de proprietário na sub-rede compartilhada. No entanto, uma conta de participante pode usar CloudTrail VPC endpoints em sub-redes que são compartilhadas com a conta do participante. Para obter informações sobre o compartilhamento da Amazon VPC, consulte Compartilhar sua VPC com outras contas no Guia do usuário do Amazon VPC.

Conta da AWS fechamento e trilhas

AWS CloudTrail monitora e registra continuamente os eventos da atividade da conta gerados por qualquer usuário, função ou AWS service (Serviço da AWS) para um Conta da AWS. Os usuários podem criar uma CloudTrail trilha para receber uma cópia desses eventos em um bucket do S3 de sua propriedade.

CloudTrail é um serviço de segurança fundamental, portanto, as trilhas criadas pelos usuários continuam existindo e entregando eventos mesmo após o fechamento de uma Conta da AWS , a menos que um usuário exclua explicitamente as trilhas Conta da AWS antes de fechá-las. Esse comportamento também se aplica às trilhas organizacionais criadas pela conta de gerenciamento ou pelo administrador delegado e às trilhas organizacionais multirregionais que são então criadas nas contas dos membros da organização. Isso garante que, se um usuário reabrir uma conta encerrada, ele tenha um registro ininterrupto da atividade da conta. Isso também fornece aos usuários visibilidade de qualquer atividade final da conta, incluindo a exclusão e o encerramento dos recursos e serviços restantes da conta.

Os usuários têm a opção de excluir trilhas antes de Conta da AWS fechá-las ou entrar em contato AWS Supportpara solicitar a exclusão da trilha após Conta da AWS o fechamento.

Para obter mais informações sobre como fechar um Conta da AWS, consulte Fechar um Conta da AWS.

> **Note**
>
> Se a validação do arquivo de CloudTrail log estiver ativada, os usuários continuarão recebendo arquivos de resumo de hora em hora que indicam se algum CloudTrail registro foi criado ou não.

CloudTrail Armazenamentos de dados de eventos do CloudTrail Lake, canais Lake para integrações, canais CloudTrail vinculados a serviços e recursos criados para trilhas (por exemplo, grupos de log do Amazon CloudWatch Logs e buckets do Amazon S3 existentes na conta fechada) seguem o AWS comportamento padrão de encerramento da conta e são excluídos permanentemente após o período pós-encerramento (normalmente 90 dias).

Definir CloudTrail configurações

Você pode usar a página Configurações no CloudTrail console para definir e revisar CloudTrail as configurações.

Para acessar a página Configurações

1. Faça login no AWS Management Console e abra o CloudTrail console em https://console.aws.amazon.com/cloudtrail/.
2. Escolha Configurações no painel de navegação esquerdo do CloudTrail console.
3. Revise e atualize suas configurações conforme necessário.

   As seguintes configurações estão disponíveis:

   - Administradores delegados da organização — Se você tiver uma AWS Organizations organização, poderá visualizar administradores CloudTrail delegados, adicionar administradores delegados (até três no máximo) e remover administradores delegados. Somente a conta de gerenciamento da organização pode adicionar ou remover administradores delegados.

     A conta de gerenciamento da organização pode designar qualquer conta dentro da organização para atuar como administrador CloudTrail delegado para gerenciar as trilhas e os armazenamentos de dados de eventos da organização em nome da organização.
   - Canais vinculados ao serviço— Você pode ver qualquer canal vinculado ao serviço criado para sua conta.

     Serviços da AWS pode criar um canal vinculado ao serviço para receber CloudTrail eventos em seu nome. O AWS serviço que cria o canal vinculado ao serviço configura seletores de eventos avançados para o canal e especifica se o canal se aplica a todos Regiões da AWS ou a um único. Região da AWS

Administrador delegado de organização

Ao usar CloudTrail com uma AWS Organizations organização, você pode atribuir qualquer conta dentro da organização para atuar como administrador CloudTrail delegado para gerenciar as trilhas e os armazenamentos de dados de eventos da organização em nome da organização. Um

administrador delegado é uma conta membro em uma organização que pode realizar as mesmas tarefas administrativas (exceto conforme indicado) na CloudTrail conta de gerenciamento.

Se você escolher um administrador delegado, essa conta-membro terá permissões administrativas em todas as trilhas da organização e os armazenamentos de dados de eventos na organização. Adicionar um administrador delegado não altera o gerenciamento ou a operação das trilhas ou dos armazenamentos de dados de eventos da organização.

Na primeira vez que você adiciona um administrador delegado no CloudTrail console, ou usando a CloudTrail API AWS CLI ou, CloudTrail verifica se a conta de gerenciamento da organização tem uma função vinculada ao serviço. Se a conta de gerenciamento não tiver uma função vinculada ao serviço, CloudTrail cria a função vinculada ao serviço para a conta de gerenciamento. Para obter mais informações sobre funções vinculadas ao serviço, consulte Usando funções vinculadas a serviços para AWS CloudTrail.

> **Note**
>
> Quando você adiciona um administrador delegado usando a operação da AWS Organizations CLI ou da API, a função vinculada ao serviço não é criada se não existir. A função vinculada ao serviço só é criada quando você faz uma chamada da conta de gerenciamento diretamente para o CloudTrail serviço, como quando você adiciona um administrador delegado ou cria uma trilha da organização ou um armazenamento de dados de eventos usando o CloudTrail console ou a API. AWS CLI CloudTrail

Anote os seguintes fatores que definem como o administrador delegado opera em CloudTrail.

A conta de gerenciamento continua sendo a proprietária de todos os recursos da CloudTrail organização criados pelo administrador delegado.

A conta de gerenciamento da organização continua sendo a proprietária de todos os recursos da CloudTrail organização criados pelo administrador delegado, como trilhas e armazenamentos de dados de eventos. Isso proporciona continuidade para a organização caso o administrador delegado mude.

A remoção de uma conta de administrador delegado não exclui nenhum recurso CloudTrail da organização que eles criaram.

As trilhas da organização e os armazenamentos de dados de eventos criados pelo administrador delegado não são excluídos quando você remove o administrador delegado, porque a conta

de gerenciamento sempre serve como proprietária dos recursos da CloudTrail organização, independentemente de serem criados pelo administrador delegado ou pela conta de gerenciamento.

Uma organização pode ter no máximo três administradores CloudTrail delegados.

Você pode ter no máximo três administradores CloudTrail delegados por organização. Para obter mais informações sobre a remoção de um administrador delegado, consulte Remover um CloudTrail administrador delegado.

A tabela a seguir mostra os recursos da conta de gerenciamento, das contas de administrador delegado e das contas que são membros da AWS Organizations organização.

Capacidades	Conta de gerenciamento	Conta de administrador delegado	Contas-membro
Adicionar ou remover contas de administrador delegado.	Sim	Não	Não
Criar uma trilha de organização.	Sim	Sim[1]	Não
Visualizar uma lista de trilhas de organização.	Sim	Sim	Sim
Atualizar uma trilha de organização.	Sim	Sim[1, 2]	Não
Excluir uma trilha de organização.	Sim	Sim	Não
Crie um armazenamento de dados de eventos da organização para CloudTrail eventos ou itens AWS Config de configuração.	Sim	Sim	Não
Habilitar o Insights em um armazenamento de dados de eventos da organização.	Sim	Não	Não

Capacidades	Conta de gerenciamento	Conta de administrador delegado	Contas-membro
Atualizar um armazenamento de dados de eventos da organização.	Sim	Sim[2]	Não
Habilitar a federação de consultas do Lake em um armazenamento de dados de eventos da organização[3].	Sim	Sim	Não
Desabilitar a federação de consultas do Lake em um armazenamento de dados de eventos da organização.	Sim	Sim	Não
Excluir um armazenamento de dados de eventos da organização.	Sim	Sim	Não
Copiar eventos de trilhas para um armazenamento de dados de eventos da organização.	Sim	Não	Não
Executar consultas em armazenamentos de dados de eventos da organização.	Sim	Sim	Não
Visualizar o painel do Lake para um armazenamento de dados de eventos da organização.	Sim	Sim	Não

[1] O administrador delegado só pode configurar um grupo de CloudWatch registros de registros usando as operações AWS CLI ou CloudTrail `CreateTrail` ou `UpdateTrail` da API. Tanto o grupo de CloudWatch registros de registros quanto a função de registro devem existir na conta de chamada.

[2] Somente a conta de gerenciamento pode converter uma trilha da organização ou armazenamento de dados de eventos em uma trilha em nível de conta ou armazenamento de dados de eventos, ou converter um armazenamento de dados de trilhas ou eventos em nível de conta em uma trilha

organizacional ou armazenamento de dados de eventos. Essas ações não são permitidas para o administrador delegado porque as trilhas e os armazenamentos de dados de eventos da organização só existem na conta de gerenciamento. Quando um armazenamento de dados de trilhas ou eventos da organização é convertido em um armazenamento de dados de trilhas ou eventos em nível de conta, somente a conta de gerenciamento tem acesso ao armazenamento de dados de trilhas ou eventos.

[3]Somente uma única conta de administrador delegado ou a conta de gerenciamento pode habilitar a federação em um armazenamento de dados de eventos da organização. Outras contas de administrador delegado podem consultar e compartilhar informações usando o recurso de compartilhamento de dados do Lake Formation. Qualquer conta de administrador delegado, bem como a conta de gerenciamento da organização, pode desabilitar a federação.

Tópicos

Permissões necessárias para atribuir um administrador delegado

Ao atribuir um administrador CloudTrail delegado, você deve ter as permissões para adicionar e remover o administrador delegado CloudTrail, bem como determinadas ações de AWS Organizations API e permissões do IAM listadas na declaração de política a seguir.

É possível adicionar a seguinte instrução ao final de uma política do IAM para conceder essas permissões:

```
{
    "Sid": "Permissions",
    "Effect": "Allow",
    "Action": [
        "cloudtrail:RegisterOrganizationDelegatedAdmin",
        "cloudtrail:DeregisterOrganizationDelegatedAdmin",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator",
        "organizations:ListAWSServiceAccessForOrganization",
        "iam:CreateServiceLinkedRole",
        "iam:GetRole"
    ],
```

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

Adicionar um administrador CloudTrail delegado

Você pode adicionar um administrador delegado para gerenciar os CloudTrail recursos de uma organização, como trilhas e armazenamentos de dados de eventos.

Você pode adicionar um administrador CloudTrail delegado para sua AWS organização usando o CloudTrail console ou o. AWS CLI

Antes de adicionar um administrador delegado, certifique-se de que ele tenha uma conta em sua organização e de que você esteja conectado com a conta de gerenciamento da organização. Para obter informações sobre como criar uma nova AWS conta para sua organização, consulte Criação de uma AWS conta em sua organização. Para obter informações sobre como convidar uma AWS conta existente para sua organização, consulte Convidar uma AWS conta para participar da sua organização.

CloudTrail console

O procedimento a seguir mostra como adicionar um administrador CloudTrail delegado usando o CloudTrail console.

1. Faça login no AWS Management Console e abra o CloudTrail console em https://console.aws.amazon.com/cloudtrail/.
2. Escolha Configurações no painel de navegação esquerdo do CloudTrail console.
3. Na seção Organization delegated administrators (Administradores delegados da organização), escolha Register administrator (Registrar administrador).
4. Insira o ID da AWS conta de doze dígitos da conta que você deseja atribuir como administrador CloudTrail delegado para os repositórios de dados de trilhas e eventos da organização.
5. Selecione Register administrator (Registrar administrador).

AWS CLI

O exemplo a seguir adiciona um administrador CloudTrail delegado.

```
aws cloudtrail register-organization-delegated-admin
```

```
  --member-account-id="memberAccountId"
```

Se for bem-sucedido, esse comando não produzirá uma saída.

Remover um CloudTrail administrador delegado

Você pode remover um administrador CloudTrail delegado usando o CloudTrail console ou o. AWS CLI

CloudTrail console

O procedimento a seguir mostra como remover um administrador CloudTrail delegado usando o CloudTrail console.

1. Faça login no AWS Management Console e abra o CloudTrail console em https://console.aws.amazon.com/cloudtrail/.
2. Escolha Configurações no painel de navegação esquerdo do CloudTrail console.
3. Na seção Organization delegated administrators (Administradores delegados da organização), escolha o administrador delegado que deseja remover.
4. Escolha Remove administrator (Remover administrador).
5. Confirme que você deseja remover o administrador delegado e escolha Remove administrator (Remover administrador).

AWS CLI

O comando a seguir remove um administrador CloudTrail delegado.

```
aws cloudtrail deregister-organization-delegated-admin
  --delegated-admin-account-id="delegatedAdminAccountId"
```

Se for bem-sucedido, esse comando não produzirá uma saída.

Canais vinculados ao serviço

AWS os serviços podem criar um canal vinculado ao serviço para receber CloudTrail eventos em seu nome. O AWS serviço que cria o canal vinculado ao serviço configura seletores de eventos

avançados para o canal e especifica se o canal se aplica a todos Regiões da AWS ou a um único. Região da AWS

Tópicos

Visualizar canais vinculados ao serviço usando o console

Usando o CloudTrail console, você pode visualizar informações sobre qualquer canal CloudTrail vinculado ao serviço criado pelos AWS serviços. A tabela ficará vazia se sua conta não tiver nenhum canal vinculado ao serviço.

Siga o procedimento abaixo para visualizar informações sobre um canal vinculado ao serviço.

1. Escolha Configurações no painel de navegação esquerdo do CloudTrail console.
2. Em Canais vinculados ao serviço, escolha um canal vinculado ao serviço para visualizar seus detalhes.
3. Na página de detalhes, revise as configurações para o canal vinculado ao serviço.

   A página de detalhes mostra as informações a seguir.

   - Nome do canal: o nome completo do canal. O formato do nome do canal é `aws-service-channel/`*`AWS_service_name`*`/slc` onde *`AWS_service_name`* representa o nome do AWS serviço que gerencia o canal.
   - ARN do canal: o ARN do canal, o qual pode ser usado em uma solicitação de API para obter detalhes sobre o canal.
   - Todas as regiões: o valor será `Yes` se o canal estiver configurado para todas as Regiões da AWS.
   - AWS service - O nome do AWS serviço que gerencia o canal.
   - Eventos de gerenciamento: mostra todos os eventos de gerenciamento configurados para o canal.
   - Eventos de dados: mostra todos os eventos de dados configurados para o canal.

Visualizando canais vinculados ao serviço usando o AWS CLI

Usando o AWS CLI, você pode visualizar informações sobre qualquer canal CloudTrail vinculado a serviços criado por AWS serviços.

Tópicos

Obtenha um canal CloudTrail vinculado ao serviço

O AWS CLI comando de exemplo a seguir retorna informações sobre um canal CloudTrail vinculado ao serviço específico, incluindo o nome do AWS serviço de destino, quaisquer seletores avançados configurados para o canal e se o canal se aplica a todas as regiões ou a uma única região.

Você deve especificar um ARN ou o sufixo de ID de um ARN para `--channel`.

```
aws cloudtrail get-channel --channel EXAMPLE-ee54-4813-92d5-999aeEXAMPLE
```

A seguir, uma exemplo de resposta. Neste exemplo, `AWS_service_name` representa o nome do AWS serviço que criou o canal.

```
{
    "ChannelArn": "arn:aws:cloudtrail:us-east-1:111122223333:channel/EXAMPLE-
ee54-4813-92d5-999aeEXAMPLE",
    "Name": "aws-service-channel/AWS_service_name/slc",
    "Source": "CloudTrail",
    "SourceConfig": {
        "ApplyToAllRegions": false,
        "AdvancedEventSelectors": [
            {
                "Name": "Management Events Only",
                "FieldSelectors": [
                    {
                        "Field": "eventCategory",
                        "Equals": [
                            "Management"
```

```
                        ]
                    }
                ]
            }
        ]
    },
    "Destinations": [
        {
            "Type": "AWS_SERVICE",
            "Location": "AWS_service_name"
        }
    ]
}
```

Listar todos os canais CloudTrail vinculados ao serviço

O AWS CLI comando de exemplo a seguir retorna informações sobre todos os canais CloudTrail vinculados a serviços que foram criados em seu nome. Parâmetros opcionais incluem `--max-results` para especificar um número máximo de resultados que você deseja que o comando retorne em uma única página. Se houver mais resultados do que o valor especificado para `--max-results`, execute o comando novamente adicionando o valor retornado `NextToken` para obter a próxima página de resultados.

```
aws cloudtrail list-channels
```

A seguir, uma exemplo de resposta. Neste exemplo, `AWS_service_name` representa o nome do AWS serviço que criou o canal.

```
{
    "Channels": [
        {
            "ChannelArn": "arn:aws:cloudtrail:us-east-1:111122223333:channel/EXAMPLE-
ee54-4813-92d5-999aeEXAMPLE",
            "Name": "aws-service-channel/AWS_service_name/slc"
        }
    ]
}
```

AWS eventos de serviço em canais vinculados a serviços

O AWS serviço que gerencia o canal vinculado ao serviço pode iniciar ações no canal vinculado ao serviço (por exemplo, criar ou atualizar um canal vinculado ao serviço). CloudTrail registra essas ações como eventos de AWS serviço e os entrega ao histórico de eventos e a quaisquer trilhas ativas e armazenamentos de dados de eventos configurados para eventos de gerenciamento. Para esses eventos, o campo `eventType` é `AwsServiceEvent`.

Veja a seguir um exemplo de entrada no arquivo de log de um evento de AWS serviço para a criação de um canal vinculado ao serviço.


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "accountId":"111122223333",
      "invokedBy":"AWS Internal"
   },
   "eventTime":"2022-08-18T17:11:22Z",
   "eventSource":"cloudtrail.amazonaws.com",
   "eventName":"CreateServiceLinkedChannel",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"AWS Internal",
   "userAgent":"AWS Internal",
   "requestParameters":null,
   "responseElements":null,
   "requestID":"564f004c-EXAMPLE",
   "eventID":"234f004b-EXAMPLE",
   "readOnly":false,
   "resources":[
      {
         "accountId":"184434908391",
         "type":"AWS::CloudTrail::Channel",
         "ARN":"arn:aws:cloudtrail:us-east-1:111122223333:channel/7944f0ec-EXAMPLE"
      }
   ],
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "recipientAccountId":"111122223333",
   "eventCategory":"Management"
}
```

Entendendo CloudTrail os eventos

Um evento em CloudTrail é o registro de uma atividade em uma AWS conta. Essa atividade pode ser uma ação realizada por uma identidade do IAM ou um serviço que pode ser monitorado por CloudTrail. CloudTrail os eventos fornecem um histórico das atividades de contas de API e não API feitas por meio de AWS SDKs AWS Management Console, ferramentas de linha de comando e outros. Serviços da AWS

CloudTrail os arquivos de log não são um rastreamento de pilha ordenado das chamadas públicas de API, portanto, os eventos não aparecem em nenhuma ordem específica.

Há três tipos de CloudTrail eventos:

- Eventos de gerenciamento
- Eventos de dados
- Eventos do Insights

Por padrão, as trilhas e os armazenamentos de dados de eventos registram eventos de gerenciamento, mas não eventos de dados ou do Insights.

Todos os tipos de eventos usam um formato de log CloudTrail JSON. O log contém informações sobre as solicitações de recursos na sua conta, como quem fez a solicitação, os serviços usados, as ações realizadas e os parâmetros da ação. Os dados do evento são incluídos em um conjunto `Records`.

Para obter informações sobre campos de registro de CloudTrail eventos, consulteCloudTrail conteúdo do registro.

Eventos de gerenciamento

Os eventos de gerenciamento fornecem informações sobre as operações de gerenciamento que são realizadas nos recursos AWS da sua conta. Elas também são conhecidas como operações de plano de controle. Exemplos de eventos de gerenciamento incluem:

- Configurando a segurança (por exemplo, operações de AWS Identity and Access Management `AttachRolePolicy` API).

- Registro de dispositivos (por exemplo, operações de API `CreateDefaultVpc` do Amazon EC2).
- Configuração de regras para roteamento de dados (por exemplo, operações de API `CreateSubnet` do Amazon EC2).
- Configurar o registro (por exemplo, operações de AWS CloudTrail `CreateTrail` API).

Os eventos de gerenciamento também podem incluir eventos que não são de API que ocorrem na sua conta. Por exemplo, quando um usuário faz login na sua conta, CloudTrail registra o `ConsoleLogin` evento. Para ter mais informações, consulte Eventos não relacionados à API capturados por CloudTrail. Para obter uma lista de eventos de gerenciamento que CloudTrail registram AWS serviços, consulteCloudTrail serviços e integrações suportados.

O exemplo a seguir mostra um único registro de log de um evento de gerenciamento. Nesse evento, um usuário do IAM chamado `Mary_Major` executou o aws cloudtrail start-logging comando para chamar a CloudTrail `StartLogging`ação para iniciar o processo de registro em uma trilha chamada`myTrail`.


```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLE6E4XEGITWATV6R",
        "arn": "arn:aws:iam::123456789012:user/Mary_Major",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Mary_Major",
        "sessionContext": {
            "attributes": {
                "creationDate": "2023-07-19T21:11:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-19T21:33:41Z",
    "eventSource": "cloudtrail.amazonaws.com",
    "eventName": "StartLogging",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
 exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/cloudtrail.start-logging",
    "requestParameters": {
```

```
        "name": "myTrail"
    },
    "responseElements": null,
    "requestID": "9d478fc1-4f10-490f-a26b-EXAMPLE0e932",
    "eventID": "eae87c48-d421-4626-94f5-EXAMPLEac994",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "cloudtrail.us-east-1.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}
```

No próximo exemplo, um usuário do IAM chamado `Paulo_Santos` executou o comando aws cloudtrail start-event-data-store-ingestion para chamar a ação `StartEventDataStoreIngestion` para iniciar a ingestão em um armazenamento de dados de eventos.

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLEPHCNW5EQV7NA54",
        "arn": "arn:aws:iam::123456789012:user/Paulo_Santos",
        "accountId": "123456789012",
        "accessKeyId": "(AKIAIOSFODNN7EXAMPLE",
        "userName": "Paulo_Santos",
        "sessionContext": {
            "attributes": {
                "creationDate": "2023-07-21T21:55:30Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-21T21:57:28Z",
    "eventSource": "cloudtrail.amazonaws.com",
    "eventName": "StartEventDataStoreIngestion",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
```

```
    "userAgent": "aws-cli/2.13.1 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
 exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/cloudtrail.start-event-data-
store-ingestion",
    "requestParameters": {
        "eventDataStore": "arn:aws:cloudtrail:us-
east-1:123456789012:eventdatastore/2a8f2138-0caa-46c8-a194-EXAMPLE87d41"
    },
    "responseElements": null,
    "requestID": "f62a3494-ba4e-49ee-8e27-EXAMPLE4253f",
    "eventID": "d97ca7e2-04fe-45b4-882d-EXAMPLEa9b2c",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "cloudtrail.us-east-1.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}
```


Eventos de dados

Os eventos de dados fornecem informações sobre as operações do recurso executadas em um recurso ou dentro de um recurso. Elas também são conhecidas como operações de plano de dados. Eventos de dados geralmente são atividades de alto volume.

Exemplos de eventos de dados incluem:

- Atividade de API em nível de objeto do Amazon S3 (por exemplo,, `GetObject`, `DeleteObject`, e operações de `PutObject` API) em objetos em buckets do S3.
- AWS Lambda atividade de execução da função (a `Invoke` API).
- CloudTrail `PutAuditEvents`atividade em um canal do CloudTrail Lake que é usada para registrar eventos externos AWS.
- Operações da API `Publish` e `PublishBatch` do Amazon SNS em tópicos.

A tabela a seguir mostra os tipos de eventos de dados disponíveis para trilhas e armazenamentos de dados de eventos. A coluna Tipo de evento de dados (console) mostra a seleção apropriada no

console. A coluna de valor resources.type mostra o `resources.type` valor que você especificaria para incluir eventos de dados desse tipo em seu armazenamento de dados de trilhas ou eventos usando as AWS CLI APIs ou. CloudTrail

Para trilhas, você pode usar seletores de eventos básicos ou avançados para registrar eventos de dados para objetos do Amazon S3, funções do Lambda e tabelas do DynamoDB (mostradas nas três primeiras linhas da tabela). É possível usar somente seletores de eventos avançados para registrar em log os tipos de eventos de dados mostrados nas linhas restantes.

Para armazenamentos de dados de eventos, é possível usar somente seletores de eventos avançados para incluir eventos de dados.

AWS service (Serviço da AWS)	Descrição	Tipo de evento de dados (console)	valor resources.type
Amazon DynamoDB	Atividade de API em nível de item do Amazon DynamoDB em tabelas (por exemplo `PutItem`, `DeleteItem`, e operações de API). `UpdateItem` **Note** Para tabelas com fluxos habilitados, o campo `resources` no evento de dados contém `AWS::DynamoDB::Stream` e `AWS::Dyna`	DynamoDB	`AWS::DynamoDB::Table`

AWS service (Serviço da AWS)	Descrição	Tipo de evento de dados (console)	valor resources.type
	`moDB::Tab le` . Se você especificar `AWS::Dyna moDB::Tab le` como `resources .type` , ele registrará os eventos da tabela do DynamoDB e dos fluxos do DynamoDB por padrão. Para excluir eventos de streams, adicione um filtro no `eventName` campo.		
AWS Lambda	AWS Lambda atividade de execução da função (a `Invoke` API).	Lambda	`AWS::Lambda::Function`

AWS service (Serviço da AWS)	Descrição	Tipo de evento de dados (console)	valor resources.type
Amazon S3	Atividade de API em nível de objeto do Amazon S3 (por exemplo,, `GetObject` `DeleteObject` , e operações de `PutObject` API) em objetos em buckets do S3.	S3	`AWS::S3::Object`
AWS AppConfig	AWS AppConfig Atividade de API para operações de configuração, como chamadas para `StartConfiguration` `Session` `GetLatestConfiguration` e.	AWS AppConfig	`AWS::AppConfig::Configuration`
AWS Intercâmbio de dados B2B	Atividade da API B2B Data Interchange para operações do Transformer, como chamadas para `GetTransformerJob` e `StartTransformerJob` .	B2B Data Interchange	`AWS::B2BI::Transformer`

AWS service (Serviço da AWS)	Descrição	Tipo de evento de dados (console)	valor resources.type
Amazon Bedrock	Atividade da API do Amazon Bedrock em um alias de agente.	Alias de agente do Bedrock	`AWS::Bedrock::AgentAlias`
	Atividade da API do Amazon Bedrock em uma base de conhecimento.	Base de conhecimento do Bedrock	`AWS::Bedrock::KnowledgeBase`
Amazon CloudFront	CloudFront Atividade de API em um KeyValueStore.	CloudFront KeyValueStore	`AWS::CloudFront::KeyValueStore`
AWS Cloud Map	AWS Cloud Map Atividade de API em um namespace.	AWS Cloud Map namespace	`AWS::ServiceDiscovery::Namespace`
	AWS Cloud Map Atividade de API em um serviço.	AWS Cloud Map serviço	`AWS::ServiceDiscovery::Service`
AWS CloudTrail	CloudTrail `PutAuditEvents` atividade em um canal do CloudTrail Lake que é usada para registrar eventos externos AWS.	CloudTrail canal	`AWS::CloudTrail::Channel`

AWS service (Serviço da AWS)	Descrição	Tipo de evento de dados (console)	valor resources.type
Amazon CodeWhisperer	Atividade de CodeWhisperer API da Amazon em uma personalização.	CodeWhisperer personalização	`AWS::CodeWhisperer::Customization`
	Atividade CodeWhisperer da API da Amazon em um perfil.	CodeWhisperer	`AWS::CodeWhisperer::Profile`
Amazon Cognito	Atividade da API do Amazon Cognito em bancos de identidades do Amazon Cognito.	Bancos de identidades do Cognito	`AWS::Cognito::IdentityPool`
Amazon DynamoDB	Atividade de API do Amazon DynamoDB em fluxos.	DynamoDB Streams	`AWS::DynamoDB::Stream`
Amazon Elastic Block Store	APIs diretas do Amazon Elastic Block Store (EBS), como `PutSnapshotBlock`, `GetSnapshotBlock` e `ListChangedBlocks` nos snapshots do Amazon EBS.	APIs diretas do Amazon EBS	`AWS::EC2::Snapshot`

AWS service (Serviço da AWS)	Descrição	Tipo de evento de dados (console)	valor resources.type
Amazon EMR	Atividade da API do Amazon EMR em um espaço de trabalho de log de gravação antecipada.	Espaço de trabalho de log de gravação antecipada do EMR	`AWS::EMRWAL::Workspace`
Amazon FinSpace	Atividade de API do Amazon FinSpace em ambientes.	FinSpace	`AWS::FinSpace::Environment`

AWS service (Serviço da AWS)	Descrição	Tipo de evento de dados (console)	valor resources.type
AWS Glue	AWS Glue Atividade de API em tabelas criadas pelo Lake Formation. **Note** AWS Glue Atualmente, os eventos de dados para tabelas são suportados somente nas seguintes regiões: • Leste dos EUA (Norte da Virgínia) • Leste dos EUA (Ohio) • Oeste dos EUA (Oregon) • Europa (Irlanda) • Região Ásia-	Lake Formation	`AWS::Glue::Table`

AWS service (Serviço da AWS)	Descrição	Tipo de evento de dados (console)	valor resources.type
	Pacífico (Tóquio)		
Amazon GuardDuty	Atividade de GuardDuty API da Amazon para um detector.	GuardDuty detector	`AWS::GuardDuty::Detector`
AWS HealthImaging	AWS HealthImaging Atividade de API em armazenamentos de dados.	Armazenamento de dados de imagens médicas	`AWS::MedicalImaging::Datastore`
AWS IoT	AWS IoT Atividade de API em certificados.	Certificado de IoT	`AWS::IoT::Certificate`
	AWS IoT Atividade de API em coisas.	Coisa de IoT	`AWS::IoT::Thing`

AWS service (Serviço da AWS)	Descrição	Tipo de evento de dados (console)	valor resources.type
AWS IoT Greengrass Version 2	Atividade da API do Greengrass de um dispositivo principal do Greengrass em uma versão de componente. **Note** O Greengrass não registra eventos de acesso negado.	Versão do componente IoT Greengrass	`AWS::GreengrassV2::ComponentVersion`
	Atividade da API do Greengrass de um dispositivo principal do Greengrass em uma implantação. **Note** O Greengrass não registra eventos de acesso negado.	Implantação do IoT Greengrass	`AWS::GreengrassV2::Deployment`
AWS IoT SiteWise	Atividade da SiteWise API de IoT em ativos.	Ativo de IoT SiteWise	`AWS::IoTSiteWise::Asset`

AWS service (Serviço da AWS)	Descrição	Tipo de evento de dados (console)	valor resources.type
	Atividade da SiteWise API de IoT em séries temporais.	Série temporal de IoT SiteWise	`AWS::IoTSiteWise::TimeSeries`
AWS IoT TwinMaker	Atividade da TwinMaker API de IoT em uma entidade.	Entidade de IoT TwinMaker	`AWS::IoTTwinMaker::Entity`
	Atividade da TwinMaker API de IoT em um espaço de trabalho.	Espaço de trabalho de IoT TwinMaker	`AWS::IoTTwinMaker::Workspace`
Amazon Kendra Intelligent Ranking	Atividade da API do Amazon Kendra Intelligent Ranking em planos de execução de reclassificação.	Kendra Ranking	`AWS::KendraRanking::ExecutionPlan`
Amazon Keyspaces (para Apache Cassandra)	Atividade da API Amazon Keyspaces em uma tabela.	Mesa Cassandra	`AWS::Cassandra::Table`
Amazon Kinesis Data Streams	Atividade da API Kinesis Data Streams em streams.	Stream do Kinesis	`AWS::Kinesis::Stream`
	Atividade da API Kinesis Data Streams em consumidores de streams.	Consumidor de streaming do Kinesis	`AWS::Kinesis::StreamConsumer`

AWS service (Serviço da AWS)	Descrição	Tipo de evento de dados (console)	valor resources.type
Amazon Kinesis Video Streams	Atividade da API Kinesis Video Streams em streams de vídeo, como chamadas para e. `GetMedia` `PutMedia`	Fluxo de vídeo do Kinesis	`AWS::KinesisVideo::Stream`
Amazon Managed Blockchain	Atividade da API do Amazon Managed Blockchain em uma rede.	Rede do Managed Blockchain	`AWS::ManagedBlockchain::Network`
	Chamadas de JSON-RPC do Amazon Managed Blockchain em nós Ethereum, como `eth_getBalance` ou `eth_getBlockByNumber` .	Managed Blockchain	`AWS::ManagedBlockchain::Node`
Gráfico do Amazon Neptune	Atividades da API de dados, por exemplo, consultas, algoritmos ou pesquisa vetorial, em um gráfico do Neptune.	Gráfico do Neptune	`AWS::NeptuneGraph::Graph`
AWS Private CA	AWS Private CA Conector para atividade da API do Active Directory.	AWS Private CA Conector para Active Directory	`AWS::PCAConnectorAD::Connector`

AWS service (Serviço da AWS)	Descrição	Tipo de evento de dados (console)	valor resources.type
Aplicativos Amazon Q	Atividade da API de dados no Amazon Q Apps.	Aplicativos Amazon Q	`AWS::QApps:QApp`
Amazon Q Business	Atividade da API do Amazon Q Business em uma aplicação.	Aplicação do Amazon Q Business	`AWS::QBusiness::Application`
	Atividade da API do Amazon Q Business em uma fonte de dados.	Fonte de dados do Amazon Q Business	`AWS::QBusiness::DataSource`
	Atividade da API do Amazon Q Business em um índice.	Índice do Amazon Q Business	`AWS::QBusiness::Index`
	Atividade da API do Amazon Q Business em uma experiência na web.	Experiência na web do Amazon Q Business	`AWS::QBusiness::WebExperience`
Amazon RDS	Atividade da API do Amazon RDS em um cluster de banco de dados.	API de dados do RDS - cluster de banco de dados	`AWS::RDS::DBCluster`
Amazon S3	Atividade da API Amazon S3 em pontos de acesso.	Ponto de acesso do S3	`AWS::S3::AccessPoint`

AWS service (Serviço da AWS)	Descrição	Tipo de evento de dados (console)	valor resources.type
	Atividade da API de pontos de acesso do Amazon S3 Object Lambda, como chamadas para e. `CompleteMultipartUpload` `GetObject`	S3 Object Lambda	`AWS::S3ObjectLambda::AccessPoint`
Amazon S3 on Outposts	Atividade da API em nível de objeto do Amazon S3 on Outposts.	S3 Outposts	`AWS::S3Outposts::Object`
Amazon SageMaker	SageMaker `InvokeEndpointWithResponseStream` Atividade da Amazon em endpoints .	SageMaker ponto final	`AWS::SageMaker::Endpoint`
	Atividade da SageMaker API da Amazon em lojas de recursos.	SageMaker feature store	`AWS::SageMaker::FeatureGroup`
	Atividade da SageMaker API da Amazon em componentes de testes experimentais.	SageMaker componente experimental de métricas	`AWS::SageMaker::ExperimentTrialComponent`

AWS service (Serviço da AWS)	Descrição	Tipo de evento de dados (console)	valor resources.type
Amazon SNS	Operações da API `Publish` do Amazon SNS em endpoints da plataforma.	Endpoint da plataforma SNS	`AWS::SNS::PlatformEndpoint`
	Operações da API `Publish` e `PublishBatch` do Amazon SNS em tópicos.	Tópico do SNS	`AWS::SNS::Topic`
Amazon SQS	Atividade da API do Amazon SQS em mensagens.	SQS	`AWS::SQS::Queue`
AWS Step Functions	Atividade da API Step Functions em uma máquina de estado.	Máquina de estado do Step Functions	`AWS::StepFunctions::StateMachine`
Cadeia de Suprimentos AWS	Cadeia de Suprimentos AWS Atividade de API em uma instância .	Cadeia de suprimentos	`AWS::SCN::Instance`
Amazon SWF	Atividade da API Amazon SWF em domínios.	Domínio SWF	`AWS::SWF::Domain`
AWS Systems Manager	Atividade da API Systems Manager nos canais de controle.	Systems Manager (Gerenciador de sistemas)	`AWS::SSMMessages::ControlChannel`

AWS service (Serviço da AWS)	Descrição	Tipo de evento de dados (console)	valor resources.type
	Atividade da API Systems Manager em nós gerenciados.	Nó gerenciado pelo Systems Manager	`AWS::SSM::ManagedNode`
Amazon Timestream	Atividade da API `Query` do Amazon Timestream em bancos de dados.	Banco de dados do Timestream	`AWS::Timestream::Database`
	Atividade da API `Query` do Amazon Timestream em tabelas.	Tabela do Timestream	`AWS::Timestream::Table`
Amazon Verified Permissions	Atividade da API do Amazon Verified Permissions em um repositório de políticas.	Amazon Verified Permissions	`AWS::VerifiedPermissions::PolicyStore`
Amazon WorkSpaces Thin Client	WorkSpaces Atividade da API Thin Client em um dispositivo.	Dispositivo Thin Client	`AWS::ThinClient::Device`
	WorkSpaces Atividade da API Thin Client em um ambiente.	Ambiente Thin Client	`AWS::ThinClient::Environment`

AWS service (Serviço da AWS)	Descrição	Tipo de evento de dados (console)	valor resources.type
AWS X-Ray	Atividade da API X-Ray em rastreamentos.	Traço de raio-X	`AWS::XRay::Trace`

Eventos de dados não são registrados em log por padrão quando você cria uma trilha ou um armazenamento de dados de eventos. Para registrar eventos de CloudTrail dados, você deve adicionar explicitamente os recursos suportados ou os tipos de recursos para os quais deseja coletar atividades. Para obter mais informações, consulte Criar uma trilha e Crie um armazenamento de dados de CloudTrail eventos para eventos com o console.

Há cobranças adicionais para o registro de eventos de dados. Para CloudTrail saber os preços, consulte AWS CloudTrail Preços.

O exemplo a seguir mostra um único registro de log de um evento de dados para a ação do Amazon SNS`Publish`.


```
{
   "eventVersion": "1.09",
   "userIdentity": {
        "type": "AssumedRole",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::123456789012:user/Bob",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
        "sessionIssuer": {
            "type": "Role",
            "principalId": "AKIAIOSFODNN7EXAMPLE",
            "arn": "arn:aws:iam::123456789012:role/Admin",
            "accountId": "123456789012",
            "userName": "ExampleUser"
            },
            "attributes": {
                "creationDate": "2023-08-21T16:44:05Z",
                "mfaAuthenticated": "false"
```

```
            }
        }
    },
    "eventTime": "2023-08-21T16:48:37Z",
    "eventSource": "sns.amazonaws.com",
    "eventName": "Publish",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/1.29.16 md/Botocore#1.31.16 ua/2.0 os/
linux#5.4.250-173.369.amzn2int.x86_64 md/arch#x86_64 lang/python#3.8.17 md/
pyimpl#CPython cfg/retry-mode#legacy botocore/1.31.16",
    "requestParameters": {
        "topicArn": "arn:aws:sns:us-east-1:123456789012:ExampleSNSTopic",
        "message": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "subject": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "messageStructure": "json",
        "messageAttributes": "HIDDEN_DUE_TO_SECURITY_REASONS"
    },
    "responseElements": {
        "messageId": "0787cd1e-d92b-521c-a8b4-90434e8ef840"
    },
    "requestID": "0a8ab208-11bf-5e01-bd2d-ef55861b545d",
    "eventID": "bb3496d4-5252-4660-9c28-3c6aebdb21c0",
    "readOnly": false,
    "resources": [{
        "accountId": "123456789012",
        "type": "AWS::SNS::Topic",
                "ARN": "arn:aws:sns:us-east-1:123456789012:ExampleSNSTopic"
    }],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "123456789012",
    "eventCategory": "Data",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "sns.us-east-1.amazonaws.com"
    }
}
```

O próximo exemplo mostra um único registro de log de um evento de dados para a ação do Amazon Cognito`GetCredentialsForIdentity`.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Unknown"
    },
    "eventTime": "2023-01-19T16:55:08Z",
    "eventSource": "cognito-identity.amazonaws.com",
    "eventName": "GetCredentialsForIdentity",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.4",
    "userAgent": "aws-cli/2.7.25 Python/3.9.11 Darwin/21.6.0 exe/x86_64 prompt/off
 command/cognito-identity.get-credentials-for-identity",
    "requestParameters": {
        "logins": {
            "cognito-idp.us-east-1.amazonaws.com/us-east-1_aaaaaaaaa":
 "HIDDEN_DUE_TO_SECURITY_REASONS"
        },
        "identityId": "us-east-1:1cf667a2-49a6-454b-9e45-23199EXAMPLE"
    },
    "responseElements": {
        "credentials": {
            "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
            "sessionToken": "aAaAaAaAaAaAab1111111111EXAMPLE",
            "expiration": "Jan 19, 2023 5:55:08 PM"
        },
        "identityId": "us-east-1:1cf667a2-49a6-454b-9e45-23199EXAMPLE"
    },
    "requestID": "659dfc23-7c4e-4e7c-858a-1abce884d645",
    "eventID": "6ad1c766-5a41-4b28-b5ca-e223ccb00f0d",
    "readOnly": false,
    "resources": [{
        "accountId": "111122223333",
        "type": "AWS::Cognito::IdentityPool",
        "ARN": "arn:aws:cognito-identity:us-east-1:111122223333:identitypool/us-
east-1:2dg778b3-50b7-565c-0f56-34200EXAMPLE"
    }],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "111122223333",
    "eventCategory": "Data"
}
```

Eventos do Insights

CloudTrail Os eventos do Insights capturam atividades incomuns de taxa de chamadas de API ou taxa de erro em sua AWS conta analisando a atividade CloudTrail de gerenciamento. Os eventos do Insights fornecem informações relevantes, como a API associada, a hora do incidente e estatísticas, que ajudam a entender e agir com relação à atividade incomum. Ao contrário de outros tipos de eventos capturados em um armazenamento de dados de CloudTrail trilhas ou eventos, os eventos do Insights são registrados somente quando CloudTrail detectam alterações no uso da API ou no registro da taxa de erro da sua conta que diferem significativamente dos padrões de uso típicos da conta.

Exemplos de atividades que podem gerar eventos do Insights incluem:

- Sua conta geralmente registra em log no máximo 20 chamadas de API do `deleteBucket` Amazon S3 por minuto, mas sua conta começa a registrar em log uma média de 100 chamadas de API `deleteBucket` por minuto. Um evento do Insights é registrado em log no início da atividade incomum e outro evento do Insights é registrado em log para marcar o fim da atividade incomum.
- Sua conta geralmente registra em log 20 chamadas por minutos para a API do `AuthorizeSecurityGroupIngress` Amazon EC2, mas sua conta começa a registrar em log zero chamada para `AuthorizeSecurityGroupIngress`. Um evento do Insights é registrado em log no início da atividade incomum, e dez minutos depois, quando a atividade incomum termina, outro evento do Insights é registrado em log para marcar o fim da atividade incomum.
- Sua conta normalmente registra menos de um `AccessDeniedException` erro em um período de sete dias no AWS Identity and Access Management API, `DeleteInstanceProfile`. Sua conta começa a registrar uma média de 12 `AccessDeniedException` erros por minuto na `DeleteInstanceProfile` chamada de API. Um evento do Insights é registrado no início da atividade incomum e outro evento do Insights é registrado para marcar o fim da atividade incomum.

Esses exemplos são fornecidos somente para fins ilustrativos. Seus resultados podem variar dependendo do seu caso de uso.

Para registrar eventos do CloudTrail Insights, você deve habilitar explicitamente os eventos do Insights em um armazenamento de dados de trilhas ou eventos novo ou existente. Para obter mais informações sobre a criação de uma trilha, consulte Criar uma trilha. Para obter mais informações sobre como criar um armazenamento de dados de eventos, consulte Crie um armazenamento de dados de eventos para eventos do CloudTrail Insights com o console.

Cobranças adicionais são aplicáveis aos eventos do Insights. Você será cobrado separadamente se ativar o Insights tanto para trilhas quanto para armazenamentos de dados de eventos. Para obter mais informações, consulte Preços do AWS CloudTrail.

Há dois eventos registrados para mostrar atividades incomuns no CloudTrail Insights: um evento inicial e um evento final. O exemplo a seguir mostra um único registro em log de um evento inicial do Insights que ocorreu quando a API do Application Auto Scaling `CompleteLifecycleAction` foi chamada um número incomum de vezes. Para eventos do Insights, o valor de `eventCategory` é `Insight`. Um bloco do `insightDetails` identifica o estado, a fonte, o nome, o tipo de Insights e o contexto do evento, incluindo estatísticas e atribuições. Para obter mais informações sobre o bloco `insightDetails`, consulte CloudTrail `insightDetails`Elemento Insights.

```
{
        "eventVersion": "1.08",
        "eventTime": "2023-07-10T01:42:00Z",
        "awsRegion": "us-east-1",
        "eventID": "55ed45c5-0b0c-4228-9fe5-EXAMPLEc3f4d",
        "eventType": "AwsCloudTrailInsight",
        "recipientAccountId": "123456789012",
        "sharedEventID": "979c82fe-14d4-4e4c-aa01-EXAMPLE3acee",
        "insightDetails": {
            "state": "Start",
            "eventSource": "autoscaling.amazonaws.com",
            "eventName": "CompleteLifecycleAction",
            "insightType": "ApiCallRateInsight",
            "insightContext": {
                "statistics": {
                    "baseline": {
                        "average": 9.82222E-5
                    },
                    "insight": {
                        "average": 5.0
                    },
                    "insightDuration": 1,
                    "baselineDuration": 10181
                },
                "attributions": [{
                    "attribute": "userIdentityArn",
                    "insight": [{
                        "value": "arn:aws:sts::123456789012:assumed-role/
CodeDeployRole1",
                        "average": 5.0
```

```
                    }, {
                        "value": "arn:aws:sts::123456789012:assumed-role/
CodeDeployRole2",
                        "average": 5.0
                    }, {
                        "value": "arn:aws:sts::123456789012:assumed-role/
CodeDeployRole3",
                        "average": 5.0
                    }],
                    "baseline": [{
                        "value": "arn:aws:sts::123456789012:assumed-role/
CodeDeployRole1",
                        "average": 9.82222E-5
                    }]
                }, {
                    "attribute": "userAgent",
                    "insight": [{
                        "value": "codedeploy.amazonaws.com",
                        "average": 5.0
                    }],
                    "baseline": [{
                        "value": "codedeploy.amazonaws.com",
                        "average": 9.82222E-5
                    }]
                }, {
                    "attribute": "errorCode",
                    "insight": [{
                        "value": "null",
                        "average": 5.0
                    }],
                    "baseline": [{
                        "value": "null",
                        "average": 9.82222E-5
                    }]
                }]
            }
        },
        "eventCategory": "Insight"
    }
```

Log de eventos de gerenciamento

Por padrão, as trilhas e os armazenamentos de dados de eventos registram em log os eventos de gerenciamento e não incluem eventos de dados nem eventos do Insights.

Há cobranças adicionais para eventos de dados ou eventos do Insights. Para obter mais informações, consulte Preços do AWS CloudTrail.

Sumário

Eventos de gerenciamento

Os eventos de gerenciamento fornecem visibilidade das operações de gerenciamento que são realizadas nos recursos AWS da sua conta. Elas também são conhecidas como operações de plano de controle. Exemplos de eventos de gerenciamento incluem:

- Configuração da segurança (por exemplo, operações de API `AttachRolePolicy` do IAM)
- Registro de dispositivos (por exemplo, operações de API `CreateDefaultVpc` do Amazon EC2)
- Configuração de regras para roteamento de dados (por exemplo, operações de API `CreateSubnet` do Amazon EC2)
- Configurando o registro (por exemplo, operações de AWS CloudTrail `CreateTrail` API)

Os eventos de gerenciamento também podem incluir eventos que não são de API que ocorrem na sua conta. Por exemplo, quando um usuário faz login na sua conta, CloudTrail registra o `ConsoleLogin` evento. Para ter mais informações, consulte Eventos não relacionados à API capturados por CloudTrail.

Por padrão, as trilhas e os armazenamentos de dados de eventos são configurados para registrar eventos de gerenciamento em log.

> **Note**
>
> O recurso Histórico de CloudTrail eventos oferece suporte somente a eventos de gerenciamento. Você não pode excluir AWS KMS nem os eventos da Amazon RDS Data API do histórico de eventos; as configurações que você aplica a um armazenamento de dados de trilhas ou eventos não se aplicam ao histórico de eventos. Para ter mais informações, consulte Trabalhando com o histórico de CloudTrail eventos.

Registrando eventos de gerenciamento com o AWS Management Console

1. Faça login no AWS Management Console e abra o CloudTrail console em https://console.aws.amazon.com/cloudtrail/.
2. Para atualizar uma trilha, abra a página Trilhas do CloudTrail console e escolha o nome da trilha.

   Para atualizar um armazenamento de dados de eventos, abra a página Armazenamentos de dados de eventos do CloudTrail console e escolha o nome do armazenamento de dados de eventos.
3. Em Management events (Eventos de gerenciamento), escolha Edit (Editar).

   - Escolha se você deseja que sua trilha ou o armazenamento de dados de eventos registre eventos de Leitura, Gravação ou ambos.
   - Escolha Excluir AWS KMS eventos para filtrar AWS Key Management Service (AWS KMS) eventos do seu armazenamento de dados de trilhas ou eventos. A configuração padrão é incluir todos os AWS KMS eventos.

     A opção de registrar ou excluir AWS KMS eventos está disponível somente se você registrar eventos de gerenciamento em sua trilha ou armazenamento de dados de eventos. Se você optar por não registrar eventos de gerenciamento, os AWS KMS eventos não serão registrados e você não poderá alterar as configurações do registro de AWS KMS eventos.

AWS KMS ações como`Encrypt`,`Decrypt`, e `GenerateDataKey` normalmente geram um grande volume (mais de 99%) de eventos. Agora essas ações são registradas em log como eventos de Leitura. AWS KMS Ações relevantes de baixo volume, como **`DisableDelete`**, e **`ScheduleKey`** (que normalmente representam menos de 0,5% do volume de AWS KMS eventos) são registradas como eventos de gravação.

Para excluir eventos de alto volume`Encrypt`, como`Decrypt`, e`GenerateDataKey`, mas ainda registrar eventos relevantes`Disable`, como `Delete` e`ScheduleKey`, escolha registrar eventos de gerenciamento de gravação e desmarque a caixa de seleção Excluir AWS KMS eventos.

- Escolha Excluir eventos da API de dados do Amazon RDS para filtrar eventos da API de dados do Amazon Relational Database Service e não incluí-los na trilha. A configuração padrão é incluir todos os eventos da API de dados do Amazon RDS. Para obter mais informações sobre eventos da API de dados do Amazon RDS, consulte Registrar em log chamadas da API de dados com o AWS CloudTrail no Manual do usuário do Amazon RDS for Aurora.

4. Após terminar, escolha Salvar alterações.

Ler e gravar eventos

Ao configurar a trilha ou o armazenamento de dados de eventos para registrar em log eventos de gerenciamento, é possível especificar se você deseja eventos somente leitura, eventos somente gravação, ou ambos.

- Read

  Os eventos somente leitura incluem operações de API que leem seus recursos, mas não fazem alterações. Por exemplo, os eventos somente leitura incluem as operações de API `DescribeSecurityGroups` e `DescribeSubnets` do Amazon EC2. Essas operações retornam apenas informações sobre os recursos do Amazon EC2. Elas não alteram suas configurações.

- Write

  Os eventos somente gravação incluem operações de API que modificam (ou podem modificar) seus recursos. Por exemplo, as operações de API `RunInstances` e `TerminateInstances` do Amazon EC2 modificam suas instâncias.

Exemplo: registro de eventos de leitura e gravação para trilhas separadas

O exemplo a seguir mostra como você pode configurar as trilhas para dividir as atividades de log de uma conta em buckets do S3 separados: um bucket recebe eventos somente leitura e um segundo bucket recebe eventos somente gravação.

1. Crie uma trilha e escolha um bucket do S3 chamado `read-only-bucket` para receber os arquivos de log. Depois, atualize a trilha para especificar se deseja eventos de gerenciamento somente Read (Leitura).
2. Crie uma segunda trilha e escolha um bucket do S3 chamado `write-only-bucket` para receber os arquivos de log. Então, atualize a trilha para especificar se deseja eventos de gerenciamento somente Write (Gravação).
3. As operações de API `DescribeInstances` e `TerminateInstances` do Amazon EC2 ocorrem na sua conta.
4. A operação de API `DescribeInstances` é um evento somente leitura que corresponde às configurações da primeira trilha. A trilha registra e fornece o evento ao `read-only-bucket`.
5. A operação de API `TerminateInstances` é um evento somente gravação que corresponde às configurações da segunda trilha. A trilha registra e fornece o evento ao `write-only-bucket`.

Registrar eventos com o AWS Command Line Interface

É possível configurar suas trilhas ou seus armazenamentos de dados de eventos para registrar eventos de gerenciamento em log usando a AWS CLI.

Tópicos

- Exemplos: registrar em log eventos de gerenciamento para trilhas
- Exemplos: registrar em log eventos de gerenciamento para armazenamentos de dados de eventos

Exemplos: registrar em log eventos de gerenciamento para trilhas

Para visualizar se a trilha está registrando em log os eventos de gerenciamento, execute o comando `get-event-selectors`.

```
aws cloudtrail get-event-selectors --trail-name TrailName
```

O exemplo a seguir retorna as configurações padrão de uma trilha. Por padrão, as trilhas registram em log todos os eventos de gerenciamento, registram em log eventos de todas as origens de evento e não registram em log eventos de dados.

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-1:111122223333:trail/TrailName",
    "AdvancedEventSelectors": [
        {
            "Name": "Management events selector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ]
}
```

Você pode usar seletores de eventos básicos ou avançados para registrar eventos de gerenciamento. Não é possível aplicar seletores de eventos e seletores de eventos avançados a uma trilha. Se você aplicar seletores de eventos avançados a uma trilha, todos os seletores de eventos básicos existentes serão substituídos. As seções a seguir fornecem exemplos de como registrar eventos de gerenciamento usando seletores de eventos avançados e seletores de eventos básicos.

Tópicos

- Exemplos: registro de eventos de gerenciamento para trilhas usando seletores de eventos avançados
- Exemplos: registro de eventos de gerenciamento para trilhas usando seletores de eventos básicos

Exemplos: registro de eventos de gerenciamento para trilhas usando seletores de eventos avançados

O exemplo a seguir cria um seletor de eventos avançado para uma trilha chamada *TrailName* para incluir eventos de gerenciamento somente para leitura e somente gravação (omitindo o `readOnly` seletor), mas para excluir eventos (). AWS Key Management Service AWS KMS Como AWS KMS

os eventos são tratados como eventos de gerenciamento e podem haver um grande volume deles, eles podem ter um impacto substancial em sua CloudTrail fatura se você tiver mais de uma trilha que capture eventos de gerenciamento.

Se você optar por não registrar eventos de gerenciamento, os AWS KMS eventos não serão registrados e você não poderá alterar as configurações do registro de AWS KMS eventos.

Para começar a registrar AWS KMS eventos em uma trilha novamente, remova o `eventSource` seletor e execute o comando novamente.

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events except KMS events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] },
      { "Field": "eventSource", "NotEquals": ["kms.amazonaws.com"] }
    ]
  }
]'
```

O exemplo retorna os seletores de eventos avançados configurados para a trilha.

```
{
  "AdvancedEventSelectors": [
    {
      "Name": "Log all management events except KMS events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Management" ]
        },
        {
          "Field": "eventSource",
          "NotEquals": [ "kms.amazonaws.com" ]
        }
      ]
    }
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Para começar a registrar eventos excluídos para uma trilha novamente, remova o seletor `eventSource` e execute o comando novamente.

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] }
    ]
  }
]'
```

O próximo exemplo cria um seletor de eventos avançado para uma trilha nomeada para incluir eventos de gerenciamento somente *TrailName*para leitura e somente gravação (omitindo o `readOnly` seletor), mas para excluir eventos de gerenciamento da API de dados do Amazon RDS. Para excluir eventos de gerenciamento da API de dados do Amazon RDS, especifique a origem do evento da API de dados do Amazon RDS no valor da string para o `eventSource` campo:. `rdsdata.amazonaws.com`

Se você optar por não registrar eventos de gerenciamento, os eventos de gerenciamento da API de dados do Amazon RDS não serão registrados e você não poderá alterar as configurações de registro de eventos da API de dados do Amazon RDS.

Para começar a registrar novamente os eventos de gerenciamento da API de dados do Amazon RDS em uma trilha, remova o `eventSource` seletor e execute o comando novamente.

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events except Amazon RDS Data API management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] },
      { "Field": "eventSource", "NotEquals": ["rdsdata.amazonaws.com"] }
    ]
  }
]'
```

O exemplo retorna os seletores de eventos avançados configurados para a trilha.

```
{
  "AdvancedEventSelectors": [
    {
      "Name": "Log all management events except Amazon RDS Data API management events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Management" ]
        },
        {
          "Field": "eventSource",
          "NotEquals": [ "rdsdata.amazonaws.com" ]
        }
      ]
    }
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Para começar a registrar eventos excluídos para uma trilha novamente, remova o seletor `eventSource` e execute o comando novamente.

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] }
    ]
  }
]'
```

Exemplos: registro de eventos de gerenciamento para trilhas usando seletores de eventos básicos

Para configurar a trilha para registrar em log eventos de gerenciamento, execute o comando `put-event-selectors`. O exemplo a seguir mostra como configurar a trilha para incluir todos os eventos de gerenciamento para dois objetos do S3. Você pode especificar seletores de eventos de 1 a 5 para uma trilha. Você pode especificar recursos de dados de 1 a 250 para uma trilha.

> **Note**
>
> O número máximo de recursos de dados do S3 é 250, independentemente do número de seletores de evento.

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-selectors
 '[{ "ReadWriteType": "All", "IncludeManagementEvents":true, "DataResources":
 [{ "Type": "AWS::S3::Object", "Values": ["arn:aws:s3:::mybucket/prefix",
 "arn:aws:s3:::mybucket2/prefix2"] }] }]'
```

O exemplo a seguir retorna o seletor de evento configurado para a trilha.

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-1:111122223333:trail/TrailName",
    "EventSelectors": [
        {
            "ReadWriteType": "All",
            "IncludeManagementEvents": true,
            "DataResources": [
                {
                    "Type": "AWS::S3::Object",
                    "Values": [
                        "arn:aws:s3:::mybucket/prefix",
                        "arn:aws:s3:::mybucket2/prefix2",
                    ]
                }
            ],
            "ExcludeManagementEventSources": []
        }
    ]
}
```

Para excluir eventos AWS Key Management Service (AWS KMS) dos registros de uma trilha, execute o `put-event-selectors` comando e adicione o atributo `ExcludeManagementEventSources` com um valor de`kms.amazonaws.com`. O exemplo a seguir cria um seletor de eventos para uma trilha chamada *TrailName*para incluir eventos de gerenciamento somente para leitura e somente gravação, mas exclui eventos. AWS KMS Como AWS KMS pode gerar um grande volume de eventos, o usuário neste exemplo pode querer limitar os eventos para gerenciar o custo de uma trilha.

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "All","ExcludeManagementEventSources":
 ["kms.amazonaws.com"],"IncludeManagementEvents": true}]'
```

O exemplo a seguir retorna o seletor de eventos configurado para a trilha:

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-1:111122223333:trail/TrailName",
    "EventSelectors": [
        {
            "ReadWriteType": "All",
            "IncludeManagementEvents": true,
            "DataResources": [],
            "ExcludeManagementEventSources": [
                "kms.amazonaws.com"
            ]
        }
    ]
}
```

Para excluir eventos de gerenciamento da API de dados do Amazon RDS dos registros de uma trilha, execute o `put-event-selectors` comando e adicione o atributo `ExcludeManagementEventSources` com um valor de`rdsdata.amazonaws.com`. O exemplo a seguir cria um seletor de eventos para uma trilha nomeada para incluir eventos de gerenciamento somente *TrailName*para leitura e somente gravação, mas exclui eventos de gerenciamento da API de dados do Amazon RDS. Como a API de dados do Amazon RDS pode gerar um alto volume de eventos de gerenciamento, o usuário neste exemplo pode querer limitar os eventos para gerenciar o custo de uma trilha.

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-1:111122223333:trail/TrailName",
    "EventSelectors": [
        {
            "ReadWriteType": "All",
            "IncludeManagementEvents": true,
            "DataResources": [],
            "ExcludeManagementEventSources": [
                "rdsdata.amazonaws.com"
            ]
        }
    ]
```

```
}
```

Para começar a registrar AWS KMS novamente os eventos de gerenciamento da API de dados do Amazon RDS em uma trilha, passe uma string vazia como o valor de`ExcludeManagementEventSources`, conforme mostrado no comando a seguir.

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "All","ExcludeManagementEventSources":
 [],"IncludeManagementEvents": true}]'
```

Para registrar AWS KMS eventos relevantes em uma trilha`Disable`, como `Delete` e`ScheduleKey`, mas excluir AWS KMS eventos de alto volume`Encrypt`, como`Decrypt`, e`GenerateDataKey`, registrar eventos de gerenciamento somente para gravação e manter a configuração padrão para registrar AWS KMS eventos, conforme mostrado no exemplo a seguir.

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "WriteOnly","ExcludeManagementEventSources":
 [],"IncludeManagementEvents": true}]'
```

Exemplos: registrar em log eventos de gerenciamento para armazenamentos de dados de eventos

Para verificar se o armazenamento de dados de eventos inclui eventos de gerenciamento, execute o comando get-event-data-store.

```
aws cloudtrail get-event-data-store
--event-data-store arn:aws:cloudtrail:us-east-1:12345678910:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE
```

A seguir, uma exemplo de resposta. A criação e os horários da última atualização estão no formato `timestamp`.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:12345678910:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "myManagementEvents",
    "Status": "ENABLED",
    "AdvancedEventSelectors": [
        {
            "Name": "Management events selector",
```

```
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "FIXED_RETENTION_PRICING",
    "RetentionPeriod": 2557,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-02-04T15:56:27.418000+00:00",
    "UpdatedTimestamp": "2023-02-04T15:56:27.544000+00:00"
}
```

Para criar um armazenamento de dados de eventos que inclua todos os eventos de gerenciamento, execute o comando create-event-data-store. Não é necessário especificar nenhum seletor de eventos avançado para incluir todos os eventos de gerenciamento.

```
aws cloudtrail create-event-data-store
--name my-event-data-store
--retention-period 90\
```

A seguir, uma exemplo de resposta.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:12345678910:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "my-event-data-store",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
```

```
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 90,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-13T16:41:57.224000+00:00",
    "UpdatedTimestamp": "2023-11-13T16:41:57.357000+00:00"
}
```

Para criar um armazenamento de dados de eventos que exclua AWS Key Management Service (AWS KMS) eventos, execute o `create-event-data-store` comando e especifique que `eventSource` não seja igual`kms.amazonaws.com`. O exemplo a seguir cria um armazenamento de dados de eventos que inclui eventos de gerenciamento somente para leitura e somente gravação, mas exclui eventos. AWS KMS

```
aws cloudtrail create-event-data-store --name event-data-store-name --retention-period
 90 --advanced-event-selectors '[
    {
        "Name": "Management events selector",
        "FieldSelectors": [
            {"Field": "eventCategory","Equals": ["Management"]},
            {"Field": "eventSource","NotEquals": ["kms.amazonaws.com"]}
        ]
    }
]'
```

A seguir, uma exemplo de resposta.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:12345678910:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "event-data-store-name",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Management events selector",
            "FieldSelectors": [
```

```
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                },
                {
                    "Field": "eventSource",
                    "NotEquals": [
                        "kms.amazonaws.com"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 90,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-13T17:02:02.067000+00:00",
    "UpdatedTimestamp": "2023-11-13T17:02:02.241000+00:00"
}
```

Para criar um armazenamento de dados de eventos que exclua eventos de gerenciamento da API de dados do Amazon RDS, execute o `create-event-data-store` comando e especifique que `eventSource` não é igual. `rdsdata.amazonaws.com` O exemplo a seguir cria um armazenamento de dados de eventos que inclui eventos de gerenciamento somente leitura e somente gravação, mas exclui eventos da API de dados do Amazon RDS.

```
aws cloudtrail create-event-data-store --name event-data-store-name --retention-period
 90 --advanced-event-selectors '[
    {
        "Name": "Management events selector",
        "FieldSelectors": [
            {"Field": "eventCategory","Equals": ["Management"]},
            {"Field": "eventSource","NotEquals": ["rdsdata.amazonaws.com"]}
        ]
    }
]'
```

A seguir, uma exemplo de resposta.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:12345678910:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "my-event-data-store",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Management events selector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                },
                {
                    "Field": "eventSource",
                    "NotEquals": [
                        "rdsdata.amazonaws.com"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 90,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-13T17:02:02.067000+00:00",
    "UpdatedTimestamp": "2023-11-13T17:02:02.241000+00:00"
}
```

Registro de eventos com os SDKs do AWS

Use a GetEventSelectorsoperação para ver se sua trilha está registrando eventos de gerenciamento de uma trilha. Você pode configurar suas trilhas para registrar eventos de gerenciamento com a PutEventSelectorsoperação. Para obter mais informações, consulte a AWS CloudTrail Referência da API do .

Execute a GetEventDataStoreoperação para ver se seu armazenamento de dados de eventos inclui eventos de gerenciamento. Você pode configurar seus armazenamentos de dados de

eventos para incluir eventos de gerenciamento executando as UpdateEventDataStoreoperações CreateEventDataStoreou. Para obter mais informações, consulte a Crie, atualize e gerencie armazenamentos de dados de eventos com o AWS CLI e a Referência da API do AWS CloudTrail.

Envio de eventos para o Amazon CloudWatch Logs

Para trilhas, CloudTrail suporta o envio de dados e eventos de gerenciamento para o CloudWatch Logs. Quando você configura sua trilha para enviar eventos ao seu grupo de CloudWatch registros de registros, CloudTrail envia somente os eventos que você especifica na trilha. Por exemplo, se você configurar sua trilha para registrar somente eventos de gerenciamento, ela entregará eventos de gerenciamento somente ao seu grupo de CloudWatch registros de registros. Para ter mais informações, consulte Monitoramento CloudTrail de arquivos de log com o Amazon CloudWatch Logs.

Eventos de dados de log

Esta seção descreve como registrar eventos de dados usando o CloudTrail console AWS CLIe.

Por padrão, trilhas e armazenamentos de dados de eventos não registram eventos de dados em log. Há cobranças adicionais para eventos de dados. Para obter mais informações, consulte Preços do AWS CloudTrail.

Os eventos de dados fornecem visibilidade nas operações do recurso executadas no recurso ou dentro de um recurso. Elas também são conhecidas como operações de plano de dados. Eventos de dados geralmente são atividades de alto volume.

Exemplos de eventos de dados incluem:

- Atividade de API em nível de objeto do Amazon S3 (por exemplo,, `GetObject`, `DeleteObject`, e operações de `PutObject` API) em objetos em buckets do S3.
- AWS Lambda atividade de execução da função (a `Invoke` API).
- CloudTrail `PutAuditEvents`atividade em um canal do CloudTrail Lake que é usada para registrar eventos externos AWS.
- Operações da API `Publish` e `PublishBatch` do Amazon SNS em tópicos.

Você pode usar seletores de eventos avançados para criar seletores refinados, que ajudam a controlar os custos registrando apenas os eventos específicos de interesse para seus casos de uso. Por exemplo, você pode usar seletores de eventos avançados para registrar chamadas de

API específicas adicionando um filtro no `eventName` campo. Para ter mais informações, consulte Filtrando eventos de dados usando seletores de eventos avançados.

> **Note**
>
> Os eventos registrados por suas trilhas estão disponíveis na Amazon EventBridge. Por exemplo, se você escolher registrar eventos de dados em log para objetos do S3, mas não eventos de gerenciamento, a trilha processará e registrará somente eventos de dados dos objetos do S3 especificados. Os eventos de dados desses objetos do S3 estão disponíveis na Amazon EventBridge. Para obter mais informações, consulte Eventos de AWS serviços no Guia do EventBridge usuário da Amazon.

Sumário

- Filtrando eventos de dados por resources.ARN
  - Filtrando eventos de dados resources.ARN usando o AWS Management Console
  - Filtrando eventos de dados resources.ARN usando o AWS CLI
- Filtrando eventos de dados por valor readOnly
  - Filtrando eventos de dados por readOnly valor usando o AWS Management Console
  - Filtrando eventos de dados por readOnly valor usando o AWS CLI
- Registrar de eventos de dados para conformidade de AWS Config
- Registrando eventos de dados com os AWS SDKs
- Envio de eventos para o Amazon CloudWatch Logs

Eventos de dados

A tabela a seguir mostra os tipos de eventos de dados disponíveis para trilhas e armazenamentos de dados de eventos. A coluna Tipo de evento de dados (console) mostra a seleção apropriada no console. A coluna de valor resources.type mostra o `resources.type` valor que você especificaria para incluir eventos de dados desse tipo em seu armazenamento de dados de trilhas ou eventos usando as AWS CLI APIs ou. CloudTrail

Para trilhas, você pode usar seletores de eventos básicos ou avançados para registrar eventos de dados para objetos do Amazon S3, funções do Lambda e tabelas do DynamoDB (mostradas nas três primeiras linhas da tabela). É possível usar somente seletores de eventos avançados para registrar em log os tipos de eventos de dados mostrados nas linhas restantes.

Para armazenamentos de dados de eventos, é possível usar somente seletores de eventos avançados para incluir eventos de dados.

AWS service (Serviço da AWS)	Descrição	Tipo de evento de dados (console)	valor resources.type
Amazon DynamoDB	Atividade de API em nível de item do Amazon DynamoDB em tabelas (por	DynamoDB	`AWS::DynamoDB::Table`

AWS service (Serviço da AWS)	Descrição	Tipo de evento de dados (console)	valor resources.type
	exemploPutItem,,Dele m , e operações de API). UpdateItem **Note** Para tabelas com fluxos habilitados, o campo resources no evento de dados contém AWS::Dyna moDB::Str eam e AWS::Dyna moDB::Tab le . Se você especificar AWS::Dyna moDB::Tab le como resources .type , ele registrará os eventos da tabela do DynamoDB e dos fluxos do DynamoDB por padrão.		

AWS service (Serviço da AWS)	Descrição	Tipo de evento de dados (console)	valor resources.type
	Para excluir eventos de streams, adicione um filtro no `eventName` campo.		
AWS Lambda	AWS Lambda atividade de execução da função (a `Invoke` API).	Lambda	`AWS::Lambda::Function`
Amazon S3	Atividade de API em nível de objeto do Amazon S3 (por exemplo,, `GetObject` `DeleteObject` , e operações de `PutObject` API) em objetos em buckets do S3.	S3	`AWS::S3::Object`

AWS service (Serviço da AWS)	Descrição	Tipo de evento de dados (console)	valor resources.type
AWS AppConfig	AWS AppConfig Atividade de API para operações de configuração, como chamadas para `StartConfiguration Session` `GetLatestConfiguration` e.	AWS AppConfig	`AWS::AppConfig::Configuration`
AWS Intercâmbio de dados B2B	Atividade da API B2B Data Interchange para operações do Transformer, como chamadas para `GetTransformerJob` e `StartTransformerJob` .	B2B Data Interchange	`AWS::B2BI::Transformer`
Amazon Bedrock	Atividade da API do Amazon Bedrock em um alias de agente.	Alias de agente do Bedrock	`AWS::Bedrock::AgentAlias`
	Atividade da API do Amazon Bedrock em uma base de conhecimento.	Base de conhecimento do Bedrock	`AWS::Bedrock::KnowledgeBase`

AWS service (Serviço da AWS)	Descrição	Tipo de evento de dados (console)	valor resources.type
Amazon CloudFront	CloudFront Atividade de API em um KeyValueStore.	CloudFront KeyValueStore	`AWS::CloudFront::KeyValueStore`
AWS Cloud Map	AWS Cloud Map Atividade de API em um namespace.	AWS Cloud Map namespace	`AWS::ServiceDiscovery::Namespace`
	AWS Cloud Map Atividade de API em um serviço.	AWS Cloud Map serviço	`AWS::ServiceDiscovery::Service`
AWS CloudTrail	CloudTrail `PutAuditEvents` atividade em um canal do CloudTrail Lake que é usada para registrar eventos externos AWS.	CloudTrail canal	`AWS::CloudTrail::Channel`
Amazon CodeWhisperer	Atividade de CodeWhisperer API da Amazon em uma personalização.	CodeWhisperer personalização	`AWS::CodeWhisperer::Customization`
	Atividade CodeWhisperer da API da Amazon em um perfil.	CodeWhisperer	`AWS::CodeWhisperer::Profile`

AWS service (Serviço da AWS)	Descrição	Tipo de evento de dados (console)	valor resources.type
Amazon Cognito	Atividade da API do Amazon Cognito em bancos de identidades do Amazon Cognito.	Bancos de identidades do Cognito	`AWS::Cognito::IdentityPool`
Amazon DynamoDB	Atividade de API do Amazon DynamoDB em fluxos.	DynamoDB Streams	`AWS::DynamoDB::Stream`
Amazon Elastic Block Store	APIs diretas do Amazon Elastic Block Store (EBS), como `PutSnapshotBlock`, `GetSnapshotBlock` e `ListChangedBlocks` nos snapshots do Amazon EBS.	APIs diretas do Amazon EBS	`AWS::EC2::Snapshot`
Amazon EMR	Atividade da API do Amazon EMR em um espaço de trabalho de log de gravação antecipada.	Espaço de trabalho de log de gravação antecipada do EMR	`AWS::EMRWAL::Workspace`
Amazon FinSpace	Atividade de API do Amazon FinSpace em ambientes.	FinSpace	`AWS::FinSpace::Environment`

AWS service (Serviço da AWS)	Descrição	Tipo de evento de dados (console)	valor resources.type
AWS Glue	AWS Glue Atividade de API em tabelas criadas pelo Lake Formation. **Note** AWS Glue Atualmente, os eventos de dados para tabelas são suportados somente nas seguintes regiões: • Leste dos EUA (Norte da Virgínia) • Leste dos EUA (Ohio) • Oeste dos EUA (Oregon) • Europa (Irlanda) • Região Ásia-	Lake Formation	`AWS::Glue::Table`

AWS service (Serviço da AWS)	Descrição	Tipo de evento de dados (console)	valor resources.type
	Pacífico (Tóquio)		
Amazon GuardDuty	Atividade de GuardDuty API da Amazon para um detector.	GuardDuty detector	`AWS::GuardDuty::Detector`
AWS HealthImaging	AWS HealthImaging Atividade de API em armazenamentos de dados.	Armazenamento de dados de imagens médicas	`AWS::MedicalImaging::Datastore`
AWS IoT	AWS IoT Atividade de API em certificados.	Certificado de IoT	`AWS::IoT::Certificate`
	AWS IoT Atividade de API em coisas.	Coisa de IoT	`AWS::IoT::Thing`

AWS service (Serviço da AWS)	Descrição	Tipo de evento de dados (console)	valor resources.type
AWS IoT Greengrass Version 2	Atividade da API do Greengrass de um dispositivo principal do Greengrass em uma versão de componente. **Note** O Greengrass não registra eventos de acesso negado.	Versão do componente IoT Greengrass	`AWS::GreengrassV2::ComponentVersion`
	Atividade da API do Greengrass de um dispositivo principal do Greengrass em uma implantação. **Note** O Greengrass não registra eventos de acesso negado.	Implantação do IoT Greengrass	`AWS::GreengrassV2::Deployment`
AWS IoT SiteWise	Atividade da SiteWise API de IoT em ativos.	Ativo de IoT SiteWise	`AWS::IoTSiteWise::Asset`

AWS service (Serviço da AWS)	Descrição	Tipo de evento de dados (console)	valor resources.type
	Atividade da SiteWise API de IoT em séries temporais.	Série temporal de IoT SiteWise	`AWS::IoTSiteWise::TimeSeries`
AWS IoT TwinMaker	Atividade da TwinMaker API de IoT em uma entidade.	Entidade de IoT TwinMaker	`AWS::IoTTwinMaker::Entity`
	Atividade da TwinMaker API de IoT em um espaço de trabalho.	Espaço de trabalho de IoT TwinMaker	`AWS::IoTTwinMaker::Workspace`
Amazon Kendra Intelligent Ranking	Atividade da API do Amazon Kendra Intelligent Ranking em planos de execução de reclassificação.	Kendra Ranking	`AWS::KendraRanking::ExecutionPlan`
Amazon Keyspaces (para Apache Cassandra)	Atividade da API Amazon Keyspaces em uma tabela.	Mesa Cassandra	`AWS::Cassandra::Table`
Amazon Kinesis Data Streams	Atividade da API Kinesis Data Streams em streams.	Stream do Kinesis	`AWS::Kinesis::Stream`
	Atividade da API Kinesis Data Streams em consumidores de streams.	Consumidor de streaming do Kinesis	`AWS::Kinesis::StreamConsumer`

AWS service (Serviço da AWS)	Descrição	Tipo de evento de dados (console)	valor resources.type
Amazon Kinesis Video Streams	Atividade da API Kinesis Video Streams em streams de vídeo, como chamadas para e. `GetMedia` `PutMedia`	Fluxo de vídeo do Kinesis	`AWS::KinesisVideo::Stream`
Amazon Managed Blockchain	Atividade da API do Amazon Managed Blockchain em uma rede.	Rede do Managed Blockchain	`AWS::ManagedBlockchain::Network`
	Chamadas de JSON-RPC do Amazon Managed Blockchain em nós Ethereum, como `eth_getBalance` ou `eth_getBlockByNumber` .	Managed Blockchain	`AWS::ManagedBlockchain::Node`
Gráfico do Amazon Neptune	Atividades da API de dados, por exemplo, consultas, algoritmos ou pesquisa vetorial, em um gráfico do Neptune.	Gráfico do Neptune	`AWS::NeptuneGraph::Graph`
AWS Private CA	AWS Private CA Conector para atividade da API do Active Directory.	AWS Private CA Conector para Active Directory	`AWS::PCAConnectorAD::Connector`

AWS service (Serviço da AWS)	Descrição	Tipo de evento de dados (console)	valor resources.type
Aplicativos Amazon Q	Atividade da API de dados no Amazon Q Apps.	Aplicativos Amazon Q	`AWS::QApps:QApp`
Amazon Q Business	Atividade da API do Amazon Q Business em uma aplicação.	Aplicação do Amazon Q Business	`AWS::QBusiness::Application`
	Atividade da API do Amazon Q Business em uma fonte de dados.	Fonte de dados do Amazon Q Business	`AWS::QBusiness::DataSource`
	Atividade da API do Amazon Q Business em um índice.	Índice do Amazon Q Business	`AWS::QBusiness::Index`
	Atividade da API do Amazon Q Business em uma experiência na web.	Experiência na web do Amazon Q Business	`AWS::QBusiness::WebExperience`
Amazon RDS	Atividade da API do Amazon RDS em um cluster de banco de dados.	API de dados do RDS - cluster de banco de dados	`AWS::RDS::DBCluster`
Amazon S3	Atividade da API Amazon S3 em pontos de acesso.	Ponto de acesso do S3	`AWS::S3::AccessPoint`

AWS service (Serviço da AWS)	Descrição	Tipo de evento de dados (console)	valor resources.type
	Atividade da API de pontos de acesso do Amazon S3 Object Lambda, como chamadas para e. `CompleteMultipartUpload` `GetObject`	S3 Object Lambda	`AWS::S3ObjectLambda::AccessPoint`
Amazon S3 on Outposts	Atividade da API em nível de objeto do Amazon S3 on Outposts.	S3 Outposts	`AWS::S3Outposts::Object`
Amazon SageMaker	SageMaker `InvokeEndpointWithResponseStream` Atividade da Amazon em endpoints .	SageMaker ponto final	`AWS::SageMaker::Endpoint`
	Atividade da SageMaker API da Amazon em lojas de recursos.	SageMaker feature store	`AWS::SageMaker::FeatureGroup`
	Atividade da SageMaker API da Amazon em componentes de testes experimentais.	SageMaker componente experimental de métricas	`AWS::SageMaker::ExperimentTrialComponent`

AWS service (Serviço da AWS)	Descrição	Tipo de evento de dados (console)	valor resources.type
Amazon SNS	Operações da API `Publish` do Amazon SNS em endpoints da plataforma.	Endpoint da plataforma SNS	`AWS::SNS::PlatformEndpoint`
	Operações da API `Publish` e `PublishBatch` do Amazon SNS em tópicos.	Tópico do SNS	`AWS::SNS::Topic`
Amazon SQS	Atividade da API do Amazon SQS em mensagens.	SQS	`AWS::SQS::Queue`
AWS Step Functions	Atividade da API Step Functions em uma máquina de estado.	Máquina de estado do Step Functions	`AWS::StepFunctions::StateMachine`
Cadeia de Suprimentos AWS	Cadeia de Suprimentos AWS Atividade de API em uma instância .	Cadeia de suprimentos	`AWS::SCN::Instance`
Amazon SWF	Atividade da API Amazon SWF em domínios.	Domínio SWF	`AWS::SWF::Domain`
AWS Systems Manager	Atividade da API Systems Manager nos canais de controle.	Systems Manager (Gerenciador de sistemas)	`AWS::SSMMessages::ControlChannel`

AWS service (Serviço da AWS)	Descrição	Tipo de evento de dados (console)	valor resources.type
	Atividade da API Systems Manager em nós gerenciados.	Nó gerenciado pelo Systems Manager	`AWS::SSM::ManagedNode`
Amazon Timestream	Atividade da API `Query` do Amazon Timestream em bancos de dados.	Banco de dados do Timestream	`AWS::Timestream::Database`
	Atividade da API `Query` do Amazon Timestream em tabelas.	Tabela do Timestream	`AWS::Timestream::Table`
Amazon Verified Permissions	Atividade da API do Amazon Verified Permissions em um repositório de políticas.	Amazon Verified Permissions	`AWS::VerifiedPermissions::PolicyStore`
Amazon WorkSpaces Thin Client	WorkSpaces Atividade da API Thin Client em um dispositivo.	Dispositivo Thin Client	`AWS::ThinClient::Device`
	WorkSpaces Atividade da API Thin Client em um ambiente.	Ambiente Thin Client	`AWS::ThinClient::Environment`

AWS service (Serviço da AWS)	Descrição	Tipo de evento de dados (console)	valor resources.type
AWS X-Ray	Atividade da API X-Ray em rastreamentos.	Traço de raio-X	`AWS::XRay::Trace`

Para registrar eventos de CloudTrail dados, você deve adicionar explicitamente cada tipo de recurso para o qual deseja coletar atividades. Para obter mais informações, consulte Criar uma trilha e Crie um armazenamento de dados de CloudTrail eventos para eventos com o console.

Em uma trilha de região única, é possível registrar em log eventos de dados somente para recursos que pode acessar nessa região. Embora os buckets do S3 sejam globais, as AWS Lambda funções e as tabelas do DynamoDB são regionais.

Há cobranças adicionais para o registro de eventos de dados. Para CloudTrail saber os preços, consulte AWS CloudTrail Preços.

Exemplos: registro de eventos de dados de objetos do Amazon S3

Registro de eventos de dados para todos os objetos do S3 em um bucket do S3

O exemplo a seguir demonstra como o registro funciona quando você configura o registro de todos os eventos de dados para um bucket do S3 chamado *`bucket-1`*. Neste exemplo, o CloudTrail usuário especificou um prefixo vazio e a opção de registrar eventos de dados de leitura e gravação.

1. Um usuário carrega um objeto no `bucket-1`.
2. A operação da API `PutObject` é uma API de nível de objeto do Amazon S3. Ele é registrado como um evento de dados em CloudTrail. Como o CloudTrail usuário especificou um bucket do S3 com um prefixo vazio, os eventos que ocorrem em qualquer objeto desse bucket são registrados. A trilha ou o armazenamento de dados de eventos processa e registra o evento no log.
3. Outro usuário carrega um objeto no `bucket-2`.

4. A operação de API `PutObject` ocorreu em um objeto em um bucket do S3 que não foi especificado para a trilha ou para o armazenamento de dados de eventos. A trilha ou o armazenamento de dados de eventos não registra o evento no log.

Registro de eventos de dados de objetos específicos do S3

O exemplo a seguir demonstra como o registro em log funciona quando você configura uma trilha ou um armazenamento de dados de eventos para registrar eventos para objetos específicos do S3. Neste exemplo, o CloudTrail usuário especificou um bucket do S3 chamado ***bucket-3***, com o prefixo ***my-images*** e a opção de registrar somente eventos de gravação de dados.

1. Um usuário exclui um objeto que começa com o prefixo `my-images` no bucket, como `arn:aws:s3:::bucket-3/my-images/example.jpg`.
2. A operação da API `DeleteObject` é uma API de nível de objeto do Amazon S3. Ele é registrado como um evento de gravação de dados em CloudTrail. O evento ocorreu em um objeto que corresponde ao bucket do S3 e ao prefixo especificado na trilha ou no armazenamento de dados de eventos. A trilha ou o armazenamento de dados de eventos processa e registra o evento no log.
3. Outro usuário exclui um objeto com um prefixo diferente no bucket do S3, como `arn:aws:s3:::bucket-3/my-videos/example.avi`.
4. O evento ocorreu em um objeto que não corresponde ao prefixo especificado na sua trilha ou no armazenamento de dados de eventos. A trilha ou o armazenamento de dados de eventos não registra o evento no log.
5. Um usuário chama a operação de API `GetObject` do objeto, `arn:aws:s3:::bucket-3/my-images/example.jpg`.
6. O evento ocorreu em um bucket e prefixo que são especificados na trilha ou no armazenamento de dados de eventos, mas `GetObject` é uma API em nível de objeto do Amazon S3 do tipo leitura. Ele é registrado como um evento de leitura de dados em CloudTrail, e o armazenamento de dados de trilha ou evento não está configurado para registrar eventos de leitura. A trilha ou o armazenamento de dados de eventos não registra o evento no log.

> **Note**
>
> Para trilhas, se você estiver registrando eventos de dados específicos para buckets do Amazon S3, recomendamos não usar um bucket do Amazon S3 para os quais você está registrando eventos de dados para receber os arquivos de log que você especificou na

seção de eventos de dados para sua trilha. Usar o mesmo bucket do Amazon S3 faz com que sua trilha registre eventos de dados cada vez que os arquivos de log são entregues ao bucket do Amazon S3. Os arquivos de log são eventos agregados entregues em intervalos, de modo que esta não é uma proporção de 1:1 de evento para arquivo de log; o evento é registrado no próximo arquivo de log. Por exemplo, ao CloudTrail entregar registros, o `PutObject` evento ocorre no bucket do S3. Se o bucket do S3 também é especificado na seção de eventos de dados, a trilha processa e registra o evento `PutObject` como um evento de dados. Essa ação é outro evento `PutObject`, e a trilha processa e registra o evento novamente.

Para evitar o registro de eventos de dados para o bucket do Amazon S3 em que você recebe arquivos de log, se você configurar uma trilha para registrar todos os eventos de dados do Amazon S3 em AWS sua conta, considere configurar a entrega de arquivos de log para um bucket do Amazon S3 que pertença a outra conta. AWS Para ter mais informações, consulte Recebendo arquivos de CloudTrail log de várias contas.

Registro de eventos de dados para objetos do S3 em outras contas AWS

Ao configurar sua trilha para registrar eventos de dados, você também pode especificar objetos do S3 que pertencem a outras AWS contas. Quando um evento ocorre em um objeto especificado, CloudTrail avalia se o evento corresponde a alguma trilha em cada conta. Se o evento corresponder às configurações de uma trilha, ela processará e registrará o evento dessa conta. Geralmente, tanto os chamadores de API quanto os proprietários de recursos podem receber eventos.

Se você tem um objeto do S3 e especifica esse objeto na sua trilha, ela registra eventos que ocorrem no objeto na sua conta. Como você possui o objeto, a trilha também registra eventos quando outras contas chamam o objeto.

Se você especificar um objeto do S3 na sua trilha e outra conta for a proprietária do objeto, a trilha registrará somente eventos que ocorrerem nesse objeto na sua conta. A trilha não registra eventos que ocorrem em outras contas.

Exemplo: registro de eventos de dados de um objeto do Amazon S3 para duas contas da AWS

O exemplo a seguir mostra como duas AWS contas são configuradas CloudTrail para registrar eventos para o mesmo objeto do S3.

1. Na sua conta, você quer que a trilha registre eventos de dados de todos os objetos no seu bucket do S3 chamado `owner-bucket`. Configure a trilha especificando o bucket do S3 com um prefixo de objeto vazio.
2. Bob tem uma conta separada que recebeu acesso ao bucket do S3. Bob também quer registrar eventos de dados de todos os objetos no mesmo bucket do S3. Ele configura sua trilha e especifica o mesmo bucket do S3 com um prefixo de objeto vazio.
3. Bob faz o upload de um objeto no bucket do S3 com a operação de API `PutObject`.
4. Esse evento ocorreu em sua conta e corresponde às configurações de sua trilha. A trilha de Bob processa e registra o evento.
5. Como você possui o bucket do S3 e o evento corresponde às configurações da sua trilha, ela também processa e registra o mesmo evento. Como agora há duas cópias do evento (uma registrada na trilha de Bob e outra registrada na sua), CloudTrail cobra por duas cópias do evento de dados.
6. Faça upload de um objeto do bucket do S3.
7. Esse evento ocorre na sua conta e corresponde às configurações da sua trilha. Sua trilha processa e registra o evento.
8. Como o evento não ocorreu na conta de Bob e ele não é dono do bucket S3, a trilha de Bob não registra o evento. CloudTrail cobra por apenas uma cópia desse evento de dados.

Exemplo: registro de eventos de dados para todos os buckets, incluindo um bucket S3 usado por duas contas AWS

O exemplo a seguir mostra o comportamento de registro quando Selecionar todos os buckets do S3 em sua conta está habilitado para trilhas que coletam eventos de dados em uma AWS conta.

1. Em sua conta, você deseja que sua trilha registre eventos de dados para todos os buckets do S3. Você configura a trilha escolhendo eventos de Read (Leitura), eventos de Write (Gravação) ou ambos para All current and future S3 buckets (Todos os buckets do S3 atuais e futuros) em Data events (Eventos de dados).
2. Bob tem uma conta separada que recebeu acesso a um bucket do S3 em sua conta. Ele deseja registrar eventos de dados para o bucket ao qual ele tem acesso. Ele configura sua trilha para obter eventos de dados para todos os buckets do S3.
3. Bob faz o upload de um objeto no bucket do S3 com a operação de API `PutObject`.
4. Esse evento ocorreu em sua conta e corresponde às configurações de sua trilha. A trilha de Bob processa e registra o evento.

5. Como você possui o bucket do S3 e o evento corresponde às configurações da sua trilha, ela também processa e registra o evento. Como agora existem duas cópias do evento (uma registrada na trilha de Bob e outra registrada na sua), CloudTrail cobra de cada conta uma cópia do evento de dados.
6. Faça upload de um objeto do bucket do S3.
7. Esse evento ocorre na sua conta e corresponde às configurações da sua trilha. Sua trilha processa e registra o evento.
8. Como o evento não ocorreu na conta de Bob e ele não é dono do bucket S3, a trilha de Bob não registra o evento. CloudTrail cobra por apenas uma cópia desse evento de dados em sua conta.
9. Um terceiro usuário, Mary, tem acesso ao bucket do S3 e executa uma operação `GetObject` no bucket. Ela tem uma trilha configurada para registrar eventos de dados em todos os buckets do S3 em sua respectiva conta. Como ela é a chamadora da API, CloudTrail registra um evento de dados em sua trilha. Embora Bob tenha acesso ao bucket, ele não é o proprietário do recurso, então nenhum evento é registrado em sua trilha dessa vez. Como proprietário do recurso, você recebe um evento em sua trilha sobre a `GetObject` operação que Mary convocou. CloudTrailcobra sua conta e a conta de Mary por cada cópia do evento de dados: uma na trilha de Mary e outra na sua.

Eventos somente leitura e somente gravação

Ao configurar a trilha ou o armazenamento de dados de eventos para registrar em log eventos de dados e de gerenciamento, é possível especificar se você deseja eventos somente leitura, eventos somente gravação, ou ambos.

- Read

  Os eventos Read (Leitura) incluem operações de API que leem seus recursos, mas não fazem alterações. Por exemplo, os eventos somente leitura incluem as operações de API `DescribeSecurityGroups` e `DescribeSubnets` do Amazon EC2. Essas operações retornam apenas informações sobre os recursos do Amazon EC2. Elas não alteram suas configurações.

- Write

  Os eventos de Write (Gravação) incluem operações de API que modificam (ou podem modificar) seus recursos. Por exemplo, as operações de API `RunInstances` e `TerminateInstances` do Amazon EC2 modificam suas instâncias.

Exemplo: registro de eventos de leitura e gravação para trilhas separadas

O exemplo a seguir mostra como você pode configurar as trilhas para dividir as atividades de log de uma conta em buckets do S3 separados: um bucket recebe eventos somente leitura e um segundo bucket recebe eventos somente gravação.

1. Crie uma trilha e escolha um bucket do S3 chamado `read-only-bucket` para receber os arquivos de log. Atualize a trilha para especificar que você deseja ver eventos de Read (Leitura) de dados e de gerenciamento.
2. Crie uma segunda trilha e escolha um bucket do S3 chamado `write-only-bucket` para receber os arquivos de log. Atualize a trilha para especificar que você deseja ver eventos de Write (Gravação) de dados e de gerenciamento.
3. As operações de API `DescribeInstances` e `TerminateInstances` do Amazon EC2 ocorrem na sua conta.
4. A operação de API `DescribeInstances` é um evento somente leitura que corresponde às configurações da primeira trilha. A trilha registra e fornece o evento ao `read-only-bucket`.
5. A operação de API `TerminateInstances` é um evento somente gravação que corresponde às configurações da segunda trilha. A trilha registra e fornece o evento ao `write-only-bucket`.

Registrando eventos de dados com o AWS Management Console

Os procedimentos a seguir descrevem como atualizar um armazenamento de dados de eventos ou trilha existente para registrar eventos de dados usando o AWS Management Console. Para obter informações sobre como criar um armazenamento de dados de eventos para registrar eventos de dados, consulte Crie um armazenamento de dados de CloudTrail eventos para eventos com o console. Para obter informações sobre como criar uma trilha para registrar eventos de dados, consulte Criar uma trilha no console.

Para trilhas, as etapas para registrar eventos de dados variam de acordo com o uso de seletores de eventos avançados ou seletores de eventos básicos. Você pode registrar eventos de dados para todos os tipos de eventos de dados usando seletores de eventos avançados, mas se você usar seletores de eventos básicos, estará limitado a registrar eventos de dados para buckets e objetos de bucket do Amazon S3 AWS Lambda , funções e tabelas do Amazon DynamoDB.

Atualizando um armazenamento de dados de eventos existente para registrar eventos de dados no AWS Management Console

Use o procedimento a seguir para atualizar um armazenamento de dados de eventos existente para registrar eventos de dados. Para obter mais informações sobre o uso de seletores de eventos avançados, consulte Filtrando eventos de dados usando seletores de eventos avançados este tópico.

1. Faça login no AWS Management Console e abra o CloudTrail console em https://console.aws.amazon.com/cloudtrail/.
2. No painel de navegação, em Lake, escolha Armazenamentos de dados de eventos.
3. Na página Armazenamentos de dados de eventos, escolha o armazenamento de dados de eventos que deseja atualizar.

   > **Note**
   >
   > Você só pode habilitar eventos de dados em armazenamentos de dados de eventos que contenham CloudTrail eventos. Você não pode habilitar eventos de dados em CloudTrail armazenamentos de dados de eventos para itens de AWS Config configuração, eventos do CloudTrail Insights ou não AWS eventos.

4. Na página de detalhes da trilha, em Eventos de dados, escolha Editar.
5. Se você ainda não estiver registrando eventos de dados, escolha a opçãoData events (Eventos de dados).
6. Em Data event type (Tipo de evento de dados), escolha o tipo de recurso no qual você deseja registrar eventos de dados.
7. Escolha um modelo de seletor de registros. CloudTrail inclui modelos predefinidos que registram todos os eventos de dados do tipo de recurso. Para criar um modelo de seletor de log personalizado, escolha Custom (Personalizado).
8. (Opcional) Em Nome do seletor, insira um nome para identificar o seletor. O nome do seletor é um nome descritivo para um seletor de eventos avançado, como "Registrar eventos de dados em log para apenas dois buckets do S3". O nome do seletor é listado como `Name` no seletor de eventos avançado e poderá ser visualizado se você expandir a visualização JSON.
9. Em Advanced event selectors (Seletores de eventos avançados), crie uma expressão para os recursos específicos nos quais você deseja registrar eventos de dados. Você poderá ignorar esta etapa se estiver usando um modelo de log predefinido.

a. Escolha um dos seguintes campos:

- **`readOnly`**- `readOnly` pode ser definido como igual a um valor de `true` ou. `false` Eventos de dados somente leitura são eventos que não alteram o estado de um recurso, como `Get*` ou `Describe*`. Eventos de gravação adicionam, alteram ou excluem recursos, atributos ou artefatos, como `Put*`, `Delete*` ou `Write*`. Para registrar os eventos `read` e `write`, não adicione um seletor `readOnly`.
- **`eventName`** - `eventName` pode usar qualquer operador. Você pode usá-lo para incluir ou excluir qualquer evento de dados registrado CloudTrail, como `PutBucketGetItem`, ou`GetSnapshotBlock`.
- **`resources.ARN`**- Você pode usar qualquer operador com`resources.`ARN, mas se usar igual ou diferente, o valor deverá corresponder exatamente ao ARN de um recurso válido do tipo que você especificou no modelo como valor de. `resources.type`

  A tabela a seguir mostra o formato de ARN válido para cada `resources.type`.

  > **Note**
  >
  > Você não pode usar o `resources.`ARN campo para filtrar tipos de recursos que não tenham ARNs.

resources.type	resources.ARN
`AWS::DynamoDB::Table` [1]	`arn:partition :dynamodb : region:account_ID :table/table_name`
`AWS::Lambda::Function`	`arn:partition :lambda:region:account_ID :function: function_name`
`AWS::S3::Object` [2]	`arn:partition :s3:::bucket_name / arn:partition :s3:::bucket_name /object_or_file_name /`

resources.type	resources.ARN
AWS::AppConfig::Configuration	arn:*partition* :appconfig: *region*:*account_ID* :application/ *application_ID* /environment/ *environment_ID* /configuration/ *configuration_profile_ID*
AWS::B2BI::Transformer	arn:*partition* :b2bi:*region*:*account_ID* :transformer/ *transformer_ID*
AWS::Bedrock::AgentAlias	arn:*partition* :bedrock: *region*:*account_ID* :agent-alias/ *agent_ID*/*alias_ID*
AWS::Bedrock::KnowledgeBase	arn:*partition* :bedrock: *region*:*account_ID* :knowledge-base/*knowledge_base_ID*
AWS::Cassandra::Table	arn:*partition* :cassandra: *region*:*account_ID* :keyspace/ *keyspace_name* /table/*table_name*
AWS::CloudFront::KeyValueStore	arn:*partition* :cloudfront: *region*:*account_ID* :key-value-store/*KVS_name*
AWS::CloudTrail::Channel	arn:*partition* :cloudtrail: *region*:*account_ID* :channel/ *channel_UUID*
AWS::CodeWhisperer::Customization	arn:*partition* :codewhisperer: *region*:*account_ID* :customization/ *customization_ID*

resources.type	resources.ARN
AWS::CodeWhisperer::Profile	arn:*partition* :codewhis perer: *region*:*account_ID* :profile/ *profile_ID*
AWS::Cognito::IdentityPool	arn:*partition* :cognito-identity: *region*:*account_ID* :identity pool/ *identity_pool_ID*
AWS::DynamoDB::Stream	arn:*partition* :dynamodb : *region*:*account_ID* :table/*table_name* / stream/*date_time*
AWS::EC2::Snapshot	arn:*partition* :ec2:*region*::snapsho t/ *snapshot_ID*
AWS::EMRWAL::Workspace	arn:*partition* :emrwal:*region*:*account_I D* :workspace/ *workspace_name*
AWS::FinSpace::Environment	arn:*partition* :finspace : *region*:*account_ID* :environm ent/ *environment_ID*
AWS::Glue::Table	arn:*partition* :glue:*region*:*account_I D* :table/*database_name* /*table_name*
AWS::GreengrassV2::Componen tVersion	arn:*partition* :greengra ss: *region*:*account_ID* :componen ts/ *component_name*
AWS::GreengrassV2::Deployment	arn:*partition* :greengra ss: *region*:*account_ID* :deployme nts/ *deployment_ID*

resources.type	resources.ARN
AWS::GuardDuty::Detector	arn:*partition* :guarddut y: *region*:*account_ID* :detector / *detector_ID*
AWS::IoT::Certificate	arn:*partition* :iot:*region*:*account_I D* :cert/*certificate_ID*
AWS::IoT::Thing	arn:*partition* :iot:*region*:*account_I D* :thing/*thing_ID*
AWS::IoTSiteWise::Asset	arn:*partition* :iotsitew ise: *region*:*account_ID* :asset/*asset_ID*
AWS::IoTSiteWise::TimeSeries	arn:*partition* :iotsitew ise: *region*:*account_ID* :timeseri es/ *timeseries_ID*
AWS::IoTTwinMaker::Entity	arn:*partition* :iottwinm aker: *region*:*account_ID* :workspac e/ *workspace_ID* /entity/*entity_ID*
AWS::IoTTwinMaker::Workspace	arn:*partition* :iottwinm aker: *region*:*account_ID* :workspac e/ *workspace_ID*
AWS::KendraRanking::Executi onPlan	arn:*partition* :kendra-r anking: *region*:*account_ID* :rescore- execution-plan/ *rescore_execution_ plan_ID*
AWS::Kinesis::Stream	arn:*partition* :kinesis: *region*:*account_ID* :stream/*stream_name*

resources.type	resources.ARN
AWS::Kinesis::StreamConsumer	arn:*partition* :kinesis: *region*:*account_ID* :*stream_type* /*stream_name* /consumer/ *consumer_name* :*consumer_creation_timestamp*
AWS::KinesisVideo::Stream	arn:*partition* :kinesisvideo: *region*:*account_ID* :stream/*stream_name* /*creation_time*
AWS::ManagedBlockchain::Network	arn:*partition* :managedblockchain:::networks/ *network_name*
AWS::ManagedBlockchain::Node	arn:*partition* :managedblockchain: *region*:*account_ID* :nodes/*node_ID*
AWS::MedicalImaging::Datastore	arn:*partition* :medical-imaging: *region*:*account_ID* :datastore/ *data_store_ID*
AWS::NeptuneGraph::Graph	arn:*partition* :neptune-graph: *region*:*account_ID* :graph/*graph_ID*
AWS::PCAConnectorAD::Connector	arn:*partition* :pca-connector-ad: *region*:*account_ID* :connector/ *connector_ID*
AWS::QApps:QApp	arn:*partition* :qapps:*region*:*account_ID* :application/ *application_UUID* / qapp/*qapp_UUID*

resources.type	resources.ARN
AWS::QBusiness::Application	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID*
AWS::QBusiness::DataSource	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID* /index/*index_ID*/ data-source/ *datasource_ID*
AWS::QBusiness::Index	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID* /index/*index_ID*
AWS::QBusiness::WebExperience	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID* /web-expe rience/ *web_experienc_ID*
AWS::RDS::DBCluster	arn:*partition* :rds:*region*:*account_I D* :cluster/ *cluster_name*
AWS::S3::AccessPoint [3]	arn:*partition* :s3:*region*:*account_I D* :accesspoint/ *access_point_name*
AWS::S3ObjectLambda::AccessPoint	arn:*partition* :s3-object-lambda: *region*:*account_ID* :accesspo int/ *access_point_name*
AWS::S3Outposts::Object	arn:*partition* :s3-outpo sts: *region*:*account_ID* :*object_path*

resources.type	resources.ARN
AWS::SageMaker::Endpoint	arn:*partition* :sagemaker: *region*:*account_ID* :endpoint/ *endpoint_name*
AWS::SageMaker::ExperimentTrialComponent	arn:*partition* :sagemaker: *region*:*account_ID* :experiment-trial-component/ *experiment_trial_component_name*
AWS::SageMaker::FeatureGroup	arn:*partition* :sagemaker: *region*:*account_ID* :feature-group/ *feature_group_name*
AWS::SCN::Instance	arn:*partition* :scn:*region*:*account_ID* :instance/ *instance_ID*
AWS::ServiceDiscovery::Namespace	arn:*partition* :servicediscovery: *region*:*account_ID* :namespace/ *namespace_ID*
AWS::ServiceDiscovery::Service	arn:*partition* :servicediscovery: *region*:*account_ID* :service/ *service_ID*
AWS::SNS::PlatformEndpoint	arn:*partition* :sns:*region*:*account_ID* :endpoint/ *endpoint_type* /*endpoint_name* /*endpoint_ID*
AWS::SNS::Topic	arn:*partition* :sns:*region*:*account_ID* :*topic_name*

resources.type	resources.ARN
AWS::SQS::Queue	arn:*partition* :sqs:*region*:*account_ID* :*queue_name*
AWS::SSM::ManagedNode	O ARN deve estar em um dos seguintes formatos: • arn:*partition* :ssm:*region*:*account_ID* :managed-instance/ *instance_ID* • arn:*partition* :ec2:*region*:*account_ID* :instance/ *instance_ID*
AWS::SSMMessages::ControlChannel	arn:*partition* :ssmmessages: *region*:*account_ID* :control-channel/ *control_channel_ID*
AWS::StepFunctions::StateMachine	O ARN deve estar em um dos seguintes formatos: • arn:*partition* :states:*region*:*account_ID* :stateMachine: *stateMachine_name* • arn:*partition* :states:*region*:*account_ID* :stateMachine: *stateMachine_name* /*label_name*
AWS::SWF::Domain	arn:*partition* :swf:*region*:*account_ID* :/domain/ *domain_name*
AWS::ThinClient::Device	arn:*partition* :thinclient: *region*:*account_ID* :device/*device_ID*

resources.type	resources.ARN
`AWS::ThinClient::Environment`	`arn:partition :thinclient: region:account_ID :environment/ environment_ID`
`AWS::Timestream::Database`	`arn:partition :timestream: region:account_ID :database/ database_name`
`AWS::Timestream::Table`	`arn:partition :timestream: region:account_ID :database/ database_name /table/table_name`
`AWS::VerifiedPermissions::PolicyStore`	`arn:partition :verifiedpermissions: region:account_ID :policy-store/ policy_store_ID`

[1] Para tabelas com fluxos habilitados, o campo `resources` no evento de dados contém `AWS::DynamoDB::Stream` e `AWS::DynamoDB::Table`. Se você especificar `AWS::DynamoDB::Table` como `resources.type`, ele registrará os eventos da tabela do DynamoDB e dos fluxos do DynamoDB por padrão. Para excluir eventos de streams, adicione um filtro no `eventName` campo.

[2] Para registrar em log todos os eventos de dados de todos os objetos em um bucket do S3 específico, use o operador `StartsWith` e inclua apenas o ARN do bucket como o valor correspondente. A barra final é intencional; não a exclua.

[3] Para registrar em log eventos de todos os objetos em um ponto de acesso do S3, recomendamos usar somente o ARN do ponto de acesso, não incluir o caminho do objeto e usar os operadores `StartsWith` ou `NotStartsWith`.

Para obter mais informações sobre os formatos do ARN de recursos de evento de dados, consulte Ações, recursos e chaves de condição no Guia do usuário do AWS Identity and Access Management .

b. Para cada campo, escolha + Condição para adicionar quantas condições forem necessárias até o máximo de 500 valores especificados para todas as condições. Por exemplo, para excluir eventos de dados de dois buckets do S3 dos eventos de dados registrados no seu armazenamento de dados de eventos, você pode definir o campo como Resources.arn, definir o operador para does not start with e, em seguida, colar em um ARN do bucket do S3 ou procurar os buckets do S3 nos quais você não deseja registrar eventos.

   Para adicionar o segundo bucket do S3, escolha + Condição e, em seguida, repita a instrução anterior, colando o ARN ou procurando um bucket diferente.

   > **Note**
   >
   > É possível ter no máximo 500 valores para todos os seletores em um armazenamento de dados de eventos. Isso inclui matrizes de vários valores para um seletor, como `eventName`. Se você tiver valores únicos para todos os seletores, poderá ter um máximo de 500 condições adicionadas a um seletor.

c. Selecione + Field (+ Campo) para adicionar outros campos, conforme necessário. Para evitar erros, não defina valores conflitantes ou duplicados para campos. Por exemplo, não especifique um ARN em um seletor para ser igual a um valor e, em seguida, especifique que o ARN não seja igual ao mesmo valor em outro seletor.

10. Para adicionar outro tipo de dados no qual registrar eventos de dados, escolha Add data event type (Adicionar tipo de evento de dados). Repita as etapas de 6 até esta para configurar seletores de eventos avançados para o tipo de evento de dados.
11. Depois de revisar e verificar suas escolhas, escolha Salvar alterações.

Atualizando uma trilha existente para registrar eventos de dados com seletores de eventos avançados no AWS Management Console

No AWS Management Console, se sua trilha estiver usando seletores de eventos avançados, você poderá escolher entre modelos predefinidos que registram todos os eventos de dados em um recurso selecionado. Depois de escolher um modelo de seletor de log, você poderá personalizar o modelo para incluir apenas os eventos de dados que mais deseja ver. Para obter mais informações sobre o uso de seletores de eventos avançados, consulte Filtrando eventos de dados usando seletores de eventos avançados este tópico.

1. Nas páginas Painel ou Trilhas do CloudTrail console, escolha a trilha que você deseja atualizar.

2. Na página de detalhes da trilha, em Eventos de dados, escolha Editar.
3. Se você ainda não estiver registrando eventos de dados, escolha a opçãoData events (Eventos de dados).
4. Em Data event type (Tipo de evento de dados), escolha o tipo de recurso no qual você deseja registrar eventos de dados.
5. Escolha um modelo de seletor de registros. CloudTrail inclui modelos predefinidos que registram todos os eventos de dados do tipo de recurso. Para criar um modelo de seletor de log personalizado, escolha Custom (Personalizado).

> **Note**
>
> A escolha de um modelo predefinido para buckets do S3 permite o registro de eventos de dados de todos os buckets atualmente em sua AWS conta e de todos os buckets que você criar depois de concluir a criação da trilha. Ele também permite o registro da atividade de eventos de dados realizada por qualquer usuário ou função em sua AWS conta, mesmo que essa atividade seja realizada em um bucket que pertença a outra AWS conta.
>
> Se a trilha se aplicar somente a uma região, a escolha da opção Select all S3 buckets in your account (Selecionar todos os buckets do S3 em sua conta) habilitará o registro de eventos de dados para todos os buckets do S3 na mesma região que a trilha e todos os buckets que você criar posteriormente nessa região. Ele não registrará eventos de dados para buckets do Amazon S3 em outras regiões da sua conta. AWS
>
> Se você estiver criando uma trilha para todas as regiões, a escolha de um modelo predefinido para as funções do Lambda permite o registro de eventos de dados para todas as funções atualmente em AWS sua conta e para quaisquer funções do Lambda que você possa criar em qualquer região depois de terminar de criar a trilha. Se você estiver criando uma trilha para uma única região (para trilhas, isso só pode ser feito usando o AWS CLI), essa seleção habilita o registro de eventos de dados para todas as funções atualmente nessa região em sua AWS conta e quaisquer funções Lambda que você possa criar nessa região depois de terminar de criar a trilha. Essa opção não permite o registro de eventos de dados para funções do Lambda criadas em outras regiões.
>
> O registro de eventos de dados para todas as funções também permite o registro da atividade de eventos de dados realizada por qualquer usuário ou função em sua AWS conta, mesmo que essa atividade seja realizada em uma função que pertença a outra AWS conta.

6. (Opcional) Em Nome do seletor, insira um nome para identificar o seletor. O nome do seletor é um nome descritivo para um seletor de eventos avançado, como "Registrar eventos de dados em log para apenas dois buckets do S3". O nome do seletor é listado como `Name` no seletor de eventos avançado e poderá ser visualizado se você expandir a visualização JSON.
7. Em Advanced event selectors (Seletores de eventos avançados), crie uma expressão para os recursos específicos nos quais você deseja registrar eventos de dados. Você poderá ignorar esta etapa se estiver usando um modelo de log predefinido.

   a. Escolha um dos seguintes campos:

   - **`readOnly`**- `readOnly` pode ser definido como igual a um valor de `true` ou. `false` Eventos de dados somente leitura são eventos que não alteram o estado de um recurso, como `Get*` ou `Describe*`. Eventos de gravação adicionam, alteram ou excluem recursos, atributos ou artefatos, como `Put*`, `Delete*` ou `Write*`. Para registrar os eventos `read` e `write`, não adicione um seletor `readOnly`.
   - **`eventName`** - `eventName` pode usar qualquer operador. Você pode usá-lo para incluir ou excluir qualquer evento de dados registrado CloudTrail, como `PutBucketGetItem`, ou`GetSnapshotBlock`.
   - **`resources.ARN`**- Você pode usar qualquer operador com`resources.ARN`, mas se usar igual ou diferente, o valor deverá corresponder exatamente ao ARN de um recurso válido do tipo que você especificou no modelo como valor de. `resources.type`

     A tabela a seguir mostra o formato de ARN válido para cada `resources.type`.

     > **Note**
     >
     > Você não pode usar o `resources.ARN` campo para filtrar tipos de recursos que não tenham ARNs.

resources.type	resources.ARN
`AWS::DynamoDB::Table` [1]	`arn:partition :dynamodb : region:account_ID :table/table_name`

resources.type	resources.ARN
AWS::Lambda::Function	arn:*partition* :lambda:*region*:*account_ID* :function: *function_name*
AWS::S3::Object [2]	arn:*partition* :s3:::*bucket_name* / arn:*partition* :s3:::*bucket_name* /*object_or_file_name* /
AWS::AppConfig::Configuration	arn:*partition* :appconfig: *region*:*account_ID* :application/ *application_ID* /environment/ *environment_ID* /configuration/ *configuration_profile_ID*
AWS::B2BI::Transformer	arn:*partition* :b2bi:*region*:*account_ID* :transformer/ *transformer_ID*
AWS::Bedrock::AgentAlias	arn:*partition* :bedrock: *region*:*account_ID* :agent-alias/ *agent_ID*/*alias_ID*
AWS::Bedrock::KnowledgeBase	arn:*partition* :bedrock: *region*:*account_ID* :knowledge-base/*knowledge_base_ID*
AWS::Cassandra::Table	arn:*partition* :cassandra: *region*:*account_ID* :keyspace/ *keyspace_name* /table/*table_name*
AWS::CloudFront::KeyValueStore	arn:*partition* :cloudfront: *region*:*account_ID* :key-value-store/*KVS_name*

resources.type	resources.ARN
AWS::CloudTrail::Channel	arn:*partition* :cloudtrail: *region*:*account_ID* :channel/ *channel_UUID*
AWS::CodeWhisperer::Customization	arn:*partition* :codewhisperer: *region*:*account_ID* :customization/ *customization_ID*
AWS::CodeWhisperer::Profile	arn:*partition* :codewhisperer: *region*:*account_ID* :profile/ *profile_ID*
AWS::Cognito::IdentityPool	arn:*partition* :cognito-identity: *region*:*account_ID* :identitypool/ *identity_pool_ID*
AWS::DynamoDB::Stream	arn:*partition* :dynamodb: *region*:*account_ID* :table/*table_name* /stream/*date_time*
AWS::EC2::Snapshot	arn:*partition* :ec2:*region*::snapshot/ *snapshot_ID*
AWS::EMRWAL::Workspace	arn:*partition* :emrwal:*region*:*account_ID* :workspace/ *workspace_name*
AWS::FinSpace::Environment	arn:*partition* :finspace: *region*:*account_ID* :environment/ *environment_ID*
AWS::Glue::Table	arn:*partition* :glue:*region*:*account_ID* :table/*database_name* /*table_name*

resources.type	resources.ARN
AWS::GreengrassV2::ComponentVersion	arn:*partition* :greengrass: *region*:*account_ID* :components/ *component_name*
AWS::GreengrassV2::Deployment	arn:*partition* :greengrass: *region*:*account_ID* :deployments/ *deployment_ID*
AWS::GuardDuty::Detector	arn:*partition* :guardduty: *region*:*account_ID* :detector/ *detector_ID*
AWS::IoT::Certificate	arn:*partition* :iot:*region*:*account_ID* :cert/*certificate_ID*
AWS::IoT::Thing	arn:*partition* :iot:*region*:*account_ID* :thing/*thing_ID*
AWS::IoTSiteWise::Asset	arn:*partition* :iotsitewise: *region*:*account_ID* :asset/*asset_ID*
AWS::IoTSiteWise::TimeSeries	arn:*partition* :iotsitewise: *region*:*account_ID* :timeseries/ *timeseries_ID*
AWS::IoTTwinMaker::Entity	arn:*partition* :iottwinmaker: *region*:*account_ID* :workspace/ *workspace_ID* /entity/*entity_ID*
AWS::IoTTwinMaker::Workspace	arn:*partition* :iottwinmaker: *region*:*account_ID* :workspace/ *workspace_ID*

resources.type	resources.ARN
AWS::KendraRanking::ExecutionPlan	arn:*partition* :kendra-ranking: *region*:*account_ID* :rescore-execution-plan/ *rescore_execution_plan_ID*
AWS::Kinesis::Stream	arn:*partition* :kinesis: *region*:*account_ID* :stream/*stream_name*
AWS::Kinesis::StreamConsumer	arn:*partition* :kinesis: *region*:*account_ID* :*stream_type* /*stream_name* /consumer/ *consumer_name* :*consumer_creation_timestamp*
AWS::KinesisVideo::Stream	arn:*partition* :kinesisvideo: *region*:*account_ID* :stream/*stream_name* /*creation_time*
AWS::ManagedBlockchain::Network	arn:*partition* :managedblockchain :::networks/ *network_name*
AWS::ManagedBlockchain::Node	arn:*partition* :managedblockchain : *region*:*account_ID* :nodes/*node_ID*
AWS::MedicalImaging::Datastore	arn:*partition* :medical-imaging: *region*:*account_ID* :datastore/ *data_store_ID*
AWS::NeptuneGraph::Graph	arn:*partition* :neptune-graph: *region*:*account_ID* :graph/*graph_ID*

resources.type	resources.ARN
AWS::PCAConnectorAD::Connector	arn:*partition* :pca-connector-ad: *region*:*account_ID* :connector/ *connector_ID*
AWS::QApps:QApp	arn:*partition* :qapps:*region*:*account_ID* :application/ *application_UUID* / qapp/*qapp_UUID*
AWS::QBusiness::Application	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID*
AWS::QBusiness::DataSource	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID* /index/*index_ID*/ data-source/ *datasource_ID*
AWS::QBusiness::Index	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID* /index/*index_ID*
AWS::QBusiness::WebExperience	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID* /web-experience/ *web_experienc_ID*
AWS::RDS::DBCluster	arn:*partition* :rds:*region*:*account_ID* :cluster/ *cluster_name*
AWS::S3::AccessPoint [3]	arn:*partition* :s3:*region*:*account_ID* :accesspoint/ *access_point_name*

resources.type	resources.ARN
AWS::S3ObjectLambda::AccessPoint	arn:*partition* :s3-object-lambda: *region*:*account_ID* :accesspoint/ *access_point_name*
AWS::S3Outposts::Object	arn:*partition* :s3-outposts: *region*:*account_ID* :*object_path*
AWS::SageMaker::Endpoint	arn:*partition* :sagemaker: *region*:*account_ID* :endpoint/ *endpoint_name*
AWS::SageMaker::ExperimentTrialComponent	arn:*partition* :sagemaker: *region*:*account_ID* :experiment-trial-component/ *experiment_trial_component_name*
AWS::SageMaker::FeatureGroup	arn:*partition* :sagemaker: *region*:*account_ID* :feature-group/ *feature_group_name*
AWS::SCN::Instance	arn:*partition* :scn:*region*:*account_ID* :instance/ *instance_ID*
AWS::ServiceDiscovery::Namespace	arn:*partition* :servicediscovery: *region*:*account_ID* :namespace/ *namespace_ID*
AWS::ServiceDiscovery::Service	arn:*partition* :servicediscovery: *region*:*account_ID* :service/ *service_ID*

resources.type	resources.ARN
AWS::SNS::PlatformEndpoint	arn:*partition* :sns:*region*:*account_ID* :endpoint/ *endpoint_type* /*endpoint_name* /*endpoint_ID*
AWS::SNS::Topic	arn:*partition* :sns:*region*:*account_ID* :*topic_name*
AWS::SQS::Queue	arn:*partition* :sqs:*region*:*account_ID* :*queue_name*
AWS::SSM::ManagedNode	O ARN deve estar em um dos seguintes formatos: • arn:*partition* :ssm:*region*:*account_ID* :managed-instance/ *instance_ID* • arn:*partition* :ec2:*region*:*account_ID* :instance/ *instance_ID*
AWS::SSMMessages::ControlChannel	arn:*partition* :ssmmessages: *region*:*account_ID* :control-channel/ *control_channel_ID*
AWS::StepFunctions::StateMachine	O ARN deve estar em um dos seguintes formatos: • arn:*partition* :states:*region*:*account_ID* :stateMachine: *stateMachine_name* • arn:*partition* :states:*region*:*account_ID* :stateMachine: *stateMachine_name* /*label_name*

resources.type	resources.ARN
AWS::SWF::Domain	arn:*partition* :swf:*region*:*account_ID* :/domain/ *domain_name*
AWS::ThinClient::Device	arn:*partition* :thinclient: *region*:*account_ID* :device/*device_ID*
AWS::ThinClient::Environment	arn:*partition* :thinclient: *region*:*account_ID* :environment/ *environment_ID*
AWS::Timestream::Database	arn:*partition* :timestream: *region*:*account_ID* :database/ *database_name*
AWS::Timestream::Table	arn:*partition* :timestream: *region*:*account_ID* :database/ *database_name* /table/*table_name*
AWS::VerifiedPermissions::PolicyStore	arn:*partition* :verifiedpermissions: *region*:*account_ID* :policy-store/ *policy_store_ID*

[1] Para tabelas com fluxos habilitados, o campo `resources` no evento de dados contém `AWS::DynamoDB::Stream` e `AWS::DynamoDB::Table`. Se você especificar `AWS::DynamoDB::Table` como `resources.type`, ele registrará os eventos da tabela do DynamoDB e dos fluxos do DynamoDB por padrão. Para excluir eventos de streams, adicione um filtro no `eventName` campo.

[2] Para registrar em log todos os eventos de dados de todos os objetos em um bucket do S3 específico, use o operador `StartsWith` e inclua apenas o ARN do bucket como o valor correspondente. A barra final é intencional; não a exclua.

[3] Para registrar em log eventos de todos os objetos em um ponto de acesso do S3, recomendamos usar somente o ARN do ponto de acesso, não incluir o caminho do objeto e usar os operadores `StartsWith` ou `NotStartsWith`.

Para obter mais informações sobre os formatos do ARN de recursos de evento de dados, consulte Ações, recursos e chaves de condição no Guia do usuário do AWS Identity and Access Management .

b. Para cada campo, escolha + Condição para adicionar quantas condições forem necessárias até o máximo de 500 valores especificados para todas as condições. Por exemplo, para excluir eventos de dados de dois buckets do S3 dos eventos de dados registrados em sua trilha, você pode definir o campo como Resources.arn, definir o operador para does not start with e, em seguida, colar o ARN de um bucket do S3 ou procurar os buckets do S3 nos quais você não deseja registrar eventos.

   Para adicionar o segundo bucket do S3, escolha + Condição e, em seguida, repita a instrução anterior, colando o ARN ou procurando um bucket diferente.

   > **Note**
   >
   > É possível ter, no máximo, 500 valores para todos os seletores em uma trilha. Isso inclui matrizes de vários valores para um seletor, como `eventName`. Se você tiver valores únicos para todos os seletores, poderá ter um máximo de 500 condições adicionadas a um seletor.

c. Selecione + Field (+ Campo) para adicionar outros campos, conforme necessário. Para evitar erros, não defina valores conflitantes ou duplicados para campos. Por exemplo, não especifique um ARN em um seletor para ser igual a um valor e, em seguida, especifique que o ARN não seja igual ao mesmo valor em outro seletor.

8. Para adicionar outro tipo de dados no qual registrar eventos de dados, escolha Add data event type (Adicionar tipo de evento de dados). Repita as etapas de 4 até esta etapa para configurar seletores de eventos avançados para o tipo de evento de dados.
9. Depois de revisar e verificar suas escolhas, escolha Salvar alterações.

Atualize uma trilha existente para registrar eventos de dados com seletores de eventos básicos no AWS Management Console

Use o procedimento a seguir para atualizar uma trilha existente para registrar eventos de dados usando seletores de eventos básicos.

1. Faça login no AWS Management Console e abra o CloudTrail console em https://console.aws.amazon.com/cloudtrail/.
2. Abra a página Trilhas do CloudTrail console e escolha o nome da trilha.

> **Note**
>
> Embora seja possível editar uma trilha existente para registrar eventos de dados em log, como prática recomendada considere criar uma trilha separada especificamente para o log de eventos de dados.

3. Em Data events (Eventos de dados), escolha Edit (Editar).
4. Para Buckets do Amazon S3:
   a. Em Data event source (Fonte do eventos de dados), escolha S3.
   b. Você pode escolher registrar All current and future S3 buckets (Todos os buckets do S3 atuais e futuros) ou pode especificar buckets ou funções individuais. Por padrão, os eventos de dados são registrados para todos os buckets do S3 atuais e futuros.

> **Note**
>
> Manter a opção padrão All current and future S3 buckets permite o registro de eventos de dados para todos os buckets atualmente em sua AWS conta e para todos os buckets que você criar depois de concluir a criação da trilha. Ele também permite o registro da atividade de eventos de dados realizada por qualquer usuário ou função em sua AWS conta, mesmo que essa atividade seja realizada em um bucket que pertença a outra AWS conta.
> Se você estiver criando uma trilha para uma única região (usando o AWS CLI), selecionar a opção Selecionar todos os buckets do S3 em sua conta habilita o registro de eventos de dados para todos os buckets na mesma região da sua trilha e quaisquer buckets que você criar posteriormente nessa região. Ele não registrará

eventos de dados para buckets do Amazon S3 em outras regiões da sua conta. AWS

c. Se você deixar a opção padrão All current and future S3 buckets (Todos os buckets do S3 atuais e futuros), escolha para registrar eventos Read (Leitura), Write (Gravação) ou ambos.

d. Para selecionar buckets individuais, desmarque as caixas de seleção Read (Leitura) e Write (Gravação) em All current and future S3 buckets (Todos os buckets do S3 atuais e futuros). Em Individual bucket selection (Seleção de bucket individual), procure por um bucket no qual registrar eventos de dados. Para localizar períodos específicos, digite um prefixo de bucket para o bucket desejado. É possível selecionar vários buckets nesta janela. Escolha Add bucket (Adicionar bucket) para registrar eventos de dados em mais buckets. Escolha se você deseja registrar eventos de Read (Leitura), como `GetObject`, Write (Gravação), como `PutObject`, ou ambos.

   Essa configuração tem precedência sobre configurações individuais que você configura para buckets individuais. Por exemplo, se você especificar o registro de eventos de Read (Leitura) para todos os buckets do S3 e escolher adicionar um bucket específico ao registro de eventos de dados, Read (Leitura) já estará selecionada para o bucket adicionado. Você não pode limpar a seleção. Você pode somente configurar a opção para Write (Gravação).

   Para remover um bucket do registro, escolha X.

5. Para adicionar outro tipo de dados no qual registrar eventos de dados, escolha Add data event type (Adicionar tipo de evento de dados).

6. Funções do Lambda:

   a. Em Data event source (Fonte do eventos de dados), escolha Lambda.

   b. Em Lambda function (Função do Lambda), escolha All regions (Todas as regiões) para registrar todas as funções do Lambda, ou Input function as ARN (Função de entrada como ARN) para registrar eventos de dados em uma função específica.

      Para registrar eventos de dados para todas as funções do Lambda em sua conta da AWS , selecione Log all current and future functions (Registrar todas as funções atuais e futuras). Essa configuração tem precedência sobre configurações individuais definidas para funções individuais. Todas as funções são registradas, mesmo se todas as funções não forem exibidas.

> **Note**
>
> Se estiver criando uma trilha para todas as regiões, essa seleção habilitará o registro de eventos de dados para todas as funções atualmente em sua conta da AWS e qualquer função Lambda que você venha a criar em qualquer região depois de concluir a criação da trilha. Se você estiver criando uma trilha para uma única região (feita usando o AWS CLI), essa seleção habilita o registro de eventos de dados para todas as funções atualmente nessa região em sua AWS conta e quaisquer funções Lambda que você possa criar nessa região depois de terminar de criar a trilha. Essa opção não permite o registro de eventos de dados para funções do Lambda criadas em outras regiões.
> O registro de eventos de dados para todas as funções também permite o registro da atividade de eventos de dados realizada por qualquer usuário ou função em sua AWS conta, mesmo que essa atividade seja realizada em uma função que pertença a outra AWS conta.

c. Se você escolher Input function as ARN (Função de entrada como ARN), insira o ARN de uma função do Lambda.

> **Note**
>
> Se você tiver mais de 15.000 funções do Lambda em sua conta, não poderá visualizar ou selecionar todas as funções no console CloudTrail ao criar uma trilha. Você ainda poderá selecionar a opção de registrar todas as funções, mesmo se elas não forem exibidas. Se você desejar registrar eventos de dados para funções específicas, poderá adicionar manualmente uma função se você souber seu ARN. Você também pode concluir a criação da trilha no console e, em seguida, usar o put-event-selectors comando AWS CLI e o para configurar o registro de eventos de dados para funções específicas do Lambda. Para ter mais informações, consulte Gerenciando trilhas com o AWS CLI.

7. Para adicionar outro tipo de dados no qual registrar eventos de dados, escolha Add data event type (Adicionar tipo de evento de dados).
8. Para tabelas do DynamoDB:

   a. Em Data event source (Fonte do eventos de dados), escolha DynamoDB.

b. Em DynamoDB table selection (Seleção da tabela do DynamoDB), escolha Browse (Navegar) para selecionar uma tabela ou cole no ARN de uma tabela do DynamoDB à qual você tem acesso. Um ARN de tabela do DynamoDB utiliza o seguinte formato:

```
arn:partition:dynamodb:region:account_ID:table/table_name
```

Para adicionar outra tabela, escolha Add row (Adicionar linha) e procure uma tabela ou cole no ARN de uma tabela à qual você tem acesso.

9. Escolha Salvar alterações.

Registrando eventos de dados com o AWS Command Line Interface

É possível configurar suas trilhas ou seus armazenamentos de dados de eventos para registrar eventos de dados em log usando a AWS CLI.

Tópicos

- Registrando eventos de dados para trilhas com o AWS CLI
- Registrando eventos de dados para armazenamentos de dados de eventos com o AWS CLI

Registrando eventos de dados para trilhas com o AWS CLI

Você pode configurar suas trilhas para registrar eventos de gerenciamento e de dados usando a AWS CLI.

> **Note**
>
> - Esteja ciente de que, se a sua conta estiver registrando mais de uma cópia de eventos de gerenciamento, você incorrerá em cobranças. Há sempre uma cobrança para o registro de eventos de dados. Para obter mais informações, consulte Preços do AWS CloudTrail.
> - Você pode usar seletores de eventos avançados ou seletores de eventos básicos, mas não ambos. Se você aplicar seletores de eventos avançados a uma trilha, todos os seletores de eventos básicos existentes serão substituídos.
> - Se sua trilha usa seletores de eventos básicos, você só pode registrar os seguintes tipos de recursos:
>   - `AWS::DynamoDB::Table`

- `AWS::Lambda::Function`
- `AWS::S3::Object`

Para registrar tipos de recursos adicionais, você precisará usar seletores de eventos avançados. Para converter uma trilha em seletores de eventos avançados, execute o comando get-event-selectors para confirmar os seletores de eventos atuais e, em seguida, configure os seletores de eventos avançados para corresponder à cobertura dos seletores de eventos anteriores e, em seguida, adicione seletores para qualquer tipo de recurso para o qual você deseja registrar eventos de dados.

- Você pode usar seletores de eventos avançados para filtrar com base no valor dos campos `eventName`, `resources.ARN` e `readOnly`, permitindo que você registre somente os eventos de dados de interesse. Para obter mais informações sobre como configurar esses campos, consulte AdvancedFieldSelectorna Referência da AWS CloudTrail API e Filtrando eventos de dados usando seletores de eventos avançados neste tópico.

Para visualizar se a trilha está registrando eventos de dados e de gerenciamento, execute o comando `get-event-selectors`.

```
aws cloudtrail get-event-selectors --trail-name TrailName
```

O comando retorna os seletores de eventos da trilha.

Tópicos

- Registar eventos utilizando seletores de eventos avançados
- Registre todos os eventos do Amazon S3 para um bucket do Amazon S3 usando seletores de eventos avançados
- Registrar o Amazon S3 no AWS Outposts usando seletores de eventos avançados
- Registar eventos utilizando seletores de eventos básicos

Registar eventos utilizando seletores de eventos avançados

> **Note**
>
> Se você aplicar seletores de eventos avançados a uma trilha, todos os seletores de eventos básicos existentes serão substituídos. Antes de configurar seletores de eventos avançados,

execute o comando get-event-selectors para confirmar os seletores de eventos atuais e, em seguida, configure os seletores de eventos avançados para corresponder à cobertura dos seletores de eventos anteriores e, em seguida, adicione seletores para qualquer tipo de recurso para o qual você deseja registrar eventos de dados.

O exemplo a seguir cria seletores de eventos avançados personalizados para uma trilha nomeada *TrailName* para incluir eventos de gerenciamento de leitura e gravação (omitindo o `readOnly` seletor) `PutObject` e eventos de `DeleteObject` dados para todas as combinações de bucket/prefixo do Amazon S3, exceto para um bucket chamado e eventos de dados para uma função chamada. `sample_bucket_name` AWS Lambda `MyLambdaFunction` Como estes são seletores de eventos avançados personalizados, cada conjunto de seletores tem um nome descritivo. Observe que uma barra à direita faz parte do valor ARN para buckets do S3.

```
aws cloudtrail put-event-selectors --trail-name TrailName --advanced-event-selectors
'[
  {
    "Name": "Log readOnly and writeOnly management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] }
    ]
  },
  {
    "Name": "Log PutObject and DeleteObject events for all but one bucket",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
      { "Field": "eventName", "Equals": ["PutObject","DeleteObject"] },
      { "Field": "resources.ARN", "NotStartsWith":
 ["arn:aws:s3:::sample_bucket_name/"] }
    ]
  },
  {
    "Name": "Log data plane actions on MyLambdaFunction",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::Lambda::Function"] },
      { "Field": "resources.ARN", "Equals": ["arn:aws:lambda:us-
east-2:111122223333:function/MyLambdaFunction"] }
    ]
  }
```

```
]'
```

O exemplo retorna os seletores de eventos avançados configurados para a trilha.

```
{
  "AdvancedEventSelectors": [
    {
      "Name": "Log readOnly and writeOnly management events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Management" ]
        }
      ]
    },
    {
      "Name": "Log PutObject and DeleteObject events for all but one bucket",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Data" ]
        },
        {
          "Field": "resources.type",
          "Equals": [ "AWS::S3::Object" ]
        },
        {
          "Field": "resources.ARN",
          "NotStartsWith": [ "arn:aws:s3:::sample_bucket_name/" ]
        },
      ]
    },
{
      "Name": "Log data plane actions on MyLambdaFunction",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Data" ]
        },
        {
          "Field": "resources.type",
          "Equals": [ "AWS::Lambda::Function" ]
        },
```

```
        {
          "Field": "eventName",
          "Equals": [ "Invoke" ]
        },
        {
          "Field": "resources.ARN",
          "Equals": [ "arn:aws:lambda:us-east-2:111122223333:function/
MyLambdaFunction" ]
        }
      ]
    }
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Registre todos os eventos do Amazon S3 para um bucket do Amazon S3 usando seletores de eventos avançados

> **Note**
>
> Se você aplicar seletores de eventos avançados a uma trilha, todos os seletores de eventos básicos existentes serão substituídos.

O exemplo a seguir mostra como configurar a trilha para registrar eventos de dados de todos os objetos do Amazon S3 em um bucket do S3. O valor para eventos do S3 para o campo `resources.type` é `AWS::S3::Object`. Como os valores de ARN para objetos do S3 e buckets do S3 são ligeiramente diferentes, você deve adicionar o operador `StartsWith` para o `resources.`ARN para capturar todos os eventos.

```
aws cloudtrail put-event-selectors --trail-name TrailName --region region \
--advanced-event-selectors \
'[
    {
            "Name": "S3EventSelector",
            "FieldSelectors": [
                { "Field": "eventCategory", "Equals": ["Data"] },
                { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
                { "Field": "resources.ARN", "StartsWith":
 ["arn:partition:s3:::bucket_name/"] }
            ]
```

```
        }
]'
```

Este comando retorna a saída de exemplo a seguir.

```
{
    "TrailARN": "arn:aws:cloudtrail:region:account_ID:trail/TrailName",
    "AdvancedEventSelectors": [
        {
            "Name": "S3EventSelector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3::Object"
                    ]
                },
                {
                    "Field": "resources.ARN",
                    "StartsWith": [
                        "arn:partition:s3:::bucket_name/"
                    ]
                }
            ]
        }
    ]
}
```

Registrar o Amazon S3 no AWS Outposts usando seletores de eventos avançados

> **Note**
>
> Se você aplicar seletores de eventos avançados a uma trilha, todos os seletores de eventos básicos existentes serão substituídos.

O exemplo a seguir mostra como configurar a trilha para incluir todos os eventos de dados para todos os objetos do Amazon S3 on Outposts em seu outpost.

```
aws cloudtrail put-event-selectors --trail-name TrailName --region region \
--advanced-event-selectors \
'[
    {
            "Name": "OutpostsEventSelector",
            "FieldSelectors": [
                { "Field": "eventCategory", "Equals": ["Data"] },
                { "Field": "resources.type", "Equals": ["AWS::S3Outposts::Object"] }
            ]
    }
]'
```

Este comando retorna a saída de exemplo a seguir.

```
{
    "TrailARN": "arn:aws:cloudtrail:region:account_ID:trail/TrailName",
    "AdvancedEventSelectors": [
        {
            "Name": "OutpostsEventSelector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3Outposts::Object"
                    ]
                }
            ]
        }
    ]
}
```

Registar eventos utilizando seletores de eventos básicos

Este é um exemplo de resultado do comando get-event-selectors mostrando seletores de eventos básicos. Por padrão, quando você cria uma trilha usando o AWS CLI, uma trilha registra todos os eventos de gerenciamento. Por padrão, as trilhas não registram em log eventos de dados.

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName",
    "EventSelectors": [
        {
            "IncludeManagementEvents": true,
            "DataResources": [],
            "ReadWriteType": "All"
        }
    ]
}
```

Para configurar a trilha para registrar eventos de gerenciamento e de dados, execute o comando `put-event-selectors`.

O exemplo a seguir mostra como usar seletores de eventos básicos para configurar a trilha para incluir todos os eventos de gerenciamento e de dados para os objetos do S3 em dois prefixos de bucket do S3. Você pode especificar seletores de eventos de 1 a 5 para uma trilha. Você pode especificar recursos de dados de 1 a 250 para uma trilha.

> **Note**
>
> O número máximo de recursos de dados do S3 será 250, se você optar por limitar eventos de dados usando seletores de evento básicos.

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-selectors
 '[{ "ReadWriteType": "All", "IncludeManagementEvents":true, "DataResources":
 [{ "Type": "AWS::S3::Object", "Values": ["arn:aws:s3:::mybucket/prefix",
 "arn:aws:s3:::mybucket2/prefix2"] }] }]'
```

O comando retorna os seletores de eventos configurados para a trilha.

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName",
    "EventSelectors": [
```

```
        {
            "IncludeManagementEvents": true,
            "DataResources": [
                {
                    "Values": [
                        "arn:aws:s3:::mybucket/prefix",
                        "arn:aws:s3:::mybucket2/prefix2",
                    ],
                    "Type": "AWS::S3::Object"
                }
            ],
            "ReadWriteType": "All"
        }
    ]
}
```

Registrando eventos de dados para armazenamentos de dados de eventos com o AWS CLI

É possível configurar seus armazenamentos de dados de eventos para incluir eventos de dados usando a AWS CLI. Use o comando `create-event-data-store` para criar um novo armazenamento de dados de eventos para registrar eventos de dados em log. Use o comando `update-event-data-store` para atualizar os seletores de eventos avançados para um armazenamento de dados de eventos existente.

Para verificar se o armazenamento de dados de eventos inclui eventos de dados, execute o comando `get-event-data-store`.

```
aws cloudtrail get-event-data-store --event-data-store EventDataStoreARN
```

O comando retorna as configurações do armazenamento de dados de eventos.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLE492-301f-4053-ac5e-EXAMPLE6441aa",
    "Name": "ebs-data-events",
    "Status": "ENABLED",
    "AdvancedEventSelectors": [
        {
            "Name": "Log all EBS direct APIs on EBS snapshots",
            "FieldSelectors": [
                {
```

```
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::EC2::Snapshot"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-04T15:57:33.701000+00:00",
    "UpdatedTimestamp": "2023-11-20T20:37:34.228000+00:00"
}
```

Tópicos

- Incluir todos os eventos do Amazon S3 para um bucket
- Incluir o Amazon S3 em eventos do AWS Outposts

Incluir todos os eventos do Amazon S3 para um bucket

O exemplo a seguir mostra como criar um armazenamento de dados de eventos para incluir todos os eventos de dados de todos os objetos do Amazon S3 em um bucket do S3 específico. O valor para eventos do S3 para o campo `resources.type` é `AWS::S3::Object`. Como os valores de ARN para objetos do S3 e buckets do S3 são ligeiramente diferentes, você deve adicionar o operador `StartsWith` para o `resources.ARN` para capturar todos os eventos.

```
aws cloudtrail create-event-data-store --name "EventDataStoreName" --multi-region-
enabled \
--advanced-event-selectors \
'[
    {
            "Name": "S3EventSelector",
```

```
            "FieldSelectors": [
                { "Field": "eventCategory", "Equals": ["Data"] },
                { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
                { "Field": "resources.ARN", "StartsWith":
 ["arn:partition:s3:::bucket_name/"] }
            ]
        }
]'
```

Este comando retorna a saída de exemplo a seguir.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLE492-301f-4053-ac5e-EXAMPLE441aa",
    "Name": "EventDataStoreName",
    "Status": "ENABLED",
    "AdvancedEventSelectors": [
        {
            "Name": "S3EventSelector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
                {
                    "Field": "resources.ARN",
                    "StartsWith": [
                        "arn:partition:s3:::bucket_name/"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3::Object"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
```

```
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-04T15:57:33.701000+00:00",
    "UpdatedTimestamp": "2023-11-20T20:49:21.766000+00:00"
}
```

Incluir o Amazon S3 em eventos do AWS Outposts

O exemplo a seguir mostra como criar um armazenamento de dados de eventos que inclua todos os eventos de dados para todos os objetos do Amazon S3 on Outposts em seu outpost.

```
aws cloudtrail create-event-data-store --name EventDataStoreName \
--advanced-event-selectors \
'[
    {
            "Name": "OutpostsEventSelector",
            "FieldSelectors": [
                { "Field": "eventCategory", "Equals": ["Data"] },
                { "Field": "resources.type", "Equals": ["AWS::S3Outposts::Object"] }
            ]
        }
]'
```

Este comando retorna a saída de exemplo a seguir.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEb4a8-99b1-4ec2-9258-EXAMPLEc890",
    "Name": "EventDataStoreName",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "OutpostsEventSelector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
                {
```

```
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3Outposts::Object"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-02-20T21:00:17.673000+00:00",
    "UpdatedTimestamp": "2023-02-20T21:00:17.820000+00:00"
}
```

Filtrando eventos de dados usando seletores de eventos avançados

Esta seção descreve como você pode usar seletores de eventos avançados para criar seletores refinados, que ajudam a controlar os custos registrando somente os eventos de dados específicos de interesse.

Por exemplo: .

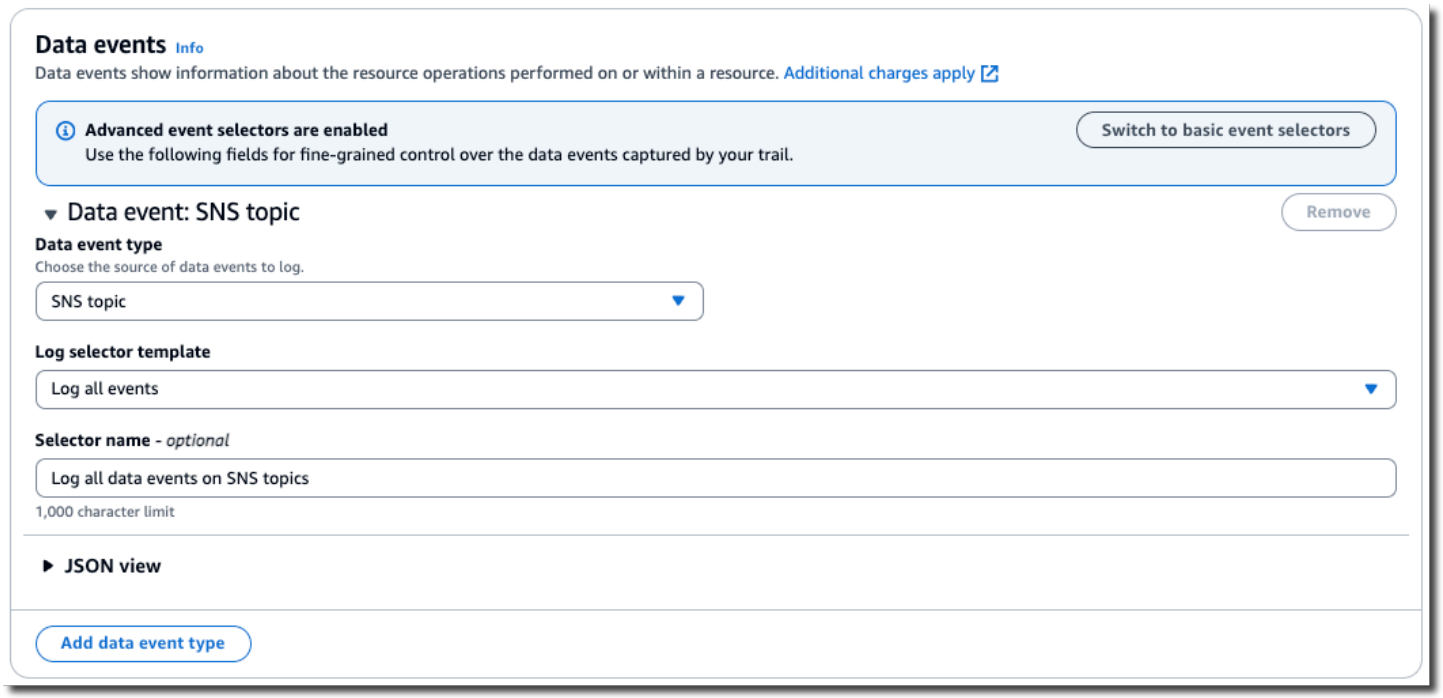
- Você pode incluir ou excluir chamadas de API específicas adicionando um filtro no `eventName` campo.
- Você pode incluir ou excluir o registro de recursos específicos adicionando um filtro no `resources.`ARN campo. Por exemplo, se você estivesse registrando eventos de dados do S3, poderia excluir o registro do bucket do S3 para sua trilha.
- Você pode optar por registrar somente eventos somente de gravação ou eventos somente de leitura adicionando um filtro no campo. `readOnly`

A tabela a seguir fornece informações adicionais sobre os campos configuráveis para seletores de eventos avançados.

Campo	Obrigatório	Operadores válidos	Descrição
eventCategory	Sim	`Equals`	Esse campo está definido `Data` para registrar eventos de dados.
resources.type	Sim	`Equals`	Esse campo é usado para selecionar o tipo de recurso para o qual você deseja registrar eventos de dados. A tabela de eventos de dados mostra os valores possíveis.
readOnly	Não	`Equals`	Esse é um campo opcional usado para incluir ou excluir eventos de dados com base no `readOnly` valor. Um valor de `true` registros só lê eventos. Um valor de `false` logs só grava eventos. Se você não adicionar esse campo, CloudTrail registrará os eventos de leitura e gravação.
eventName	Não	Any	Esse é um campo opcional usado para filtrar ou filtrar qualquer evento de dados registrado, como ou. CloudTrail `PutBucket GetSnapshotBlock` Se você estiver usando o AWS CLI, você pode especificar vários valores separando cada valor com uma vírgula. Se você estiver usando o console, poderá especificar vários valores criando uma condição para cada um `eventName` que você deseja filtrar.
resources.ARN	Não	Any	Esse é um campo opcional usado para excluir ou incluir eventos de dados para um recurso específico fornecendo `resources.ARN` o. Você pode usar qualquer operador com`resources.ARN` , mas se usar `Equals`

Campo	Obrigatório	Operadores válidos	Descrição
			ou`NotEquals` , o valor deve corresponder exatamente ao ARN de um recurso válido para o que `resoureces.type` você especificou. Se você estiver usando o AWS CLI, você pode especificar vários valores separando cada valor com uma vírgula. Se você estiver usando o console, poderá especificar vários valores criando uma condição para cada um `resources.ARN` que você deseja filtrar.

Para registrar eventos de dados usando o CloudTrail console, você escolhe a opção Eventos de dados e, em seguida, seleciona o tipo de evento de dados de interesse ao criar ou atualizar um armazenamento de dados de trilhas ou eventos. A tabela Eventos de dados mostra os possíveis tipos de eventos de dados que você pode escolher no CloudTrail console.



Para registrar eventos de dados com o AWS CLI, configure o `--advanced-event-selector` parâmetro para definir o valor `eventCategory` igual `Data` e igual ao `resources.type` valor do tipo de recurso para o qual você deseja registrar eventos de dados. A tabela de eventos de dados lista os tipos de recursos disponíveis.

Por exemplo, se você quisesse registrar eventos de dados para todos os pools de Identidade do Cognito, você configuraria o `--advanced-event-selectors` parâmetro para ter a seguinte aparência:

```
--advanced-event-selectors '[
    {
       "Name": "Log Cognito data events on Identity pools",
       "FieldSelectors": [
         { "Field": "eventCategory", "Equals": ["Data"] },
         { "Field": "resources.type", "Equals": ["AWS::Cognito::IdentityPool"] }
       ]
     }
]'
```

O exemplo anterior registra todos os eventos de dados do Cognito nos grupos de identidade. Você pode refinar ainda mais os seletores de eventos avançados para filtrar os `resources.`ARN campos `eventName``readOnly`,, e para registrar eventos específicos de interesse ou excluir eventos que não sejam de interesse.

Você pode configurar seletores de eventos avançados para filtrar eventos de dados com base em várias condições. Por exemplo, você pode configurar seletores de eventos avançados para registrar todas as chamadas do Amazon `PutObject` S3 `DeleteObject` e da API, mas excluir o registro de eventos para um bucket específico do S3, conforme mostrado no exemplo a seguir.

```
--advanced-event-selectors
'[
  {
    "Name": "Log PutObject and DeleteObject events for all but one bucket",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
      { "Field": "eventName", "Equals": ["PutObject","DeleteObject"] },
      { "Field": "resources.ARN", "NotStartsWith":
 ["arn:aws:s3:::sample_bucket_name/"] }
    ]
  }
```

```
]'
```

Você pode usar seletores de eventos avançados para registrar eventos de gerenciamento e dados. Para registrar eventos de dados para vários tipos de recursos, adicione uma instrução seletora de campo para cada tipo de recurso para o qual você deseja registrar eventos de dados.

> **Note**
>
> As trilhas podem usar seletores de eventos básicos ou seletores de eventos avançados, mas não ambos. Se você aplicar seletores de eventos avançados a uma trilha, todos os seletores de eventos básicos existentes serão substituídos.

Tópicos

Filtrando eventos de dados por **`eventName`**

Usando seletores de eventos avançados, você pode incluir ou excluir eventos com base no valor do `eventName` campo. A filtragem do `eventName` pode ajudar a controlar os custos, pois você evita incorrer em custos ao AWS service (Serviço da AWS) registrar eventos de dados para adicionar suporte a novas APIs de dados.

Você pode usar qualquer operador com o `eventName` campo. Você pode usá-lo para filtrar ou filtrar qualquer evento de dados registrado, como ou. CloudTrail `PutBucket` `GetSnapshotBlock`

Tópicos

Filtrando eventos de dados **`eventName`** usando o AWS Management Console

Siga as etapas a seguir para filtrar no `eventName` campo usando o CloudTrail console.

1. Siga as etapas do procedimento de criação de trilha ou siga as etapas do procedimento de criação de armazenamento de dados de eventos.
2. Ao seguir as etapas para criar o armazenamento de dados da trilha ou do evento, faça as seguintes seleções:

   a. Escolha Eventos de dados.

   b. Escolha o tipo de evento de dados para o qual você deseja registrar eventos de dados.

   c. Em Modelo de seletor de registros, escolha Personalizado.

   d. (Opcional) Em Nome do seletor, insira um nome para identificar o seletor. O nome do seletor é um nome descritivo para um seletor de eventos avançado, como "Registrar eventos de dados em log para apenas dois buckets do S3". O nome do seletor é listado como `Name` no seletor de eventos avançado e poderá ser visualizado se você expandir a visualização JSON.

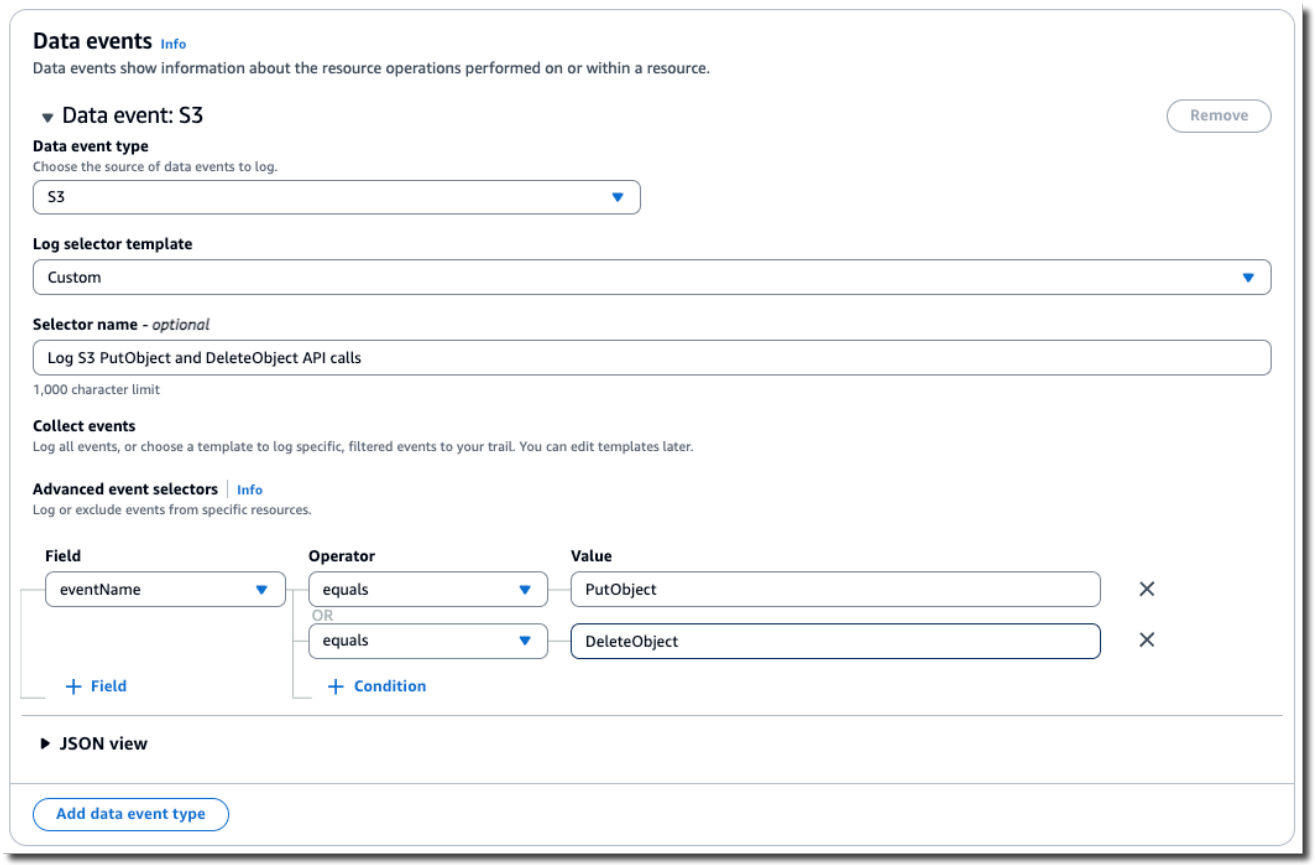
   e. Em Seletores de eventos avançados, faça o seguinte para filtrar o`eventName`:

      i. Em Field, escolha eventName.

      ii. Em Operador, escolha o operador de condição. Neste exemplo, escolheremos equals porque queremos registrar uma chamada de API específica.

      iii. Em Valor, insira o nome do evento que você deseja filtrar.

      iv. Para filtrar por outro`eventName`, escolha + Condição.



f. Escolha +Campo para adicionar filtros em outros campos.

Filtrando eventos de dados **`eventName`** usando o AWS CLI

Usando o AWS CLI, você pode filtrar no `eventName` campo para incluir ou excluir eventos específicos.

O exemplo a seguir registra eventos de dados do S3 em uma trilha. Eles `--advanced-event-selectors` são configurados para registrar somente eventos de dados para as chamadas de `DeleteObject` API `GetObjectPutObject`, e.

```
aws cloudtrail put-event-selectors \
--trail-name trailName \
--advanced-event-selectors '[
  {
    "Name": "Log GetObject, PutObject and DeleteObject S3 data events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
```

```
      { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
      { "Field": "eventName", "Equals": ["GetObject","PutObject","DeleteObject"] }
    ]
  }
]'
```

O próximo exemplo cria um novo armazenamento de dados de eventos que registra eventos de dados para as APIs do EBS Direct, mas exclui `ListChangedBlocks` as chamadas de API. Você pode usar o update-event-data-storecomando para atualizar um armazenamento de dados de eventos existente.

```
aws cloudtrail create-event-data-store \
--name "eventDataStoreName"
--advanced-event-selectors '[
    {
        "Name": "Log all EBS Direct API data events except ListChangedBlocks",
        "FieldSelectors": [
            { "Field": "eventCategory", "Equals": ["Data"] },
            { "Field": "resources.type", "Equals": ["AWS::EC2::Snapshot"] },
            { "Field": "eventName", "NotEquals": ["ListChangedBlocks"] }
         ]
    }
]'
```

Filtrando eventos de dados por **`resources.ARN`**

Usando seletores de eventos avançados, você pode filtrar o valor do `resources.ARN` campo.

Você pode usar qualquer operador com`resources.ARN`, mas se usar `Equals` ou`NotEquals`, o valor deve corresponder exatamente ao ARN de um recurso válido para o `resources.type` valor que você especificou. Para registrar todos os eventos de dados de todos os objetos do em um bucket do S3 específico, use a propriedade `StartsWith` e inclua apenas o ARN do bucket como o valor correspondente.

A tabela a seguir mostra o formato de ARN válido para cada `resources.type`.

> **Note**
>
> Você não pode usar o `resources.ARN` campo para filtrar tipos de recursos que não tenham ARNs.

resources.type	resources.ARN
AWS::DynamoDB::Table [1]	arn:*partition* :dynamodb : *region*:*account_ID* :table/*table_name*
AWS::Lambda::Function	arn:*partition* :lambda:*region*:*account_ID* :function: *function_name*
AWS::S3::Object [2]	arn:*partition* :s3:::*bucket_name* / arn:*partition* :s3:::*bucket_name* /*object_or_file_name* /
AWS::AppConfig::Configuration	arn:*partition* :appconfig: *region*:*account_ID* :application/ *application_ID* /environment/ *environment_ID* /configuration/ *configuration_profile_ID*
AWS::B2BI::Transformer	arn:*partition* :b2bi:*region*:*account_ID* :transformer/ *transformer_ID*
AWS::Bedrock::AgentAlias	arn:*partition* :bedrock: *region*:*account_ID* :agent-alias/ *agent_ID*/*alias_ID*
AWS::Bedrock::KnowledgeBase	arn:*partition* :bedrock: *region*:*account_ID* :knowledge-base/*knowledge_base_ID*
AWS::Cassandra::Table	arn:*partition* :cassandra: *region*:*account_ID* :keyspace/ *keyspace_name* /table/*table_name*

resources.type	resources.ARN
AWS::CloudFront::KeyValueStore	arn:*partition* :cloudfront: *region*:*account_ID* :key-value-store/*KVS_name*
AWS::CloudTrail::Channel	arn:*partition* :cloudtrail: *region*:*account_ID* :channel/ *channel_UUID*
AWS::CodeWhisperer::Customization	arn:*partition* :codewhisperer: *region*:*account_ID* :customization/ *customization_ID*
AWS::CodeWhisperer::Profile	arn:*partition* :codewhisperer: *region*:*account_ID* :profile/ *profile_ID*
AWS::Cognito::IdentityPool	arn:*partition* :cognito-identity: *region*:*account_ID* :identitypool/ *identity_pool_ID*
AWS::DynamoDB::Stream	arn:*partition* :dynamodb: *region*:*account_ID* :table/*table_name* /stream/*date_time*
AWS::EC2::Snapshot	arn:*partition* :ec2:*region*::snapshot/ *snapshot_ID*
AWS::EMRWAL::Workspace	arn:*partition* :emrwal:*region*:*account_ID* :workspace/ *workspace_name*

resources.type	resources.ARN
AWS::FinSpace::Environment	arn:*partition* :finspace : *region*:*account_ID* :environment/ *environment_ID*
AWS::Glue::Table	arn:*partition* :glue:*region*:*account_ID* :table/*database_name* /*table_name*
AWS::GreengrassV2::ComponentVersion	arn:*partition* :greengrass: *region*:*account_ID* :components/ *component_name*
AWS::GreengrassV2::Deployment	arn:*partition* :greengrass: *region*:*account_ID* :deployments/ *deployment_ID*
AWS::GuardDuty::Detector	arn:*partition* :guardduty: *region*:*account_ID* :detector/ *detector_ID*
AWS::IoT::Certificate	arn:*partition* :iot:*region*:*account_ID* :cert/*certificate_ID*
AWS::IoT::Thing	arn:*partition* :iot:*region*:*account_ID* :thing/*thing_ID*
AWS::IoTSiteWise::Asset	arn:*partition* :iotsitewise: *region*:*account_ID* :asset/*asset_ID*
AWS::IoTSiteWise::TimeSeries	arn:*partition* :iotsitewise: *region*:*account_ID* :timeseries/ *timeseries_ID*

resources.type	resources.ARN
AWS::IoTTwinMaker::Entity	arn:*partition* :iottwinmaker: *region*:*account_ID* :workspace/ *workspace_ID* /entity/*entity_ID*
AWS::IoTTwinMaker::Workspace	arn:*partition* :iottwinmaker: *region*:*account_ID* :workspace/ *workspace_ID*
AWS::KendraRanking::ExecutionPlan	arn:*partition* :kendra-ranking: *region*:*account_ID* :rescore-execution-plan/ *rescore_execution_plan_ID*
AWS::Kinesis::Stream	arn:*partition* :kinesis: *region*:*account_ID* :stream/*stream_name*
AWS::Kinesis::StreamConsumer	arn:*partition* :kinesis: *region*:*account_ID* :*stream_type* /*stream_name* /consumer/ *consumer_name* :*consumer_creation_timestamp*
AWS::KinesisVideo::Stream	arn:*partition* :kinesisvideo: *region*:*account_ID* :stream/*stream_name* /*creation_time*
AWS::ManagedBlockchain::Network	arn:*partition* :managedblockchain:::networks/ *network_name*
AWS::ManagedBlockchain::Node	arn:*partition* :managedblockchain: *region*:*account_ID* :nodes/*node_ID*

resources.type	resources.ARN
AWS::MedicalImaging::Datastore	arn:*partition* :medical-imaging: *region*:*account_ID* :datastore/ *data_store_ID*
AWS::NeptuneGraph::Graph	arn:*partition* :neptune-graph: *region*:*account_ID* :graph/*graph_ID*
AWS::PCAConnectorAD::Connector	arn:*partition* :pca-connector-ad: *region*:*account_ID* :connector/ *connector_ID*
AWS::QApps:QApp	arn:*partition* :qapps:*region*:*account_ID* :application/ *application_UUID* / qapp/*qapp_UUID*
AWS::QBusiness::Application	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID*
AWS::QBusiness::DataSource	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID* /index/*index_ID*/data-source/ *datasource_ID*
AWS::QBusiness::Index	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID* /index/*index_ID*
AWS::QBusiness::WebExperience	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID* /web-experience/ *web_experienc_ID*

resources.type	resources.ARN
AWS::RDS::DBCluster	arn:*partition* :rds:*region*:*account_ID* :cluster/ *cluster_name*
AWS::S3::AccessPoint [3]	arn:*partition* :s3:*region*:*account_ID* :accesspoint/ *access_point_name*
AWS::S3ObjectLambda::AccessPoint	arn:*partition* :s3-object-lambda: *region*:*account_ID* :accesspoint/ *access_point_name*
AWS::S3Outposts::Object	arn:*partition* :s3-outposts: *region*:*account_ID* :*object_path*
AWS::SageMaker::Endpoint	arn:*partition* :sagemaker: *region*:*account_ID* :endpoint/ *endpoint_name*
AWS::SageMaker::ExperimentTrialComponent	arn:*partition* :sagemaker: *region*:*account_ID* :experiment-trial-component/ *experiment_trial_component_name*
AWS::SageMaker::FeatureGroup	arn:*partition* :sagemaker: *region*:*account_ID* :feature-group/ *feature_group_name*
AWS::SCN::Instance	arn:*partition* :scn:*region*:*account_ID* :instance/ *instance_ID*
AWS::ServiceDiscovery::Namespace	arn:*partition* :servicediscovery: *region*:*account_ID* :namespace/ *namespace_ID*

resources.type	resources.ARN
AWS::ServiceDiscovery::Service	arn:*partition* :servicediscovery: *region*:*account_ID* :service/ *service_ID*
AWS::SNS::PlatformEndpoint	arn:*partition* :sns:*region*:*account_ID* :endpoint/ *endpoint_type* /*endpoint_name* /*endpoint_ID*
AWS::SNS::Topic	arn:*partition* :sns:*region*:*account_ID* :*topic_name*
AWS::SQS::Queue	arn:*partition* :sqs:*region*:*account_ID* :*queue_name*
AWS::SSM::ManagedNode	O ARN deve estar em um dos seguintes formatos: • arn:*partition* :ssm:*region*:*account_ID* :managed-instance/ *instance_ID* • arn:*partition* :ec2:*region*:*account_ID* :instance/ *instance_ID*
AWS::SSMMessages::ControlChannel	arn:*partition* :ssmmessages: *region*:*account_ID* :control-channel/ *control_channel_ID*

resources.type	resources.ARN
AWS::StepFunctions::StateMachine	O ARN deve estar em um dos seguintes formatos: • arn:*partition* :states:*region*:*account_ID* :stateMachine: *stateMachine_name* • arn:*partition* :states:*region*:*account_ID* :stateMachine: *stateMachine_name* /*label_name*
AWS::SWF::Domain	arn:*partition* :swf:*region*:*account_ID* :/domain/ *domain_name*
AWS::ThinClient::Device	arn:*partition* :thinclient: *region*:*account_ID* :device/*device_ID*
AWS::ThinClient::Environment	arn:*partition* :thinclient: *region*:*account_ID* :environment/ *environment_ID*
AWS::Timestream::Database	arn:*partition* :timestream: *region*:*account_ID* :database/ *database_name*
AWS::Timestream::Table	arn:*partition* :timestream: *region*:*account_ID* :database/ *database_name* /table/*table_name*

resources.type	resources.ARN
`AWS::VerifiedPermissions::PolicyStore`	`arn:partition :verifiedpermissions: region:account_ID :policy-store/ policy_store_ID`

[1] Para tabelas com fluxos habilitados, o campo `resources` no evento de dados contém `AWS::DynamoDB::Stream` e `AWS::DynamoDB::Table`. Se você especificar `AWS::DynamoDB::Table` como `resources.type`, ele registrará os eventos da tabela do DynamoDB e dos fluxos do DynamoDB por padrão. Para excluir eventos de streams, adicione um filtro no `eventName` campo.

[2] Para registrar em log todos os eventos de dados de todos os objetos em um bucket do S3 específico, use o operador `StartsWith` e inclua apenas o ARN do bucket como o valor correspondente. A barra final é intencional; não a exclua.

[3] Para registrar em log eventos de todos os objetos em um ponto de acesso do S3, recomendamos usar somente o ARN do ponto de acesso, não incluir o caminho do objeto e usar os operadores `StartsWith` ou `NotStartsWith`.

Tópicos

- Filtrando eventos de dados resources.ARN usando o AWS Management Console
- Filtrando eventos de dados resources.ARN usando o AWS CLI

Filtrando eventos de dados **`resources.ARN`** usando o AWS Management Console

Siga as etapas a seguir para filtrar no `resources.ARN` campo usando o CloudTrail console.

1. Siga as etapas do procedimento de criação de trilha ou siga as etapas do procedimento de criação de armazenamento de dados de eventos.
2. Ao seguir as etapas para criar o armazenamento de dados da trilha ou do evento, faça as seguintes seleções:
   a. Escolha Eventos de dados.
   b. Escolha o tipo de evento de dados para o qual você deseja registrar eventos de dados.
   c. Em Modelo de seletor de registros, escolha Personalizado.

d. (Opcional) Em Nome do seletor, insira um nome para identificar o seletor. O nome do seletor é um nome descritivo para um seletor de eventos avançado, como "Registrar eventos de dados em log para apenas dois buckets do S3". O nome do seletor é listado como `Name` no seletor de eventos avançado e poderá ser visualizado se você expandir a visualização JSON.

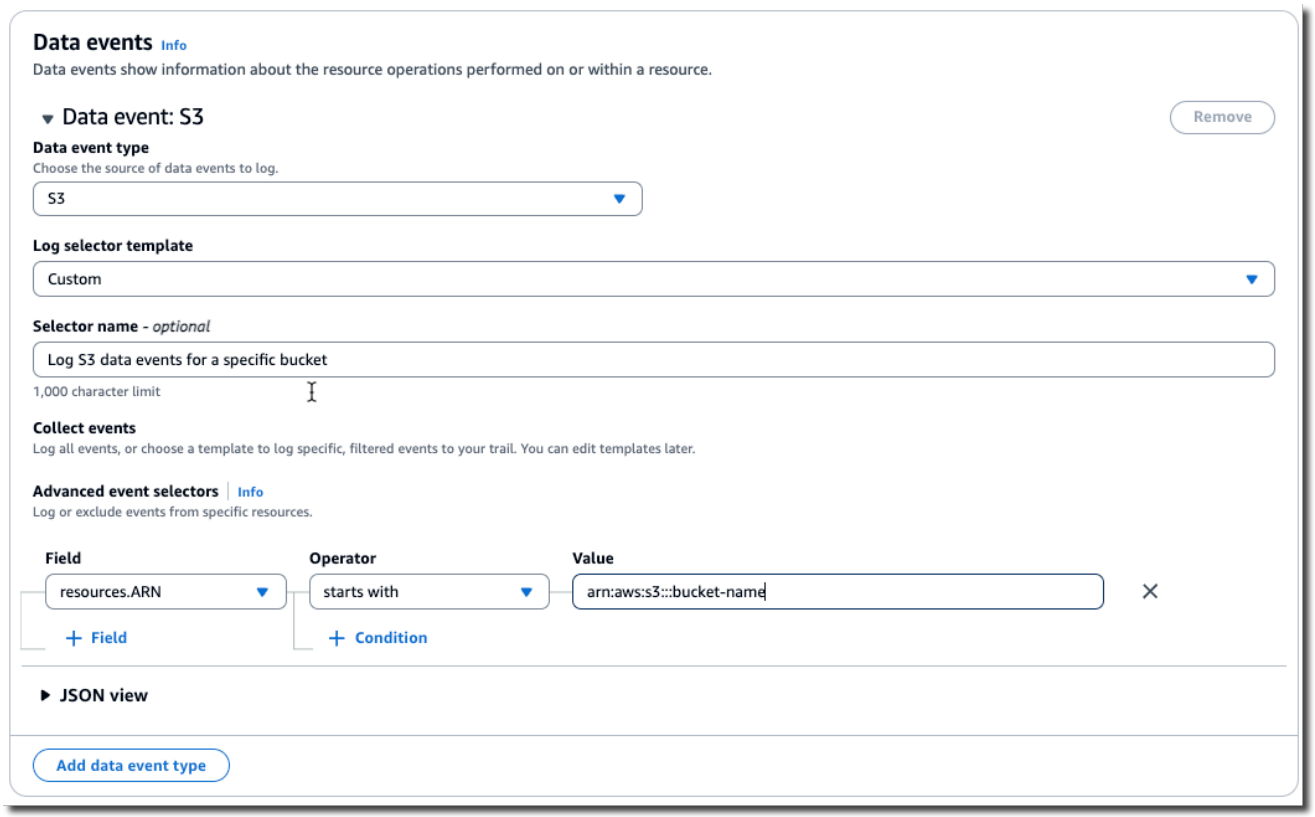
e. Em Seletores de eventos avançados, faça o seguinte para filtrar `oresources.`ARN:

   i. Em Campo, escolha resources.ARN.

   ii. Em Operador, escolha o operador de condição. Neste exemplo, escolheremos start with porque queremos registrar eventos de dados para um bucket S3 específico.

   iii. Em Valor, insira o ARN do seu tipo de recurso (por exemplo, *`arn:aws:s3: ::bucket-name`*).

   iv. Para filtrar outro`resources.`ARN, escolha + Condição.



f. Escolha +Campo para adicionar filtros em outros campos.

Filtrando eventos de dados **`resources.ARN`** usando o AWS CLI

Usando o AWS CLI, você pode filtrar no `resources.ARN` campo para registrar eventos para um ARN específico ou excluir o registro para um ARN específico.

O exemplo a seguir mostra como configurar a trilha para registrar eventos de dados de todos os objetos do Amazon S3 em um bucket do S3. O valor para eventos do S3 para o campo `resources.type` é `AWS::S3::Object`. Como os valores de ARN para objetos do S3 e buckets do S3 são ligeiramente diferentes, você deve adicionar o operador `StartsWith` para o `resources.ARN` para capturar todos os eventos.

```
aws cloudtrail put-event-selectors \
--trail-name TrailName \
--region region \
--advanced-event-selectors \
'[
    {
        "Name": "S3EventSelector",
        "FieldSelectors": [
            { "Field": "eventCategory", "Equals": ["Data"] },
                { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
                { "Field": "resources.ARN", "StartsWith":
 ["arn:aws:s3:::bucket_name/"] }
            ]
    }
]'
```

Filtrando eventos de dados por valor **`readOnly`**

Usando seletores de eventos avançados, você pode filtrar com base no valor do `readOnly` campo.

Você só pode usar o `Equals` operador com o `readOnly` campo. Você pode definir o `readOnly` valor como `true` ou`false`. Se você não adicionar esse campo, CloudTrail registrará os eventos de leitura e gravação. Um valor de `true` registros só lê eventos. Um valor de `false` logs só grava eventos.

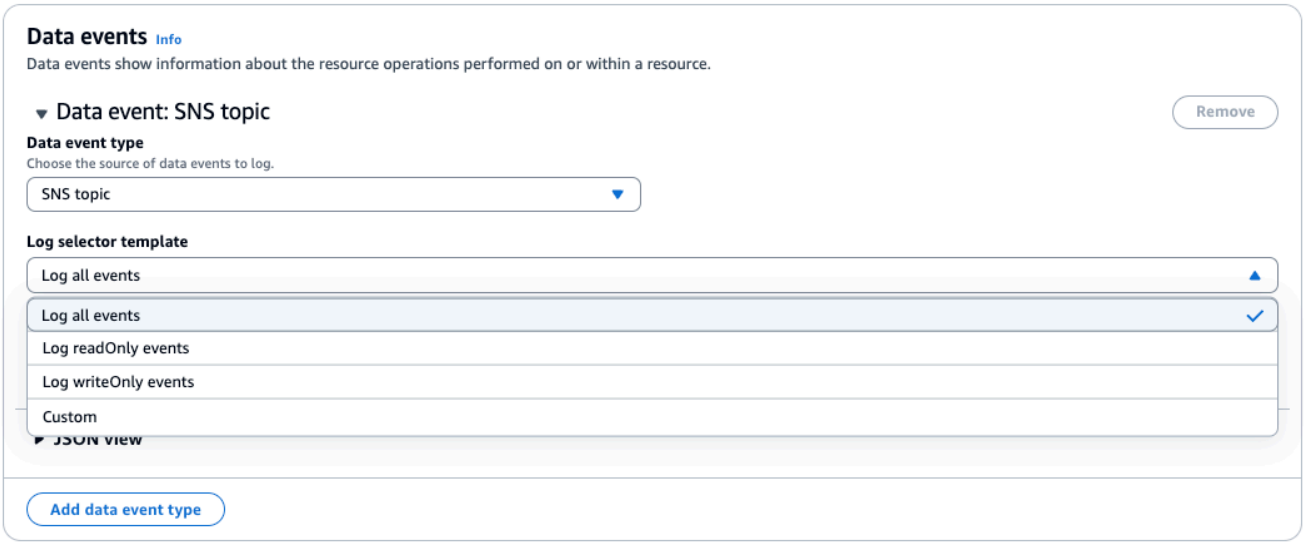
Tópicos

- Filtrando eventos de dados por readOnly valor usando o AWS Management Console
- Filtrando eventos de dados por readOnly valor usando o AWS CLI

Filtrando eventos de dados por **`readOnly`** valor usando o AWS Management Console

Siga as etapas a seguir para filtrar no `readOnly` campo usando o CloudTrail console.

1. Siga as etapas do procedimento de criação de trilha ou siga as etapas do procedimento de criação de armazenamento de dados de eventos.
2. Ao seguir as etapas para criar o armazenamento de dados da trilha ou do evento, faça as seguintes seleções:
   a. Escolha Eventos de dados.
   b. Escolha o tipo de evento de dados para o qual você deseja registrar eventos de dados.
   c. Para Modelo de seletor de registros, escolha o modelo apropriado para seu caso de uso.



Se você planeja fazer isso	Escolha esse modelo de seletor de registros
Registre somente eventos de leitura e não aplique outros filtros (por exemplo, no `resources.ARN` valor).	Registrar eventos ReadOnly
Registre somente eventos de gravação e não aplique outros filtros (por exemplo, no `resources.ARN` valor).	Registrar eventos WriteOnly

Se você planeja fazer isso	Escolha esse modelo de seletor de registros
Filtre o `readOnly` valor e aplique filtros adicionais (por exemplo, no `resources.ARN` valor).	Custom (Personalizado) Em Seletores de eventos avançados, faça o seguinte para filtrar o `readOnly` valor: Para registrar eventos de gravação a. Em Campo, escolha readOnly. b. Em Operador, escolha equals. c. Em Valor, insira **`false`**. d. Escolha +Campo para adicionar filtros em outros campos. Para registrar eventos de leitura a. Em Campo, escolha readOnly. b. Em Operador, escolha equals. c. Em Valor, insira **`true`**. d. Escolha +Campo para adicionar filtros em outros campos.

Filtrando eventos de dados por **`readOnly`** valor usando o AWS CLI

Usando o AWS CLI, você pode filtrar no `readOnly` campo.

Você só pode usar o `Equals` operador com o `readOnly` campo. Você pode definir o `readOnly` valor como `true` ou`false`. Se você não adicionar esse campo, CloudTrail registrará os eventos de leitura e gravação. Um valor de `true` registros só lê eventos. Um valor de `false` logs só grava eventos.

O exemplo a seguir mostra como configurar sua trilha para registrar eventos de dados somente para leitura para todos os objetos do Amazon S3.

```
aws cloudtrail put-event-selectors \
```

```
--trail-name TrailName \
--region region \
--advanced-event-selectors '[
    {
            "Name": "Log read-only S3 data events",
            "FieldSelectors": [
                { "Field": "eventCategory", "Equals": ["Data"] },
                { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
                { "Field": "readOnly", "Equals": ["true"] }
            ]
    }
]'
```

O próximo exemplo cria um novo armazenamento de dados de eventos que registra somente eventos de dados somente de gravação para as APIs do EBS Direct. Você pode usar o update-event-data-storecomando para atualizar um armazenamento de dados de eventos existente.

```
aws cloudtrail create-event-data-store \
--name "eventDataStoreName" \
--advanced-event-selectors \
'[
    {
            "Name": "Log write-only EBS Direct API data events",
            "FieldSelectors": [
                { "Field": "eventCategory", "Equals": ["Data"] },
                { "Field": "resources.type", "Equals": ["AWS::EC2::Snapshot"] },
                { "Field": "readOnly", "Equals": ["false"] }
            ]
     }
]'
```

Registrar de eventos de dados para conformidade de AWS Config

Se você estiver usando pacotes de AWS Config conformidade para ajudar sua empresa a manter a conformidade com padrões formalizados, como os exigidos pelo Programa Federal de Gerenciamento de Riscos e Autorizações (FedRAMP) ou pelo Instituto Nacional de Padrões e Tecnologia (NIST), os pacotes de conformidade para estruturas de conformidade geralmente exigem que você registre eventos de dados para buckets do Amazon S3, no mínimo. Os pacotes de conformidade para estruturas de conformidade incluem umaregra gerenciada chamada `cloudtrail-s3-dataevents-enabled` que verifica o registro de eventos de dados do S3 em sua conta. Muitos pacotes de conformidade que não estão associados a estruturas de conformidade

também exigem log de eventos de dados do S3. Veja a seguir exemplos de pacotes de conformidade que incluem essa regra.

- Melhores práticas operacionais para o pilar de segurança do AWS Well-Architected Framework
- Operational Best Practices for FDA Title 21 CFR Part 11
- Práticas recomendadas operacionais para o FFIEC
- Práticas recomendadas operacionais para o FedRAMP (Moderado)
- Práticas recomendadas operacionais para a segurança da HIPAA
- Práticas recomendadas operacionais para o K-ISMS
- Práticas recomendadas operacionais para o Registro

Para obter uma lista completa dos exemplos de pacotes de conformidade disponíveis em AWS Config, consulte Modelos de amostra de pacotes de conformidade no Guia do desenvolvedor.AWS Config

Registrando eventos de dados com os AWS SDKs

Execute a GetEventSelectorsoperação para ver se sua trilha está registrando eventos de dados. Você pode configurar suas trilhas para registrar eventos de dados executando a PutEventSelectorsoperação. Para obter mais informações, consulte a AWS CloudTrail Referência da API do .

Execute a GetEventDataStoreoperação para ver se seu armazenamento de dados de eventos está registrando eventos de dados. Você pode configurar seus armazenamentos de dados de eventos para incluir eventos de dados executando as UpdateEventDataStoreoperações CreateEventDataStoreou e especificando seletores de eventos avançados. Para obter mais informações, consulte a Crie, atualize e gerencie armazenamentos de dados de eventos com o AWS CLI e a Referência da API do AWS CloudTrail.

Envio de eventos para o Amazon CloudWatch Logs

CloudTrail suporta o envio de eventos de dados para o CloudWatch Logs. Quando você configura sua trilha para enviar eventos ao seu grupo de CloudWatch registros de registros, CloudTrail envia somente os eventos que você especifica em sua trilha. Por exemplo, se você configurar sua trilha para registrar somente eventos de dados, ela entregará eventos de dados somente ao seu grupo de CloudWatch registros de registros. Para ter mais informações, consulte Monitoramento CloudTrail de arquivos de log com o Amazon CloudWatch Logs.

Registrar eventos do Insights

AWS CloudTrail O Insights ajuda AWS os usuários a identificar e responder a atividades incomuns associadas a chamadas de API e taxas de erro de API, analisando continuamente os eventos CloudTrail de gerenciamento. CloudTrail O Insights analisa seus padrões normais de volume de chamadas de API e taxas de erro de API, também chamados de linha de base, e gera eventos do Insights quando o volume de chamadas ou as taxas de erro estão fora dos padrões normais. Eventos de insights no volume de chamadas de API são gerados para `write` APIs de gerenciamento e eventos do Insights na taxa de erros da API são gerados para ambos`read` e `write` APIs de gerenciamento.

> **Note**
>
> Para registrar em log eventos do Insights sobre o volume de chamadas à API, a trilha ou o armazenamento de dados de eventos deve registrar em log os eventos de gerenciamento de `write`. Para registrar em log eventos do Insights sobre a taxa de erros da API, a trilha ou o armazenamento de dados de eventos deve registrar em log os eventos de gerenciamento de `read` ou `write`.

CloudTrail O Insights analisa eventos de gerenciamento que ocorrem em uma única região, não globalmente. Um evento do CloudTrail Insights é gerado na mesma região em que seus eventos de gerenciamento de apoio são gerados.

Cobranças adicionais são aplicáveis aos eventos do Insights. Você será cobrado separadamente se ativar o Insights tanto para trilhas quanto para armazenamentos de dados de eventos. Para obter mais informações, consulte Preços do AWS CloudTrail.

Sumário

Entender a entrega de eventos do Insights

Ao contrário de outros tipos de eventos que CloudTrail capturam, os eventos do Insights são registrados somente quando CloudTrail detectam alterações no uso da API da sua conta que diferem significativamente dos padrões de uso típicos da conta.

CloudTrail O local de entrega dos eventos e o tempo necessário para receber os eventos do Insights diferem entre trilhas e armazenamentos de dados de eventos.

Entrega de eventos do Insights para trilhas

Se você ativou eventos do Insights em uma trilha e CloudTrail detectou atividades incomuns, CloudTrail entrega os eventos do Insights na `/CloudTrail-Insight` pasta no bucket S3 de destino escolhido para sua trilha. Depois de ativar o CloudTrail Insights pela primeira vez em uma trilha, pode levar até 36 horas CloudTrail para entregar o primeiro evento do Insights, se uma atividade incomum for detectada.

Se você desativar o registro de eventos do Insights em uma trilha e depois reativar os eventos do Insights, ou parar e reiniciar o registro em uma trilha, pode levar até 36 horas CloudTrail para reiniciar a entrega dos eventos do Insights, se uma atividade incomum for detectada.

Entrega de eventos do Insights para armazenamentos de dados de eventos

Se você habilitou os eventos do Insights em um armazenamento de dados de eventos de origem, CloudTrail entrega os eventos do Insights para o armazenamento de dados do evento de destino. Depois de ativar o CloudTrail Insights pela primeira vez no armazenamento de dados do evento de origem, pode levar até 7 dias CloudTrail para entregar o primeiro evento do Insights ao armazenamento de dados do evento de destino, se uma atividade incomum for detectada.

Se você desativar o registro de eventos do Insights em um armazenamento de dados de eventos de origem e, em seguida, reativar os eventos do Insights ou interromper e reiniciar a ingestão de eventos em um armazenamento de dados de eventos de origem, pode levar até 7 dias CloudTrail para reiniciar a entrega dos eventos do Insights, caso uma atividade incomum seja detectada. Cobranças adicionais se aplicam à ingestão de eventos do Insights em CloudTrail Lake. Você será cobrado separadamente se ativar o Insights tanto para trilhas quanto para armazenamentos de dados de eventos. Para obter informações sobre CloudTrail preços, consulte AWS CloudTrail Preços.

Registrando eventos do Insights com o AWS Management Console

É possível habilitar eventos do Insights em uma trilha ou em um armazenamento de dados de eventos usando o console.

Tópicos

Habilitando eventos do CloudTrail Insights em uma trilha existente

Use o procedimento a seguir para ativar eventos do CloudTrail Insights em uma trilha existente. Por padrão, os eventos do Insights não estão habilitados.

1. No painel de navegação esquerdo do CloudTrail console, abra a página Trilhas e escolha o nome de uma trilha.
2. Em Insights events (Eventos do Insights), escolha Edit (Editar).

> **Note**
>
> Há cobranças adicionais para o registro em log de eventos do Insights. Para CloudTrail saber os preços, consulte AWS CloudTrail Preços.

3. Em Event type (Tipo de evento), selecione Insights events (Eventos do Insights).
4. Em Insights events (Eventos do Insights), em Choose Insights types (Escolha tipos do Insights), escolha API call rate (Taxa de chamada da API), API error rate (Taxa de erro da API) ou ambos. Sua trilha deve registrar em log eventos de gerenciamento de gravação para registrar em log eventos do Insights sobre a taxa de chamadas à API. Sua trilha deve registrar em log eventos de gerenciamento de leitura ou de gravação para registrar em log eventos do Insights sobre a taxa de erros da API.
5. Escolha Salvar alterações para salvar suas alterações.

Pode levar até 36 horas CloudTrail para entregar os primeiros eventos do Insights, se uma atividade incomum for detectada.

Habilitando eventos do CloudTrail Insights em um armazenamento de dados de eventos existente

Use o procedimento a seguir para habilitar eventos do CloudTrail Insights em um armazenamento de dados de eventos existente. Por padrão, os eventos do Insights não estão habilitados.

Cobranças adicionais se aplicam à ingestão de eventos do Insights em CloudTrail Lake. Você será cobrado separadamente se ativar o Insights tanto para trilhas quanto para armazenamentos de dados de eventos. Para obter informações sobre CloudTrail preços, consulte AWS CloudTrail Preços.

> **Note**
>
> Você só pode habilitar eventos do CloudTrail Insights em armazenamentos de dados de eventos contendo eventos CloudTrail de gerenciamento. Você não pode habilitar eventos do CloudTrail Insights em outros tipos de armazenamento de dados de eventos.

1. No painel de navegação esquerdo do CloudTrail console, em Lake, escolha Armazenamentos de dados de eventos.
2. Escolha o nome do armazenamento de dados de eventos.
3. Em Eventos de gerenciamento, escolha Editar.
4. Escolha Habilitar Insights.
5. Escolha o armazenamento de dados do evento de destino onde CloudTrail entregará os eventos do Insights. O armazenamento de dados de eventos de destino coletará eventos do Insights com

base na atividade de gerenciamento de eventos nesse armazenamento de dados de eventos. Para obter informações sobre como criar o armazenamento de dados de eventos de destino, consulte Para criar um armazenamento de dados de eventos de destino que registra eventos do Insights.

6. Em Escolher tipos de Insights, escolha Taxa de chamadas à API, Taxa de erros da API ou ambas. Seu armazenamento de dados de eventos deve registrar em log eventos de gerenciamento de gravação para registrar em log eventos do Insights sobre a taxa de chamadas à API. O armazenamento de dados de eventos deve registrar em log eventos de gerenciamento de leitura ou de gravação para registrar em log eventos do Insights sobre a taxa de erros da API.
7. Escolha Salvar alterações para salvar suas alterações.

Pode levar até 7 dias CloudTrail para entregar os primeiros eventos do Insights, se uma atividade incomum for detectada.

Registrando eventos do Insights com o AWS Command Line Interface

É possível configurar suas trilhas e seus armazenamentos de dados de eventos para registrar eventos do Insights em log usando a AWS CLI.

> **Note**
>
> Para registrar em log eventos do Insights sobre o volume de chamadas à API, a trilha ou o armazenamento de dados de eventos deve registrar em log os eventos de gerenciamento de `write`. Para registrar em log eventos do Insights sobre a taxa de erros da API, a trilha ou o armazenamento de dados de eventos deve registrar em log os eventos de gerenciamento de `read` ou `write`.

Tópicos

- Registrando eventos do Insights para uma trilha usando o AWS CLI
- Registrando eventos do Insights para um armazenamento de dados de eventos usando o AWS CLI

Registrando eventos do Insights para uma trilha usando o AWS CLI

Para visualizar se a trilha está registrando em log os eventos do Insights, execute o comando `get-insight-selectors`.

```
aws cloudtrail get-insight-selectors --trail-name TrailName
```

O resultado a seguir mostra as configurações padrão para uma trilha. Por padrão, as trilhas não registram em log eventos do Insights. O valor do atributo `InsightType` está vazio, e nenhum seletor de eventos do Insight é especificado, pois a coleção de eventos do Insights não está ativada.

Se você não adicionar seletores do Insights, o get-insight-selectors comando retornará a seguinte mensagem de erro: “Ocorreu um erro (InsightNotEnabledException) ao chamar a GetInsightSelectors operação: O *nome* da trilha não tem o Insights ativado. Edite as configurações da trilha para habilitar o Insights e tente a operação novamente.”

```
{
  "InsightSelectors": [ ],
  "TrailARN": "arn:aws:cloudtrail:us-east-1:123456789012:trail/TrailName"
}
```

Para configurar a trilha para registrar em log eventos do Insights, execute o comando `put-insight-selectors`. O exemplo a seguir mostra como configurar a trilha para incluir eventos do Insights. Os valores do seletor Insights podem ser `ApiCallRateInsight`, `ApiErrorRateInsight` ou ambos.

```
aws cloudtrail put-insight-selectors --trail-name TrailName --insight-selectors
 '[{"InsightType": "ApiCallRateInsight"},{"InsightType": "ApiErrorRateInsight"}]'
```

O resultado a seguir mostra o seletor de eventos do Insights que está configurado para a trilha.

```
{
  "InsightSelectors":
      [
         {
            "InsightType": "ApiErrorRateInsight"
         },
         {
            "InsightType": "ApiCallRateInsight"
         }
```

```
      ],
  "TrailARN": "arn:aws:cloudtrail:us-east-1:123456789012:trail/TrailName"
}
```

Registrando eventos do Insights para um armazenamento de dados de eventos usando o AWS CLI

Para habilitar o Insights em um armazenamento de dados de eventos, é necessário ter um armazenamento de dados de eventos de origem que registre eventos de gerenciamento e um armazenamento de dados de eventos de destino que registre eventos do Insights.

Para ver se os eventos do Insights estão habilitados em um armazenamento de dados de eventos, execute o comando get-insight-selectors.

```
aws cloudtrail get-insight-selectors --event-data-store arn:aws:cloudtrail:us-
east-1:123456789012:eventdatastore/EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
```

Para ver se um armazenamento de dados de eventos está configurado para receber eventos do Insights ou eventos de gerenciamento, execute o comando get-event-data-store.

```
aws cloudtrail get-event-data-store --event-data-store arn:aws:cloudtrail:us-
east-1:123456789012:eventdatastore/EXAMPLE-d483-5c7d-4ac2-adb5dEXAMPLE
```

O procedimento a seguir mostra como criar os armazenamentos de dados de eventos de destino e origem e, em seguida, habilitar os eventos do Insights.

1. Execute o comando aws cloudtrail create-event-data-store para criar um armazenamento de dados de eventos de destino que coleta eventos do Insights. O valor de `eventCategory` deve ser `Insight`. *`retention-period-days`*Substitua pelo número de dias em que você gostaria de reter eventos em seu armazenamento de dados de eventos.

   Se você estiver conectado com a conta de gerenciamento de uma AWS Organizations organização, inclua o `--organization-enabled` parâmetro se quiser dar ao administrador delegado acesso ao armazenamento de dados do evento.

   ```
   aws cloudtrail create-event-data-store \
   --name insights-event-data-store \
   --no-multi-region-enabled \
   --retention-period retention-period-days \
   ```

```
--advanced-event-selectors '[
    {
      "Name": "Select Insights events",
      "FieldSelectors": [
          { "Field": "eventCategory", "Equals": ["Insight"] }
        ]
    }
  ]'
```

A seguir, uma exemplo de resposta.

```
{
    "Name": "insights-event-data-store",
    "ARN": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE",
    "AdvancedEventSelectors": [
        {
           "Name": "Select Insights events",
           "FieldSelectors": [
              {
                  "Field": "eventCategory",
                  "Equals": [
                      "Insight"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": false,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": "90",
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-08T15:22:33.578000+00:00",
    "UpdatedTimestamp": "2023-11-08T15:22:33.714000+00:00"
}
```

Você usará o ARN (ou o sufixo de ID do ARN) da resposta como o valor do parâmetro `--insights-destination` na etapa 3.

2. Execute o comando aws cloudtrail create-event-data-store para criar um armazenamento de dados de eventos que registre eventos de gerenciamento no log. Por padrão, os

armazenamentos de dados de eventos registram todos os eventos de gerenciamento. Não é necessário especificar nenhum seletor de eventos avançado para registrar todos os eventos de gerenciamento. *retention-period-days*Substitua pelo número de dias em que você gostaria de reter eventos em seu armazenamento de dados de eventos. Se você estiver criando um armazenamento de dados de eventos da organização, inclua o parâmetro `--organization-enabled`.

```
aws cloudtrail create-event-data-store --name source-event-data-store --retention-
period retention-period-days
```

A seguir, uma exemplo de resposta.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLE9952-4ab9-49c0-b788-f4f3EXAMPLE",
    "Name": "source-event-data-store",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 90,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-08T15:25:35.578000+00:00",
    "UpdatedTimestamp": "2023-11-08T15:25:35.714000+00:00"
}
```

Você usará o ARN (ou o sufixo de ID do ARN) da resposta como o valor do parâmetro `--event-data-store` na etapa 3.

3. Execute o comando put-insight-selectors para ativar os eventos do Insights. Os valores do seletor Insights podem ser `ApiCallRateInsight`, `ApiErrorRateInsight` ou ambos. Para o parâmetro `--event-data-store`, especifique o ARN (ou sufixo de ID do ARN) do armazenamento de dados de eventos de origem que registra os eventos de gerenciamento e ativará o Insights. Para o parâmetro `--insights-destination`, especifique o ARN (ou sufixo de ID do ARN) do armazenamento de dados de eventos de destino que registrará os eventos do Insights.

```
aws cloudtrail put-insight-selectors --event-data-store arn:aws:cloudtrail:us-
east-1:111122223333:eventdatastore/EXAMPLE9952-4ab9-49c0-b788-f4f3EXAMPLE --
insights-destination arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE --insight-selectors '[{"InsightType":
 "ApiCallRateInsight"},{"InsightType": "ApiErrorRateInsight"}]'
```

O resultado a seguir mostra o seletor de eventos do Insights que está configurado para o armazenamento de dados de eventos.

```
{
  "EventDataStoreARN": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLE9952-4ab9-49c0-b788-f4f3EXAMPLE",
  "InsightsDestination": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE",
  "InsightSelectors":
      [
         {
            "InsightType": "ApiErrorRateInsight"
         },
         {
            "InsightType": "ApiCallRateInsight"
         }
      ]
}
```

Depois de ativar o CloudTrail Insights pela primeira vez em um armazenamento de dados de eventos, pode levar até 7 dias CloudTrail para entregar o primeiro evento do Insights, se uma atividade incomum for detectada.

CloudTrail O Insights analisa eventos de gerenciamento que ocorrem em uma única região, não globalmente. Um evento do CloudTrail Insights é gerado na mesma região em que seus eventos de gerenciamento de apoio são gerados.

Para um armazenamento de dados de eventos da organização, CloudTrail analisa os eventos de gerenciamento da conta de cada membro em vez de analisar a agregação de todos os eventos de gerenciamento da organização.

Cobranças adicionais se aplicam à ingestão de eventos do Insights em CloudTrail Lake. Você será cobrado separadamente se ativar o Insights tanto para trilhas quanto para armazenamentos de dados de eventos. Para obter informações sobre CloudTrail preços, consulte AWS CloudTrail Preços.

Registrando eventos com os AWS SDKs

Execute a GetInsightSelectorsoperação para ver se seu armazenamento de dados de trilhas ou eventos habilita eventos do Insights. Você pode configurar suas trilhas ou armazenamentos de dados de eventos para habilitar eventos do Insights com a PutInsightSelectorsoperação. Para obter mais informações, consulte a AWS CloudTrail Referência da API do .

Informações adicionais sobre trilhas

Esta seção fornece informações adicionais específicas para trilhas. Esta seção descreve como você pode visualizar eventos para suas trilhas inscritas na página Insights no CloudTrail console e como você pode, opcionalmente, enviar esses eventos ao CloudWatch Logs para monitoramento.

Tópicos

- Visualizar eventos do Insights para trilhas no console
- Envio de eventos de trilha para o Amazon CloudWatch Logs

Visualizar eventos do Insights para trilhas no console

Para trilhas, você também pode acessar e visualizar eventos do Insights na página do Insights no CloudTrail console. Para obter mais informações sobre como acessar e visualizar eventos do Insights no console e usando o AWS CLI, consulte Visualizando eventos do CloudTrail Insights para trilhas este guia.

A imagem a seguir mostra um exemplo de eventos do Insights para uma trilha. Abra páginas de detalhes para um evento do Insights escolhendo um nome de evento do Insights nas páginas Dashboard (Painel) ou Insights.

Se você desativar o CloudTrail Insights em uma trilha ou parar de se registrar em uma trilha (o que desativa o CloudTrail Insights), você pode ter eventos do Insights armazenados no bucket do S3 de destino ou exibidos na página do Insights do console, com data da data anterior em que você ativou o Insights.

Filtrar coluna

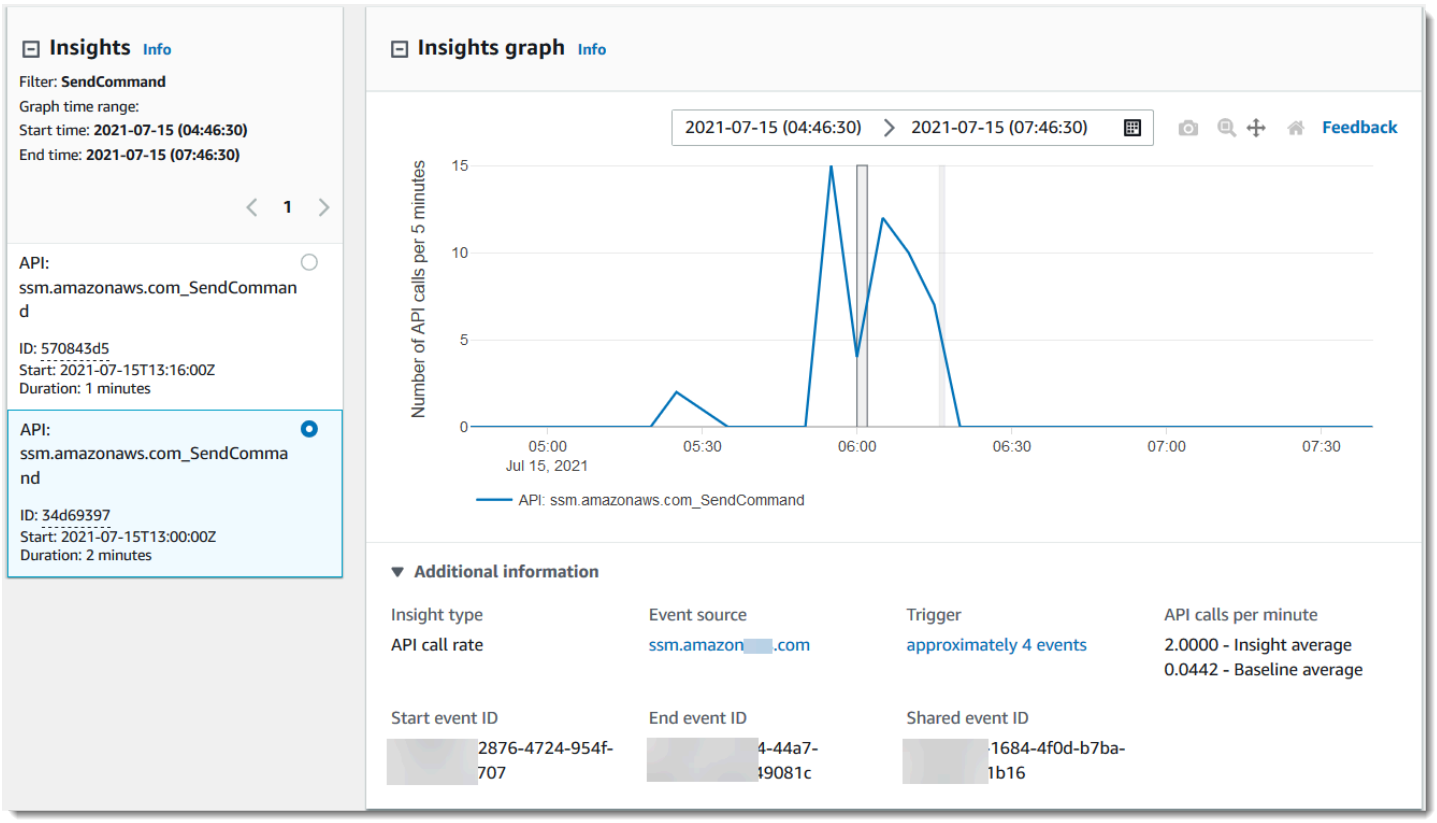
A coluna da esquerda lista eventos do Insights relacionados à API de assunto e que têm o mesmo tipo de evento do Insights. A coluna permite que você escolha o evento do Insights sobre o qual deseja obter mais informações. Quando você escolhe um evento nesta coluna, ele é destacado no gráfico na guia Insights graph (Gráfico de Insights). Por padrão, CloudTrail aplica um filtro que limita os eventos mostrados na guia de CloudTraileventos àqueles sobre a API específica que foi chamada durante o período de atividade incomum que acionou o evento do Insights. Para mostrar todos os CloudTrail eventos chamados durante o período de atividade incomum, incluindo eventos não relacionados ao evento do Insights, desative o filtro.

Guia Insights graph (Gráfico do Insights)

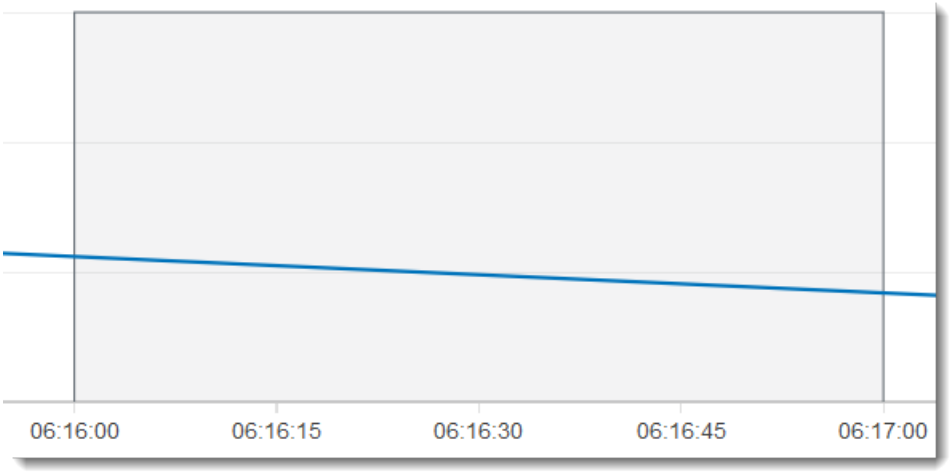
Na guia Insights graph (Gráfico do Insights), a página de detalhes de um evento do Insights mostra um gráfico do volume de chamadas de uma API que ocorreu durante um período antes e depois de um ou mais eventos do Insights a serem registrados em log. No gráfico, os eventos do Insights são destacados com barras verticais, com a largura da barra mostrando a hora de início e de término do evento do Insights.

Neste exemplo, uma faixa de destaque vertical mostra números incomuns de chamadas de AWS Systems Manager `SendCommand` API em uma conta. Na área destacada, como o número de `SendCommand` chamadas subiu acima da média básica da conta de 0,0442 chamadas por minuto, CloudTrail registrou um evento do Insights ao detectar a atividade incomum. O evento do Insights registrou que até 15 `SendCommand` chamadas foram feitas em um período de cinco minutos entre 5h50 e 5h55. Isso é cerca de duas mais chamadas para essa API por minuto do que o esperado para a conta. Neste exemplo, o intervalo de tempo do gráfico é de três horas: 4h30. PDT em 15 de julho de 2021 às 7h30 PDT em 15 de julho de 2021. Este evento tem a hora de início às 6h00. PDT em 15 de julho de 2021, e uma hora de término dois minutos depois. Um evento final do Insights, não destacado, mostra que a atividade incomum terminou por volta das 6h16.

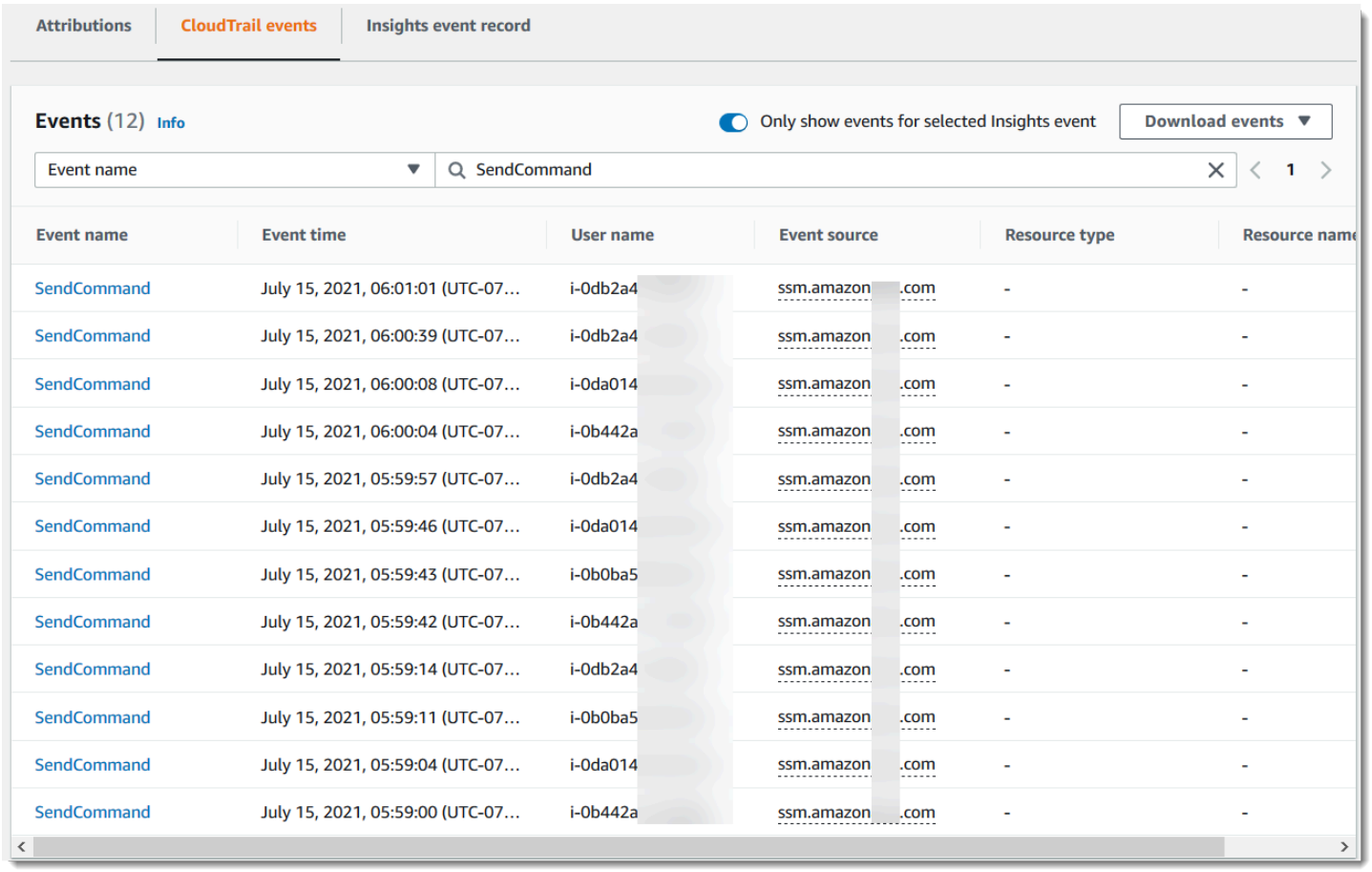
A linha de base é calculada ao longo dos sete dias anteriores ao início de um evento do Insights. Embora o valor da duração da linha de base — o período que CloudTrail analisa a atividade normal nas APIs — seja de aproximadamente sete dias, CloudTrail arredonda a duração da linha de base para um dia inteiro inteiro, de modo que a duração exata da linha de base possa variar.



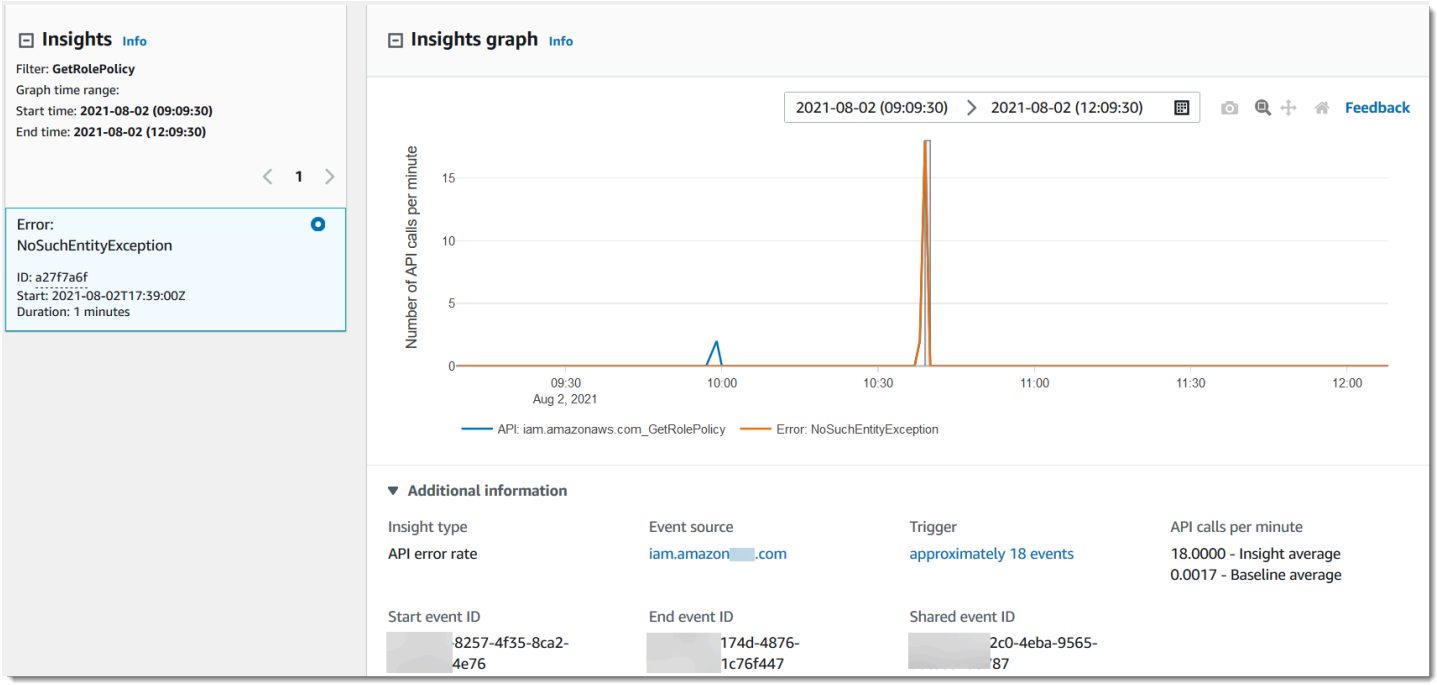
Você pode usar o comando Zoom na barra de ferramentas para ampliar o evento Insights final, mostrando a hora de início e término. Neste exemplo, escolher Zoom e, em seguida, arrastando o cursor Zoom a uma distância muito curta sobre uma borda do evento Insights destacado expande o evento Insights e mostra mais detalhes da linha do tempo.



Para visualizar CloudTrail eventos que foram analisados para determinar atividades incomuns, abra a guia de CloudTrail eventos. Neste exemplo, CloudTrail analisou 12 eventos, quatro dos quais acionaram o evento Insights.

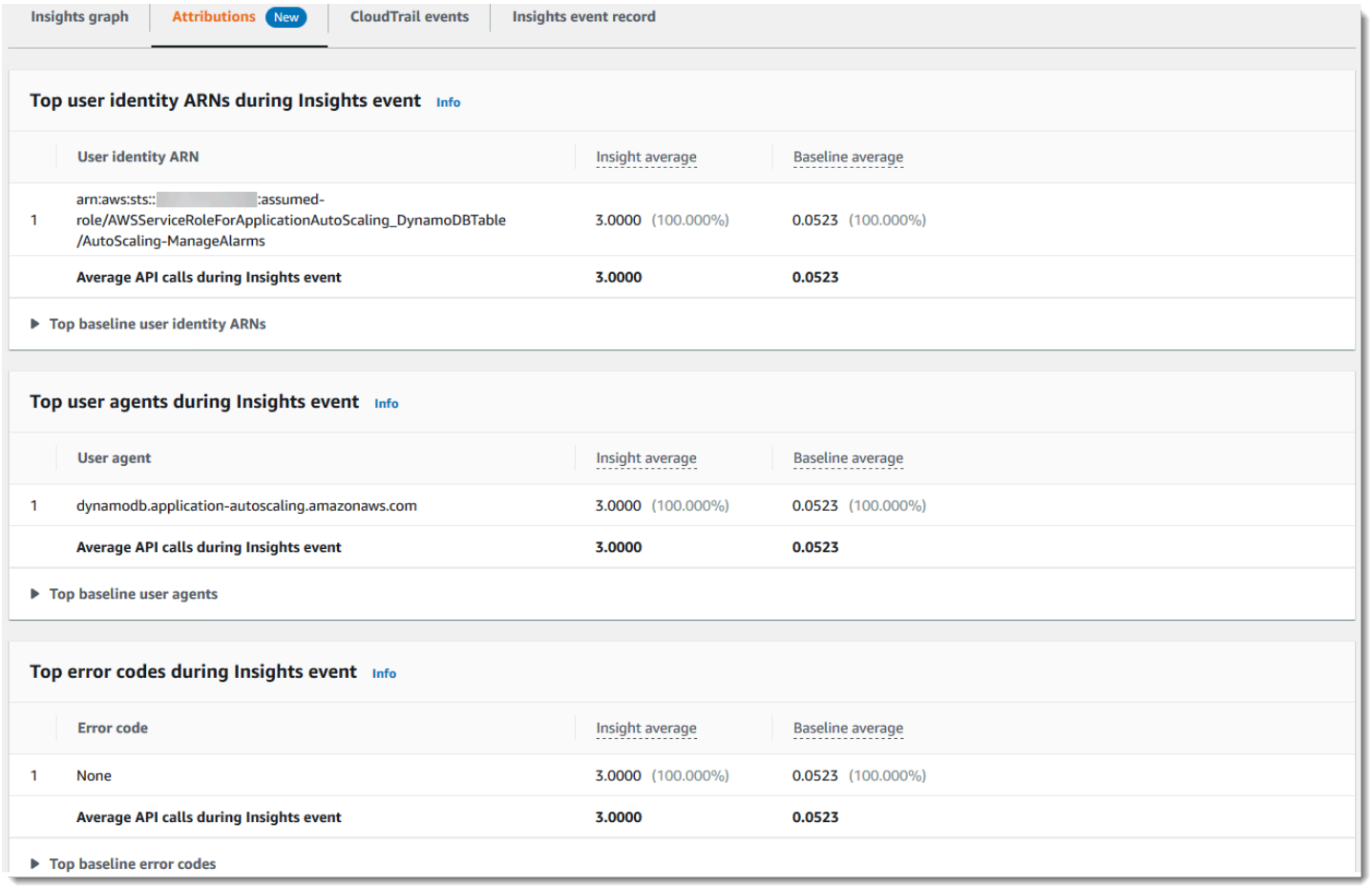


A imagem a seguir mostra uma guia de gráfico do Insights para um evento do Insights de taxa de erros da API. A área destacada mostra que um evento do Insights foi registrado devido às ocorrências do erro `NoSuchEntityException` na chamada da API do IAM `GetRolePolicy` subiu acima da média da linha de base de 0,0017 erros `NoSuchEntityException` por minuto nesta chamada de API, com média de 18 erros por minuto durante o período de insight. O número de CloudTrail eventos que acionaram o evento Insights corresponde à média do Insights de 18 `NoSuchEntityException` erros em um minuto, neste exemplo. Ao contrário de um gráfico de taxa de chamada de API, a taxa de erro da API mostra duas linhas, em cores contrastantes: uma linha de medição de chamadas para a API do IAM, `GetRolePolicy`, que resultou em um número incomum de erros, e uma linha medindo o erro no qual a atividade incomum foi registrada, `NoSuchEntityException`.

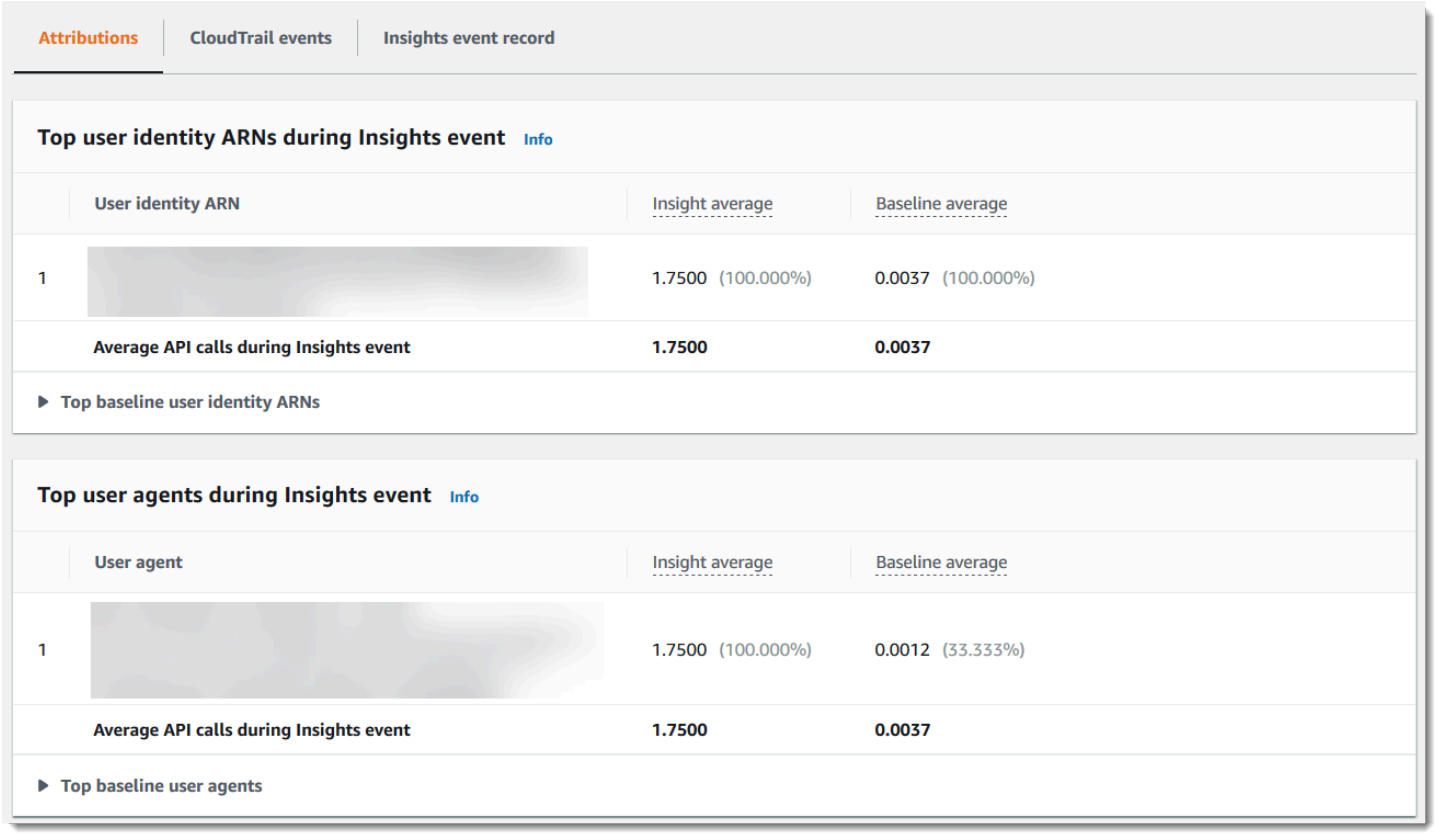


Guia Attibutions (Atribuições)

A guia Attributions (Atribuições) mostra as informações a seguir sobre um evento do Insights. Informações na aba Atribuições pode ajudá-lo a identificar as causas e fontes da atividade do Insights. Expanda as principais áreas de linha de base para comparar a identidade do usuário, o agente do usuário e a atividade do código de erro durante períodos normais com aqueles atribuídos durante a atividade do Insights. Em Top baseline user identity ARNs (Principais ARNs de identidade de usuário de linha de base), Top baseline user agents (Principais agentes de usuário de linha de base), e Top baseline error codes (Códigos de erro da linha de base), apenas a baseline average (média de linha de base), ou seja, a média histórica de eventos da API que são registrados em log pela identidade do usuário, pelo agente do usuário ou que resultam no código de erro, aproximadamente nos sete dias antes da hora de início do evento Insights, é mostrada.



A aba Atribuições mostra apenas os principais ARNs de identidade de usuário e os principais agentes de usuário para um evento Insights de taxa de erro, conforme mostrado na imagem a seguir. Os principais códigos de erro não são necessários para eventos do Insights de taxa de erro.



- Principais ARNs de identidade de usuário - Esta tabela mostra até os cinco principais AWS usuários ou funções do IAM (identidades de usuário) que contribuíram para as chamadas de API durante os períodos incomuns de atividade e linha de base, em ordem decrescente pelo número médio de chamadas de API contribuídas. A porcentagem das médias como um total de atividade que contribuiu para a atividade incomum é mostrada entre parênteses. Se mais de cinco ARNs de identidade de usuário contribuíram para a atividade incomum, sua atividade será resumida em uma linha Other (Outros).
- Principais agentes de usuário - Esta tabela mostra até as cinco principais AWS ferramentas pelas quais a identidade do usuário contribuiu para as chamadas de API durante os períodos incomuns de atividade e linha de base, em ordem decrescente pelo número médio de chamadas de API contribuídas. Essas ferramentas incluem o AWS Management Console AWS CLI, ou os AWS SDKs. Por exemplo, um agente de usuário chamado `ec2.amazonaws.com` indica que o console do Amazon EC2 estava entre as ferramentas usadas para chamar a API. A porcentagem das médias como um total de atividade que contribuiu para a atividade incomum é mostrada entre parênteses. Se mais de cinco ARNs de agentes contribuíram para a atividade incomum, sua atividade será resumida em uma linha Other (Outros).

- Códigos de erro principais: mostrados apenas para eventos API call rate (Taxa de chamada da API) do Insights. Esta tabela mostra até os cinco principais códigos de erro que ocorreram em chamadas de API durante a atividade incomum e períodos de linha de base, em ordem decrescente do maior número de chamadas de API para o menor. A porcentagem das médias como um total de atividade que contribuiu para a atividade incomum é mostrada entre parênteses. Se ocorrerem mais de cinco códigos de erro durante a atividade incomum ou de linha de base, sua atividade será resumida em uma linha Other (Outros).

  Um valor de `None` como um dos cinco principais valores de código de erro significa que uma porcentagem significativa das chamadas que contribuíram para o evento Insights não resultou em erros. Se o valor do código de erro for `None` e não houver outros códigos de erro na tabela, os valores de Insight average (Média de insights) e Baseline average (Média de base) serão iguais aos do evento do Insights. Você também pode ver esses valores exibidos na legenda de Insight average (Média de insights) e Baseline average (Média de base) do Gráfico de insights em API calls per minute (Chamadas de API por minuto).

Média de linha de base e média do Insights

Média de linha de base e Médio do Insights são mostrados para as principais identidades de usuário, os principais agentes de usuário e os principais códigos de erro.

- Baseline average (Média da linha de base) – A taxa típica de chamadas por minuto para essa API, conforme medida aproximadamente nos sete dias anteriores em uma região específica da sua conta.
- Média do Insights – A taxa de chamadas por minuto para essa API que acionou o evento do Insights. A média do CloudTrail Insights para o evento inicial é a taxa de chamadas ou erros por minuto na API que acionou o evento do Insights. Normalmente, esse é o primeiro minuto de atividade incomum. A média do Insights para o evento de término é a taxa de chamadas de API por minuto sobre a duração da atividade incomum, entre o evento do Insights de início e o evento do Insights de término.

CloudTrail aba de eventos

Na guia CloudTrail Eventos, visualize os eventos relacionados que CloudTrail foram analisados para determinar a ocorrência de uma atividade incomum. Por padrão, um filtro já está aplicado ao nome do evento do Insights, que também é o nome da API relacionada. Para mostrar todos os CloudTrail eventos registrados durante o período de atividade incomum, desative Mostrar somente eventos

para o evento selecionado do Insights. A guia de CloudTrail eventos mostra eventos CloudTrail de gerenciamento relacionados à API do assunto que ocorreram entre a hora de início e término do evento do Insights. Esses eventos ajudam a executar uma análise mais profunda para determinar a provável causa de um evento do Insights e os motivos da atividade de API incomum.

Guia Insights event record (Registro de evento do Insights)

Como qualquer CloudTrail evento, um evento do CloudTrail Insights é um registro no formato JSON. A guia Insights event record (Registro de evento do Insights) mostra a estrutura JSON e o conteúdo dos eventos de início e fim do Insights, às vezes chamados de evento de carga útil. Para obter mais informações sobre os campos e o conteúdo do registro de evento do Insights, consulte Campos de registro para eventos do Insights e CloudTrail `insightDetails`Elemento Insights neste guia.

Envio de eventos de trilha para o Amazon CloudWatch Logs

CloudTrail suporta o envio de eventos do Insights para trilhas para o CloudWatch Logs. Quando você configura sua trilha para enviar eventos do Insights ao seu grupo de CloudWatch registros de registros, o CloudTrail Insights envia somente os eventos que você especifica em sua trilha. Por exemplo, se você configurar sua trilha para gerenciamento de registros e eventos do Insights, sua trilha entregará eventos de gerenciamento e do Insights ao seu grupo de CloudWatch registros do Logs. Para ter mais informações, consulte Monitoramento CloudTrail de arquivos de log com o Amazon CloudWatch Logs.

CloudTrail conteúdo do registro

O corpo do registro contém campos que ajudam você a determinar a ação solicitada, bem como quando e onde a solicitação foi feita. Quando o valor de Opcional for True, o campo estará presente somente quando se aplicar ao serviço, à API ou ao tipo de evento. Um valor opcional de False (Falso) significa que o campo está sempre presente ou que sua presença não depende do serviço, da API ou do tipo de evento. Um exemplo é `responseElements`, que está presente em eventos para ações que fazem alterações (criar, atualizar ou excluir ações).

CloudTrail trunca um campo se o conteúdo do campo exceder o tamanho máximo do campo. Se um campo estiver truncado, `omitted` estará presente com um valor de `true`.

`eventTime`

A data e a hora em que a solicitação foi concluída no formato de Tempo Universal Coordenado (UTC). O carimbo de data/hora de um evento vem do host local que fornece o endpoint da

API de serviço no qual a chamada de API foi feita. Por exemplo, um evento de CreateBucket API executado na região Oeste dos EUA (Oregon) teria seu registro de data e hora a partir do momento em um AWS host executando o endpoint do Amazon S3,. `s3.us-west-2.amazonaws.com` Em geral, AWS os serviços usam o Network Time Protocol (NTP) para sincronizar os relógios do sistema.

Desde: 1.0

Opcional: False

`eventVersion`

A versão do formato do evento de log. A versão atual é 1.10.

O valor de `eventVersion` é uma versão principal e secundária no formulário *`major_version`*.*`minor_version`*. Por exemplo, é possível ter um valor `eventVersion` de `1.09`, onde `1` é a versão principal, e`09` é a versão secundária.

CloudTrail incrementa a versão principal se for feita uma alteração na estrutura do evento que não seja compatível com versões anteriores. Isso inclui remover um campo JSON que já existe ou alterar a forma como o conteúdo de um campo é representado (por exemplo, um formato de data). CloudTrail incrementa a versão secundária se uma alteração adicionar novos campos à estrutura do evento. Isso poderá ocorrer se novas informações forem fornecidas para alguns ou todos os eventos existentes ou se novas informações estiverem disponíveis somente para novos tipos de evento. As aplicações podem ignorar novos campos para permanecerem compatíveis com novas versões secundárias da estrutura do evento.

Se CloudTrail introduzir novos tipos de eventos, mas a estrutura do evento permanecer inalterada, a versão do evento não será alterada.

Para garantir que suas aplicações possam analisar a estrutura do evento, recomendamos que você faça uma comparação "igual a" no número da versão principal. Para garantir que os campos esperados pelo seu aplicativo existam, também recomendamos realizar uma comparação greater-than-or-equal -to na versão secundária. Não há zeros à esquerda na versão secundária. É possível interpretar *`major_version`* e *`minor_version`* como números e executar operações de comparação.

Desde: 1.0

Opcional: False

`userIdentity`

Informações sobre a identidade do IAM que fez uma solicitação. Para ter mais informações, consulte CloudTrail Elemento UserIdentity.

Desde: 1.0

Opcional: False

`eventSource`

O serviço para o qual a solicitação foi feita. Esse nome normalmente é uma forma curta do nome do serviço sem espaços, mais `.amazonaws.com`. Por exemplo: .

- AWS CloudFormation é`cloudformation.amazonaws.com`.
- O Amazon EC2 é `ec2.amazonaws.com`.
- O Amazon Simple Workflow Service é `swf.amazonaws.com`.

Essa convenção tem algumas exceções. Por exemplo, o `eventSource` para a Amazon CloudWatch é`monitoring.amazonaws.com`.

Desde: 1.0

Opcional: False

`eventName`

A ação solicitada, que é uma das ações na API desse serviço.

Desde: 1.0

Opcional: False

`awsRegion`

Região da AWS Aquele para o qual a solicitação foi feita, como`us-east-2`. Consulte CloudTrail Regiões suportadas.

Desde: 1.0

Opcional: False

`sourceIPAddress`

O endereço IP do qual a solicitação foi feita. Para ações originadas do console de serviço, o endereço informado é do recurso do cliente subjacente, e não do servidor web do console. Para serviços em AWS, somente o nome DNS é exibido.

> **Note**
>
> Para eventos originados pela AWS, esse campo geralmente é `AWS Internal/#`, onde `#` é um número usado para finalidades internas.

Desde: 1.0

Opcional: False

`userAgent`

O agente por meio do qual a solicitação foi feita AWS Management Console, como um AWS serviço, os AWS SDKs ou o. AWS CLI Esse campo tem um tamanho máximo de 1 KB; o conteúdo que exceder esse limite ficará truncado. Veja a seguir exemplos de valores:

- `lambda.amazonaws.com` – A solicitação foi feita com o AWS Lambda.
- `aws-sdk-java` – A solicitação foi feita com o AWS SDK for Java.
- `aws-sdk-ruby` – A solicitação foi feita com o AWS SDK for Ruby.
- `aws-cli/1.3.23 Python/2.7.6 Linux/2.6.18-164.el5`— A solicitação foi feita com o AWS CLI instalado no Linux.

> **Note**
>
> Para eventos originados por AWS, se CloudTrail souber quem AWS service (Serviço da AWS) fez a chamada, esse campo é a origem do evento do serviço de chamada (por exemplo,`ec2.amazonaws.com`). Caso contrário, esse campo é`AWS Internal/#`, onde `#` é um número usado para fins internos.

Desde: 1.0

Opcional: True

`errorCode`

O erro de AWS serviço se a solicitação retornar um erro. Para obter um exemplo que mostra esse campo, consulte Exemplos de código de erro e log de mensagens. Esse campo tem um tamanho máximo de 1 KB; o conteúdo que exceder esse limite ficará truncado.

Desde: 1.0

Opcional: True

`errorMessage`

Se a solicitação retornar um erro, a descrição do erro. Essa mensagem inclui mensagens de falhas de autorização. CloudTrail captura a mensagem registrada pelo serviço em seu tratamento de exceções. Para ver um exemplo, consulte Exemplos de código de erro e log de mensagens. Esse campo tem um tamanho máximo de 1 KB; o conteúdo que exceder esse limite ficará truncado.

> **Note**
>
> Alguns AWS serviços fornecem os `errorCode` e `errorMessage` como campos de alto nível no evento. Outros serviços do AWS fornecem informações de erro como parte do `responseElements`.

Desde: 1.0

Opcional: True

`requestParameters`

Os parâmetros, se houver, que foram enviados com a solicitação. Esses parâmetros estão documentados na documentação de referência da API para o AWS serviço apropriado. Esse campo tem um tamanho máximo de 100 KB; o conteúdo que exceder esse limite ficará truncado.

Desde: 1.0

Opcional: False

`responseElements`

Os elementos de resposta, se houver, para ações que fazem alterações (criar, atualizar ou excluir ações). Se a ação não retorna elementos de resposta, esse campo é`null`. Se uma ação não muda de estado (por exemplo, uma solicitação para obter ou listar objetos), esse elemento é omitido. Os elementos de resposta para ações estão documentados na referência da API documentação para o apropriado AWS service (Serviço da AWS). Esse campo tem um tamanho máximo de 100 KB; o conteúdo que excede esse limite é truncado.

O `responseElements` valor é útil para ajudar você a rastrear uma solicitação. com AWS Support. Ambos `x-amz-request-id` e `x-amz-id-2` contêm informações que ajudam você a rastrear uma solicitação com AWS Support. Esses valores são os mesmos que o serviço retorna na resposta à solicitação que inicia os eventos, para que você possa usá-los para combinar o evento com o pedido.

Desde: 1.0

Opcional: False

`additionalEventData`

Dados adicionais sobre o evento que não faziam parte da solicitação ou resposta. Esse campo tem um tamanho máximo de 28 KB; o conteúdo que exceder esse limite ficará truncado.

Desde: 1.0

Opcional: True

`requestID`

O valor que identifica a solicitação. O serviço que está sendo chamado gera esse valor. Esse campo tem um tamanho máximo de 1 KB; o conteúdo que exceder esse limite ficará truncado.

Desde: 1.01

Opcional: True

`eventID`

GUID gerado por CloudTrail para identificar de forma exclusiva cada evento. Você pode usar esse valor para identificar um único evento. Por exemplo, você pode usar o ID como uma chave primária para recuperar dados de log de um banco de dados que pode ser pesquisado.

Desde: 1.01

Opcional: False

`eventType`

Identifica o tipo de evento que gerou o registro de eventos. Pode ser um dos valores a seguir:

- `AwsApiCall` – Uma API foi chamada.
- `AwsServiceEvent` – O serviço gerou um evento relacionado à sua trilha. Por exemplo, isso pode ocorrer quando outra conta fez uma chamada com um recurso seu.
- `AwsConsoleAction` – Foi executada uma ação no console que não era uma chamada de API.
- `AwsConsoleSignIn`— Um usuário em sua conta (root, IAM, federado, SAML ou SwitchRole) conectado ao. AWS Management Console
- `AwsCloudTrailInsight`— Se os eventos do Insights estiverem ativados, CloudTrail gera eventos do Insights ao CloudTrail detectar atividades operacionais incomuns, como picos no provisionamento de recursos ou surtos de AWS Identity and Access Management ações (IAM).

  Eventos de `AwsCloudTrailInsight` não usam os seguintes campos:

  - `eventName`
  - `eventSource`
  - `sourceIPAddress`
  - `userAgent`
  - `userIdentity`

Desde: 1.02

Opcional: False

`apiVersion`

Identifica a versão da API associada ao valor de `AwsApiCall` `eventType`.

Desde: 1.01

Opcional: True

`managementEvent`

Um valor booliano que identifica se o evento é um evento de gerenciamento. `managementEvent` será mostrado em um registro de evento se `eventVersion` for 1.06 ou superior e o tipo de evento for um dos seguintes:

- `AwsApiCall`
- `AwsConsoleAction`
- `AwsConsoleSignIn`
- `AwsServiceEvent`

Desde: 1.06

Opcional: True

`readOnly`

Identifica se essa operação é somente leitura. Pode ter um dos valores a seguir:

- `true` – A operação é somente leitura (por exemplo, `DescribeTrails`).
- `false` – A operação é somente gravação (por exemplo, `DeleteTrail`).

Desde: 1.01

Opcional: True

`resources`

Uma lista de recursos acessados no evento. O campo pode conter as seguintes informações:

- ARNs de recursos
- ID da conta do proprietário do recurso
- Identificador de tipo de recurso no formato: `AWS::`*`aws-service-name`*`::`*`data-type-name`*

Por exemplo, quando um evento `AssumeRole` é registrado, o campo `resources` pode ter esta aparência:

- ARN: `arn:aws:iam::123456789012:role/myRole`
- ID da conta: `123456789012`
- Identificador de tipo de recurso: `AWS::IAM::Role`

Por exemplo, registros com o `resources` campo, consulte Evento de AWS STS API no arquivo de CloudTrail registro no Guia do usuário do IAM ou Registro de chamadas de AWS KMS API no Guia do AWS Key Management Service desenvolvedor.

Desde: 1.01

Opcional: True

`recipientAccountId`

Representa o ID da conta que recebeu esse evento. O `recipientAccountID` pode ser diferente do CloudTrail Elemento UserIdentity `accountId`. Isso pode ocorrer no acesso a recursos entre contas. Por exemplo, se uma chave do KMS, também conhecida como AWS KMS key, foi usada por uma conta separada para chamar a API de criptografia, os valores `accountId` e `recipientAccountID` serão os mesmos para o evento fornecido à conta que fez a chamada, mas os valores serão diferentes para o evento fornecido à conta que possui a chave do KMS.

Desde: 1.02

Opcional: True

`serviceEventDetails`

Identifica o evento de serviço, incluindo o que acionou o evento e o resultado. Para ter mais informações, consulte AWS eventos de serviço. Esse campo tem um tamanho máximo de 100 KB; o conteúdo que exceder esse limite ficará truncado.

Desde: 1.05

Opcional: True

`sharedEventID`

GUID gerado por CloudTrail para identificar de forma exclusiva CloudTrail eventos da mesma AWS ação que é enviada para contas diferentes. AWS

Por exemplo, quando uma conta usa uma AWS KMS keyque pertence a outra conta, a conta que usou a chave KMS e a conta que possui a chave KMS recebem CloudTrail eventos separados para a mesma ação. Cada CloudTrail evento realizado para esta AWS ação compartilha o mesmo`sharedEventID`, mas também tem um único `eventID` `recipientAccountID` e.

Para ter mais informações, consulte Exemplo de sharedEventID.

> **Note**
>
> O `sharedEventID` campo está presente somente quando CloudTrail os eventos são entregues em várias contas. Se o chamador e o proprietário forem da mesma AWS conta, CloudTrail enviará somente um evento e o `sharedEventID` campo não estará presente.

Desde: 1.03

Opcional: True

`vpcEndpointId`

Identifica o endpoint da VPC em que as solicitações foram feitas a partir de uma VPC para outro serviço da AWS , como o Amazon S3.

Desde: 1.04

Opcional: True

`eventCategory`

Mostra a categoria do evento. O `eventCategory` é usado em `LookupEvents`chamadas para gerenciamento e eventos do Insights.

- Para eventos de gerenciamento, o valor é `Management`.
- Para eventos de dados, o valor é `Data`.
- Para eventos do Insights, o valor é `Insight`.

Desde: 1.07

Opcional: False

addendum

Se uma entrega de evento estiver atrasada ou informações adicionais sobre um evento existente se tornarem disponíveis após o evento ser registrado, um campo de adendo mostrará informações sobre o motivo do atraso do evento. Se as informações estiverem ausentes de um evento existente, o campo de adendo incluirá as informações ausentes e um motivo pelo qual elas estavam ausentes. O conteúdo inclui o seguinte:

- **reason** - A razão pela qual o evento ou parte de seu conteúdo estavam faltando. Os valores podem ser qualquer um dos valores a seguir.
  - **DELIVERY_DELAY** - Houve um atraso na entrega de eventos. Isso pode ser causado por alto tráfego de rede, problemas de conectividade ou problemas de CloudTrail serviço.
  - **UPDATED_DATA** - Um campo no registro de eventos estava ausente ou tinha um valor incorreto.
  - **SERVICE_OUTAGE**— Um serviço que registra eventos em CloudTrail que houve uma interrupção e não conseguiu registrar CloudTrail eventos em. Isso é excepcionalmente raro.
- **updatedFields** - Os campos de registro de eventos que são atualizados pelo adendo. Isso só será fornecido se o motivo for `UPDATED_DATA`.
- **originalRequestID** - O ID exclusivo original da solicitação. Isso só será fornecido se o motivo for `UPDATED_DATA`.
- **originalEventID** - O ID do evento original. Isso só será fornecido se o motivo for `UPDATED_DATA`.

Desde: 1.08

Opcional: True

sessionCredentialFromConsole

Mostra se um evento se originou ou não de uma AWS Management Console sessão. Este campo não é mostrado a menos que o valor seja `true`, o que significa que o cliente que foi usado para fazer a chamada de API era um proxy ou um cliente externo. Se um cliente proxy foi usado, campo do evento `tlsDetails` não é mostrado.

Desde: 1.08

Opcional: True

`edgeDeviceDetails`

Mostra informações sobre dispositivos de borda que são alvos de uma solicitação. No momento, os eventos do dispositivo `S3 Outposts` incluem este campo. Esse campo tem um tamanho máximo de 28 KB; o conteúdo que exceder esse limite ficará truncado.

Desde: 1.08

Opcional: True

`tlsDetails`

Mostra informações sobre a versão TLS (Transport Layer Security), pacotes de criptografia e o nome de domínio totalmente qualificado (FQDN) do nome de host fornecido pelo cliente usado na chamada da API de serviço, que normalmente é o FQDN do endpoint do serviço. CloudTrailainda registra detalhes parciais do TLS se as informações esperadas estiverem ausentes ou vazias. Por exemplo, se a versão do TLS e o conjunto de cifras estiverem presentes, mas o `HOST` cabeçalho estiver vazio, os detalhes do TLS disponíveis ainda serão registrados no evento. CloudTrail

- **`tlsVersion`** - A versão do TLS de uma solicitação.
- **`cipherSuite`** - O conjunto de cifras (combinação de algoritmos de segurança usados) de uma solicitação.
- **`clientProvidedHostHeader`** — O nome do host fornecido pelo cliente usado na chamada da API de serviço, que geralmente é o FQDN do endpoint de serviço.

> **Note**
>
> Há alguns casos em que o campo `tlsDetails` não está presente em um registro de evento.
>
> - O `tlsDetails` campo não estará presente se a chamada da API tiver sido feita por um AWS service (Serviço da AWS) em seu nome. O campo `invokedBy` no elemento `userIdentity` identifica o AWS service (Serviço da AWS) que fez a chamada à API.
> - Se `sessionCredentialFromConsole` estiver presente com um valor true, o `tlsDetails` estará presente em um registro de evento somente se um cliente externo tiver sido usado para fazer a chamada de API.

Desde: 1.08

Opcional: True

Campos de registro para eventos do Insights

Veja a seguir os atributos mostrados na estrutura JSON de um evento do Insights que difere daqueles em um evento de dados ou de gerenciamento.

`sharedEventId`

Os eventos A `sharedEventID` for CloudTrail Insights diferem dos `sharedEventID` CloudTrail eventos de gerenciamento e dados. Em eventos do Insights, a `sharedEventID` é um GUID gerado pelo CloudTrail Insights para identificar de forma exclusiva um evento do Insights. `sharedEventID`é comum entre os eventos iniciais e finais do Insights e ajuda a conectar os dois eventos para identificar de forma exclusiva atividades incomuns. É possível pensar no `sharedEventID` como o ID de evento do Insights geral.

Desde: 1.07

Opcional: False

`insightDetails`

Somente eventos do Insights. Mostra informações sobre os acionadores subjacentes de um evento do Insights, como a fonte do evento, as estatísticas, o nome da API e se o evento é o início ou o fim do evento do Insights. Para obter mais informações sobre a estrutura e o conteúdo do arquivo `insightDetails`, consulte CloudTrail `insightDetails`Elemento Insights.

Desde: 1.07

Opcional: False

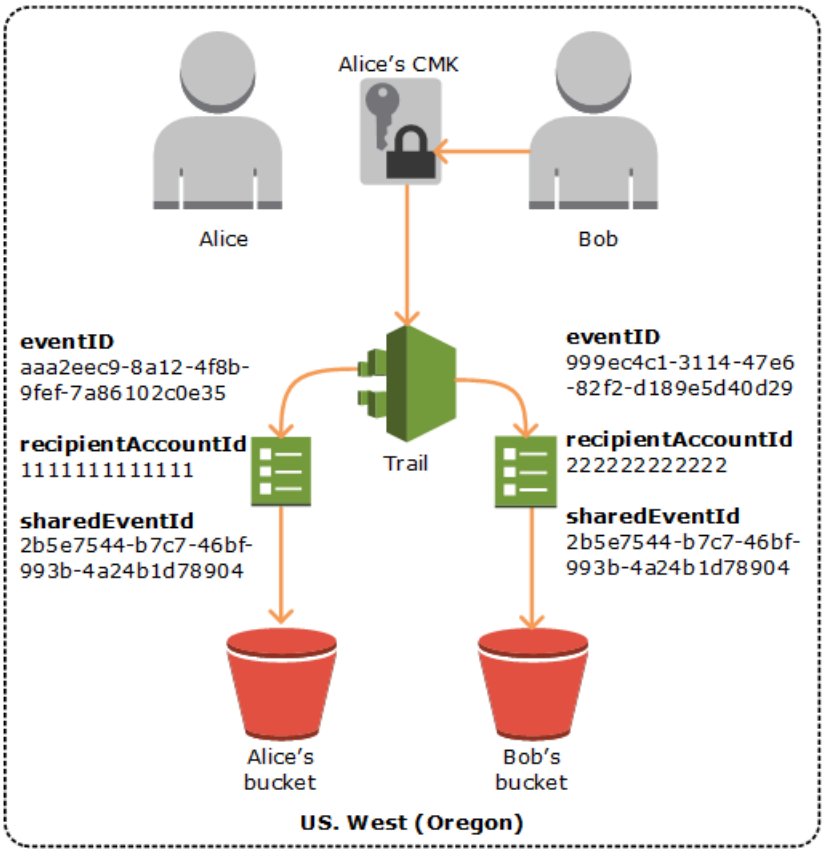
Exemplo de sharedEventID

Veja a seguir um exemplo que descreve como CloudTrail entrega dois eventos para a mesma ação:

1. Alice tem uma AWS conta (111111111111) e cria uma. AWS KMS key Ela é a proprietária dessa chave do KMS.
2. Bob tem uma AWS conta (222222222222). Alice concede a Bob permissão para usar a chave do KMS.

3. Cada conta tem uma trilha e um bucket separado.
4. Bob usa a chave do KMS para chamar a API `Encrypt`.
5. CloudTrail envia dois eventos separados.

   - Um evento é enviado a Bob. O evento mostra que ele usou a chave do KMS.
   - Um evento é enviado a Alice. O evento mostra que o Bob usou a chave do KMS.
   - Os eventos têm o mesmo `sharedEventID`, mas o `eventID` e o `recipientAccountID` são exclusivos.



IDs de eventos compartilhados no CloudTrail Insights

Os eventos A `sharedEventID` for CloudTrail Insights diferem dos `sharedEventID` CloudTrail eventos de gerenciamento e dados. Em eventos do Insights, a `sharedEventID` é um GUID gerado pelo CloudTrail Insights para identificar de forma exclusiva um par inicial e final de eventos do Insights. `sharedEventID`é comum entre o início e o final do evento Insights e ajuda a criar uma correlação entre os dois eventos para identificar de forma exclusiva atividades incomuns.

É possível pensar no `sharedEventID` como o ID de evento do Insights geral.

CloudTrail Elemento UserIdentity

AWS Identity and Access Management (IAM) fornece diferentes tipos de identidades. O elemento `userIdentity` contém detalhes sobre o tipo de identidade do IAM que fez a solicitação e quais credenciais foram usadas. Se forem usadas credenciais temporárias, o elemento mostrará como elas foram obtidas.

Sumário

Exemplos

`userIdentity` com credenciais de usuário do IAM

O exemplo a seguir mostra o elemento `userIdentity` de uma solicitação simples feita com as credenciais da usuária do IAM chamada `Alice`.

```
"userIdentity": {
  "type": "IAMUser",
  "principalId": "AIDAJ45Q7YFFAREXAMPLE",
  "arn": "arn:aws:iam::123456789012:user/Alice",
  "accountId": "123456789012",
  "accessKeyId": "",
  "userName": "Alice"
}
```

`userIdentity` com credenciais de segurança temporárias

O exemplo a seguir mostra um elemento `userIdentity` de uma solicitação feita com credenciais de segurança temporárias obtidas com uma função do IAM. O elemento contém detalhes adicionais sobre a função que foi assumida para obter credenciais.

```
"userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAIDPPEZS35WEXAMPLE:AssumedRoleSessionName",
    "arn": "arn:aws:sts::123456789012:assumed-role/RoleToBeAssumed/MySessionName",
```

```
    "accountId": "123456789012",
    "accessKeyId": "",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "20131102T010628Z"
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAIDPPEZS35WEXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/RoleToBeAssumed",
        "accountId": "123456789012",
        "userName": "RoleToBeAssumed"
      }
    }
}
```

`userIdentity` para uma solicitação feita em nome de um usuário do Centro de Identidade do IAM

O exemplo a seguir mostra um elemento `userIdentity` de uma solicitação feita em nome de um usuário do Centro de Identidade do IAM.

```
"userIdentity": {
 "type": "IdentityCenterUser",
 "accountId": "123456789012",
 "onBehalfOf": {
  "userId": "544894e8-80c1-707f-60e3-3ba6510dfac1",
  "identityStoreArn": "arn:aws:identitystore::123456789012:identitystore/d-9067642ac7"
 },
 "credentialId": "EXAMPLEVHULjJdTUdPJfofVa1sufHDoj7aYcOYcxFVllWR_Whr1fEXAMPLE"
}
```

Campos

Os campos a seguir podem aparecer em um elemento `userIdentity`.

`type`

O tipo da identidade. Os seguintes valores são possíveis:

- `Root`— A solicitação foi feita com suas Conta da AWS credenciais. Se o `userIdentity` tipo for `Root` e você definir um alias para a sua conta, o campo `userName` conterá o alias da conta. Para obter mais informações, consulte ID da sua Conta da AWS e seu alias.

- `IAMUser` – A solicitação foi feita com as credenciais de um usuário do IAM.
- `AssumedRole` — A solicitação foi feita com credenciais de segurança temporárias que foram obtidas com uma função por meio de uma chamada para a API AWS Security Token Service AWS STS do `AssumeRole` (). Isso pode incluir funções para o Amazon EC2 e acesso à API entre contas.
- `Role` — A solicitação foi feita com uma identidade do IAM persistente que tem permissões específicas. O emissor das sessões de perfil é sempre o perfil. Para obter mais informações sobre funções, consulte Termos e conceitos de funções, no Guia do usuário do IAM.
- `FederatedUser`— A solicitação foi feita com credenciais de segurança temporárias obtidas de uma chamada para a AWS STS `GetFederationToken`API. O elemento `sessionIssuer` indica se a API foi chamada com raiz ou com credenciais de usuário do IAM.

  Para obter mais informações sobre credenciais de segurança temporárias, consulte Credenciais de segurança temporárias no Manual do usuário do IAM.
- `Directory` – A solicitação foi feita para um serviço de diretório e o tipo é desconhecido. Os serviços de diretório incluem o seguinte: Amazon WorkDocs e Amazon QuickSight.
- `AWSAccount`— O pedido foi feito por outro Conta da AWS
- `AWSService`— A solicitação foi feita por um Conta da AWS que pertence a um AWS service (Serviço da AWS). Por exemplo, AWS Elastic Beanstalk assume uma função do IAM em sua conta para ligar para outra pessoa Serviços da AWS em seu nome.
- `IdentityCenterUser`: a solicitação foi feita em nome de um usuário do Centro de Identidade do IAM.
- `Unknown`— A solicitação foi feita com um tipo de identidade que não é CloudTrail possível determinar.

Opcional: False

`AWSAccount` e `AWSService` aparecem para `type` em seus logs quando há acesso entre contas usando uma função do IAM que você possui.

Exemplo: acesso entre contas iniciado por outra conta da AWS

1. Você possui uma função do IAM na sua conta.
2. Outra AWS conta muda para essa função para assumir a função da sua conta.

3. Como você é o proprietário da função do IAM, recebe um log que mostra que a outra conta assumiu a função. O `type` é `AWSAccount`. Para ver um exemplo de entrada de registro, consulte Evento de AWS STS API no arquivo de CloudTrail registro.

Exemplo: acesso entre contas iniciado por um serviço AWS

1. Você possui uma função do IAM na sua conta.
2. Uma AWS conta pertencente a um AWS serviço assume essa função.
3. Como você é o proprietário da função do IAM, recebe um log que mostra que o serviço da AWS assumiu a função. O `type` é `AWSService`.

`userName`

O nome fácil da identidade que fez a chamada. O valor que aparece em `userName` se baseia no valor em `type`. A tabela a seguir mostra a relação entre `type` e `userName`:

`type`	**`userName`**	Descrição
`Root` (nenhum alias definido)	Não está presente	Se você não configurou um alias para o seu Conta da AWS, o `userName` campo não aparece. Para obter mais informações sobre aliases de conta, consulte Seu Conta da AWS ID e seu alias. Observe que o campo `userName` não pode conter `Root`, porque `Root` é um tipo de identidade, e não um nome de usuário.
`Root` (alias definido)	O alias da conta	Para obter mais informações sobre Conta da AWS aliases, consulte Seu Conta da AWS ID e seu alias.
`IAMUser`	O nome de usuário do IAM	
`AssumedRole`	Não está presente	Para o tipo `AssumedRole` , você pode encontrar o campo `userName` em `sessionContext`

type	userName	Descrição
		como parte do elemento **sessionIssuer** . Para ver um exemplo de entrada, consulte Exemplos.
Role	Definido pelo usuário	A seção sessionContext e sessionIssuer contém informações sobre a identidade que emitiu a sessão para a função.
FederatedUser	Não está presente	A seção sessionContext e sessionIssuer contém informações sobre a identidade que emitiu a sessão para o usuário federado.
Directory	Pode estar presente	Por exemplo, o valor pode ser o alias da conta ou o endereço de email do ID da Conta da AWS associada.
AWSService	Não está presente	
AWSAccount	Não está presente	
IdentityCenterUser	Não está presente	A seção onBehalfOf contém informações sobre o ID de usuário do Centro de Identidade do IAM e o ARN do repositório de identidades para o qual a chamada foi feita. Para obter mais informações sobre o Centro de Identidade do IAM, consulte o Guia do usuário do AWS IAM Identity Center .
Unknown	Pode estar presente	Por exemplo, o valor pode ser o alias da conta ou o endereço de email do ID da Conta da AWS associada.

> **Note**
>
> O campo `userName` contém a string `HIDDEN_DUE_TO_SECURITY_REASONS` quando o evento registrado é uma falha de login do console causada pela inserção incorreta de um nome do usuário. CloudTrail não registra o conteúdo nesse caso porque o texto pode conter informações confidenciais, como nos exemplos a seguir:
>
> - Um usuário digita acidentalmente uma senha no campo de nome do usuário.
> - Um usuário clica no link da página de login de uma AWS conta, mas depois digita o número da conta de outra.
> - Um usuário digita acidentalmente o nome de uma conta de email pessoal, um identificador de login de um banco ou algum outro ID privado.

Opcional: True

`principalId`

Um identificador exclusivo para a entidade que fez a chamada. Para solicitações feitas com credenciais de segurança temporárias, esse valor inclui o nome da sessão que é transmitido à chamada da API `AssumeRole`, `AssumeRoleWithWebIdentity` ou `GetFederationToken`.

Opcional: True

`arn`

O Nome de recurso da Amazon (ARN) do principal que fez a chamada. A última seção do ARN contém o usuário ou a função que fez a chamada.

Opcional: True

`accountId`

A conta proprietária da entidade que concedeu permissões para a solicitação. Se a solicitação foi feita com credenciais de segurança temporárias, essa é a conta proprietária do perfil ou do usuário do IAM usado para obter as credenciais.

Se a solicitação foi feita com um token de acesso autorizado do Centro de Identidade do IAM, essa é a conta proprietária da instância do Centro de Identidade do IAM.

Opcional: True

`accessKeyId`

O ID da chave de acesso da que foi usada para assinar a solicitação. Se a solicitação foi feita com credenciais de segurança temporárias, esse é o ID da chave de acesso delas. Por razões de segurança, `accessKeyId` pode não estar presente ou pode ser exibido como uma string vazia.

Opcional: True

`sessionContext`

Se a solicitação foi feita com credenciais de segurança temporárias, `sessionContext` fornece informações sobre a sessão criada para essas credenciais. Você cria uma sessão ao chamar qualquer API que retorna credenciais temporárias. Os usuários também criam sessões quando trabalham no console e fazem solicitações com APIs que incluem autenticação multifator. Esse elemento tem os seguintes atributos:

- `creationDate` – A data e a hora em que as credenciais de segurança temporárias foram emitidas. Representadas em notação básica ISO 8601.
- `mfaAuthenticated`: o valor será `true` se o usuário raiz ou o usuário do IAM cujas credenciais foram usadas para a solicitação também for autenticado com um dispositivo com MFA; caso contrário, o valor será `false`.
- `sourceIdentity` – Consulte AWS STS identidade de origem neste tópico. O campo `sourceIdentity` ocorre em eventos quando os usuários assumem um perfil do IAM para executar uma ação. `sourceIdentity` identifica a identidade do usuário original que faz a solicitação, seja essa identidade um usuário do IAM, perfil do IAM, usuário autenticado via federação baseada em SAML ou usuário autenticado via federação de identidades da Web compatível com OpenID Connect (OIDC). Para obter mais informações sobre AWS STS a configuração para coletar informações de identidade de origem, consulte Monitorar e controlar ações realizadas com funções assumidas no Guia do usuário do IAM.
- `ec2RoleDelivery`: o valor será `1.0` se as credenciais foram fornecidas pelo Instance Metadata Service Version 1 (IMDSv1) do Amazon EC2. O valor será `2.0` se as credenciais foram fornecidas usando o novo esquema do IMDS.

  AWS as credenciais fornecidas pelo Amazon EC2 Instance Metadata Service (IMDS) incluem uma chave de contexto RoleDelivery ec2: IAM. Essa chave de contexto facilita a imposição do uso do novo esquema em uma resource-by-resource base service-by-service ou usando a chave de contexto como condição nas políticas do IAM, nas políticas de recursos ou nas políticas de controle AWS Organizations de serviços. Para obter mais informações, consulte

Metadados de instância e dados do usuário no Manual do usuário para instâncias do Linux do Amazon EC2.

Opcional: True

`invokedBy`

O nome de quem fez AWS service (Serviço da AWS) a solicitação, quando uma solicitação é feita por alguém AWS service (Serviço da AWS) como Amazon EC2 Auto Scaling ou. AWS Elastic Beanstalk Esse campo só está presente quando uma solicitação é feita por um AWS service (Serviço da AWS). Isso inclui solicitações feitas por serviços usando sessões de acesso direto (FAS), AWS service (Serviço da AWS) diretores, funções vinculadas a serviços ou funções de serviço usadas por um. AWS service (Serviço da AWS)

Opcional: True

`sessionIssuer`

Se um usuário fez uma solicitação com credenciais de segurança temporárias, `sessionIssuer` fornece informações sobre como elas foram obtidas. Por exemplo, se o usuário obteve credenciais de segurança temporárias ao assumir um perfil, esse elemento fornece informações sobre a função assumida. Se as credenciais foram obtidas com credenciais de usuário raiz ou do IAM para chamar AWS STS `GetFederationToken`, o elemento fornece informações sobre a conta raiz ou o usuário do IAM. Esse elemento tem os seguintes atributos:

- `type` – A origem das credenciais de segurança temporárias, como `Root`, `IAMUser` ou `Role`.
- `userName` – O nome fácil do usuário ou da função que emitiu a sessão. O valor que aparece depende da `sessionIssuer` identidade `type`. A tabela a seguir mostra a relação entre `sessionIssuer type` e `userName`:

Tipo de **`sessionIssuer`**	**`userName`**	Descrição
`Root` (nenhum alias definido)	Não está presente	Se você não tiver configurado um alias para a sua conta, o campo `userName` não será exibido. Para obter mais informações sobre Conta da AWS aliases, consulte Seu Conta da AWS ID e seu alias. Observe que o campo `userName` não pode conter `Root`, porque `Root` é um tipo de identidade, e não um nome de usuário.

Tipo de **sessionIssuer**	**userName**	Descrição
`Root` (alias definido)	O alias da conta	Para obter mais informações sobre Conta da AWS aliases, consulte Seu ID de AWS conta e seu alias.
`IAMUser`	O nome de usuário do IAM	Isso também se aplica quando um usuário federado usa uma sessão emitida pelo `IAMUser`.
`Role`	O nome da função	Uma função assumida por um usuário do IAM ou usuário federado de identidade da web em uma sessão de função. AWS service (Serviço da AWS)

- `principalId`: o ID interno da entidade usada para obter credenciais.
- `arn` – O ARN da fonte (conta, usuário ou função do IAM) usado para obter credenciais de segurança temporárias.
- `accountId` – A conta proprietária da entidade que foi usada para obter credenciais.

Opcional: True

`onBehalfOf`

Se a solicitação foi feita por um chamador do Centro de Identidade do IAM, `onBehalfOf` fornece informações sobre o ID de usuário do Centro de Identidade do IAM e o ARN do repositório de identidades para o qual a chamada foi feita. Esse elemento tem os seguintes atributos:

- `userId`: o ID do usuário do Centro de Identidade do IAM em nome do qual a chamada foi feita.
- `identityStoreArn`: o ARN do armazenamento de identidades do Centro de Identidade do IAM em nome do qual a chamada foi feita.

Opcional: True

`credentialId`

O ID da credencial da solicitação. Isso só é definido quando o chamador usa um token portador, como um token de acesso autorizado do Centro de Identidade do IAM.

Opcional: True

`webIdFederationData`

Se a solicitação foi feita com credenciais de segurança temporárias obtidas por federação de identidades da Web, `webIdFederationData` lista informações sobre o provedor de identidade.

Esse elemento tem os seguintes atributos:

- `federatedProvider` — O nome do principal do provedor de identidade (por exemplo, `www.amazon.com` para o Login with Amazon ou `accounts.google.com` no Google).
- `attributes` — O ID da aplicação e o ID do usuário como informados pelo provedor (por exemplo, `www.amazon.com:app_id` e `www.amazon.com:user_id` para o Login with Amazon).

> **Note**
>
> A omissão desse campo ou a presença desse campo com um valor vazio significa que não há informações sobre o provedor de identidade.

Opcional: True

Valores para AWS STS APIs com SAML e federação de identidade da web

AWS CloudTrail suporta chamadas de API logging AWS Security Token Service (AWS STS) feitas com Security Assertion Markup Language (SAML) e federação de identidade da web. Quando um usuário faz uma chamada para as `AssumeRoleWithWebIdentity`APIs `AssumeRoleWithSAML`e, CloudTrail grava a chamada e entrega o evento ao seu bucket do Amazon S3.

O elemento `userIdentity` para essas APIs contém os valores a seguir.

`type`

O tipo de identidade.

- `SAMLUser` – A solicitação foi feita com declaração do SAML.
- `WebIdentityUser` – A solicitação foi feita por um provedor de federação de identidades da web.

`principalId`

Um identificador exclusivo para a entidade que fez a chamada.

- Para `SAMLUser`, é uma combinação das chaves `saml:namequalifier` e `saml:sub`.
- Para `WebIdentityUser`, é uma combinação de emissor, ID da aplicação e ID do usuário.

`userName`

O nome da identidade que fez a chamada.

- Para `SAMLUser`, é a chave `saml:sub`.
- Para `WebIdentityUser`, é o ID do usuário.

`identityProvider`

O nome do principal do provedor de identidade externo. Esse campo aparece somente para os tipos `SAMLUser` ou `WebIdentityUser`.

- Para `SAMLUser`, é a chave `saml:namequalifier` da declaração do SAML.
- Para `WebIdentityUser`, é o nome do emissor do provedor de federação de identidades da web. Pode ser um provedor que você configurou, como:
  - `cognito-identity.amazon.com` para Amazon Cognito
  - `www.amazon.com` para o Login with Amazon
  - `accounts.google.com` para o Google
  - `graph.facebook.com` para o Facebook

Veja a seguir um exemplo de elemento `userIdentity` para a ação `AssumeRoleWithWebIdentity`.

```
"userIdentity": {
    "type": "WebIdentityUser",
    "principalId": "accounts.google.com:application-id.apps.googleusercontent.com:user-id",
    "userName": "user-id",
    "identityProvider": "accounts.google.com"
  }
```

Por exemplo, registros de como o `userIdentity` elemento aparece `SAMLUser` e `WebIdentityUser` digita, consulte Registro de chamadas de IAM e AWS STS API com AWS CloudTrail.

AWS STS identidade de origem

Um administrador do IAM pode configurar AWS Security Token Service para exigir que os usuários especifiquem sua identidade ao usarem credenciais temporárias para assumir funções. O campo `sourceIdentity` ocorre em eventos quando os usuários assumem um perfil do IAM ou executam qualquer ação com a função assumida.

O campo `sourceIdentity` identifica a identidade do usuário original que faz a solicitação. Ele identifica se a identidade desse usuário é um usuário do IAM, uma função do IAM, um usuário autenticado usando federação baseada em SAML ou um usuário autenticado usando federação de identidades da Web compatível com OpenID Connect (OIDC). Depois que o administrador do IAM configura AWS STS, CloudTrail registra as `sourceIdentity` informações nos seguintes eventos e locais no registro do evento:

- As `AssumeRoleWithWebIdentity` chamadas AWS STS `AssumeRoleAssumeRoleWithSAML`,, ou que uma identidade de usuário faz quando assume uma função. `sourceIdentity`é encontrado no `requestParameters` bloco das AWS STS chamadas.
- As `AssumeRoleWithWebIdentity` chamadas AWS STS `AssumeRoleAssumeRoleWithSAML`,, ou que uma identidade de usuário faz se usa uma função para assumir outra função, conhecidas como encadeamento de funções. `sourceIdentity`é encontrado no `requestParameters` bloco das AWS STS chamadas.
- A API AWS de serviço chama o que a identidade do usuário faz ao assumir uma função e usar as credenciais temporárias atribuídas por. AWS STS Em eventos da API de serviço, a `sourceIdentity` é encontrada no bloco `sessionContext`. Por exemplo, se uma identidade de usuário criar um novo bucket do S3, a `sourceIdentity` ocorrerá na `sessionContext` bloco do evento `CreateBucket`.

Para obter mais informações sobre como configurar AWS STS para coletar informações de identidade de origem, consulte Monitorar e controlar ações realizadas com funções assumidas no Guia do usuário do IAM. Para obter mais informações sobre AWS STS eventos registrados CloudTrail, consulte Registrar chamadas de IAM e AWS STS API AWS CloudTrail no Guia do usuário do IAM.

Veja a seguir snippets de exemplo de eventos que mostram o campo `sourceIdentity`.

Exemplo da seção **`requestParameters`**

No exemplo de trecho de evento a seguir, um usuário faz uma AWS STS `AssumeRole` solicitação e define uma identidade de origem, representada aqui por. *`source-identity-value-set`* O usuário assume uma função representada pelo ARN da função `arn:aws:iam::123456789012:role/Assumed_Role`. O campo `sourceIdentity` está no bloco do evento `requestParameters`.

```
"eventVersion": "1.05",
    "userIdentity": {
        "type": "AWSAccount",
        "principalId": "AIDAJ45Q7YFFAREXAMPLE",
        "accountId": "123456789012"
    },
    "eventTime": "2020-04-02T18:20:53Z",
    "eventSource": "sts.amazonaws.com",
    "eventName": "AssumeRole",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "203.0.113.64",
    "userAgent": "aws-cli/1.16.96 Python/3.6.0 Windows/10 botocore/1.12.86",
    "requestParameters": {
        "roleArn": "arn:aws:iam::123456789012:role/Assumed_Role",
        "roleSessionName": "Test1",
        "sourceIdentity": "source-identity-value-set",
    },
```

Exemplo da seção **`responseElements`**

No exemplo de trecho de evento a seguir, um usuário faz uma AWS STS `AssumeRole` solicitação para assumir uma função chamada `Developer_Role` e define uma identidade de origem. `Admin` O usuário assume uma função representada pelo ARN da função `arn:aws:iam::111122223333:role/Developer_Role`. O campo `sourceIdentity` é exibido nos blocos de evento `requestParameters` e `responseElements`. As credenciais temporárias usadas para assumir a função, a string de token de sessão e o ID da função assumida, o nome da sessão e o ARN da sessão são mostrados no bloco `responseElements`, junto da identidade da fonte.

```
    "requestParameters": {
        "roleArn": "arn:aws:iam::111122223333:role/Developer_Role",
        "roleSessionName": "Session_Name",
        "sourceIdentity": "Admin"
    },
    "responseElements": {
```

```
        "credentials": {
            "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
            "expiration": "Jan 22, 2021 12:46:28 AM",
            "sessionToken": "XXYYaz...
                             EXAMPLE_SESSION_TOKEN
                             XXyYaZAz"
        },
        "assumedRoleUser": {
            "assumedRoleId": "AROACKCEVSQ6C2EXAMPLE:Session_Name",
            "arn": "arn:aws:sts::111122223333:assumed-role/Developer_Role/Session_Name"
        },
        "sourceIdentity": "Admin"
    }
...
```

Exemplo da seção **`sessionContext`**

No exemplo de trecho de evento a seguir, um usuário está assumindo uma função chamada `DevRole` para chamar uma AWS API de serviço. O usuário define uma identidade de origem, representada aqui por *`source-identity-value-set`*. O campo `sourceIdentity` está no bloco `sessionContext`, dentro do bloco do evento `userIdentity`.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAJ45Q7YFFAREXAMPLE: Dev1",
    "arn": "arn: aws: sts: : 123456789012: assumed-role/DevRole/Dev1",
    "accountId": "123456789012",
    "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAJ45Q7YFFAREXAMPLE",
        "arn": "arn: aws: iam: : 123456789012: role/DevRole",
        "accountId": "123456789012",
        "userName": "DevRole"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-02-21T23: 46: 28Z"
      },
```

```
      "sourceIdentity": "source-identity-value-set"
    }
  }
}
```

CloudTrail **`insightDetails`**Elemento Insights

AWS CloudTrail Os registros de eventos do Insights incluem campos que são diferentes de outros CloudTrail eventos em sua estrutura JSON, às vezes chamados de carga útil. Um registro de evento do CloudTrail Insights inclui um `insightDetails` bloco que contém informações sobre os acionadores subjacentes de um evento do Insights, como fonte do evento, identidades do usuário, agentes do usuário, médias históricas ou linhas de base, estatísticas, nome da API e se o evento é o início ou o fim do evento do Insights. O bloco do `insightDetails` contém as informações a seguir.

- **`state`** - Se o evento é o evento inicial ou final do Insights. O valor pode ser `Start` ou `End`.

  Desde: 1.07

  Opcional: False

- **`eventSource`**- O endpoint do AWS serviço que foi a fonte da atividade incomum, como`ec2.amazonaws.com`.

  Desde: 1.07

  Opcional: False

- **`eventName`** - O nome do evento do Insights, geralmente o nome da API que foi a fonte da atividade incomum.

  Desde: 1.07

  Opcional: False

- **`insightType`** - O tipo de evento do Insights. Esse valor pode ser `ApiCallRateInsight`, `ApiErrorRateInsight` ou os dois.

  Desde: 1.07

  Opcional: False

- **`insightContext`** -

Informações sobre as AWS ferramentas (chamadas de agentes de usuário), usuários e funções do IAM (chamados de identidades de usuário) e códigos de erro associados aos eventos CloudTrail analisados para gerar o evento Insights. Este elemento também inclui estatísticas que mostram como a atividade incomum em um evento do Insights se compara às atividades de linha de base, ou normais.

Desde: 1.07

Opcional: False

- **`statistics`** - Inclui dados sobre a linha de base ou a taxa média típica de chamadas para a API do assunto de uma conta, conforme medida durante o período da linha de base, a taxa média de chamadas que acionou o evento do Insights no primeiro minuto do evento do Insights, a duração, em minutos, do evento do Insights e a duração, em minutos, do período de medição da linha de base.

  Desde: 1.07

  Opcional: False

  - **`baseline`** - O número médio de chamadas de API por minuto durante a duração da linha de base na API de assunto do evento do Insights para a conta, calculado ao longo dos sete dias anteriores ao início do evento do Insights.

    Desde: 1.07

    Opcional: False

  - **`insight`** -

    Para um evento inicial do Insights, esse valor é o número médio de chamadas de API por minuto durante o início da atividade incomum. Para um evento de término do Insights, esse valor é o número médio de chamadas de API por minuto sobre a duração da atividade incomum.

    Desde: 1.07

    Opcional: False

  - **`insightDuration`**: a duração, em minutos, de um evento do Insights (o período do início ao fim da atividade incomum da API de assunto). O `insightDuration` somente ocorre em eventos do Insights de término.

Desde: 1.07

Opcional: False

- **`baselineDuration`**: a duração, em minutos, do período da linha de base (o período em que a atividade normal é medida na API de assunto). `baselineDuration` é, no mínimo, sete dias (10.080 minutos) anteriores a um evento do Insights. Esse campo ocorre em eventos de início e término do Insights. A hora de término do `baselineDuration` é sempre o início de um evento do Insights.

  Desde: 1.07

  Opcional: False

- **`attributions`**: esse bloco inclui informações sobre as identidades de usuário, agentes de usuário e códigos de erro correlacionados com atividades incomuns e de linha de base. Um máximo de cinco identidades de usuário, cinco agentes de usuário e cinco códigos de erro são capturados em um bloco `attributions` de evento do Insights, ordenados por uma média da contagem de atividade, em ordem decrescente do mais alto para o mais baixo.

  Desde: 1.07

  Opcional: True

  - **`attribute`**: contém o tipo de atributo. Os valores podem ser `userIdentityArn`, `userAgent` ou `errorCode`.
    - **`userIdentityArn`**- Um bloco que mostra até os cinco principais AWS usuários ou funções do IAM que contribuíram para chamadas ou erros de API durante atividades incomuns e períodos de referência. Veja também `userIdentity` em CloudTrail conteúdo do registro.

      Desde: 1.07

      Opcional: False

      - **`insight`**: um bloco que mostra até os cinco principais ARNs de identidade de usuário que contribuíram para as chamadas de API feitas durante o período de atividade incomum, em ordem decrescente do maior número de chamadas de API para o menor. Ele também mostra o número médio de chamadas de API feitas pelas identidades de usuário durante o período de atividade incomum.

        Desde: 1.07

Opcional: False

- **`value`**: o ARN de uma das cinco principais identidades de usuário que contribuíram para as chamadas de API feitas durante o período de atividade incomum.

  Desde: 1.07

  Opcional: False

- **`average`** - O número de chamadas de API por minuto durante o período de atividade incomum para a identidade do usuário no campo`value`.

  Desde: 1.07

  Opcional: False

- **`baseline`** - Um bloco que mostra até os cinco principais ARNs de identidade de usuário que mais contribuíram para as chamadas de API feitas durante o período normal de atividade. Ele também mostra o número médio de chamadas de API ou erros registrados pelas identidades de usuário durante o período normal de atividade.

  Desde: 1.07

  Opcional: False

  - **`value`** - O ARN de uma das cinco principais identidades de usuário que contribuíram para as chamadas de API feitas durante o período normal de atividade.

    Desde: 1.07

    Opcional: False

  - **`average`** - A média histórica de chamadas de API por minuto durante os sete dias anteriores à hora de início da atividade do Insights para a identidade do usuário no campo`value`.

    Desde: 1.07

    Opcional: False

- **`userAgent`**- Um bloco que mostra até as cinco principais AWS ferramentas pelas quais a identidade do usuário contribuiu para as chamadas de API durante os períodos incomuns de atividade e linha de base. Essas ferramentas incluem o AWS Management Console, AWS CLI, ou os AWS SDKs. Veja também `userAgent` em CloudTrail conteúdo do registro.

Desde: 1.07

Opcional: False

- **`insight`**: um bloco que mostra até os cinco principais agentes de usuário que contribuíram para as chamadas de API feitas durante o período de atividade incomum, em ordem decrescente do maior número de chamadas de API para o menor. Ele também mostra o número médio de chamadas de API ou erros registrados pelos agentes do usuário durante o período de atividade incomum.

  Desde: 1.07

  Opcional: False

  - **`value`**: um dos cinco principais agentes que contribuíram para as chamadas de API feitas durante o período de atividade incomum.

    Desde: 1.07

    Opcional: False

  - **`average`** - O número de chamadas de API ou erros registrados por minuto durante o período de atividade incomum para o agente do usuário no campo`value`.

    Desde: 1.07

    Opcional: False

- **`baseline`**: um bloco que mostra até os cinco principais agentes do usuário que mais contribuíram para as chamadas de API feitas durante o período normal de atividade. Ele também mostra o número médio de chamadas de API ou erros registrados pelos agentes do usuário durante o período normal de atividade.

  Desde: 1.07

  Opcional: False

  - **`value`** - Um dos cinco principais agentes do usuários que contribuíram para as chamadas de API ou erros registrados durante o período de atividade normal.

    Desde: 1.07

    Opcional: False

- **`average`** - A média histórica de chamadas de API ou erros por minuto durante os sete dias anteriores à hora de início da atividade do Insights para o agente do usuário no campo`value`.

  Desde: 1.07

  Opcional: False

- **`errorCode`**: um bloco que mostra até os cinco principais códigos de erro que ocorreram em chamadas de API feitas durante a atividade incomum e períodos de linha de base, em ordem decrescente do maior número de chamadas de API para o menor. Veja também `errorCode` em CloudTrail conteúdo do registro.

  Desde: 1.07

  Opcional: False

  - **`insight`**: um bloco que mostra até os cinco principais códigos de erro que ocorreram em chamadas de API durante o período de atividade incomum, em ordem decrescente do maior número de chamadas de API associadas para o menor. Ele também mostra o número médio de chamadas de API nas quais os erros ocorreram durante o período de atividade incomum.

    Desde: 1.07

    Opcional: False

    - **`value`**: um dos cinco principais códigos de erro que ocorreram nas chamadas de API feitas durante o período de atividade incomum, como `AccessDeniedException`.

      Se nenhuma das chamadas que acionou o evento do Insights tiver resultado em erros, esse valor será `null`.

      Desde: 1.07

      Opcional: False

    - **`average`**: o número de chamadas de API por minuto durante o período do código de erro no campo `value`.

      Se o valor do código de erro for `null` e não houver outros códigos de erro no `insight`, o valor de `average` será igual ao do bloco `statistics` do evento do Insights em geral.

Desde: 1.07

Opcional: False

- **`baseline`**: um bloco que mostra até os cinco principais códigos que ocorreram nas chamadas de API feitas durante o período normal de atividade. Ele também mostra o número médio de chamadas de API feitas pelos agentes do usuário durante o período normal de atividade.

  Desde: 1.07

  Opcional: False

  - **`value`**: um dos cinco principais códigos de erro que ocorreram nas chamadas de API feitas durante o período de atividade normal, como `AccessDeniedException`.

    Desde: 1.07

    Opcional: False

  - **`average`** - A média histórica de chamadas de API ou erros por minuto durante os sete dias anteriores à hora de início da atividade do Insights para o código de erro no campo`value`.

    Desde: 1.07

    Opcional: False

Exemplo do bloco **`insightDetails`**

O exemplo a seguir mostra um bloco `insightDetails` de evento do Insights que ocorreu quando a API do Application Auto Scaling `CompleteLifecycleAction` foi chamada um número incomum de vezes. Para obter um exemplo de um evento completo do Insights, consulte Eventos do Insights.

Este é um exemplo de um evento inicial do Insights, indicado por `"state": "Start"`. As principais identidades de usuário que chamaram as APIs associadas ao evento do Insights `CodeDeployRole1`, `CodeDeployRole2` e `CodeDeployRole3` são mostrados no bloco `attributions`, juntamente com suas taxas médias de chamada de API para este evento do Insights e a linha de base para a função do `CodeDeployRole1`. O `attributions` bloco também mostra que o agente do usuário é`codedeploy.amazonaws.com`, o que significa que as principais identidades de usuário usaram o AWS CodeDeploy console para executar as chamadas de API.

Como não há códigos de erro associados aos eventos que foram analisados para gerar o evento do Insights (o valor é `null`), a média `insight` para o código de erro é a mesma que a média geral do `insight` para todo o evento do Insights, mostrado no bloco `statistics`.


```
          "insightDetails": {
            "state": "Start",
            "eventSource": "autoscaling.amazonaws.com",
            "eventName": "CompleteLifecycleAction",
            "insightType": "ApiCallRateInsight",
            "insightContext": {
              "statistics": {
                "baseline": {
                  "average": 0.0000882145
                },
                "insight": {
                  "average": 0.6
                },
                "insightDuration": 5,
                "baselineDuration": 11336
              },
              "attributions": [
                {
                  "attribute": "userIdentityArn",
                  "insight": [
                    {
                      "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole1",
                      "average": 0.2
                    },
                    {
                      "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole2",
                      "average": 0.2
                    },
                    {
                      "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole3",
                      "average": 0.2
                    }
                  ],
                  "baseline": [
                    {
```

```
                    "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole1",
                    "average": 0.0000882145
                  }
                ]
              },
              {
                "attribute": "userAgent",
                "insight": [
                  {
                    "value": "codedeploy.amazonaws.com",
                    "average": 0.6
                  }
                ],
                "baseline": [
                  {
                    "value": "codedeploy.amazonaws.com",
                    "average": 0.0000882145
                  }
                ]
              },
              {
                "attribute": "errorCode",
                "insight": [
                  {
                    "value": "null",
                    "average": 0.6
                  }
                ],
                "baseline": [
                  {
                    "value": "null",
                    "average": 0.0000882145
                  }
                ]
              }
            ]
          }
        }
```

Eventos não relacionados à API capturados por CloudTrail

Além de registrar chamadas de AWS API, CloudTrail captura outros eventos relacionados que podem ter um impacto na segurança ou na conformidade da sua AWS conta ou que podem ajudá-lo a solucionar problemas operacionais.

Tópicos

AWS eventos de serviço

CloudTrail suporta o registro de eventos de serviços não relacionados à API. Esses eventos são criados por AWS serviços, mas não são acionados diretamente por uma solicitação a uma AWS API pública. Para esses eventos, o campo `eventType` é `AwsServiceEvent`.

Veja a seguir um exemplo de cenário de um evento de AWS serviço quando uma chave gerenciada pelo cliente é automaticamente girada em AWS Key Management Service (AWS KMS). Para obter mais informações sobre a alternância de chaves do KMS, consulte Alternância de chaves do KMS.


```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "accountId": "123456789012",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2019-06-02T00:06:08Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "RotateKey",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "234f004b-EXAMPLE",
    "readOnly": false,
    "resources": [
        {
            "ARN": "arn:aws:kms:us-east-2:123456789012:key/7944f0ec-EXAMPLE",
            "accountId": "123456789012",
```

```
            "type": "AWS::KMS::Key"
        }
    ],
    "eventType": "AwsServiceEvent",
    "recipientAccountId": "123456789012",
    "serviceEventDetails": {
        "keyId": "7944f0ec-EXAMPLE"
    }
}
```

AWS Management Console eventos de login

CloudTrail registra tentativas de entrar no AWS Management Console, nos Fóruns de AWS Discussão e no AWS Support Center. Todos os eventos de login do usuário raiz e do usuário do IAM, bem como todos os eventos de login do usuário federado, geram registros em arquivos de log. CloudTrail Para obter mais informações sobre como encontrar e visualizar logs, consulte Encontrando seus arquivos CloudTrail de log e Baixando seus arquivos CloudTrail de log.

> **Note**
>
> A região registrada em um `ConsoleLogin` evento varia de acordo com o tipo de usuário e se você usa um endpoint global ou regional para fazer login.
>
> - Se você fizer login como usuário root, CloudTrail registrará o evento em us-east-1.
> - Se você fizer login com um usuário do IAM e usar o endpoint global, CloudTrail registrará a região do `ConsoleLogin` evento da seguinte forma:
>   - Se um cookie de alias de conta estiver presente no navegador, CloudTrail registra o `ConsoleLogin` evento em uma das seguintes regiões: us-east-2, eu-north-1 ou ap-southeast-2. Isso ocorre porque o proxy do console redireciona o usuário com base na latência do local de login do usuário.
>   - Se um cookie de alias de conta não estiver presente no navegador, CloudTrail registra o `ConsoleLogin` evento em us-east-1. Isso ocorre porque o proxy do console redireciona de volta para o login global.
> - Se você fizer login com um usuário do IAM e usar um endpoint regional, CloudTrail registra o `ConsoleLogin` evento na região apropriada para o endpoint. Para obter mais informações sobre Início de Sessão da AWS endpoints, consulte Início de Sessão da AWS endpoints e cotas.

Tópicos

Exemplo de registros de eventos para usuários do IAM

Os exemplos a seguir mostram registros de eventos para vários cenários de login de usuário do IAM.

Tópicos

Usuário do IAM, login bem-sucedido sem MFA

O registro a seguir mostra que um usuário chamado fez login `Anaya` com sucesso no AWS Management Console sem usar a autenticação multifator (MFA).


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLE6E4XEGITWATV6R",
        "arn": "arn:aws:iam::999999999999:user/Anaya",
        "accountId": "999999999999",
        "userName": "Anaya"
    },
    "eventTime": "2023-07-19T21:44:40Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101
 Firefox/102.0",
    "requestParameters": null,
```

```
    "responseElements": {
        "ConsoleLogin": "Success"
    },
    "additionalEventData": {
        "LoginTo": "https://console.aws.amazon.com/console/home?hashArgs=
%23&isauthcode=true&state=hashArgsFromTB_us-east-1_examplee9aba7f8",
        "MobileVersion": "No",
        "MFAUsed": "No"
    },
    "eventID": "e1bf1000-86a4-4a78-81d7-EXAMPLE83102",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "999999999999",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "us-east-1.signin.aws.amazon.com"
    }
}
```

Usuário do IAM, login bem-sucedido com MFA

O registro a seguir mostra que um usuário do IAM chamado `Anaya` fez login com sucesso no AWS Management Console usando a autenticação multifator (MFA).

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLE6E4XEGITWATV6R",
        "arn": "arn:aws:iam::999999999999:user/Anaya",
        "accountId": "999999999999",
        "userName": "Anaya"
    },
    "eventTime": "2023-07-19T22:01:30Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101
 Firefox/102.0",
```

```
    "requestParameters": null,
    "responseElements": {
        "ConsoleLogin": "Success"
    },
    "additionalEventData": {
        "LoginTo": "https://console.aws.amazon.com/console/home?hashArgs=
%23&isauthcode=true&state=hashArgsFromTB_us-east-1_examplebde32f3c9",
        "MobileVersion": "No",
        "MFAIdentifier": "arn:aws:iam::999999999999:mfa/mfa-device",
        "MFAUsed": "Yes"
    },
    "eventID": "e1f76697-5beb-46e8-9cfc-EXAMPLEbde31",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "999999999999",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "us-east-1.signin.aws.amazon.com"
    }
}
```

Usuário do IAM, login sem êxito

O registro a seguir mostra uma tentativa de login malsucedida de um usuário do IAM chamado `Paulo`.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLE6E4XEGITWATV6R",
        "accountId": "123456789012",
        "accessKeyId": "",
        "userName": "Paulo"
    },
    "eventTime": "2023-07-19T22:01:20Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
```

```
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101
 Firefox/102.0",
    "errorMessage": "Failed authentication",
    "requestParameters": null,
    "responseElements": {
        "ConsoleLogin": "Failure"
    },
    "additionalEventData": {
        "LoginTo": "https://console.aws.amazon.com/console/home?hashArgs=
%23&isauthcode=true&state=hashArgsFromTB_us-east-1_examplebde32f3c9",
        "MobileVersion": "No",
        "MFAUsed": "Yes"
    },
    "eventID": "66c97220-2b7d-43b6-a7a0-EXAMPLEbae9c",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "us-east-1.signin.aws.amazon.com"
    }
}
```

Usuário do IAM, verificações de processo de login para MFA (um só tipo de dispositivo de MFA)

A tabela a seguir mostra que o processo de login verificou se a autenticação multifator (MFA) é necessária para um usuário do IAM durante o login. Neste exemplo, o valor de `mfaType` é `U2F MFA`, o que indica que o usuário do IAM habilitou somente um dispositivo de MFA ou vários dispositivos de MFA do mesmo tipo (`U2F MFA`).

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLE6E4XEGITWATV6R",
        "accountId": "123456789012",
        "accessKeyId": "",
        "userName": "Alice"
    },
    "eventTime": "2023-07-19T22:01:26Z",
```

```
    "eventSource": "signin.amazonaws.com",
    "eventName": "CheckMfa",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101
 Firefox/102.0",
    "requestParameters": null,
    "responseElements": {
        "CheckMfa": "Success"
    },
    "additionalEventData": {
        "MfaType": "Virtual MFA"
    },
    "eventID": "7d8a0746-b2e7-44f5-9917-EXAMPLEfb77c",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "us-east-1.signin.aws.amazon.com"
    }
}
```

Usuário do IAM, verificações de processo de login para MFA (vários tipos de dispositivos de MFA)

A tabela a seguir mostra que o processo de login verificou se a autenticação multifator (MFA) é necessária para um usuário do IAM durante o login. Neste exemplo, o valor de `mfaType` é `Multiple MFA Devices`, indicando que o usuário do IAM habilitou vários tipos de dispositivos de MFA.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLE6E4XEGITWATV6R",
        "accountId": "123456789012",
        "accessKeyId": "",
        "userName": "Mary"
    },
    "eventTime": "2023-07-19T23:10:09Z",
```

```
    "eventSource": "signin.amazonaws.com",
    "eventName": "CheckMfa",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101
 Firefox/102.0",
    "requestParameters": null,
    "responseElements": {
        "CheckMfa": "Success"
    },
    "additionalEventData": {
        "MfaType": "Multiple MFA Devices"
    },
    "eventID": "19bd1a1c-76b1-4806-9d8f-EXAMPLE02a96",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "signin.aws.amazon.com"
    }
}
```

Exemplo de registros de eventos de usuários raiz

Os exemplos a seguir mostram registros de eventos para vários cenários de login do usuário `root`. Quando você faz login usando o usuário root, CloudTrail registra o `ConsoleLogin` evento em us-east-1.

Tópicos

- Usuário raiz, login bem-sucedido sem MFA
- Usuário raiz, login bem-sucedido com MFA
- Usuário raiz, login com êxito
- Usuário raiz, MFA alterado
- Usuário raiz, senha alterada

Usuário raiz, login bem-sucedido sem MFA

O exemplo a seguir mostra um evento de login bem-sucedido para um usuário raiz que não usa autenticação multifator (MFA).


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Root",
        "principalId": "111122223333",
        "arn": "arn:aws:iam::111122223333:root",
        "accountId": "111122223333",
        "accessKeyId": ""
    },
    "eventTime": "2023-07-12T13:35:31Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/114.0.0.0 Safari/537.36",
    "requestParameters": null,
    "responseElements": {
        "ConsoleLogin": "Success"
    },
    "additionalEventData": {
        "LoginTo": "https://console.aws.amazon.com/console/home?hashArgs=
%23&isauthcode=true&nc2=h_ct&src=header-signin&state=hashArgsFromTB_ap-
southeast-2_example80afacd389",
        "MobileVersion": "No",
        "MFAUsed": "No"
    },
    "eventID": "4217cc13-7328-4820-a90c-EXAMPLE8002e6",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "signin.aws.amazon.com"
    }
```

```
}
```

Usuário raiz, login bem-sucedido com MFA

O exemplo a seguir mostra um evento de login bem-sucedido para um usuário raiz que usa autenticação multifator (MFA).


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Root",
        "principalId": "444455556666",
        "arn": "arn:aws:iam::444455556666:root",
        "accountId": "444455556666",
        "accessKeyId": ""
    },
    "eventTime": "2023-07-13T03:04:43Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
 Gecko) Chrome/114.0.0.0 Safari/537.36",
    "requestParameters": null,
    "responseElements": {
        "ConsoleLogin": "Success"
    },
    "additionalEventData": {
        "LoginTo": "https://ap-southeast-1.console.aws.amazon.com/ec2/home?region=ap-
southeast-1&state=hashArgs%23Instances%3Av%3D3%3B%24case%3Dtags%3Atrue%255C%2Cclient
%3Afalse%3B%24regex%3Dtags%3Afalse%255C%2Cclient%3Afalse&isauthcode=true",
        "MobileVersion": "No",
        "MFAIdentifier": "arn:aws:iam::444455556666:mfa/root-account-mfa-device",
        "MFAUsed": "Yes"
    },
    "eventID": "e0176723-ea76-4275-83a3-EXAMPLEf03fb",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "444455556666",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
```

```
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "signin.aws.amazon.com"
    }
}
```

Usuário raiz, login com êxito

A tabela a seguir mostra um evento de login sem êxito de um usuário raiz que não usa MFA.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Root",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:root",
        "accountId": "123456789012",
        "accessKeyId": ""
    },
    "eventTime": "2023-07-16T04:33:40Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/111.0.0.0 Safari/537.36",
    "errorMessage": "Failed authentication",
    "requestParameters": null,
    "responseElements": {
        "ConsoleLogin": "Failure"
    },
    "additionalEventData": {
        "LoginTo": "https://us-east-1.console.aws.amazon.com/billing/home?region=us-
east-1&state=hashArgs%23%2Faccount&isauthcode=true",
        "MobileVersion": "No",
        "MFAUsed": "No"
    },
    "eventID": "f28d4329-5050-480b-8de0-EXAMPLE07329",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
```

```
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "signin.aws.amazon.com"
    }
}
```

Usuário raiz, MFA alterado

Veja a seguir um exemplo de evento de um usuário raiz alterando as configurações de autenticação multifator (MFA).

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Root",
        "principalId": "111122223333",
        "arn": "arn:aws:iam::111122223333:root",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE4XX3IEV4PFQTH",
        "userName": "AWS ROOT USER",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-07-15T03:51:12Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-15T04:37:08Z",
    "eventSource": "iam.amazonaws.com",
    "eventName": "EnableMFADevice",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/111.0.0.0 Safari/537.36",
    "requestParameters": {
        "userName": "AWS ROOT USER",
        "serialNumber": "arn:aws:iam::111122223333:mfa/root-account-mfa-device"
    },
    "responseElements": null,
    "requestID": "9b45cd4c-a598-41e7-9170-EXAMPLE535f0",
    "eventID": "b4f18d55-d36f-49a0-afcb-EXAMPLEc026b",
    "readOnly": false,
```

```
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management",
    "sessionCredentialFromConsole": "true"
}
```

Usuário raiz, senha alterada

Veja a seguir um exemplo de evento de um usuário raiz alterando sua senha.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Root",
        "principalId": "444455556666",
        "arn": "arn:aws:iam::444455556666:root",
        "accountId": "444455556666",
        "accessKeyId": "EXAMPLEAOTKEG44KPW5P",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-11-25T13:01:14Z",
                "mfaAuthenticated": "false"
             }
        }
    },
    "eventTime": "2022-11-25T13:01:14Z",
    "eventSource": "iam.amazonaws.com",
    "eventName": "ChangePassword",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/111.0.0.0 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "c64254c2-e4ff-49c0-900e-EXAMPLE9e6d2",
    "eventID": "d059176c-4f4d-4a9e-b8d7-EXAMPLE2b7b3",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "444455556666",
    "eventCategory": "Management"
```

```
}
```

Exemplo de registros de eventos para usuários federados

Os exemplos a seguir mostram registros de eventos para usuários federados. Os usuários federados recebem credenciais de segurança temporárias para acessar AWS recursos por meio de uma `AssumeRole`solicitação.

A seguir é mostrado um exemplo de evento para uma solicitação de criptografia de federação. O ID da chave de acesso original é fornecido no campo `accessKeyId` do elemento `userIdentity`. O campo `accessKeyId` em `responseElements` conterá um novo ID de chave de acesso se a `sessionDuration` solicitada for passada na solicitação de criptografia. Caso contrário, ele conterá o valor do ID da chave de acesso original.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "EXAMPLEUU4MH7OYK5ZCOA:JohnDoe",
        "arn": "arn:aws:sts::123456789012:assumed-role/roleName/JohnDoe",
        "accountId": "123456789012",
        "accessKeyId": "originalAccessKeyID",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "EXAMPLEUU4MH7OYK5ZCOA",
                "arn": "arn:aws:iam::123456789012:role/roleName",
                "accountId": "123456789012",
                "userName": "roleName"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-09-25T21:30:39Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-09-25T21:30:39Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "GetSigninToken",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
```

```
    "userAgent": "Java/1.8.0_382",
    "requestParameters": null,
    "responseElements": {
        "credentials": {
            "accessKeyId": "accessKeyID"
        },
        "GetSigninToken": "Success"
    },
    "additionalEventData": {
        "MobileVersion": "No",
        "MFAUsed": "No"
    },
    "eventID": "1d66615b-a417-40da-a38e-EXAMPLE8c89b",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "us-east-1.signin.aws.amazon.com"
    }
}
```

O exemplo a seguir mostra um evento de login bem-sucedido para um usuário federado que não usa autenticação multifator (MFA).

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "EXAMPLEPHCNW7ZCASLJOH:JohnDoe",
        "arn": "arn:aws:sts::123456789012:assumed-role/RoleName/JohnDoe",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "EXAMPLEPHCNW7ZCASLJOH",
                "arn": "arn:aws:iam::123456789012:role/RoleName",
                "accountId": "123456789012",
                "userName": "RoleName"
```

```
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-09-22T16:15:47Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-09-22T16:15:47Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36",
    "requestParameters": null,
    "responseElements": {
        "ConsoleLogin": "Success"
    },
    "additionalEventData": {
        "MobileVersion": "No",
        "MFAUsed": "No"
    },
    "eventID": "b73f1ec6-c064-4cd3-ba83-EXAMPLE441d7",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "us-east-1.signin.aws.amazon.com"
    }
}
```

Trabalhando com arquivos CloudTrail de log

Você pode realizar tarefas mais avançadas com seus CloudTrail arquivos.

- Crie várias trilhas por região.
- Monitore os arquivos de CloudTrail log enviando-os para o CloudWatch Logs.
- Compartilhe arquivos de log entre contas.
- Use a Biblioteca AWS CloudTrail de Processamento para escrever aplicativos de processamento de log em Java.
- Valide seus arquivos de log para verificar se eles não foram alterados após a entrega. CloudTrail

Quando um evento ocorre em sua conta, CloudTrail avalia se o evento corresponde às configurações de suas trilhas. Somente eventos que correspondam às suas configurações de trilha são entregues ao seu bucket do Amazon S3 e ao grupo de registros do Amazon CloudWatch Logs.

Você pode configurar várias trilhas de maneiras diferentes para que elas processem e registrem somente os eventos que você especificar. Por exemplo, uma trilha pode registrar dados somente leitura e gerenciamento de eventos para que todos os eventos somente leitura sejam entregues a um bucket do S3. Outra trilha pode registrar apenas dados somente gravação e eventos de gerenciamento para que todos os eventos somente gravação sejam fornecidos a um bucket separado do S3.

Você também pode configurar suas trilhas para ter um log de trilha e fornecer todos os eventos de gerenciamento a um bucket do S3 e configurar outra trilha para registrar e fornecer todos os eventos de dados de a outro bucket do S3.

Você pode configurar suas trilhas para registrar o seguinte:

- Eventos de dados: esses eventos fornecem visibilidade nas operações do recurso executadas no recurso ou dentro de um recurso. Elas também são conhecidas como operações de plano de dados.
- Eventos de gerenciamento: os eventos de gerenciamento fornecem visibilidade das operações de gerenciamento que são realizadas nos recursos AWS da sua conta. Elas também são conhecidas como operações de plano de controle. Os eventos de gerenciamento também podem incluir eventos que não são de API que ocorrem na sua conta. Por exemplo, quando um usuário faz login na sua conta, CloudTrail registra o `ConsoleLogin` evento. Para ter mais informações, consulte Eventos não relacionados à API capturados por CloudTrail.

- Eventos do Insights: os eventos do Insights capturam atividades incomuns detectadas em sua conta. Se você tiver eventos do Insights ativados e CloudTrail detectar atividades incomuns, os eventos do Insights serão registrados no bucket do S3 de destino da sua trilha, mas em uma pasta diferente. Você também pode ver o tipo de evento do Insights e o período do incidente ao visualizar os eventos do Insights no CloudTrail console. Ao contrário de outros tipos de eventos capturados em uma CloudTrail trilha, os eventos do Insights são registrados somente quando CloudTrail detectam alterações no uso da API da sua conta que diferem significativamente dos padrões de uso típicos da conta.

  Os eventos do Insights são gerados somente para APIs de gerenciamento. Para ter mais informações, consulte Registrar eventos do Insights.

> **Note**
>
> CloudTrail normalmente entrega registros em uma média de cerca de 5 minutos após uma chamada de API. Desta vez não há garantias. Consulte o Acordo de Nível de Serviço do AWS CloudTrail para obter mais informações.
> Se você configurar incorretamente sua trilha (por exemplo, o bucket do S3 está inacessível), CloudTrail tentará reenviar os arquivos de log para o bucket do S3 por 30 dias, e esses attempted-to-deliver eventos estarão sujeitos às cobranças padrão. CloudTrail Para evitar cobranças em uma trilha mal configurada, você precisa excluir a trilha.

Tópicos

- Recebendo arquivos de CloudTrail log de várias regiões
- Gerenciando a consistência dos dados em CloudTrail
- Monitoramento CloudTrail de arquivos de log com o Amazon CloudWatch Logs
- Recebendo arquivos de CloudTrail log de várias contas
- Compartilhamento CloudTrail de arquivos de log entre AWS contas
- Validando a integridade CloudTrail do arquivo de log
- CloudTrail exemplos de arquivos de log
- Usando a Biblioteca CloudTrail de Processamento

Recebendo arquivos de CloudTrail log de várias regiões

Você pode configurar CloudTrail para entregar arquivos de log de várias regiões para um único bucket do S3 para uma única conta. Por exemplo, você tem uma trilha na região Oeste dos EUA (Oregon) que está configurada para entregar arquivos de log para um bucket do S3 e um grupo de registros de CloudWatch registros. Quando você altera uma trilha existente em uma única região para registrar todas as regiões, CloudTrail registra eventos de todas as regiões que estão em uma única AWS partição na sua conta. CloudTrail entrega arquivos de log para o mesmo bucket do S3 e grupo de CloudWatch registros de registros. Desde CloudTrail que tenha permissões para gravar em um bucket do S3, o bucket de uma trilha multirregional não precisa estar na região de origem da trilha.

Para registrar eventos em todas as regiões em todas as AWS partições da sua conta, crie uma trilha multirregional em cada partição.

No console, por padrão, você cria uma trilha que registra eventos em todas as Regiões da AWS na partição da AWS na qual está trabalhando. Essa é uma prática recomendada. Para registrar eventos em uma única região (não recomendado), use a AWS CLI. Para configurar uma trilha de região única para registrar em log em todas as regiões, é necessário usar o comando AWS CLI.

Para alterar uma trilha existente para que ela se aplique a todas as regiões, adicione a opção `--is-multi-region-trail` ao comando update-trail.

```
aws cloudtrail update-trail --name my-trail --is-multi-region-trail
```

Para confirmar se a trilha agora se aplica a todas as regiões, o elemento `IsMultiRegionTrail` no resultado mostra `true`.

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": false,
    "S3BucketName": "my-bucket"
}
```

> **Note**
>
> Quando uma nova região é iniciada na awspartição, cria CloudTrail automaticamente uma trilha para você na nova região com as mesmas configurações da trilha original.

Para obter mais informações, consulte os seguintes recursos do :

- Trabalhando com CloudTrail trilhas
- CloudTrail Perguntas frequentes

Gerenciando a consistência dos dados em CloudTrail

CloudTrail usa um modelo de computação distribuída chamado consistência eventual. Qualquer alteração que você fizer em sua CloudTrail configuração (ou em outros AWS serviços), incluindo tags usadas no controle de acesso baseado em atributos (ABAC), leva tempo para ficar visível em todos os endpoints possíveis. Parte do atraso resulta do tempo necessário para enviar os dados de servidor para servidor, de zona de replicação para zona de replicação e de região para região em todo o mundo. CloudTrail também usa o cache para melhorar o desempenho, mas em alguns casos isso pode aumentar o tempo. A alteração talvez não fique visível enquanto os dados armazenados em cache anteriormente não atingirem o tempo limite.

Suas aplicações devem ser projetadas para levar em conta esses possíveis atrasos. Garanta que eles funcionem conforme o esperado, mesmo quando uma alteração feita em um local não fique imediatamente visível em outro. Essas mudanças incluem criar ou atualizar trilhas ou armazenamentos de dados de eventos, atualizar seletores de eventos e iniciar ou interromper o registro em log. Quando você cria ou atualiza um armazenamento de dados de trilhas ou eventos, CloudTrail entrega registros ao bucket do S3 ou ao armazenamento de dados de eventos com base na última configuração conhecida até que as alterações se propaguem para todos os locais.

Para obter mais informações sobre como isso afeta outras Serviços da AWS pessoas, consulte os seguintes recursos:

- Amazon DynamoDB: Qual é o modelo de consistência do DynamoDB? nas Perguntas frequentes sobre o DynamoDB e Consistência de leitura no Guia do desenvolvedor do Amazon DynamoDB.
- Amazon EC2: Consistência eventual na Referência de API do Amazon Elastic Compute Cloud.

- Amazon EMR: garantindo a consistência ao usar o Amazon S3 e o MapReduce Amazon Elastic para fluxos de trabalho AWS de ETL no blog de big data.
- AWS Identity and Access Management (IAM): As alterações que eu faço nem sempre são imediatamente visíveis no Guia do usuário do IAM.
- Amazon Redshift: Gerenciamento da consistência de dados no Guia do desenvolvedor de banco de dados do Amazon Redshift.
- Amazon S3: Modelo de consistência de dados do Amazon S3 no Guia do usuário do Amazon Simple Storage Service.

Monitoramento CloudTrail de arquivos de log com o Amazon CloudWatch Logs

Você pode configurar CloudTrail com o CloudWatch Logs para monitorar seus registros de trilhas e ser notificado quando ocorrer uma atividade específica.

1. Configure sua trilha para enviar eventos de registro para o CloudWatch Logs.
2. Defina filtros métricos de CloudWatch registros para avaliar eventos de registro em busca de correspondências em termos, frases ou valores. Por exemplo, você pode monitorar eventos `ConsoleLogin`.
3. Atribua CloudWatch métricas aos filtros métricos.
4. Crie CloudWatch alarmes que sejam acionados de acordo com os limites e períodos de tempo que você especificar. Você pode configurar alertas para enviar notificações quando os alarmes forem acionados. Assim, você poderá realizar uma ação.
5. Você também pode configurar CloudWatch para executar automaticamente uma ação em resposta a um alarme.

Aplica-se o preço padrão da Amazon CloudWatch e do Amazon CloudWatch Logs. Para obter mais informações, consulte Amazon CloudWatch Pricing.

Para obter mais informações sobre as regiões nas quais você pode configurar suas trilhas para enviar CloudWatch registros para Logs, consulte Regiões e cotas do Amazon CloudWatch Logs na Referência AWS geral.

Tópicos

- Envio de eventos para o CloudWatch Logs

- Criação CloudWatch de alarmes para CloudTrail eventos: exemplos
- Parando CloudTrail de enviar eventos para o CloudWatch Logs
- CloudWatch nome do grupo de registros e do fluxo de registros para CloudTrail
- Documento de política de funções CloudTrail para usar CloudWatch registros para monitoramento

Envio de eventos para o CloudWatch Logs

Quando você configura sua trilha para enviar eventos para o CloudWatch Logs, CloudTrail envia somente os eventos que correspondem às suas configurações de trilha. Por exemplo, se você configurar sua trilha para registrar somente eventos de dados, ela enviará eventos de dados somente para seu grupo de CloudWatch registros de registros. CloudTrail suporta o envio de dados, Insights e eventos de gerenciamento para o CloudWatch Logs. Para ter mais informações, consulte Trabalhando com arquivos CloudTrail de log.

> **Note**
>
> Somente a conta de gerenciamento pode configurar um grupo de CloudWatch registros de registros para uma trilha da organização usando o console. O administrador delegado pode configurar um grupo de CloudWatch registros de registros usando as operações AWS CLI ou CloudTrail `CreateTrail` ou `UpdateTrail` da API.

Para enviar eventos para um grupo de CloudWatch registros de registros:

- Verifique se você tem permissões suficientes para criar ou especificar uma função do IAM. Para ter mais informações, consulte Conceder permissão para visualizar e configurar as informações do Amazon CloudWatch Logs no console CloudTrail .
- Se você estiver configurando o grupo de CloudWatch registros de registros usando o AWS CLI, verifique se você tem permissões suficientes para criar um fluxo de CloudWatch registros de registros no grupo de registros especificado e para entregar CloudTrail eventos a esse fluxo de registros. Para ter mais informações, consulte Criar um documento de política.
- Crie uma nova trilha ou especifique uma existente. Para ter mais informações, consulte Criar e atualizar uma trilha com o console.
- Crie um grupo de logs ou especifique um existente.
- Especifique uma função do IAM. Se você estiver modificando uma função do IAM existente de uma trilha da organização, deverá atualizar manualmente a política para permitir o registro da

trilha. Para obter mais informações, consulte este exemplo de política e Criar uma trilha para uma organização.

- Anexe uma política de função ou use a política padrão.

Sumário

Configurando o monitoramento CloudWatch de registros com o console

Você pode usar o AWS Management Console para configurar sua trilha para enviar eventos ao CloudWatch Logs para monitoramento.

Criar um grupo de logs ou especificar um existente

CloudTrail usa um grupo de CloudWatch registros de registros como um endpoint de entrega para eventos de registro. Você pode criar um grupo de logs ou especificar um existente.

Para criar ou especificar um grupo de logs para uma trilha existente

1. Certifique-se de fazer login com um usuário ou função administrativa com permissões suficientes para configurar a integração do CloudWatch Logs. Para ter mais informações, consulte Conceder permissão para visualizar e configurar as informações do Amazon CloudWatch Logs no console CloudTrail .

> **Note**
>
> Somente a conta de gerenciamento pode configurar um grupo de CloudWatch registros de registros para uma trilha da organização usando o console. O administrador delegado pode configurar um grupo de CloudWatch registros de registros usando as operações AWS CLI ou CloudTrail `CreateTrail` ou `UpdateTrail` da API.

2. Abra o CloudTrail console em https://console.aws.amazon.com/cloudtrail/.
3. Escolha o nome da trilha. Se você escolher uma trilha que se aplica a todas as regiões, será redirecionado para a região em que ela foi criada. Você pode criar um grupo de logs ou escolher um existente na mesma região que a trilha.

> **Note**
>
> Uma trilha que se aplica a todas as regiões envia arquivos de log de todas as regiões para o grupo de CloudWatch registros de registros que você especificar.

4. Em CloudWatch Registros, escolha Editar.
5. Em CloudWatch Registros, escolha Ativado.
6. Em Nome do grupo de logs, escolha Novo para criar um novo grupo de logs ou Existente para usar um existente. Se você escolher Novo, CloudTrail especifica um nome para o novo grupo de registros para você ou pode digitar um nome. Para obter mais informações sobre nomenclatura, consulte CloudWatch nome do grupo de registros e do fluxo de registros para CloudTrail.
7. Se escolher Existing (Existente), escolha um grupo de logs na lista suspensa.
8. Em Nome da função, escolha Novo para criar uma nova função do IAM para obter permissões para enviar CloudWatch registros para Logs. Escolha Existing (Existente) para escolher uma função do IAM existente na lista suspensa. A declaração de política para a função nova ou existente é exibida quando você expande Policy document (Documento de política). Para obter mais informações sobre essa função, consulte Documento de política de funções CloudTrail para usar CloudWatch registros para monitoramento.

> **Note**
>
> Quando você configurar uma trilha, você pode escolher um bucket do S3 e um tópico do SNS que pertençam a outra conta. No entanto, se você quiser CloudTrail entregar

eventos a um grupo de CloudWatch registros de registros, deverá escolher um grupo de registros que exista na sua conta atual.

9. Escolha Salvar alterações.

Especificar uma função do IAM

Você pode especificar uma função CloudTrail a ser assumida para entregar eventos ao fluxo de registros.

Para especificar uma função

1. Por padrão, a `CloudTrail_CloudWatchLogs_Role` é especificada para você. A política de função padrão tem as permissões necessárias para criar um fluxo de CloudWatch registros de registros em um grupo de registros especificado por você e para entregar CloudTrail eventos a esse fluxo de registros.

   > **Note**
   >
   > Se você quiser usar essa função para um grupo de logs de uma trilha da organização, deverá modificar manualmente a política após a criação da função. Para obter mais informações, consulte este exemplo de política e Criar uma trilha para uma organização.

   a. Para verificar a função, acesse o AWS Identity and Access Management console em https://console.aws.amazon.com/iam/.
   b. Escolha Funções e, em seguida, escolha a CloudTrail_ CloudWatchLogs _Função.
   c. Na guia Permissões, expanda a política para visualizar seu conteúdo.
2. Você pode especificar outra função, mas deve anexar a política de função necessária à função existente se quiser usá-la para enviar eventos ao CloudWatch Logs. Para ter mais informações, consulte Documento de política de funções CloudTrail para usar CloudWatch registros para monitoramento.

Visualizando eventos no CloudWatch console

Depois de configurar sua trilha para enviar eventos ao seu grupo de CloudWatch registros de registros, você pode ver os eventos no CloudWatch console. CloudTrail normalmente entrega

eventos ao seu grupo de registros em uma média de cerca de 5 minutos após uma chamada de API. Desta vez não há garantias. Consulte o Acordo de Nível de Serviço do AWS CloudTrail para obter mais informações.

Para visualizar eventos no CloudWatch console

1. Abra o CloudWatch console em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação esquerdo, em Logs, escolha Grupos de logs.
3. Escolha o grupo de logs que você especificou para a sua trilha.
4. Escolha o fluxo de logs que deseja visualizar.
5. Para ver os detalhes do evento que sua trilha registrou, escolha um evento.

> **Note**
>
> A coluna Hora (UTC) no CloudWatch console mostra quando o evento foi entregue ao seu grupo de registros. Para ver a hora real em que o evento foi registrado CloudTrail, consulte o `eventTime` campo.

Configurando o monitoramento CloudWatch de registros com o AWS CLI

Você pode usar o AWS CLI to configure CloudTrail para enviar eventos ao CloudWatch Logs para monitoramento.

Criar um grupo de logs

1. Se você não tiver um grupo de registros existente, crie um grupo de CloudWatch registros de registros como um endpoint de entrega para eventos de registro usando o `create-log-group` comando CloudWatch Logs.

   ```
   aws logs create-log-group --log-group-name name
   ```

   O exemplo a seguir cria um grupo de logs chamado `CloudTrail/logs`:

   ```
   aws logs create-log-group --log-group-name CloudTrail/logs
   ```

2. Recupere o grupo de logs Nome de recurso da Amazon (ARN).

```
aws logs describe-log-groups
```

Criar uma função

Criar uma função para CloudTrail que ela possa enviar eventos para o grupo de CloudWatch registros de registros. O comando `create-role` do IAM usa dois parâmetros: um nome de função e um caminho de arquivo para um documento de política para assumir uma função no formato JSON. O documento de política que você usa concede `AssumeRole` permissões CloudTrail a. O comando `create-role` cria a função com as permissões necessárias.

Para criar o arquivo JSON que conterá o documento de política, abra um editor de texto e salve o conteúdo de política a seguir em um arquivo chamado `assume_role_policy_document.json`.

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

Execute o comando a seguir para criar a função com `AssumeRole` permissões para CloudTrail.

```
aws iam create-role --role-name role_name --assume-role-policy-document file://<path to
 assume_role_policy_document>.json
```

Quando o comando for concluído, anote o ARN da função no resultado.

Criar um documento de política

Crie o seguinte documento de política de função para CloudTrail. Este documento concede CloudTrail as permissões necessárias para criar um fluxo de CloudWatch registros de registros no grupo de registros especificado e para entregar CloudTrail eventos a esse fluxo de registros.

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

      "Sid": "AWSCloudTrailCreateLogStream2014110",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream"
      ],
      "Resource": [
        "arn:aws:logs:region:accountID:log-group:log_group_name:log-
stream:accountID_CloudTrail_region*"
      ]

    },
    {
      "Sid": "AWSCloudTrailPutLogEvents20141101",
      "Effect": "Allow",
      "Action": [
        "logs:PutLogEvents"
      ],
      "Resource": [
        "arn:aws:logs:region:accountID:log-group:log_group_name:log-
stream:accountID_CloudTrail_region*"
      ]
    }
  ]
}
```

Salve o documento de política em um arquivo chamado `role-policy-document.json`.

Se você criar uma política que também pode ser usada para trilhas da organização, precisará configurá-la de maneira um pouco diferente. *Por exemplo, a política a seguir concede CloudTrail as permissões necessárias para criar um fluxo de registros de CloudWatch registros no grupo de registros que você especifica e para entregar CloudTrail eventos a esse fluxo de registros para trilhas na AWS conta 111111111111 e para trilhas da organização criadas na conta 111111111111 que são aplicadas à organização com o ID de o-example.orgid: AWS Organizations*

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailCreateLogStream20141101",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream"
            ],
            "Resource": [
                "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:111111111111_CloudTrail_us-east-2*",
                "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:o-exampleorgid_*"
            ]
        },
        {
            "Sid": "AWSCloudTrailPutLogEvents20141101",
            "Effect": "Allow",
            "Action": [
                "logs:PutLogEvents"
            ],
            "Resource": [
                "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:111111111111_CloudTrail_us-east-2*",
                "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:o-exampleorgid_*"
            ]
        }
    ]
}
```

Para obter mais informações sobre trilhas da organização, consulte Criar uma trilha para uma organização.

Execute o comando a seguir para aplicar a política à função.

```
aws iam put-role-policy --role-name role_name --policy-name cloudtrail-policy --policy-
document file://<path to role-policy-document>.json
```

Atualizar a trilha

Atualize a trilha com o grupo de registros e as informações da função usando o CloudTrail `update-trail` comando.

```
aws cloudtrail update-trail --name trail_name --cloud-watch-logs-log-group-
arn log_group_arn --cloud-watch-logs-role-arn role_arn
```

Para obter mais informações sobre os AWS CLI comandos, consulte a Referência da linha de AWS CloudTrail comando.

Limitação

CloudWatch Os registros e EventBridge cada um permitem um tamanho máximo de evento de 256 KB. Embora a maioria dos eventos de serviço tenha um tamanho máximo de 256 KB, alguns serviços ainda têm eventos maiores. CloudTrail não envia esses eventos para CloudWatch Logs ou EventBridge.

A partir da versão 1.05 do CloudTrail evento, os eventos têm um tamanho máximo de 256 KB. Isso ajuda a evitar a exploração por agentes mal-intencionados e permite que os eventos sejam consumidos por outros AWS serviços, como CloudWatch Logs EventBridge e.

Criação CloudWatch de alarmes para CloudTrail eventos: exemplos

Este tópico descreve como configurar alarmes para CloudTrail eventos e inclui exemplos.

Tópicos

- Pré-requisitos
- Criar um filtro de métrica e um alarme
- Exemplo: alterações de configuração no grupo de segurança
- Exemplo de AWS Management Console falhas de login
- Exemplo: alterações na política do IAM
- Configurando notificações para alarmes de CloudWatch registros

Pré-requisitos

Antes de usar os exemplos deste tópico, você deve:

- Criar uma trilha com o console do ou a CLI.
- Crie um grupo de logs, que você pode fazer como parte da criação de uma trilha. Para obter mais informações sobre a criação de uma trilha, consulte Criar uma trilha.

- Especifique ou crie uma função do IAM que CloudTrail conceda as permissões para criar um stream de CloudWatch registros de registros no grupo de registros que você especifica e para entregar CloudTrail eventos a esse stream de registros. O `CloudTrail_CloudWatchLogs_Role` padrão cuida disso para você.

Para ter mais informações, consulte Envio de eventos para o CloudWatch Logs. Os exemplos nesta seção são apresentados no console do Amazon CloudWatch Logs. Para obter mais informações sobre como criar filtros métricos e alarmes, consulte Criação de métricas a partir de eventos de log usando filtros e Uso de CloudWatch alarmes da Amazon no Guia CloudWatch do usuário da Amazon.

Criar um filtro de métrica e um alarme

Para criar um alarme, você deve primeiro criar um filtro de métrica e configurar um alarme com base no filtro. Os procedimentos são mostrados para todos os exemplos. Para obter mais informações sobre a sintaxe de filtros métricos e padrões para eventos de CloudTrail log, consulte as seções relacionadas a JSON de Filtro e sintaxe de padrões no Guia do usuário do Amazon CloudWatch Logs.

Exemplo: alterações de configuração no grupo de segurança

Siga este procedimento para criar um CloudWatch alarme da Amazon que é acionado quando ocorrem alterações de configuração em grupos de segurança.

Criar um filtro de métrica

1. Abra o CloudWatch console em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação, em Logs, escolha Grupos de logs.
3. Na lista de grupos de logs, escolha aquele que você criou para sua trilha.
4. No menu Filtros métricos ou Ações, escolha Criar filtro métrico.
5. Na página Define pattern (Definir padrão), em Create filter pattern (Criar padrão de filtro), insira as opções a seguir para Filter pattern (Padrão de filtro).

```
{ ($.eventName = AuthorizeSecurityGroupIngress) || ($.eventName =
 AuthorizeSecurityGroupEgress) || ($.eventName = RevokeSecurityGroupIngress) ||
 ($.eventName = RevokeSecurityGroupEgress) || ($.eventName = CreateSecurityGroup)
 || ($.eventName = DeleteSecurityGroup) }
```

6. Em Test pattern (Padrão de teste), deixe os valores padrão. Escolha Next.
7. Na página Atribuir métrica, em Nome do filtro, insira **`SecurityGroupEvents`**.
8. Em Detalhes da métrica, ative Criar nova e, em seguida, insira **`CloudTrailMetrics`** em Namespace da métrica.
9. Em Nome da métrica, digite **`SecurityGroupEventCount`**.
10. Em Valor da métrica, digite **`1`**.
11. Deixe Default value (Valor padrão) em branco.
12. Escolha Next.
13. Na página Review and create (Revisar e criar), revise as suas escolhas. Selecione Create metric filter (Criar filtro de métrica) para criar o filtro ou escolha Edit (Editar) para voltar e alterar os valores.

Criar um alarme

Depois de criar o filtro métrico, a página de detalhes do grupo de CloudWatch registros de registros do seu grupo de registros de CloudTrail trilhas é aberta. Siga este procedimento para criar um alarme.

1. Na guia Metric filters (Filtros de métrica), localize o filtro de métrica que você criou no the section called “Criar um filtro de métrica”. Preencha a caixa de seleção para o filtro de métrica. Na barra Metric filters (Filtros de métrica), escolha Create alarm (Criar alarme).
2. Em Especificar métrica e condições, insira o seguinte.
    a. Em Graph (Gráfico), a linha é definida em **`1`** com base em outras configurações que você faz ao criar seu alarme.
    b. Em Metric name (Nome da métrica), mantenha o nome da métrica atual, **`SecurityGroupEventCount`**.
    c. Em Statistic (Estatística), mantenha os valores padrão, **`Sum`**.
    d. Em Period (Período), mantenha os valores padrão, **`5 minutes`**.
    e. Na seção Conditions (Condições), em Threshold type (Tipo de limite), escolha Static (Estático).
    f. Em Whenever ***`metric_name`*** is (Quando a métrica for), escolha Greater/Equal (Maior/Igual).
    g. Para o valor do limite, insira **`1`**.

h. Em Additional configuration (Configuração adicional), deixe os valores padrão. Escolha Next.

3. Na página Configurar ações, escolha Notificação e, em seguida, escolha Em alarme, o que indica que a ação é tomada quando o limite de 1 evento de alteração em 5 minutos é ultrapassado e SecurityGroupEventCountestá em estado de alarme.

   a. Em Enviar uma notificação para o seguinte tópico do SNS, escolha Criar tópico.

   b. Insira **`SecurityGroupChanges_CloudWatch_Alarms_Topic`** como o nome do novo tópico do Amazon SNS.

   c. Em Endpoints de e-mail que receberão notificação, insira os endereços de e-mail dos usuários que você deseja que recebam notificações se esse alarme for acionado. Separe endereços de e-mail por vírgulas.

      Cada destinatário de email receberá uma mensagem de e-mail solicitando que confirme que deseja se inscrever no tópico do Amazon SNS.

   d. Escolha Criar tópico.

4. Para este exemplo, ignore os outros tipos de ação. Escolha Next.

5. Na página Add name and description (Adicionar nome e descrição), insira um nome amigável para o alarme e uma descrição. Neste exemplo, insira **`Security group configuration changes`** para o nome e **`Raises alarms if security group configuration changes occur`** para a descrição. Escolha Next.

6. Na página Preview and create (Visualizar e criar), verifique suas opções. Selecione Edit (Editar) para fazer alterações ou escolha Create alarm (Criar alarme) para criar o alarme.

   Depois de criar o alarme, CloudWatch abre a página Alarmes. O alarme Actions (Ações) mostrará a coluna Pending confirmation (Confirmação pendente) até que todos os destinatários de e-mail no tópico do SNS tenham confirmado que desejam se inscrever nas notificações do SNS.

Exemplo de AWS Management Console falhas de login

Siga este procedimento para criar um CloudWatch alarme da Amazon que é acionado quando há três ou mais falhas de AWS Management Console login durante um período de cinco minutos.

Criar um filtro de métrica

1. Abra o CloudWatch console em https://console.aws.amazon.com/cloudwatch/.

2. No painel de navegação, em Logs, escolha Grupos de logs.
3. Na lista de grupos de logs, escolha aquele que você criou para sua trilha.
4. No menu Filtros métricos ou Ações, escolha Criar filtro métrico.
5. Na página Define pattern (Definir padrão), em Create filter pattern (Criar padrão de filtro), insira as opções a seguir para Filter pattern (Padrão de filtro).

```
{ ($.eventName = ConsoleLogin) && ($.errorMessage = "Failed authentication") }
```

6. Em Test pattern (Padrão de teste), deixe os valores padrão. Escolha Next.
7. Na página Atribuir métrica, em Nome do filtro, insira **`ConsoleSignInFailures`**.
8. Em Detalhes da métrica, ative Criar nova e, em seguida, insira **`CloudTrailMetrics`** em Namespace da métrica.
9. Em Nome da métrica, digite **`ConsoleSigninFailureCount`**.
10. Em Valor da métrica, digite **`1`**.
11. Deixe Default value (Valor padrão) em branco.
12. Escolha Next.
13. Na página Review and create (Revisar e criar), revise as suas escolhas. Selecione Create metric filter (Criar filtro de métrica) para criar o filtro ou escolha Edit (Editar) para voltar e alterar os valores.

Criar um alarme

Depois de criar o filtro métrico, a página de detalhes do grupo de CloudWatch registros de registros do seu grupo de registros de CloudTrail trilhas é aberta. Siga este procedimento para criar um alarme.

1. Na guia Metric filters (Filtros de métrica), localize o filtro de métrica que você criou no the section called “Criar um filtro de métrica”. Preencha a caixa de seleção para o filtro de métrica. Na barra Metric filters (Filtros de métrica), escolha Create alarm (Criar alarme).
2. Na página Create Alarm (Criar alarme), em Specify metric and conditions (Especificar métrica e condições), faça o seguinte:
   a. Em Graph (Gráfico), a linha é definida em **`3`** com base em outras configurações que você faz ao criar seu alarme.

b. Em Metric name (Nome da métrica), mantenha o nome da métrica atual, **`ConsoleSigninFailureCount`**.

c. Em Statistic (Estatística), mantenha os valores padrão, **`Sum`**.

d. Em Period (Período), mantenha os valores padrão, **`5 minutes`**.

e. Na seção Conditions (Condições), em Threshold type (Tipo de limite), escolha Static (Estático).

f. Em Whenever ***`metric_name`*** is (Quando a métrica for), escolha Greater/Equal (Maior/Igual).

g. Para o valor do limite, insira **`3`**.

h. Em Additional configuration (Configuração adicional), deixe os valores padrão. Escolha Next.

3. Na página Configurar ações, em Notificação, escolha Em alarme, que indica que a ação é tomada quando o limite de 3 eventos de alteração em 5 minutos é ultrapassado e ConsoleSigninFailureCountestá em estado de alarme.

   a. Em Enviar uma notificação para o seguinte tópico do SNS, escolha Criar tópico.

   b. Insira **`ConsoleSignInFailures_CloudWatch_Alarms_Topic`** como o nome do novo tópico do Amazon SNS.

   c. Em Endpoints de e-mail que receberão notificação, insira os endereços de e-mail dos usuários que você deseja que recebam notificações se esse alarme for acionado. Separe endereços de e-mail por vírgulas.

      Cada destinatário de email receberá uma mensagem de e-mail solicitando que confirme que deseja se inscrever no tópico do Amazon SNS.

   d. Escolha Criar tópico.

4. Para este exemplo, ignore os outros tipos de ação. Escolha Next.

5. Na página Add name and description (Adicionar nome e descrição), insira um nome amigável para o alarme e uma descrição. Neste exemplo, insira **`Console sign-in failures`** para o nome e **`Raises alarms if more than 3 console sign-in failures occur in 5 minutes`** para a descrição. Escolha Next.

6. Na página Preview and create (Visualizar e criar), verifique suas opções. Selecione Edit (Editar) para fazer alterações ou escolha Create alarm (Criar alarme) para criar o alarme.

   Depois de criar o alarme, CloudWatch abre a página Alarmes. O alarme Actions (Ações) mostrará a coluna Pending confirmation (Confirmação pendente) até que todos os destinatários

de e-mail no tópico do SNS tenham confirmado que desejam se inscrever nas notificações do SNS.

Exemplo: alterações na política do IAM

Siga este procedimento para criar um CloudWatch alarme da Amazon que é acionado quando uma chamada de API é feita para alterar uma política do IAM.

Criar um filtro de métrica

1. Abra o CloudWatch console em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação, selecione Logs.
3. Na lista de grupos de logs, escolha aquele que você criou para sua trilha.
4. Escolha Actions (Ações) e Create metric filter (Criar filtro de métrica).
5. Na página Define pattern (Definir padrão), em Create filter pattern (Criar padrão de filtro), insira as opções a seguir para Filter pattern (Padrão de filtro).

```
{($.eventName=DeleteGroupPolicy)||($.eventName=DeleteRolePolicy)||
($.eventName=DeleteUserPolicy)||($.eventName=PutGroupPolicy)||
($.eventName=PutRolePolicy)||($.eventName=PutUserPolicy)||
($.eventName=CreatePolicy)||($.eventName=DeletePolicy)||
($.eventName=CreatePolicyVersion)||($.eventName=DeletePolicyVersion)||
($.eventName=AttachRolePolicy)||($.eventName=DetachRolePolicy)||
($.eventName=AttachUserPolicy)||($.eventName=DetachUserPolicy)||
($.eventName=AttachGroupPolicy)||($.eventName=DetachGroupPolicy)}
```

6. Em Test pattern (Padrão de teste), deixe os valores padrão. Escolha Next.
7. Na página Atribuir métrica, em Nome do filtro, insira **`IAMPolicyChanges`**.
8. Em Detalhes da métrica, ative Criar nova e, em seguida, insira **`CloudTrailMetrics`** em Namespace da métrica.
9. Em Nome da métrica, digite **`IAMPolicyEventCount`**.
10. Em Valor da métrica, digite **`1`**.
11. Deixe Default value (Valor padrão) em branco.
12. Escolha Next.
13. Na página Review and create (Revisar e criar), revise as suas escolhas. Selecione Create metric filter (Criar filtro de métrica) para criar o filtro ou escolha Edit (Editar) para voltar e alterar os valores.

Criar um alarme

Depois de criar o filtro métrico, a página de detalhes do grupo de CloudWatch registros de registros do seu grupo de registros de CloudTrail trilhas é aberta. Siga este procedimento para criar um alarme.

1. Na guia Metric filters (Filtros de métrica), localize o filtro de métrica que você criou no the section called “Criar um filtro de métrica”. Preencha a caixa de seleção para o filtro de métrica. Na barra Metric filters (Filtros de métrica), escolha Create alarm (Criar alarme).
2. Na página Create Alarm (Criar alarme), em Specify metric and conditions (Especificar métrica e condições), faça o seguinte:
   a. Em Graph (Gráfico), a linha é definida em **1** com base em outras configurações que você faz ao criar seu alarme.
   b. Em Metric name (Nome da métrica), mantenha o nome da métrica atual, **`IAMPolicyEventCount`**.
   c. Em Statistic (Estatística), mantenha os valores padrão, **`Sum`**.
   d. Em Period (Período), mantenha os valores padrão, **`5 minutes`**.
   e. Na seção Conditions (Condições), em Threshold type (Tipo de limite), escolha Static (Estático).
   f. Em Whenever ***`metric_name`*** is (Quando a métrica for), escolha Greater/Equal (Maior/Igual).
   g. Para o valor do limite, insira **1**.
   h. Em Additional configuration (Configuração adicional), deixe os valores padrão. Escolha Next.
   i.
3. Na página Configurar ações, em Notificação, escolha Em alarme, que indica que a ação é tomada quando o limite de 1 evento de alteração em 5 minutos é ultrapassado e o IAM PolicyEventCount está em estado de alarme.
   a. Em Enviar uma notificação para o seguinte tópico do SNS, escolha Criar tópico.
   b. Insira **`IAM_Policy_Changes_CloudWatch_Alarms_Topic`** como o nome do novo tópico do Amazon SNS.

c. Em Endpoints de e-mail que receberão notificação, insira os endereços de e-mail dos usuários que você deseja que recebam notificações se esse alarme for acionado. Separe endereços de e-mail por vírgulas.

   Cada destinatário de email receberá uma mensagem de e-mail solicitando que confirme que deseja se inscrever no tópico do Amazon SNS.

d. Escolha Criar tópico.

4. Para este exemplo, ignore os outros tipos de ação. Escolha Next.
5. Na página Add name and description (Adicionar nome e descrição), insira um nome amigável para o alarme e uma descrição. Neste exemplo, insira **`IAM Policy Changes`** para o nome e **`Raises alarms if IAM policy changes occur`** para a descrição. Escolha Next.
6. Na página Preview and create (Visualizar e criar), verifique suas opções. Selecione Edit (Editar) para fazer alterações ou escolha Create alarm (Criar alarme) para criar o alarme.

   Depois de criar o alarme, CloudWatch abre a página Alarmes. O alarme Actions (Ações) mostrará a coluna Pending confirmation (Confirmação pendente) até que todos os destinatários de e-mail no tópico do SNS tenham confirmado que desejam se inscrever nas notificações do SNS.

Configurando notificações para alarmes de CloudWatch registros

Você pode configurar o CloudWatch Logs para enviar uma notificação sempre que um alarme for acionado CloudTrail. Isso permite que você responda rapidamente a eventos operacionais críticos capturados em CloudTrail eventos e detectados pelo CloudWatch Logs. CloudWatch usa o Amazon Simple Notification Service (SNS) para enviar e-mails. Para obter mais informações, consulte Configuração de notificações do Amazon SNS no Guia do CloudWatch usuário.

Parando CloudTrail de enviar eventos para o CloudWatch Logs

Você pode parar de enviar AWS CloudTrail eventos para o Amazon CloudWatch Logs atualizando uma trilha para desativar as configurações de CloudWatch registros.

Parar de enviar eventos para o CloudWatch Logs (console)

Para parar de enviar CloudTrail eventos para o CloudWatch Logs

1. Faça login no AWS Management Console e abra o CloudTrail console em https://console.aws.amazon.com/cloudtrail/.
2. No painel de navegação, selecione Trilhas.
3. Escolha o nome da trilha para a qual você deseja desativar a integração de CloudWatch registros.
4. Em CloudWatch Registros, escolha Editar.
5. Desmarque a caixa de seleção Enabled (Habilitado).
6. Escolha Salvar alterações.

Pare de enviar eventos para CloudWatch Logs (CLI)

Você pode remover o grupo de CloudWatch registros de registros como um endpoint de entrega executando o update-trailcomando. O comando a seguir limpa o grupo de registros e a função da configuração da trilha substituindo os valores do ARN do grupo de registros CloudWatch e do ARN da função de registros por valores vazios.

```
aws cloudtrail update-trail --name trail_name --cloud-watch-logs-log-group-arn="" --
cloud-watch-logs-role-arn=""
```

CloudWatch nome do grupo de registros e do fluxo de registros para CloudTrail

A Amazon CloudWatch exibirá o grupo de registros que você criou para CloudTrail eventos junto com quaisquer outros grupos de registros que você tenha em uma região. Recomendamos que você use um nome para o grupo de logs que o ajude a distingui-lo facilmente de outros. Por exemplo, **`CloudTrail/logs`**.

Siga estas diretrizes ao nomear um grupos de log:

- Os nomes de grupos de logs devem ser exclusivos em uma região para uma Conta da AWS.
- Os nomes de grupos de log podem ter entre 1 e 512 caracteres.
- Os nomes de grupos de logs são formados pelos seguintes caracteres: a-z, A-Z, 0-9, '_' (sublinhado), '-' (hífen), '/' (barra), '.' (ponto) e '#' (símbolo numérico).

Quando CloudTrail cria o fluxo de registros para o grupo de registros, ele nomeia o fluxo de registros de acordo com o seguinte formato: Account_ID _ CloudTrail _ trail_region.

> **Note**
>
> Se o volume de CloudTrail registros for grande, vários fluxos de registros poderão ser criados para entregar dados de registro ao seu grupo de registros. *Quando houver vários fluxos de log, CloudTrail nomeie cada fluxo de log de acordo com o seguinte formato: Account_ID _ _ trail_region CloudTrail _ number.*

Para obter mais informações sobre grupos de CloudWatch registros, consulte Trabalho com grupos de registros e fluxos de registros no Guia do usuário do Amazon CloudWatch Logs e CreateLogGroupna Referência da API Amazon CloudWatch Logs.

Documento de política de funções CloudTrail para usar CloudWatch registros para monitoramento

Esta seção descreve a política de permissões necessária para que a CloudTrail função envie eventos de registro para o CloudWatch Logs. Você pode anexar um documento de política a uma função CloudTrail ao configurar o envio de eventos, conforme descrito emEnvio de eventos para o CloudWatch Logs. Você também pode criar uma função usando o IAM. Para obter mais informações, consulte Criação de uma função para delegar permissões a uma AWS service (Serviço da AWS) ou Criação de uma função do IAM (AWS CLI).

O exemplo de documento de política a seguir contém as permissões necessárias para criar um fluxo de CloudWatch registros no grupo de registros que você especifica e para entregar CloudTrail eventos a esse fluxo de registros na região Leste dos EUA (Ohio). (Essa é a política padrão da função padrão do IAM `CloudTrail_CloudWatchLogs_Role`.)

> **Note**
>
> A prevenção delegada confusa não se aplica à política de funções de monitoramento de CloudWatch registros. A política de funções não suporta o uso de `aws:SourceArn` `aws:SourceAccount` e.

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

      "Sid": "AWSCloudTrailCreateLogStream2014110",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream"
      ],
      "Resource": [
        "arn:aws:logs:us-east-2:accountID:log-group:log_group_name:log-
stream:CloudTrail_log_stream_name_prefix*"
      ]

    },
    {
      "Sid": "AWSCloudTrailPutLogEvents20141101",
      "Effect": "Allow",
      "Action": [
        "logs:PutLogEvents"
      ],
      "Resource": [
        "arn:aws:logs:us-east-2:accountID:log-group:log_group_name:log-
stream:CloudTrail_log_stream_name_prefix*"
      ]
    }
  ]
}
```

Se você criar uma política que também pode ser usada para trilhas da organização, será necessário modificá-la na política padrão criada para a função. *Por exemplo, a política a seguir concede CloudTrail as permissões necessárias para criar um fluxo de registros de CloudWatch registros no grupo de registros que você especifica como o valor de log_group_name e para entregar CloudTrail eventos a esse fluxo de registros para as trilhas na conta 111111111111 e para as trilhas da organização criadas na AWS conta 111111111111 que são aplicadas à organização com o ID de o-example.orgid: AWS Organizations*

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

```
    "Statement": [
        {
            "Sid": "AWSCloudTrailCreateLogStream20141101",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream"
            ],
            "Resource": [
                "arn:aws:logs:us-east-2:111111111111:log-group:log_group_name:log-
stream:111111111111_CloudTrail_us-east-2*",
                "arn:aws:logs:us-east-2:111111111111:log-group:log_group_name:log-
stream:o-exampleorgid_*"
            ]
        },
        {
            "Sid": "AWSCloudTrailPutLogEvents20141101",
            "Effect": "Allow",
            "Action": [
                "logs:PutLogEvents"
            ],
            "Resource": [
                "arn:aws:logs:us-east-2:111111111111:log-group:log_group_name:log-
stream:111111111111_CloudTrail_us-east-2*",
                "arn:aws:logs:us-east-2:111111111111:log-group:log_group_name:log-
stream:o-exampleorgid_*"
            ]
        }
    ]
}
```

Para obter mais informações sobre trilhas da organização, consulte Criar uma trilha para uma organização.

Recebendo arquivos de CloudTrail log de várias contas

Você pode CloudTrail entregar arquivos de log de vários Contas da AWS em um único bucket do Amazon S3. Por exemplo, você tem quatro Contas da AWS com as IDs de conta 111111111111, 2222222222, 333333333333 e 444444444444 e deseja configurar para entregar arquivos de log de todas essas quatro contas para um bucket pertencente à conta 111111111111. CloudTrail Para fazer isso, siga estas etapas na ordem:

1. Crie uma trilha na conta à qual o bucket de destino pertencerá (neste exemplo, 111111111111). Não crie ainda uma trilha para outras contas.

   Para obter instruções, consulte Criar uma trilha no console.

2. Atualize a política de bucket em seu bucket de destino para conceder permissões entre contas a. CloudTrail

   Para obter instruções, consulte Definir a política de bucket para várias contas.

3. Crie uma trilha nas outras contas (222222222222, 333333333333 e 444444444444 neste exemplo) para o qual deseja registrar atividades em log. Ao criar a trilha em cada conta, especifique o bucket do Amazon S3 pertencente à conta que você especificou na etapa 1 (neste exemplo, 111111111111). Para obter instruções, consulte Criar trilhas em contas adicionais.

   > **Note**
   >
   > Se você optar por habilitar a criptografia SSE-KMS, a política de chaves KMS deverá permitir o uso da chave CloudTrail para criptografar seus arquivos de log e permitir que os usuários que você especificar leiam arquivos de log em formato não criptografado. Para obter informações sobre como editar manualmente a política de chaves, consulte Configure as AWS KMS principais políticas para CloudTrail.

Redação de IDs de conta de proprietário do bucket para eventos de dados chamados por outras contas

Historicamente, se CloudTrail os eventos de dados fossem ativados em um chamador Conta da AWS da API de eventos de dados do Amazon S3 CloudTrail , mostrava o ID da conta do proprietário do bucket do S3 no evento de dados (como). `PutObject` Isso ocorria mesmo quando a conta do proprietário do bucket não tinha eventos de dados do S3 habilitados.

Agora, CloudTrail remove o ID da conta do proprietário do bucket do S3 no `resources` bloco se as duas condições a seguir forem atendidas:

- A chamada da API do evento de dados é de um proprietário Conta da AWS diferente do proprietário do bucket do Amazon S3.
- O chamador da API recebia um erro `AccessDenied` que era apenas para a conta do chamador.

O proprietário do recurso no qual a chamada de API era feita ainda recebe o evento completo.

Os trechos de registro de eventos a seguir são um exemplo do comportamento esperado. No snippet `Historic`, o ID da conta 123456789012 do proprietário do bucket S3 é mostrado para um chamador de API de uma conta diferente. No exemplo do comportamento atual, o ID da conta do proprietário do bucket não é mostrado.

```
# Historic

"resources": [
    {
        "type": "AWS::S3::Object",
        "ARNPrefix": "arn:aws:s3:::test-my-bucket-2/"
    },
    {
        "accountId": "123456789012",
        "type": "AWS::S3::Bucket",
        "ARN": "arn:aws:s3:::test-my-bucket-2"
    }
]
```

O comportamento atual é mostrado a seguir.

```
# Current

"resources": [
    {
        "type": "AWS::S3::Object",
        "ARNPrefix": "arn:aws:s3:::test-my-bucket-2/"
    },
    {
        "accountId": "",
        "type": "AWS::S3::Bucket",
        "ARN": "arn:aws:s3:::test-my-bucket-2"
    }
]
```

Tópicos

- Definir a política de bucket para várias contas
- Criar trilhas em contas adicionais

Definir a política de bucket para várias contas

Para que um bucket receba arquivos de log de várias contas, sua política de bucket deve conceder CloudTrail permissão para gravar arquivos de log de todas as contas que você especificar. Isso significa que você deve modificar a política do bucket em seu bucket de destino para conceder CloudTrail permissão para gravar arquivos de log de cada conta especificada.

> **Note**
>
> Por motivos de segurança, usuários não autorizados não podem criar uma trilha que incluaAWSLogs/ como o parâmetro S3KeyPrefix.

Para modificar as permissões do bucket para que os arquivos possam ser recebidos de várias contas

1. Faça login AWS Management Console usando a conta que possui o bucket (111111111111 neste exemplo) e abra o console do Amazon S3.
2. Escolha o bucket onde CloudTrail entrega seus arquivos de log e, em seguida, escolha Permissões.
3. Em Bucket policy (Política de bucket), escolha Edit (Editar).
4. Modifique a política existente para adicionar uma linha para cada conta adicional cujos arquivos de log devem ser fornecidos a esse bucket. Veja o exemplo de política a seguir e observe a linha Resource sublinhada especificando o ID de uma segunda conta. Como uma prática recomendada de segurança, adicione uma aws:SourceArn chave de condição para a política de bucket do Amazon S3. Isso ajuda a impedir o acesso não autorizado à conta do seu bucket do S3. Se você tiver trilhas existentes, certifique-se de adicionar uma ou mais chaves de condição.

   > **Note**
   >
   > O ID AWS da conta é um número de doze dígitos, incluindo zeros à esquerda.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSCloudTrailAclCheck20131101",
```

```
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::myBucketName",
      "Condition": {
          "StringEquals": {
            "aws:SourceArn": [
              "arn:aws:cloudtrail:region:111111111111:trail/primaryTrailName",
              "arn:aws:cloudtrail:region:222222222222:trail/secondaryTrailName"
            ]
          }
       }
    },
    {
      "Sid": "AWSCloudTrailWrite20131101",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": [
        "arn:aws:s3:::myBucketName/optionalLogFilePrefix/AWSLogs/111111111111/*",
        "arn:aws:s3:::myBucketName/optionalLogFilePrefix/AWSLogs/222222222222/*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:SourceArn": [
            "arn:aws:cloudtrail:region:111111111111:trail/primaryTrailName",
            "arn:aws:cloudtrail:region:222222222222:trail/secondaryTrailName"
          ],
          "s3:x-amz-acl": "bucket-owner-full-control"
        }
      }
    }
  ]
}
```

Criar trilhas em contas adicionais

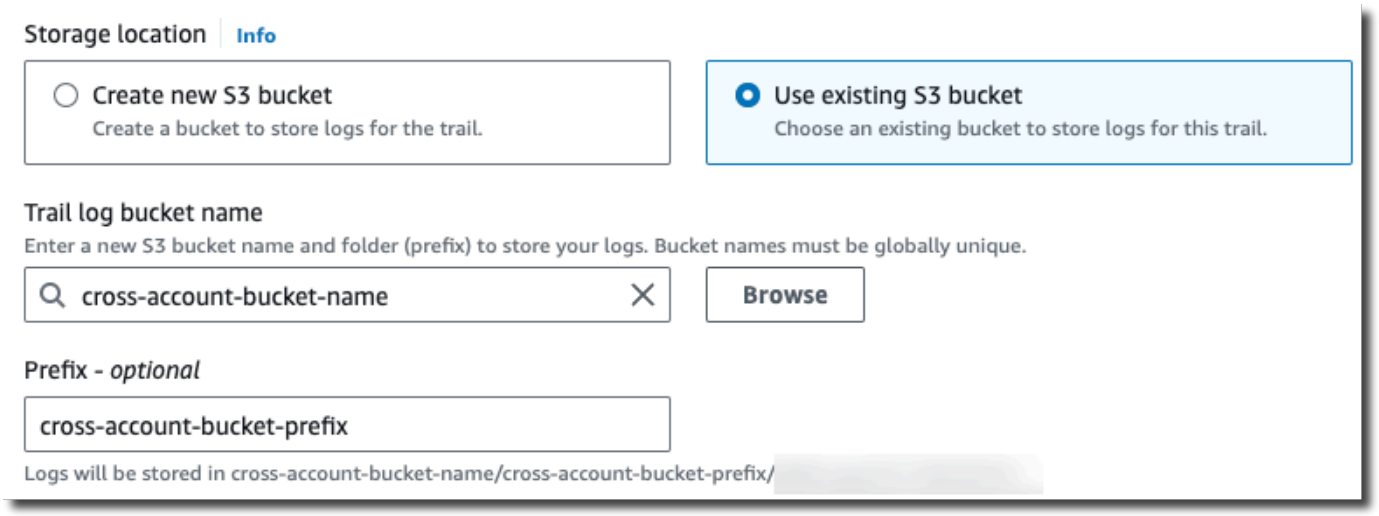
Você pode usar o console ou o AWS CLI para criar trilhas adicionais Contas da AWS e agregar seus arquivos de log em um bucket do Amazon S3. Como alternativa, você pode criar uma trilha organizacional para registrar todos os Contas da AWS que fazem parte de uma organização AWS Organizations. Para ter mais informações, consulte Criar uma trilha para uma organização.

Usando o console para criar trilhas em AWS contas adicionais

Você pode usar o CloudTrail console para criar trilhas em contas adicionais.

1. Faça login AWS Management Console com a conta para a qual você deseja criar uma trilha. Siga estas etapas em Criar uma trilha no console para criar uma trilha usando o console.
2. Em Storage location (Local de armazenamento), escolha Use existing S3 bucket (Usar bucket S3 existente). Use a caixa de texto para inserir o nome do bucket que você está usando para armazenar arquivos de log nas contas.

> **Note**
>
> A política do bucket deve conceder CloudTrail permissão para gravar nela. Para obter informações sobre como editar manualmente a política de bucket, consulte Definir a política de bucket para várias contas.



3. Em Prefixo, insira o prefixo que você está usando para armazenar arquivos de log nas contas. Se você optar por usar um prefixo diferente do especificado na política do bucket, deverá editar

a política do bucket no bucket de destino CloudTrail para permitir a gravação de arquivos de log no bucket usando esse novo prefixo.

Usando a CLI para criar uma trilha em contas adicionais AWS

Você pode usar as ferramentas de linha de AWS comando para criar trilhas em contas adicionais e agregar seus arquivos de log em um bucket do Amazon S3. Para obter mais informações sobre essas ferramentas, consulte cloudtrail na Referência de AWS CLI comandos.

Para criar uma trilha usando o comando create-trail, especifique o seguinte:

- `--name` especifica o nome da trilha.
- `--s3-bucket-name` especifica o bucket do Amazon S3 que você está usando para armazenar arquivos de log entre contas.
- `--s3-prefix` especifica um prefixo para o caminho de entrega de arquivos de log (opcional).
- `--is-multi-region-trail`especifica que essa trilha registrará eventos em todas as AWS regiões na partição em que você está trabalhando.

Você pode criar uma trilha para cada região na qual uma conta está administrando AWS recursos.

O exemplo de comando a seguir mostra como criar uma trilha para suas contas adicionais usando a AWS CLI. Para que os arquivos de log dessa conta sejam fornecidos ao bucket que você criou em sua primeira conta (neste exemplo, 111111111111), especifique o nome do bucket na opção `--s3-bucket-name`. Os nomes dos buckets do Amazon S3 são globalmente exclusivos.

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name my-bucket --is-multi-region-trail
```

Quando você executar o comando, verá um resultado semelhante a este:

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "AWSCloudTrailExample",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:222222222222:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": false,
    "S3BucketName": "MyBucketBelongingToAccount111111111111"
```

```
}
```

Para obter mais informações sobre como usar as ferramentas CloudTrail da linha de AWS comando, consulte a referência da linha de CloudTrail comando.

Compartilhamento CloudTrail de arquivos de log entre AWS contas

Esta seção explica como compartilhar arquivos de CloudTrail log entre várias AWS contas. A abordagem que você usa para compartilhar registros Contas da AWS depende da configuração do seu bucket do S3. Estas são as opções para compartilhar arquivos de log:

- Aplicada pelo proprietário do bucket: a Propriedade de objeto do S3 é uma configuração no nível do bucket do Amazon S3 que você pode usar para controlar a propriedade de objetos carregados no bucket e desabilitar ou habilitar as listas de controle de acesso (ACLs). Por padrão, a Propriedade de objeto está definida com a configuração Aplicada pelo proprietário do bucket e todas as ACLs estão desabilitadas. Quando as ACLs são desabilitadas, o proprietário do bucket possui todos os objetos do bucket e gerencia o acesso aos dados usando políticas de gerenciamento de acesso. Quando a opção Aplicada pelo proprietário do bucket é definida, o acesso é gerenciado por meio da política do bucket, eliminando a necessidade de os usuários presumirem um perfil.
- Presumir um perfil para compartilhar arquivos de log: se você não tiver escolhido a configuração Aplicada pelo proprietário do bucket, os usuários precisarão presumir um perfil para acessar os arquivos de log em seu bucket do S3.

Compartilhar arquivos de log entre contas presumindo um perfil

> **Note**
>
> Esta seção se aplica somente aos buckets do Amazon S3 que não estão usando a configuração Aplicada pelo proprietário do bucket.

Esta seção explica como compartilhar arquivos de CloudTrail log entre vários Contas da AWS assumindo uma função e descreve os cenários para compartilhar arquivos de log.

- Cenário 1: concede acesso somente leitura às contas que geraram os arquivos de log que foram colocados no seu bucket do Amazon S3.

- Cenário 2: concede acesso a todos os arquivos de log em seu bucket do Amazon S3 a uma conta de terceiros que possa analisar os arquivos de log para você.

Para conceder acesso somente leitura aos arquivos de log em seu bucket do Amazon S3

1. Crie um perfil do IAM para cada conta com a qual você deseja compartilhar arquivos de log. Você precisa ser administrador para conceder permissão.

   Ao criar o perfil, faça o seguinte:

   - Escolha a opção Outra Conta da AWS.
   - Insira o ID de doze dígitos da conta que receberá o acesso.
   - Marque a caixa Require MFA se você quiser que o usuário forneça autenticação multifator antes de assumir a função.
   - Escolha a política do AmazonS3 ReadOnlyAccess.

   > **Note**
   >
   > Por padrão, a ReadOnlyAccess política do AmazonS3 concede direitos de recuperação e lista a todos os buckets do Amazon S3 em sua conta.

   Para ver detalhes sobre o gerenciamento de permissões de perfis do IAM, consulte Perfis do IAM no Manual do usuário do IAM.
2. Crie uma política de acesso que conceda acesso somente leitura à conta com a qual você deseja compartilhar arquivos de log.
3. Instrua cada conta a presumir um perfil para recuperar os arquivos de log.

Para conceder acesso somente leitura aos arquivos de log com uma conta de terceiros

1. Crie um perfil do IAM para a conta de terceiro com a qual você deseja compartilhar arquivos de log. Você precisa ser administrador para conceder permissão.

   Ao criar o perfil, faça o seguinte:

   - Escolha a opção Outra Conta da AWS.
   - Insira o ID de doze dígitos da conta que receberá o acesso.

- Insira um ID externo que proporcione mais controle sobre quem pode assumir a função. Para obter mais informações, consulte Como usar uma ID externa ao conceder acesso aos seus AWS recursos a terceiros no Guia do usuário do IAM.
- Escolha a política do AmazonS3 ReadOnlyAccess.

> **Note**
>
> Por padrão, a ReadOnlyAccess política do AmazonS3 concede direitos de recuperação e lista a todos os buckets do Amazon S3 em sua conta.

2. Crie uma política de acesso que conceda acesso somente leitura à conta de terceiro com a qual você deseja compartilhar arquivos de log.
3. Instrua a conta de terceiro a presumir um perfil para recuperar os arquivos de log.

As seções a seguir oferecem mais detalhes sobre essas etapas.

Tópicos

- Criar uma política de acesso padrão para conceder acesso às suas contas
- Criar uma política de acesso padrão para conceder acesso a um terceiro
- Assumir uma função
- Pare de compartilhar arquivos de CloudTrail log entre AWS contas

Criar uma política de acesso padrão para conceder acesso às suas contas

Como proprietário do bucket do Amazon S3, você tem controle total sobre o bucket do Amazon S3 no CloudTrail qual grava arquivos de log para as outras contas. Você deseja compartilhar os arquivos de log de cada unidade de negócios com a unidade de negócios que os criou. Entretanto, você não quer que uma unidade consiga ler os arquivos de log das outras.

Por exemplo, para compartilhar os arquivos de log da conta B com a conta B, mas não com a conta C, será necessário criar um novo perfil do IAM na sua conta que especifique que a conta B é uma conta confiável. Essa política de confiança de perfil especifica que a conta B é confiável para presumir o perfil criado pela sua conta e deve ter a aparência mostrada no exemplo a seguir. A política de confiança é criada automaticamente quando você cria a função usando o console. Se você usar o SDK para criar a função, será necessário fornecer a política de confiança como

um parâmetro para a API `CreateRole`. Se você usar a CLI para criar a função, será necessário especificar a política de confiança no comando `create-role` da CLI.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::account-B-id:root"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Você também precisará criar uma política de acesso padrão para especificar que a conta B só pode ler do local em que B criou seus arquivos de log. A política de acesso padrão terá a aparência a seguir. Observe que o ARN do recurso inclui o ID da conta de doze dígitos para a conta B e o prefixo que você especificou, se houver, ao ativar a conta B CloudTrail durante o processo de agregação. Para obter mais informações sobre como especificar um prefixo, consulte Criar trilhas em contas adicionais.

> **Important**
>
> Você deve garantir que o prefixo na política de acesso seja exatamente o mesmo que você especificou quando ativou a conta B. Se não for, você deverá editar a política de acesso à função do IAM em sua conta para incorporar o prefixo real da conta B. Se o prefixo na política de acesso à função não for exatamente o mesmo que você especificou quando ativou a conta B, a conta B não poderá acessar seus arquivos de registro. CloudTrail CloudTrail

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

```
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*"
      ],
      "Resource": "arn:aws:s3:::bucket-name/prefix/AWSLogs/account-B-id/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*"
      ],
      "Resource": "arn:aws:s3:::bucket-name"
    }
  ]
}
```

Use o processo anterior para contas adicionais.

Após você criar perfis para cada conta e especificar as políticas apropriadas de acesso e confiança e depois que um usuário do IAM de cada conta tiver recebido o acesso concedido pelo administrador dessa conta, um usuário do IAM das Contas B ou C poderá assumir o perfil de maneira programática.

Para ter mais informações, consulte Assumir uma função.

Criar uma política de acesso padrão para conceder acesso a um terceiro

Você precisa criar um perfil do IAM diferente para uma conta de terceiros. Ao criar o perfil, a AWS cria automaticamente a relação de confiança, que especifica que a conta do terceiro será confiável para assumir o perfil. A política de acesso padrão do perfil especifica quais ações a conta pode realizar. Para obter mais informações sobre a criação de perfis, consulte Criar um perfil do IAM.

Por exemplo, a relação de confiança criada por AWS especifica que a conta de terceiros (conta Z neste exemplo) é confiável para assumir a função que você criou. Veja abaixo um exemplo de política de confiança:

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

```
    "Statement": [{
        "Sid": "",
        "Effect": "Allow",
        "Principal": {"AWS": "arn:aws:iam::account-Z-id:root"},
        "Action": "sts:AssumeRole"
    }]
}
```

Se você tiver especificado um ID externo quando criou o perfil para a conta de terceiro, sua política de acesso padrão contém um elemento `Condition` adicional que testa o ID exclusivo atribuído por essa conta. O teste é realizado quando o perfil é presumido. O exemplo a seguir de política de acesso padrão tem um elemento `Condition`.

Para obter mais informações, consulte Como usar uma ID externa ao conceder acesso aos seus AWS recursos a terceiros no Guia do usuário do IAM.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "",
        "Effect": "Allow",
        "Principal": {"AWS": "arn:aws:iam::account-Z-id:root"},
        "Action": "sts:AssumeRole",
        "Condition": {"StringEquals": {"sts:ExternalId": "external-ID-issued-by-
account-Z"}}
    }]
}
```

Você também precisa criar uma política de acesso para a conta para especificar que a conta de terceiro pode ler todos os logs do bucket do Amazon S3. A política de acesso padrão deve ser parecida com o exemplo a seguir. O caractere curinga (*) no final do valor `Resource` indica que a conta de terceiro pode acessar qualquer arquivo de log no bucket do S3 ao qual ela recebeu acesso.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:Get*",
                "s3:List*"
```

```
            ],
            "Resource": "arn:aws:s3:::bucket-name/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:Get*",
                "s3:List*"
            ],
            "Resource": "arn:aws:s3:::bucket-name"
        }
    ]
}
```

Depois que você criar um perfil para a conta de terceiro e especificar a política de acesso e a relação de confiança apropriada, um usuário do IAM na conta de terceiro precisará presumir o perfil de modo programático para poder ler os arquivos de log do bucket. Para ter mais informações, consulte Assumir uma função.

Assumir uma função

É necessário designar um usuário do IAM separado para assumir cada perfil criado em cada conta. Em seguida, você deve garantir que cada usuário do IAM tenha as permissões apropriadas.

Usuários e perfis do IAM

Depois de criar as políticas e os perfis necessários, você precisará designar um usuário do IAM em cada uma das contas com as quais deseja compartilhar arquivos. Cada usuário do IAM presume de maneira programática o perfil apropriado para acessar os arquivos de log. Quando um usuário presume um perfil, a AWS retorna credenciais de segurança temporárias para esse usuário. Em seguida, o usuário pode fazer solicitações para listar, recuperar, copiar ou excluir arquivos de log, dependendo das permissões concedidas pela política de acesso associada ao perfil.

Para obter mais informações sobre como trabalhar com identidades do IAM, consulte Identidades do IAM (usuários, grupos de usuários e perfis).

A principal diferença na política de acesso que você cria para cada perfil do IAM em cada cenário.

- No cenário 1, a política de acesso limita cada conta à leitura de seus próprios arquivos de log. Para ter mais informações, consulte Criar uma política de acesso padrão para conceder acesso às suas contas.

- No cenário 2, a política de acesso da conta de terceiro permite que ela leia todos os arquivos de log que estão agregados no bucket do Amazon S3. Para ter mais informações, consulte Criar uma política de acesso padrão para conceder acesso a um terceiro.

Criar políticas de permissões para usuários do IAM

Para realizar as ações permitidas por uma função, o usuário do IAM precisa ter permissão para chamar a AWS STS `AssumeRole`API. Você deve editar a política para cada usuário a fim de conceder a eles as permissões apropriadas. Desse modo, você define um elemento Recurso na política, que é anexado ao usuário do IAM. O exemplo a seguir mostra uma política de um usuário do IAM em outra conta que permite que o usuário presuma um perfil chamado `Test`, criado anteriormente pela conta A.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["sts:AssumeRole"],
      "Resource": "arn:aws:iam::account-A-id:role/Test"
    }
  ]
}
```

Para editar uma política gerenciada pelo cliente (console)

1. Faça login AWS Management Console e abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação, escolha Policies.
3. Na lista de políticas, escolha o nome da política a editar. Você pode usar a caixa de pesquisa para filtrar a lista de políticas.
4. Escolha a guia Permissões e depois escolha Editar.
5. Execute um destes procedimentos:

    - Escolha a opção Visual para alterar a política sem necessidade de compreender a sintaxe JSON. Você pode fazer alterações nos serviços, ações, recursos ou condições opcionais para cada bloco de permissões na política. Também é possível importar uma política e acrescentar

permissões adicionais no final da sua política. Quando terminar de fazer alterações, escolha Avançar para continuar.

- Escolha a opção JSON para modificar a política digitando ou colando texto na caixa de texto JSON. Também é possível importar uma política e acrescentar permissões adicionais no final da sua política. Resolva os avisos de segurança, erros ou avisos gerais gerados durante a validação de política e depois escolha Próximo.

> **Note**
>
> Você pode alternar entre as opções de editor Visual e JSON a qualquer momento. Porém, se você fizer alterações ou escolher Próximo no editor Visual, o IAM poderá reestruturar a política a fim de otimizá-la para o editor visual. Para obter mais informações, consulte Restruturação de política no Guia do usuário do IAM.

6. Na página Revisar e salvar, revise Permissões definidas nessa política e escolha Salvar alterações para salvar seu trabalho.
7. Se a política gerenciada já tiver o máximo de cinco versões e você escolher Salvar alterações, uma caixa de diálogo será exibida. Para salvar a nova versão, a versão não padrão mais antiga da política será removida e substituída por essa nova versão. Opcionalmente, você pode definir a nova versão como a versão padrão da política.

   Escolha Salvar alterações para salvar a nova versão da política.

Chamando AssumeRole

Um usuário pode assumir uma função criando um aplicativo que chama a AWS STS `AssumeRole`API e passa o nome da sessão da função, o Amazon Resource Number (ARN) da função a ser assumida e uma ID externa opcional. O nome da sessão do perfil é definido pela conta quando ela cria o perfil a ser presumido. O ID externo, se houver, é definido pela conta de terceiro e transmitido à conta de propriedade para inclusão durante a criação do perfil. Para obter mais informações, consulte Como usar uma ID externa ao conceder acesso aos seus AWS recursos a terceiros no Guia do usuário do IAM. Você pode recuperar o Nome de região da Amazon (ARN) da Conta A ao abrir o console do IAM.

Para encontrar o valor do Nome de região da Amazon (ARN) na Conta A com o console do IAM

1. Escolha Roles (Funções)

2. Escolha a função que você deseja examinar.
3. Procure por Role ARN (ARN da função) na seção Summary (Resumo).

A AssumeRole API retorna credenciais temporárias para usar para acessar recursos na conta própria. Neste exemplo, os recursos que você deseja acessar são o bucket do Amazon S3 e os arquivos de log contidos no bucket. As credenciais temporárias têm as permissões que você definiu na política de acesso padrão da função.

O exemplo de Python a seguir (usando AWS SDK for Python (Boto)) mostra como chamar `AssumeRole` e como usar as credenciais de segurança temporárias retornadas para listar todos os buckets do Amazon S3 controlados pela Conta A.

```
def list_buckets_from_assumed_role(user_key, assume_role_arn, session_name):
    """
    Assumes a role that grants permission to list the Amazon S3 buckets in the account.
    Uses the temporary credentials from the role to list the buckets that are owned
    by the assumed role's account.

    :param user_key: The access key of a user that has permission to assume the role.
    :param assume_role_arn: The Amazon Resource Name (ARN) of the role that
                            grants access to list the other account's buckets.
    :param session_name: The name of the STS session.
    """
    sts_client = boto3.client(
        "sts", aws_access_key_id=user_key.id, aws_secret_access_key=user_key.secret
    )
    try:
        response = sts_client.assume_role(
            RoleArn=assume_role_arn, RoleSessionName=session_name
        )
        temp_credentials = response["Credentials"]
        print(f"Assumed role {assume_role_arn} and got temporary credentials.")
    except ClientError as error:
        print(
            f"Couldn't assume role {assume_role_arn}. Here's why: "
            f"{error.response['Error']['Message']}"
        )
        raise

    # Create an S3 resource that can access the account with the temporary credentials.
    s3_resource = boto3.resource(
```

```
        "s3",
        aws_access_key_id=temp_credentials["AccessKeyId"],
        aws_secret_access_key=temp_credentials["SecretAccessKey"],
        aws_session_token=temp_credentials["SessionToken"],
    )
    print(f"Listing buckets for the assumed role's account:")
    try:
        for bucket in s3_resource.buckets.all():
            print(bucket.name)
    except ClientError as error:
        print(
            f"Couldn't list buckets for the account. Here's why: "
            f"{error.response['Error']['Message']}"
        )
        raise
```

Pare de compartilhar arquivos de CloudTrail log entre AWS contas

Para parar de compartilhar arquivos de log com outra pessoa Conta da AWS, exclua a função que você criou para essa conta. Para obter mais informações sobre como excluir um perfil, consulte Excluir perfis ou perfis de instância.

Validando a integridade CloudTrail do arquivo de log

Para determinar se um arquivo de log foi modificado, excluído ou inalterado após a CloudTrail entrega, você pode usar a validação de integridade do arquivo de CloudTrail log. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computacionalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção. Você pode usar o AWS CLI para validar os arquivos no local em que CloudTrail foram entregues.

Por que usá-la?

Os arquivos de log validados são valiosíssimos para segurança e investigações forenses. Por exemplo, um arquivo de log validado permite que você declare positivamente que o arquivo de log não foi alterado ou que determinadas credenciais de usuário realizaram atividades específicas de API. O processo de validação da integridade do arquivo de CloudTrail log também permite que você

saiba se um arquivo de log foi excluído ou alterado, ou afirme positivamente que nenhum arquivo de log foi entregue à sua conta durante um determinado período de tempo.

Como funciona

Quando você ativa a validação da integridade do arquivo de log, CloudTrail cria um hash para cada arquivo de log que ele entrega. A cada hora, CloudTrail também cria e entrega um arquivo que faz referência aos arquivos de log da última hora e contém um hash de cada um. Esse arquivo é chamado de arquivo de resumo. CloudTrail assina cada arquivo de resumo usando a chave privada de um par de chaves pública e privada. Após a entrega, você pode usar a chave pública para validar o arquivo de resumo. CloudTrail usa pares de chaves diferentes para cada um Região da AWS.

Os arquivos de resumo são entregues no mesmo bucket do Amazon S3 associado à sua trilha que seus arquivos de log CloudTrail . Se seus arquivos de log forem entregues de todas as regiões ou de várias contas em um único bucket do Amazon S3, CloudTrail entregará os arquivos de resumo dessas regiões e contas no mesmo bucket.

Os arquivos de resumo são colocados em uma pasta separada dos arquivos de log. Essa separação de arquivos de resumo e de log permite que você aplique as políticas de segurança granulares e que as soluções de processamento de log existentes continuem a operar sem modificação. Cada arquivo de resumo também contém a assinatura digital do arquivo de resumo anterior, se existir. A assinatura do arquivo de resumo atual está nas propriedades de metadados do objeto do Amazon S3 do arquivo de resumo. Para obter mais informações sobre o conteúdo do arquivo de resumo, consulte CloudTrail estrutura do arquivo digest.

Armazenar arquivos de log e de compilação

Você pode armazenar os arquivos de CloudTrail log e os arquivos de resumo no Amazon S3 ou no S3 Glacier de forma segura, durável e econômica por um período indefinido. Para aumentar a segurança do arquivos de resumo armazenados no Amazon S3, você pode usar o Amazon S3 MFA Delete.

Habilitar a validação e validar arquivos

Para habilitar a validação da integridade do arquivo de log AWS Management Console, você pode usar a CloudTrail API AWS CLI, the ou. Habilitar CloudTrail a validação da integridade do arquivo de log permite entregar arquivos de log de resumo para seu bucket do Amazon S3, mas não valida a integridade dos arquivos. Para ter mais informações, consulte Habilitando a validação da integridade do arquivo de log para CloudTrail.

Para validar a integridade dos arquivos de CloudTrail log, você pode usar o AWS CLI ou criar sua própria solução. Eles AWS CLI validarão os arquivos no local em que CloudTrail foram entregues. Se você desejar validar logs que foram movidos para outro local, como o Amazon S3 ou outro local, poderá criar suas próprias ferramentas de validação.

Para obter informações sobre como validar registros usando o AWS CLI, consulteValidando a integridade do arquivo de CloudTrail log com o AWS CLI. Para obter informações sobre o desenvolvimento de implementações personalizadas de validação de arquivos de CloudTrail log, consulteImplementações personalizadas da validação da integridade do arquivo de CloudTrail log.

Habilitando a validação da integridade do arquivo de log para CloudTrail

Você pode ativar a validação da integridade do arquivo de log usando a AWS Management Console interface de linha de AWS comando (AWS CLI) ou a CloudTrail API. CloudTrail começa a entregar os arquivos de resumo em cerca de uma hora.

AWS Management Console

Para habilitar a validação da integridade do arquivo de log com o CloudTrail console, escolha Sim para a opção Habilitar validação do arquivo de log ao criar ou atualizar uma trilha. Por padrão, esse recurso é ativado para as novas trilhas. Para ter mais informações, consulte Criar e atualizar uma trilha com o console.

AWS CLI

Para habilitar a validação da integridade do arquivo de log com o AWS CLI, use a `--enable-log-file-validation` opção com os comandos create-trail ou update-trail. Para desativar a validação da integridade dos arquivos de log, use a opção `--no-enable-log-file-validation`.

Exemplo

O comando `update-trail` a seguir permite a validação do arquivo de log e começa a fornecer arquivos de resumo ao bucket do Amazon S3 para a trilha especificada.

```
aws cloudtrail update-trail --name your-trail-name --enable-log-file-validation
```

CloudTrail API

Para habilitar a validação da integridade do arquivo de log com a CloudTrail API, defina o parâmetro de `EnableLogFileValidation` solicitação como `true` ao chamar `CreateTrail` ou`UpdateTrail`.

Para obter mais informações, consulte CreateTraile UpdateTrailna Referência AWS CloudTrail da API.

Validando a integridade do arquivo de CloudTrail log com o AWS CLI

Para validar os registros com o AWS Command Line Interface, use o CloudTrail `validate-logs` comando. O comando usa os arquivos de resumo fornecidos ao bucket do Amazon S3 para executar a validação. Para obter informações sobre os arquivos de resumo, consulte CloudTrail estrutura do arquivo digest.

O AWS CLI permite que você detecte os seguintes tipos de alterações:

- Modificação ou exclusão de arquivos de CloudTrail log
- Modificação ou exclusão de arquivos de CloudTrail resumo
- Modificação ou exclusão de ambos

> **Note**
>
> O AWS CLI valida somente arquivos de log que são referenciados por arquivos de resumo. Para ter mais informações, consulte Verificando se um arquivo específico foi entregue por CloudTrail.

Pré-requisitos

Para validar a integridade do arquivo de log com o AWS CLI, as seguintes condições devem ser atendidas:

- Você deve ter conectividade on-line com AWS.
- Você precisa ter acesso de leitura ao bucket do Amazon S3 que contém os arquivos de resumo e de log.
- Os arquivos de resumo e log não devem ter sido movidos do local original do Amazon S3 CloudTrail onde foram entregues.

> **Note**
>
> Os arquivos de log que foram baixados para o disco local não podem ser validados com a AWS CLI. Para obter informações sobre como criar suas próprias ferramentas para validação, consulte Implementações personalizadas da validação da integridade do arquivo de CloudTrail log.

validate-logs

Sintaxe

Veja a seguir a sintaxe de `validate-logs`. Os parâmetros opcionais são mostrados entre colchetes.

```
aws cloudtrail validate-logs --trail-arn <trailARN> --start-time <start-time> [--end-time <end-time>] [--s3-bucket <bucket-name>] [--s3-prefix <prefix>] [--account-id <account-id>] [--verbose]
```

> **Note**
>
> O comando `validate-logs` é específico da região. Você deve especificar a opção `--region` global para validar os registros de um determinado Região da AWS.

Opções

Veja a seguir as opções de linha de comando de `validate-logs`. As opções `--trail-arn` e `--start-time` são obrigatórias. A opção `--account-id` também é necessária para trilhas organizacionais.

`--start-time`

Especifica que os arquivos de log fornecidos no horário UTC especificado ou depois dele serão validados. Exemplo: `2015-01-08T05:21:42Z`.

`--end-time`

Opcionalmente, especifica que os arquivos de log fornecidos no horário UTC especificado ou antes dele serão validados. O valor padrão é o horário UTC atual (`Date.now()`). Exemplo: `2015-01-08T12:31:41Z`.

> **Note**
>
> Para o período especificado, o comando `validate-logs` verifica somente os arquivos de log que são referenciados em seus arquivos de resumo correspondentes. Nenhum outro arquivo de log no bucket do Amazon S3 é verificado. Para ter mais informações, consulte Verificando se um arquivo específico foi entregue por CloudTrail.

`--s3-bucket`

Opcionalmente, especifica o bucket do Amazon S3 em que os arquivos de resumo são armazenados. Se um nome de bucket não for especificado, eles o AWS CLI recuperarão `DescribeTrails()` chamando.

`--s3-prefix`

Opcionalmente, especifica o prefixo do Amazon S3 em que os arquivos de resumo são armazenados. Se não for especificado, ele o AWS CLI recuperará `DescribeTrails()` chamando.

> **Note**
>
> Você deve usar essa opção somente se o prefixo atual for diferente daquele que estava em uso durante o período que você especificar.

`--account-id`

Opcionalmente, especifica a conta para validar os logs. Esse parâmetro é necessário para trilhas da organização para validação de logs da conta específica dentro de uma organização.

`--trail-arn`

Especifica o Nome de recurso da Amazon (ARN) da trilha a ser validada. O formato de uma trilha que o Nome de recurso da Amazon (ARN) segue.

```
arn:aws:cloudtrail:us-east-2:111111111111:trail/MyTrailName
```

> **Note**
>
> Para obter o Nome de recurso da Amazon (ARN) de uma trilha, você pode usar o comando `describe-trails` antes de executar `validate-logs`.
> Convém especificar o prefixo e o nome do bucket, além do Nome de recurso da Amazon (ARN) da trilha, se os arquivos de log foram fornecidos a mais de um bucket no período especificado e você quiser restringir a validação aos arquivos de log em apenas um dos buckets.

`--verbose`

Opcionalmente, fornece informações de validação de cada arquivo de log ou de compilação no período especificado. Os resultados indicam se o arquivo permanece inalterado ou foi modificado ou excluído. No modo não detalhado (o padrão), as informações são retornadas somente para os casos em que havia uma falha de validação.

Exemplo

O exemplo a seguir valida os arquivos de log do horário de início especificado até o presente, usando o bucket do Amazon S3 configurado para a trilha atual e especificando os resultados detalhados.

```
aws cloudtrail validate-logs --start-time 2015-08-27T00:00:00Z --end-time
 2015-08-28T00:00:00Z --trail-arn arn:aws:cloudtrail:us-east-2:111111111111:trail/my-
trail-name --verbose
```

Como a **`validate-logs`** funciona

O comando `validate-logs` começa validando o arquivo de resumo mais recente no período especificado. Primeiro, ele verifica se o arquivo de resumo foi baixado do local ao qual ele afirma que

pertence. Em outras palavras, se a CLI fizer download do arquivo de resumo `df1` do local do S3 `p1`, validate-logs verificará se `p1 == df1.digestS3Bucket + '/' + df1.digestS3Object`.

Se a assinatura do arquivo de resumo for válida, ela verificará o valor de hash de cada um dos logs referenciados no arquivo de resumo. Então, o comando volta no tempo, validando os arquivos de resumo anteriores e seus arquivos de log referenciados sucessivamente. Ele continuará até que o valor especificado para `start-time` seja atingido ou até que a cadeia de compilação termine. Se um arquivo de resumo é ausente ou não é válido, o período que não pode ser validado é indicado nos resultados.

Resultados da validação

Os resultados da validação começam com um cabeçalho de resumo no seguinte formato:

```
Validating log files for trail trail_ARN  between time_stamp and time_stamp
```

Cada linha dos resultados principais contém os resultados da validação para um único arquivo de resumo ou de log no seguinte formato:

```
<Digest file | Log file> <S3 path> <Validation Message>
```

A tabela a seguir descreve as possíveis mensagens de validação do arquivo de log e de compilação.

Tipo de arquivo	Mensagem de validação	Descrição
`Digest file`	`valid`	A assinatura do arquivo de resumo é válida. Os arquivos de log aos quais ela faz referência podem ser verificados. Essa mensagem é incluída apenas no modo detalhado.
`Digest file`	`INVALID: has been moved from its original location`	O bucket do S3 ou o objeto do S3 do qual o arquivo de resumo foi recuperado não corresponde aos locais do bucket do S3 ou do objeto do S3 que são registrados no próprio arquivo de resumo.

Tipo de arquivo	Mensagem de validação	Descrição
Digest file	INVALID: invalid format	O formato do arquivo de resumo é inválido. Os arquivos de log correspondentes ao período que o arquivo de resumo representa não podem ser validados.
Digest file	INVALID: not found	O arquivo de resumo não foi encontrado. Os arquivos de log correspondentes ao período que o arquivo de resumo representa não podem ser validados.
Digest file	INVALID: public key not found for fingerprint *impressão digital*	A chave pública correspondente à impressão digital registrada no arquivo de resumo não foi encontrada. O arquivo de resumo não pode ser validado.
Digest file	INVALID: signature verification failed	A assinatura do arquivo de resumo não é válida. Como o arquivo de resumo não é válido, os arquivos de log aos quais ele faz referência não podem ser validados, e nenhuma declaração pode ser feita sobre a atividade da API neles.
Digest file	INVALID: Unable to load PKCS #1 key with fingerprint *impressão digital*	Como a chave pública DER codificada no formato PKCS #1 que contém a impressão digital especificada não pode ser carregada, o arquivo de resumo não pode ser validado.
Log file	valid	O arquivo de log foi validado e não foi modificado desde o horário do fornecimento. Essa mensagem é incluída apenas no modo detalhado.
Log file	INVALID: hash value doesn't match	O hash do arquivo de log não é correspon dente. O arquivo de log foi modificado após a entrega por CloudTrail.

Tipo de arquivo	Mensagem de validação	Descrição
`Log file`	`INVALID: invalid format`	O formato do arquivo de log é inválido. O arquivo de log não pode ser validado.
`Log file`	`INVALID: not found`	O arquivo de log não foi encontrado e não pode ser validado.

A saída inclui informações resumidas sobre os resultados retornados.

Exemplos de resultados

Detalhado

O exemplo de comando `validate-logs` usa o sinalizador `--verbose` e produz o exemplo de resultado a seguir. `[...]` indica que o resultado de amostra foi abreviado.

```
aws cloudtrail validate-logs --trail-arn arn:aws:cloudtrail:us-
east-2:111111111111:trail/example-trail-name --start-time 2015-08-31T22:00:00Z --end-
time 2015-09-01T19:17:29Z --verbose
```

```
Validating log files for trail arn:aws:cloudtrail:us-east-2:111111111111:trail/example-
trail-name between 2015-08-31T22:00:00Z and 2015-09-01T19:17:29Z

Digest file    s3://example-bucket/AWSLogs/111111111111/CloudTrail-Digest/us-
east-2/2015/09/01/111111111111_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T201728Z.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1925Z_WZZw1RymnjCRjxXc.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1915Z_POuvV87nu6pfAV2W.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1930Z_l2QgXhAKVm1QXiIA.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1920Z_eQJteBBrfpBCqOqw.json.gz valid
```

```
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1950Z_9g5A6qlR2B5KaRdq.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1920Z_i4DNCC12BuXd6Ru7.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1915Z_Sg5caf2RH6Jdx0EJ.json.gz valid
Digest file    s3://example-bucket/AWSLogs/111111111111/CloudTrail-Digest/us-
east-2/2015/09/01/111111111111_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T191728Z.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1910Z_YYSFiuFQk4nrtnEW.json.gz valid
[...]
Log file       s3://example-bucket/AWSLogs/144218288521/
CloudTrail/us-east-2/2015/09/01/144218288521_CloudTrail_us-
east-2_20150901T1055Z_0Sfy6m9f6iBzmoPF.json.gz valid
Log file       s3://example-bucket/AWSLogs/144218288521/
CloudTrail/us-east-2/2015/09/01/144218288521_CloudTrail_us-
east-2_20150901T1040Z_lLa3QzVLpOed7igR.json.gz valid

Digest file    s3://example-bucket/AWSLogs/144218288521/CloudTrail-Digest/us-
east-2/2015/09/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T101728Z.json.gz INVALID: signature verification failed

Digest file    s3://example-bucket/AWSLogs/144218288521/CloudTrail-Digest/us-
east-2/2015/09/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T091728Z.json.gz valid
Log file       s3://example-bucket/AWSLogs/144218288521/
CloudTrail/us-east-2/2015/09/01/144218288521_CloudTrail_us-
east-2_20150901T0830Z_eaFvO3dwHo4NCqqc.json.gz valid
Digest file    s3://example-bucket/AWSLogs/144218288521/CloudTrail-Digest/us-
east-2/2015/09/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T081728Z.json.gz valid
Digest file    s3://example-bucket/AWSLogs/144218288521/CloudTrail-Digest/us-
east-2/2015/09/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T071728Z.json.gz valid
[...]
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/08/31/111111111111_CloudTrail_us-
east-2_20150831T2245Z_mbJkEO5kNcDnVhGh.json.gz valid
```

```
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/08/31/111111111111_CloudTrail_us-
east-2_20150831T2225Z_IQ6kXy8sKU03RSPr.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/08/31/111111111111_CloudTrail_us-
east-2_20150831T2230Z_eRPVRTxHQ5498ROA.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/08/31/111111111111_CloudTrail_us-
east-2_20150831T2255Z_IlWawYZGvTWB5vYN.json.gz valid
Digest file    s3://example-bucket/AWSLogs/111111111111/CloudTrail-Digest/us-
east-2/2015/08/31/111111111111_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150831T221728Z.json.gz valid

Results requested for 2015-08-31T22:00:00Z to 2015-09-01T19:17:29Z
Results found for 2015-08-31T22:17:28Z to 2015-09-01T20:17:28Z:

22/23 digest files valid, 1/23 digest files INVALID
63/63 log files valid
```

Não detalhado

O exemplo de comando `validate-logs` não usa o sinalizador `--verbose`. No exemplo de resultado a seguir, um erro foi encontrado. Somente o cabeçalho, o erro e as informações resumidas são retornados.

```
aws cloudtrail validate-logs --trail-arn arn:aws:cloudtrail:us-
east-2:111111111111:trail/example-trail-name --start-time 2015-08-31T22:00:00Z --end-
time 2015-09-01T19:17:29Z
```

```
Validating log files for trail arn:aws:cloudtrail:us-east-2:111111111111:trail/example-
trail-name between 2015-08-31T22:00:00Z and 2015-09-01T19:17:29Z

Digest file s3://example-bucket/AWSLogs/144218288521/CloudTrail-Digest/us-
east-2/2015/09/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T101728Z.json.gz INVALID: signature verification failed

Results requested for 2015-08-31T22:00:00Z to 2015-09-01T19:17:29Z
Results found for 2015-08-31T22:17:28Z to 2015-09-01T20:17:28Z:

22/23 digest files valid, 1/23 digest files INVALID
63/63 log files valid
```

Verificando se um arquivo específico foi entregue por CloudTrail

Para verificar se um arquivo específico em seu bucket foi entregue por CloudTrail, execute `validate-logs` no modo detalhado durante o período que inclui o arquivo. Se o arquivo aparecer na saída de`validate-logs`, então o arquivo foi entregue por CloudTrail.

CloudTrail estrutura do arquivo digest

Cada arquivo de resumo contém os nomes dos arquivos de log que foram fornecidos ao seu bucket do Amazon S3 durante a última hora, os valores de hash desses arquivos de log e a assinatura digital do arquivo de resumo anterior. A assinatura do arquivo de resumo atual está armazenada nas propriedades de metadados do objeto do arquivo de resumo. As assinaturas digitais e os hashes são usados para validar a integridade dos arquivos de log e do próprio arquivo de resumo.

Local do arquivo de resumo

Os arquivos de resumo são fornecidos ao local de um bucket do Amazon S3 que segue essa sintaxe.

```
s3://s3-bucket-name/optional-prefix/AWSLogs/aws-account-id/CloudTrail-Digest/
    region/digest-end-year/digest-end-month/digest-end-date/
    aws-account-id_CloudTrail-Digest_region_trail-
name_region_digest_end_timestamp.json.gz
```

> **Note**
>
> Para trilhas de organização, o local do bucket também inclui o ID da unidade organizacional, da seguinte forma:
>
> ```
> s3://s3-bucket-name/optional-prefix/AWSLogs/O-ID/aws-account-id/CloudTrail-
> Digest/
>     region/digest-end-year/digest-end-month/digest-end-date/
>     aws-account-id_CloudTrail-Digest_region_trail-
> name_region_digest_end_timestamp.json.gz
> ```

Amostra de conteúdo dos arquivos de resumo

O exemplo de arquivo de resumo a seguir contém informações para um CloudTrail log.

```
{
  "awsAccountId": "111122223333",
  "digestStartTime": "2015-08-17T14:01:31Z",
  "digestEndTime": "2015-08-17T15:01:31Z",
  "digestS3Bucket": "S3-bucket-name",
  "digestS3Object": "AWSLogs/111122223333/CloudTrail-Digest/us-
east-2/2015/08/17/111122223333_CloudTrail-Digest_us-east-2_your-trail-name_us-
east-2_20150817T150131Z.json.gz",
  "digestPublicKeyFingerprint": "31e8b5433410dfb61a9dc45cc65b22ff",
  "digestSignatureAlgorithm": "SHA256withRSA",
  "newestEventTime": "2015-08-17T14:52:27Z",
  "oldestEventTime": "2015-08-17T14:42:27Z",
  "previousDigestS3Bucket": "S3-bucket-name",
  "previousDigestS3Object": "AWSLogs/111122223333/CloudTrail-Digest/us-
east-2/2015/08/17/111122223333_CloudTrail-Digest_us-east-2_your-trail-name_us-
east-2_20150817T140131Z.json.gz",
  "previousDigestHashValue":
 "97fb791cf91ffc440d274f8190dbdd9aa09c34432aba82739df18b6d3c13df2d",
  "previousDigestHashAlgorithm": "SHA-256",
  "previousDigestSignature":
 "50887ccffad4c002b97caa37cc9dc626e3c680207d41d27fa5835458e066e0d3652fc4dfc30937e4d5f4cc7f796e7
  "logFiles": [
    {
      "s3Bucket": "S3-bucket-name",
      "s3Object": "AWSLogs/111122223333/CloudTrail/us-
east-2/2015/08/17/111122223333_CloudTrail_us-
east-2_20150817T1445Z_9nYN7gp2eWAJHIfT.json.gz",
      "hashValue": "9bb6196fc6b84d6f075a56548feca262bd99ba3c2de41b618e5b6e22c1fc71f6",
      "hashAlgorithm": "SHA-256",
      "newestEventTime": "2015-08-17T14:52:27Z",
      "oldestEventTime": "2015-08-17T14:42:27Z"
    }
  ]
}
```


Descrições dos campos dos arquivos de resumo

Veja a seguir descrições de cada campo no arquivo de resumo:

`awsAccountId`

O ID da AWS conta para a qual o arquivo de resumo foi entregue.

`digestStartTime`

O intervalo de tempo UTC inicial que o arquivo de resumo cobre, tomando como referência o horário em que os arquivos de log foram entregues. CloudTrail Isso significa que, se o período é [Ta, TB], o arquivo de resumo conterá todos os arquivos de log fornecidos ao cliente entre Ta e TB.

`digestEndTime`

O intervalo de tempo UTC final que o arquivo de resumo cobre, tomando como referência o horário em que os arquivos de log foram entregues. CloudTrail Isso significa que, se o período é [Ta, TB], o arquivo de resumo conterá todos os arquivos de log fornecidos ao cliente entre Ta e TB.

`digestS3Bucket`

O nome do bucket do Amazon S3 ao qual o arquivo de resumo atual foi fornecido.

`digestS3Object`

A chave do objeto do Amazon S3 (ou seja, o local do bucket do Amazon S3) do arquivo de resumo atual. As duas primeiras regiões na string mostram a região da qual o arquivo de resumo foi fornecido. A última região (após `your-trail-name`) é a região de origem da trilha. A região de origem é aquela em que a trilha foi criada. No caso de uma trilha com várias regiões, isso pode ser diferente da região da qual o arquivo de resumo foi entregue.

`newestEventTime`

O horário UTC do evento mais recente entre todos os eventos nos arquivos de log da compilação.

`oldestEventTime`

O horário UTC do evento mais antigo entre todos os eventos nos arquivos de log da compilação.

> **Note**
>
> Se o arquivo de resumo for fornecido com atraso, o valor de `oldestEventTime` será anterior ao de `digestStartTime`.

`previousDigestS3Bucket`

O bucket do Amazon S3 ao qual o arquivo de resumo anterior foi fornecido.

`previousDigestS3Object`

A chave do objeto do Amazon S3 (ou seja, o local do bucket do Amazon S3) do arquivo de resumo anterior.

`previousDigestHashValue`

O valor de hash codificado hexadecimal do conteúdo não compactado do arquivo de resumo anterior.

`previousDigestHashAlgorithm`

O nome do algoritmo de hash que foi usado para fazer hash do arquivo de resumo anterior.

`publicKeyFingerprint`

A impressão digital com codificação hexadecimal da chave pública que corresponde à chave privada usada para assinar esse arquivo de resumo. Você pode recuperar as chaves públicas para o intervalo de tempo correspondente ao arquivo de resumo usando a AWS CLI ou a CloudTrail API. Das chaves públicas retornadas, aquela cuja impressão digital corresponde a esse valor pode ser usada para validar o arquivo de resumo. Para obter informações sobre como recuperar chaves públicas para arquivos de resumo, consulte o AWS CLI `list-public-keys`comando ou a CloudTrail `ListPublicKeys`API.

> **Note**
>
> CloudTrail usa diferentes pares de chaves privadas/públicas por região. Cada arquivo de resumo é assinado com uma chave privada exclusiva de sua respectiva região. Portanto,

quando você valida um arquivo de resumo de uma região específica, precisa procurar a chave pública correspondente na mesma região.

`digestSignatureAlgorithm`

O algoritmo usado para assinar o arquivo de resumo.

`logFiles.s3Bucket`

O nome do bucket do Amazon S3 do arquivo de log.

`logFiles.s3Object`

A chave do objeto do Amazon S3 do arquivo de log atual.

`logFiles.newestEventTime`

O horário UTC do evento mais recente no arquivo de log. Esse horário também corresponde ao time stamp do arquivo de log em si.

`logFiles.oldestEventTime`

O horário UTC do evento mais antigo no arquivo de log.

`logFiles.hashValue`

O valor de hash codificado hexadecimal do conteúdo do arquivo de log não compactado.

`logFiles.hashAlgorithm`

O algoritmo de hash usado para fazer hash do arquivo de log.

Arquivo de resumo inicial

Quando a validação da integridade do arquivo de log é iniciada, um arquivo de resumo inicial é gerado. Um arquivo de resumo inicial também é gerado quando a validação da integridade dos arquivos de log é reiniciada (com a desativação e a reativação da validação da integridade dos

arquivos de log ou a interrupção e a reinicialização do registro com a validação ativada). Em um arquivo de resumo inicial, os seguintes campos relacionados ao arquivo de resumo anterior serão nulos:

- `previousDigestS3Bucket`
- `previousDigestS3Object`
- `previousDigestHashValue`
- `previousDigestHashAlgorithm`
- `previousDigestSignature`

Arquivos de resumo "vazios"

CloudTrail entregará um arquivo de resumo mesmo quando não houver atividade de API em sua conta durante o período de uma hora que o arquivo de resumo representa. Isso pode ser útil quando você precisa confirmar que nenhum arquivo de log foi fornecido durante a hora informada pelo arquivo de resumo.

O exemplo a seguir mostra o conteúdo de um arquivo de resumo que registrou uma hora na qual não ocorreram atividades de API. O campo `logFiles:[ ]` no final do conteúdo do arquivo de resumo está vazio.

```
{
  "awsAccountId": "111122223333",
  "digestStartTime": "2015-08-20T17:01:31Z",
  "digestEndTime": "2015-08-20T18:01:31Z",
  "digestS3Bucket": "example-bucket-name",
  "digestS3Object": "AWSLogs/111122223333/CloudTrail-Digest/us-
east-2/2015/08/20/111122223333_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150820T180131Z.json.gz",
  "digestPublicKeyFingerprint": "31e8b5433410dfb61a9dc45cc65b22ff",
  "digestSignatureAlgorithm": "SHA256withRSA",
  "newestEventTime": null,
  "oldestEventTime": null,
  "previousDigestS3Bucket": "example-bucket-name",
  "previousDigestS3Object": "AWSLogs/111122223333/CloudTrail-Digest/us-
east-2/2015/08/20/111122223333_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150820T170131Z.json.gz",
  "previousDigestHashValue":
 "ed96c4bac9eaa8fe9716ca0e515da51938be651b1db31d781956416a9d05cdfa",
  "previousDigestHashAlgorithm": "SHA-256",
```

```
  "previousDigestSignature":
 "82705525fb0fe7f919f9434e5b7138cb41793c776c7414f3520c0242902daa8cc8286b29263d2627f2f259471c745
  "logFiles": []
}
```

Assinatura do arquivo de resumo

As informações da assinatura de um arquivo de resumo estão localizadas em duas propriedades de metadados do objeto do arquivo de resumo do Amazon S3. Cada arquivo de resumo tem as seguintes entradas de metadados:

- `x-amz-meta-signature`

  O valor codificado hexadecimal da assinatura do arquivo de resumo. Veja a seguir um exemplo de assinatura:

  ```
  3be472336fa2989ef34de1b3c1bf851f59eb030eaff3e2fb6600a082a23f4c6a82966565b994f9de4a5989d053d9d
  28f1cc237f372264a51b611c01da429565def703539f4e71009051769469231bc22232fa260df02740047af53222
  05d3ffcb5d2dd5dc28f8bb5b7993938e8a5f912a82b448a367eccb2ec0f198ba71e23eb0b97278cf65f3c8d1e652c
  ```

- `x-amz-meta-signature-algorithm`

  Veja a seguir um exemplo de valor do algoritmo usado para gerar a assinatura de compilação:

  `SHA256withRSA`

Encadeamento de arquivos de resumo

O fato de cada arquivo de resumo conter uma referência ao arquivo de resumo anterior permite um “encadeamento” que permite que ferramentas de validação como a AWS CLI detectem se um arquivo de resumo foi excluído. Ele também permite que os arquivos de resumo em um período específico sejam sucessivamente inspecionados, começando pelo mais recente.

> **Note**
>
> Quando você desativa a validação da integridade do arquivo de log, a cadeia de arquivos de resumo é interrompida após uma hora. CloudTrail não criará arquivos de resumo para arquivos de log que foram entregues durante um período em que a validação da integridade

do arquivo de log foi desativada. Por exemplo, se você ativar a validação da integridade dos arquivos de log ao meio-dia em 1º de janeiro, desativá-la ao meio-dia em 2 de janeiro e reativá-la em 10 de janeiro ao meio-dia, os arquivos de resumo não serão criados para os arquivos de log fornecidos a partir do meio-dia em 2 de janeiro ao meio-dia em 10 de janeiro. O mesmo se aplica sempre que você para de CloudTrail registrar ou excluir uma trilha.

Se a política de bucket do S3 da sua trilha estiver configurada incorretamente ou CloudTrail sofrer uma interrupção inesperada do serviço, talvez você não receba todos ou alguns arquivos de resumo. Para confirmar se sua trilha tem algum erro de entrega de resumo, execute o `get-trail-status`comando e verifique se há erros no `LatestDigestDeliveryError` parâmetro. Depois que o problema de entrega for resolvido (por exemplo, corrigindo a política do bucket), CloudTrail tentará reentregar todos os arquivos de resumo ausentes. Durante o período de reentrega, os arquivos de resumo podem ser entregues fora de ordem, então a cadeia pode parecer temporariamente quebrada.

Se o registro for interrompido ou a trilha for excluída, CloudTrail entregará um arquivo de resumo final. Esse arquivo de resumo pode conter informações de todos os arquivos de log restantes que abrangem eventos até o evento `StopLogging` (inclusive).

Implementações personalizadas da validação da integridade do arquivo de CloudTrail log

Como CloudTrail usa algoritmos criptográficos e funções de hash padrão do setor e disponíveis abertamente, você pode criar suas próprias ferramentas para validar a integridade dos arquivos de log. CloudTrail Quando a validação da integridade do arquivo de log está habilitada, CloudTrail entrega os arquivos de resumo para o seu bucket do Amazon S3. Você pode usar esses arquivos para implementar sua própria solução de validação. Para obter mais informações sobre os arquivos de resumo, consulte CloudTrail estrutura do arquivo digest.

Este tópico descreve como os arquivos de resumo são assinados e explica detalhadamente as etapas que você precisará seguir para implementar uma solução que valida os arquivos de resumo e os arquivos de log aos quais eles fazem referência.

Entendendo como os arquivos de CloudTrail resumo são assinados

CloudTrail os arquivos de resumo são assinados com assinaturas digitais RSA. Para cada arquivo de resumo, CloudTrail faça o seguinte:

1. Cria uma string para assinatura de dados com base em campos de arquivos de resumo designados (descritos na próxima seção).
2. Obtém uma chave privada exclusiva para a região.
3. Transmite o hash SHA-256 da string e a chave privada ao algoritmo de assinatura RSA, que produz uma assinatura digital.
4. Codifica o código de byte da assinatura em formato hexadecimal.
5. Insere a assinatura digital na propriedade de metadados `x-amz-meta-signature` do objeto do arquivo de resumo do Amazon S3.

Conteúdo da string de assinatura de dados

Os seguintes CloudTrail objetos são incluídos na string para assinatura de dados:

- O carimbo de data e hora final do arquivo de resumo no formato estendido UTC (por exemplo, `2015-05-08T07:19:37Z`)
- O caminho atual do arquivo de resumo do S3
- O hash SHA-256 com codificação hexadecimal do arquivo de resumo atual
- A assinatura com codificação hexadecimal do arquivo de resumo anterior

O formato para calcular essa string e uma string de exemplo são fornecidos posteriormente neste documento.

Etapas da implementação da validação personalizada

Ao implementar uma solução de validação personalizada, você precisará validar o arquivo de resumo primeiro e os arquivos de log aos quais ele faz referência.

Validar o arquivo de resumo

Para validar um arquivo de resumo, você precisa da assinatura dele, da chave pública cuja chave privada foi usada para assiná-lo e de uma string de assinatura de dados computada.

1. Obtenha o arquivo de resumo.
2. Verifique se o arquivo de resumo foi recuperado de seu local original.
3. Obtenha a assinatura com codificação hexadecimal do arquivo de resumo.
4. Obtenha a impressão digital com codificação hexadecimal da chave pública cuja chave privada foi usada para assinar o arquivo de resumo.

5. Recupere as chaves públicas do período correspondente ao arquivo de resumo.
6. Entre as chaves públicas recuperadas, escolha aquela cuja impressão digital corresponde à impressão digital do arquivo de resumo.
7. Usando o hash do arquivo de resumo e outros campos de arquivos de resumo, recrie a string de assinatura de dados usada para verificar a assinatura do arquivo de resumo.
8. Para validar a assinatura, transmita o hash SHA-256 da string, a chave pública e a assinatura como parâmetros ao algoritmo de verificação de assinatura RSA. Se o resultado for verdadeiro, o arquivo de resumo será válido.

Validar os arquivos de log

Se o arquivo de resumo for válido, valide cada um dos arquivos de log aos quais o arquivo de resumo faz referência.

1. Para validar a integridade de um arquivo de log, compute o valor de hash SHA-256 dele em seu conteúdo não compactado e compare os resultados com o hash do arquivo de log gravado em formato hexadecimal na compilação. Se os hashes forem correspondentes, o arquivo de log será válido.
2. Com as informações sobre o arquivo de resumo anterior que está incluído no arquivo de resumo atual, valide os arquivos de resumo anteriores e seus arquivos de log correspondentes de maneira consecutiva.

As seções a seguir descrevem essas etapas em detalhes.

A. Obter o arquivo de resumo

As primeiras etapas são: obter o arquivo de resumo mais recente, verificar se você o recuperou do local original dele, verificar sua assinatura digital e obter a impressão digital da chave pública.

1. Usando a classe S3 `GetObject`ou a classe AmazonS3Client (por exemplo), obtenha o arquivo de resumo mais recente do seu bucket do Amazon S3 para o intervalo de tempo que você deseja validar.
2. Verifique se o bucket e o objeto do S3 usados para recuperar o arquivo correspondem aos locais do bucket e do objeto do S3 que são registrados no próprio arquivo de resumo.
3. Em seguida, obtenha a assinatura digital do arquivo de resumo da propriedade de metadados `x-amz-meta-signature` do objeto do arquivo de resumo no Amazon S3.

4. No arquivo de resumo, obtenha a impressão digital da chave pública cuja chave privada foi usada para assinar o arquivo de resumo do campo `digestPublicKeyFingerprint`.

B. Recupere a chave pública para validar o arquivo de resumo

Para obter a chave pública para validar o arquivo de resumo, você pode usar a API AWS CLI ou a CloudTrail API. Em ambos os casos, você especifica um período (ou seja, um horário de início e de término) para os arquivos de resumo que você deseja validar. Uma ou mais chaves públicas podem ser retornadas para o período que você especificar. As chaves retornadas podem ter períodos de validade que se sobrepõem.

> **Note**
>
> Como CloudTrail usa diferentes pares de chaves privadas/públicas por região, cada arquivo de resumo é assinado com uma chave privada exclusiva para sua região. Portanto, quando você valida um arquivo de resumo de uma região específica, precisa recuperar a chave pública da mesma região.

Use o AWS CLI para recuperar chaves públicas

Para recuperar chaves públicas para arquivos de resumo usando o AWS CLI, use o `cloudtrail list-public-keys` comando. O comando tem o formato a seguir:

```
aws cloudtrail list-public-keys [--start-time <start-time>] [--end-time <end-time>]
```

Os parâmetros de horário de início e de término são carimbos de data e hora UTC opcionais. Se eles não forem especificados, a hora atual será usada, e a chave ou as chaves públicas atualmente ativas serão retornadas.

Exemplo de resposta

A resposta será uma lista de objetos JSON que representam a chave ou as chaves retornadas:

```
{
    "publicKeyList": [
        {
            "ValidityStartTime": "1436317441.0",
            "ValidityEndTime": "1438909441.0",
```

```
            "Value": "MIIBCgKCAQEAn11L2YZ9h7onug2ILi1MWyHiMRsTQjfWE
+pHVRLk1QjfWhirG+lpOa8NrwQ/r7Ah5bNL6HepznOU9XTDSfmmnP97mqyc7z/upfZdS/AHhYcGaz7n6Wc/
RRBU6VmiPCrAUojuSk6/GjvA8iOPFsYDuBtviXarvuLPlrT9kAd4Lb+rFfR5peEgBEkhlzc5HuWO7S0y
+KunqxX6jQBnXGMtxmPBPP0FylgWGNdFtks/4YSKcgqwH0YDcawP9GGGDAeCIqPWIXDLG1jOjRRzWfCmD0iJUkz8vTsn4hq
            "Fingerprint": "8eba5db5bea9b640d1c96a77256fe7f2"
        },
        {
            "ValidityStartTime": "1434589460.0",
            "ValidityEndTime": "1437181460.0",
            "Value": "MIIBCgKCAQEApfYL2FiZhpN74LNWVUzhR
+VheYhwhYm8w0n5Gf6i95ylW5kBAWKVEmnAQG7BvS5g9SMqFDQx52fW7NWV44IvfJ2xGXT
+wT+DgR6ZQ+6yxskQNqV5YcXj4Aa5Zz4jJfsYjDuO2MDTZNIzNvBNzaBJ+r2WIWAJ/
Xq54kyF63B6WE38vKuDE7nSd1FqQuEoNBFLPInvgggYe2Ym1Refe2z71wNcJ2kY
+q0h1BSHrSM8RWuJIw7MXwF9iQncg9jYzUlNJomozQzAG5wSRfbplcCYNY40xvGd/aAmO0m+Y
+XFMrKwtLCwseHPvj843qVno6x4BJN9bpWnoPo9sdsbGoiK3QIDAQAB",
            "Fingerprint": "8933b39ddc64d26d8e14ffbf6566fee4"
        },
        {
            "ValidityStartTime": "1434589370.0",
            "ValidityEndTime": "1437181370.0",
            "Value":
 "MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAqlzPJbvZJ42UdcmLfPUqXYNfOs6I8lCfao/
tOs8CmzPOEdtLWugB9xoIUz78qVHdKIqxbaG4jWHfJBiOSSFBM0lt8cdVo4TnRa7oG9io5pysS6DJhBBAeXsicufsiFJR
+wrUNh8RSLxL4k6G1+BhLX20tJkZ/erT97tDGBujAelqseGg3vPZbTx9SMfOLN65PdLFudLP7Gat0Z9p5jw/
rjpclKfo9Bfc3heeBxWGKwBBOKnFAaN9V57pOaosCvPKmHd9bg7jsQkI9Xp22IzGLsTFJZYVA3KiTAElDMu80iFXPHEq9hK
+1utKVEiLkR2disdCmPTK0VQIDAQAB",
            "Fingerprint": "31e8b5433410dfb61a9dc45cc65b22ff"
        }
    ]
}
```


Use a CloudTrail API para recuperar chaves públicas

Para recuperar chaves públicas para arquivos de resumo usando a CloudTrail API, transmita os valores de hora de início e hora de término para a `ListPublicKeys` API. A API `ListPublicKeys` retorna as chaves públicas cujas chaves privadas foram usadas para assinar arquivos de resumo dentro do período especificado. Para cada chave pública, a API também retorna a impressão digital correspondente.

`ListPublicKeys`

Esta seção descreve os parâmetros de solicitação e os elementos de resposta da API `ListPublicKeys`.

> **Note**
>
> A codificação dos campos binários de `ListPublicKeys` está sujeita a alterações.

Parâmetros de solicitação

Nome	Descrição
`StartTime`	Opcionalmente, especifica, em UTC, o início do intervalo de tempo para pesquisar chaves públicas para arquivos de resumo. CloudTrail Se não StartTime for especificado, a hora atual será usada e a chave pública atual será retornada. Tipo: DateTime
`EndTime`	Opcionalmente, especifica, em UTC, o final do intervalo de tempo para pesquisar chaves públicas para arquivos de resumo. CloudTrail Se não EndTime for especificado, a hora atual será usada. Tipo: DateTime

Elementos de resposta

`PublicKeyList`, um conjunto de `PublicKey` objetos que contém:

Name (Nome)	Descrição
`Value`	O valor de chave pública codificado DER no formato PKCS #1. Tipo: Blob
`ValidityStartTime`	O horário de início da validade da chave pública. Tipo: DateTime
`ValidityEndTime`	O horário de término da validade da chave pública. Tipo: DateTime

`Fingerprint`	A impressão digital da chave pública. A impressão digital pode ser usada para identificar a chave pública que você precisa usar para validar o arquivo de resumo. Tipo: string

C. Escolha a chave pública a ser usada para a validação

Entre as chaves públicas recuperadas por `list-public-keys` ou `ListPublicKeys`, escolha a chave retornada cuja impressão digital corresponde à impressão digital gravada no campo `digestPublicKeyFingerprint` do arquivo de resumo. Esta é a chave pública que você usará para validar o arquivo de resumo.

D. Recrie a string de assinatura de dados

Agora que você tem a assinatura do arquivo de resumo e a chave pública associada, precisa calcular a string de assinatura de dados. Depois que você calcular a string de assinatura de dados, terá o necessário para verificar a assinatura.

A string de assinatura de dados tem o seguinte formato:

```
Data_To_Sign_String =
  Digest_End_Timestamp_in_UTC_Extended_format + '\n' +
  Current_Digest_File_S3_Path + '\n' +
  Hex(Sha256(current-digest-file-content)) + '\n' +
  Previous_digest_signature_in_hex
```

Veja a seguir um exemplo de `Data_To_Sign_String`.

```
2015-08-12T04:01:31Z
S3-bucket-name/AWSLogs/111122223333/CloudTrail-Digest/us-
east-2/2015/08/12/111122223333_us-east-2_CloudTrail-Digest_us-
east-2_20150812T040131Z.json.gz
4ff08d7c6ecd6eb313257e839645d20363ee3784a2328a7d76b99b53cc9bcacd
6e8540b83c3ac86a0312d971a225361d28ed0af20d70c211a2d405e32abf529a8145c2966e3bb47362383a52441545e
d4c7c09dd152b84e79099ce7a9ec35d2b264eb92eb6e090f1e5ec5d40ec8a0729c02ff57f9e30d5343a8591638f8b79
98b0aee2c1c8af74ec620261529265e83a9834ebef6054979d3e9a6767dfa6fdb4ae153436c567d6ae208f988047ccf
```

Depois que você recriar essa string, poderá validar o arquivo de resumo.

E. Valide o arquivo de resumo

Transmita o hash SHA-256 da string de assinatura de dados recriada, a assinatura digital e a chave pública ao algoritmo de verificação de assinatura RSA. Se o resultado for verdadeiro, a assinatura do arquivo de resumo será verificada, e o arquivo de resumo será válido.

F. Valide os arquivos de log

Depois que você validar o arquivo de resumo, poderá validar os arquivos de log aos quais ele faz referência. O arquivo de resumo contém os hashes SHA-256 dos arquivos de log. Se um dos arquivos de log for modificado após a CloudTrail entrega, os hashes SHA-256 serão alterados e a assinatura do arquivo de resumo não corresponderá.

Veja a seguir como validar os arquivos de log:

1. Faça um `S3 Get` do arquivo de log usando as informações de local do S3 nos campos `logFiles.s3Bucket` e `logFiles.s3Object` do arquivo de resumo.
2. Se a operação `S3 Get` for bem-sucedida, percorra os arquivos de log listados no conjunto de arquivos de log seguindo estas etapas:
   a. Recupere o hash original do arquivo no campo `logFiles.hashValue` do log correspondente no arquivo de resumo.
   b. Faça hash do conteúdo descompactado do arquivo de log com o algoritmo de hashing especificado em `logFiles.hashAlgorithm`.
   c. Compare o valor de hash que você gerou com o valor do log no arquivo de resumo. Se os hashes forem correspondentes, o arquivo de log será válido.

G. Valide arquivos de log e de compilação adicionais

Em cada arquivo de resumo, os campos a seguir fornecem o local e a assinatura do arquivo de resumo anterior:

- `previousDigestS3Bucket`
- `previousDigestS3Object`
- `previousDigestSignature`

Use essas informações para acessar os arquivos de resumo anteriores em sequência, validando a assinatura de cada um deles e os arquivos de log aos quais eles fazem referência seguindo as

etapas das seções anteriores. A única diferença é que, para os arquivos de resumo anteriores, você não precisa recuperar a assinatura digital das propriedades de metadados do Amazon S3 do objeto do arquivo de resumo. A assinatura do arquivo de resumo anterior é fornecida a você no campo `previousDigestSignature`.

Você pode voltar até que o arquivo de resumo inicial seja atingido ou até que a cadeia de arquivos de resumo seja interrompida, o que ocorrer primeiro.

Validar arquivos de log e de resumo offline

Ao validar os arquivos de log e de compilação offline, você pode seguir os procedimentos descritos nas seções anteriores. No entanto, é necessário levar em conta as seguintes áreas:

Processar o arquivo de resumo mais recente

A assinatura digital do arquivo de resumo mais recente (ou seja, "atual") está nas propriedades de metadados do Amazon S3 do objeto do arquivo de resumo. Em um cenário offline, a assinatura digital do arquivo de resumo atual não é disponibilizada.

Veja a seguir duas possíveis maneiras de fazer isso:

- Como a assinatura digital do arquivo de resumo anterior está no arquivo de resumo atual, comece a validar a partir do next-to-last arquivo de resumo. Com esse método, não é possível validar o arquivo de resumo mais recente.
- Como etapa preliminar, obtenha a assinatura do arquivo de resumo atual das propriedades de metadados do objeto do arquivo de resumo e armazene-a offline com segurança. Isso permite que o arquivo de resumo atual seja validado, além dos arquivos anteriores da cadeia.

Resolução de caminho

Os campos nos arquivos de resumo obtidos por download, como `s3Object` e `previousDigestS3Object`, ainda apontarão para os locais online do Amazon S3 dos arquivos de log e de resumo. Uma solução offline precisa encontrar uma maneira de redirecioná-los para o caminho atual dos arquivos de log e de compilação baixados.

Chaves públicas

Para fazer a validação offline, todas as chaves públicas de que você precisa para validar os arquivos de log em um determinado período precisam primeiro ser obtidas online (ao chamar `ListPublicKeys`, por exemplo) e, depois, armazenadas offline com segurança. Essa etapa

precisará ser repetida sempre que você quiser validar arquivos adicionais fora do período inicial que especificou.

Exemplo de snippet de validação

O trecho de amostra a seguir fornece código básico para validar arquivos de CloudTrail resumo e log. O código esqueleto pode ser online ou offline, ou seja, você decide se o implementará com ou sem conectividade online na AWS. A implementação sugerida usa Java Cryptography Extension (JCE) e Bouncy Castle como um provedor de segurança.

O exemplo de snippet mostra:

- Como criar a string de assinatura de dados usada para validar a assinatura do arquivo de resumo.
- Como verificar a assinatura do arquivo de resumo.
- Como verificar os hashes do arquivo de log.
- Uma estrutura de código para validar uma cadeia de arquivos de resumo.

```
import java.util.Arrays;
import java.security.MessageDigest;
import java.security.KeyFactory;
import java.security.PublicKey;
import java.security.Security;
import java.security.Signature;
import java.security.spec.X509EncodedKeySpec;
import org.json.JSONObject;
import org.bouncycastle.jce.provider.BouncyCastleProvider;
import org.apache.commons.codec.binary.Hex;

public class DigestFileValidator {

    public void validateDigestFile(String digestS3Bucket, String digestS3Object, String
 digestSignature) {

        // Using the Bouncy Castle provider as a JCE security provider - http://
www.bouncycastle.org/
        Security.addProvider(new BouncyCastleProvider());

        // Load the digest file from S3 (using Amazon S3 Client) or from your local
 copy
        JSONObject digestFile = loadDigestFileInMemory(digestS3Bucket, digestS3Object);
```

```
        // Check that the digest file has been retrieved from its original location
        if (!digestFile.getString("digestS3Bucket").equals(digestS3Bucket) ||
                !digestFile.getString("digestS3Object").equals(digestS3Object)) {
            System.err.println("Digest file has been moved from its original
location.");
        } else {
            // Compute digest file hash
            MessageDigest messageDigest = MessageDigest.getInstance("SHA-256");
            messageDigest.update(convertToByteArray(digestFile));
            byte[] digestFileHash = messageDigest.digest();
            messageDigest.reset();

            // Compute the data to sign
            String dataToSign = String.format("%s%n%s/%s%n%s%n%s",
                                digestFile.getString("digestEndTime"),
                                digestFile.getString("digestS3Bucket"),
digestFile.getString("digestS3Object"), // Constructing the S3 path of the digest file
as part of the data to sign
                                Hex.encodeHexString(digestFileHash),
                                digestFile.getString("previousDigestSignature"));

            byte[] signatureContent = Hex.decodeHex(digestSignature);

            /*
                NOTE:
                To find the right public key to verify the signature, call CloudTrail
ListPublicKey API to get a list
                of public keys, then match by the publicKeyFingerprint in the digest
file. Also, the public key bytes
                returned from ListPublicKey API are DER encoded in PKCS#1 format:

                PublicKeyInfo ::= SEQUENCE {
                    algorithm       AlgorithmIdentifier,
                    PublicKey       BIT STRING
                }

                AlgorithmIdentifier ::= SEQUENCE {
                    algorithm       OBJECT IDENTIFIER,
                    parameters      ANY DEFINED BY algorithm OPTIONAL
                }
            */
            pkcs1PublicKeyBytes =
getPublicKey(digestFile.getString("digestPublicKeyFingerprint")));
```

```
            // Transform the PKCS#1 formatted public key to x.509 format.
            RSAPublicKey rsaPublicKey = RSAPublicKey.getInstance(pkcs1PublicKeyBytes);
            AlgorithmIdentifier rsaEncryption = new
AlgorithmIdentifier(PKCSObjectIdentifiers.rsaEncryption, null);
            SubjectPublicKeyInfo publicKeyInfo = new
SubjectPublicKeyInfo(rsaEncryption, rsaPublicKey);

            // Create the PublicKey object needed for the signature validation
            PublicKey publicKey = KeyFactory.getInstance("RSA",
"BC").generatePublic(new X509EncodedKeySpec(publicKeyInfo.getEncoded()));

            // Verify signature
            Signature signature = Signature.getInstance("SHA256withRSA", "BC");
            signature.initVerify(publicKey);
            signature.update(dataToSign.getBytes("UTF-8"));

            if (signature.verify(signatureContent)) {
                System.out.println("Digest file signature is valid, validating log
files…");
                for (int i = 0; i < digestFile.getJSONArray("logFiles").length(); i++)
{

                    JSONObject logFileMetadata =
digestFile.getJSONArray("logFiles").getJSONObject(i);

                    // Compute log file hash
                    byte[] logFileContent = loadUncompressedLogFileInMemory(
                                                logFileMetadata.getString("s3Bucket"),
                                                logFileMetadata.getString("s3Object")
                                            );
                    messageDigest.update(logFileContent);
                     byte[] logFileHash = messageDigest.digest();
                    messageDigest.reset();

                    // Retrieve expected hash for the log file being processed
                    byte[] expectedHash =
Hex.decodeHex(logFileMetadata.getString("hashValue"));

                    boolean signaturesMatch = Arrays.equals(expectedHash, logFileHash);
                    if (!signaturesMatch) {
                        System.err.println(String.format("Log file: %s/%s hash doesn't
match.\tExpected: %s Actual: %s",
```

```
                                logFileMetadata.getString("s3Bucket"),
 logFileMetadata.getString("s3Object"),
                                Hex.encodeHexString(expectedHash),
 Hex.encodeHexString(logFileHash)));
                    } else {
                        System.out.println(String.format("Log file: %s/%s hash match",
                                logFileMetadata.getString("s3Bucket"),
 logFileMetadata.getString("s3Object")));
                    }
                }

            } else {
                System.err.println("Digest signature failed validation.");
            }

            System.out.println("Digest file validation completed.");

            if (chainValidationIsEnabled()) {
                // This enables the digests' chain validation
                validateDigestFile(
                        digestFile.getString("previousDigestS3Bucket"),
                        digestFile.getString("previousDigestS3Object"),
                        digestFile.getString("previousDigestSignature"));
            }
        }
    }
}
```

CloudTrail exemplos de arquivos de log

CloudTrail monitora eventos da sua conta. Se você criar uma trilha, ele fornecerá esses eventos como arquivos de log para o seu bucket do Amazon S3. Se você criar um armazenamento de dados de eventos no CloudTrail Lake, os eventos serão registrados no seu armazenamento de dados de eventos. Os armazenamentos de dados de eventos não usam buckets do S3.

Tópicos

- CloudTrail formato do nome do arquivo de log
- Exemplos de arquivos de log

CloudTrail formato do nome do arquivo de log

CloudTrail usa o seguinte formato de nome de arquivo para os objetos de arquivo de log que ele entrega ao seu bucket do Amazon S3:

```
AccountID_CloudTrail_RegionName_YYYYMMDDTHHmmZ_UniqueString.FileNameFormat
```

- YYYY, MM, DD, HH e mm são os dígitos do ano, mês, dia, hora e minuto quando o arquivo de log foi fornecido. Os horários estão no formato de 24 horas. O Z indica que o horário está em UTC.

  > **Note**
  >
  > Um arquivo de log entregue em um horário específico pode conter registros gravados a qualquer momento até aquele horário.

- O componente `UniqueString` de 16 caracteres do nome do arquivo de log está presente para evitar a substituição de arquivos. Ele não tem significado, e o software de processamento de logs deve ignorá-lo.
- `FileNameFormat` é a codificação do arquivo. Atualmente, ele é o `json.gz`, que é um arquivo de texto JSON em formato gzip compactado.

Exemplo de nome CloudTrail de arquivo de log

```
111122223333_CloudTrail_us-east-2_20150801T0210Z_Mu0KsOhtH1ar15ZZ.json.gz
```

Exemplos de arquivos de log

Um arquivo de log contém um ou mais registros. Os exemplos a seguir são fragmentos de logs que mostram os registros de uma ação que iniciou a criação de um arquivo de log.

Para obter informações sobre campos de registro de CloudTrail eventos, consulteCloudTrail conteúdo do registro.

Sumário

- Exemplos de código de erro e log de mensagens
- CloudTrail Exemplo de registro de eventos do Insights

Exemplos de log do Amazon EC2

O Amazon Elastic Compute Cloud (Amazon EC2) oferece uma capacidade de computação escalável na Nuvem Nuvem AWS. Você pode ativar servidores virtuais, configurar a segurança e a rede e gerenciar o armazenamento. O Amazon EC2 também pode fazer o escalonamento para cima ou para baixo rapidamente para gerenciar alterações em requisitos ou picos de popularidade, reduzindo assim a sua necessidade de prever o tráfego do servidor. Para obter mais informações, consulte o Guia do usuário do Amazon EC2 para instâncias do Linux.

O exemplo a seguir mostra que um usuário do IAM chamado `Mateo` executou o comando aws ec2 start-instances para chamar a ação `StartInstances` do Amazon EC2 para instâncias `i-EXAMPLE56126103cb` e `i-EXAMPLEaff4840c22`.


```
{"Records": [{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLE6E4XEGITWATV6R",
        "arn": "arn:aws:iam::123456789012:user/Mateo",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Mateo",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-07-19T21:11:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-19T21:17:28Z",
    "eventSource": "ec2.amazonaws.com",
    "eventName": "StartInstances",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
 exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/ec2.start-instances",
```

```
    "requestParameters": {
        "instancesSet": {
            "items": [
                {
                    "instanceId": "i-EXAMPLE56126103cb"
                },
                {
                    "instanceId": "i-EXAMPLEaff4840c22"
                }
            ]
        }
    },
    "responseElements": {
        "requestId": "e4336db0-149f-4a6b-844d-EXAMPLEb9d16",
        "instancesSet": {
            "items": [
                {
                    "instanceId": "i-EXAMPLEaff4840c22",
                    "currentState": {
                        "code": 0,
                        "name": "pending"
                    },
                    "previousState": {
                        "code": 80,
                        "name": "stopped"
                    }
                },
                {
                    "instanceId": "i-EXAMPLE56126103cb",
                    "currentState": {
                        "code": 0,
                        "name": "pending"
                    },
                    "previousState": {
                        "code": 80,
                        "name": "stopped"
                    }
                }
            ]
        }
    },
    "requestID": "e4336db0-149f-4a6b-844d-EXAMPLEb9d16",
    "eventID": "e755e09c-42f9-4c5c-9064-EXAMPLE228c7",
    "readOnly": false,
```

```
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
     "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "ec2.us-east-1.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}]}
```

O exemplo a seguir mostra que um usuário do IAM chamado `Nikki` executou o comando aws ec2 stop-instances para chamar a ação `StopInstances` do Amazon EC2 para parar duas instâncias.

```
{"Records": [{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLE6E4XEGITWATV6R",
        "arn": "arn:aws:iam::777788889999:user/Nikki",
        "accountId": "777788889999",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "Nikki",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-07-19T21:11:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-19T21:14:20Z",
    "eventSource": "ec2.amazonaws.com",
    "eventName": "StopInstances",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
 exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/ec2.stop-instances",
    "requestParameters": {
        "instancesSet": {
            "items": [
```

```
                {
                    "instanceId": "i-EXAMPLE56126103cb"
                },
                {
                    "instanceId": "i-EXAMPLEaff4840c22"
                }
            ]
        },
        "force": false
    },
    "responseElements": {
        "requestId": "c308a950-e43e-444e-afc1-EXAMPLE73e49",
        "instancesSet": {
            "items": [
                {
                    "instanceId": "i-EXAMPLE56126103cb",
                    "currentState": {
                        "code": 64,
                        "name": "stopping"
                    },
                    "previousState": {
                        "code": 16,
                        "name": "running"
                    }
                },
                {
                    "instanceId": "i-EXAMPLEaff4840c22",
                    "currentState": {
                        "code": 64,
                        "name": "stopping"
                    },
                    "previousState": {
                        "code": 16,
                        "name": "running"
                    }
                }
            ]
        }
    },
    "requestID": "c308a950-e43e-444e-afc1-EXAMPLE73e49",
    "eventID": "9357a8cc-a0eb-46a1-b67e-EXAMPLE19b14",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
```

```
    "recipientAccountId": "777788889999",
    "eventCategory": "Management",
     "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "ec2.us-east-1.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}]}
```

O exemplo a seguir mostra que um usuário do IAM chamado `Arnav` executou o comando aws ec2 create-key-pair para chamar a ação `CreateKeyPair`. Observe que eles `responseElements` contêm um hash do par de chaves e isso AWS removeu o material da chave.

```
{"Records": [{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDA6ON6E4XEGIEXAMPLE",
        "arn": "arn:aws:iam::444455556666:user/Arnav",
        "accountId": "444455556666",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "Arnav",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-07-19T21:11:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-19T21:19:22Z",
    "eventSource": "ec2.amazonaws.com",
    "eventName": "CreateKeyPair",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
 exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/ec2.create-key-pair",
    "requestParameters": {
        "keyName": "my-key",
        "keyType": "rsa",
        "keyFormat": "pem"
```

```
    },
    "responseElements": {
        "requestId": "9aa4938f-720f-4f4b-9637-EXAMPLE9a196",
        "keyName": "my-key",
        "keyFingerprint":
 "1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f",
        "keyPairId": "key-abcd12345eEXAMPLE",
        "keyMaterial": "<sensitiveDataRemoved>"
    },
    "requestID": "9aa4938f-720f-4f4b-9637-EXAMPLE9a196",
    "eventID": "2ae450ff-e72b-4de1-87b0-EXAMPLE5227cb",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "444455556666",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "ec2.us-east-1.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}]}
```

Exemplos de logs do IAM

AWS Identity and Access Management (IAM) é um serviço web que ajuda você a controlar com segurança o acesso aos AWS recursos. Com o IAM, é possível gerenciar, de maneira centralizada, permissões que controlam quais recursos da AWS os usuários poderão acessar. Você usa o IAM para controlar quem é autenticado (fez login) e autorizado (tem permissões) a usar os recursos. Para obter mais informações, consulte o Guia do usuário do IAM.

O exemplo a seguir mostra que o usuário do IAM chamado `Mary` executou o comando aws iam create-user para chamar a ação `CreateUser` para criar um novo usuário chamado `Richard`.

```
{"Records": [{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDA6ON6E4XEGITEXAMPLE",
        "arn": "arn:aws:iam::888888888888:user/Mary",
```

```
        "accountId": "888888888888",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Mary",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-07-19T21:11:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-19T21:25:09Z",
    "eventSource": "iam.amazonaws.com",
    "eventName": "CreateUser",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/iam.create-user",
    "requestParameters": {
        "userName": "Richard"
    },
    "responseElements": {
        "user": {
            "path": "/",
            "arn": "arn:aws:iam::888888888888:user/Richard",
            "userId": "AIDA6ON6E4XEP7EXAMPLE",
            "createDate": "Jul 19, 2023 9:25:09 PM",
            "userName": "Richard"
        }
    },
    "requestID": "2d528c76-329e-410b-9516-EXAMPLE565dc",
    "eventID": "ba0801a1-87ec-4d26-be87-EXAMPLE75bbb",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "888888888888",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "iam.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
```

```
}]}
```

O exemplo a seguir mostra que o usuário do IAM chamado `Paulo` executou o comando aws iam add-user-to-group para chamar a ação `AddUserToGroup` para adicionar um usuário chamado `Jane` ao grupo `Admin`.

```
{"Records": [{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDA6ON6E4XEGIEXAMPLE",
        "arn": "arn:aws:iam::555555555555:user/Paulo",
        "accountId": "555555555555",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Paulo",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-07-19T21:11:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-19T21:25:09Z",
    "eventSource": "iam.amazonaws.com",
    "eventName": "AddUserToGroup",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
 exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/iam.add-user-to-group",
    "requestParameters": {
        "groupName": "Admin",
        "userName": "Jane"
    },
    "responseElements": null,
    "requestID": "ecd94349-b36f-44bf-b6f5-EXAMPLE9c463",
    "eventID": "2939ba50-1d26-4a5a-83bd-EXAMPLE85850",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "555555555555",
    "eventCategory": "Management",
```

```
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "iam.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}]}
```

O exemplo a seguir mostra que o usuário do IAM chamado `Saanvi` executou o comando aws iam create-role para chamar a ação `CreateRole` para criar um perfil.

```
{"Records": [{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDA6ON6E4XEGITEXAMPLE",
        "arn": "arn:aws:iam::777777777777:user/Saanvi",
        "accountId": "777777777777",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Saanvi",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-07-19T21:11:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-19T21:29:12Z",
    "eventSource": "iam.amazonaws.com",
    "eventName": "CreateRole",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
 exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/iam.create-role",
    "requestParameters": {
        "roleName": "TestRole",
        "description": "Allows EC2 instances to call AWS services on your behalf.",
        "assumeRolePolicyDocument": "{\"Version\":\"2012-10-17\",\"Statement\":
[{\"Effect\":\"Allow\",\"Action\":[\"sts:AssumeRole\"],\"Principal\":{\"Service\":
[\"ec2.amazonaws.com\"]}}]}"
    },
```

```
    "responseElements": {
        "role": {
            "assumeRolePolicyDocument": "%7B%22Version%22%3A%222012-10-17%22%2C
%22Statement%22%3A%5B%7B%22Effect%22%3A%22Allow%22%2C%22Action%22%3A%5B%22sts
%3AAssumeRole%22%5D%2C%22Principal%22%3A%7B%22Service%22%3A%5B%22ec2.amazonaws.com
%22%5D%7D%7D%5D%7D",
            "arn": "arn:aws:iam::777777777777:role/TestRole",
            "roleId": "AROA6ON6E4XEFFEXAMPLE",
            "createDate": "Jul 19, 2023 9:29:12 PM",
            "roleName": "TestRole",
            "path": "/"
        }
    },
    "requestID": "ff38f36e-ebd3-425b-9939-EXAMPLE1bbe",
    "eventID": "9da77cd0-493f-4c89-8852-EXAMPLEa887c",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "777777777777",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "iam.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}]}
```

Exemplos de código de erro e log de mensagens

O exemplo a seguir mostra que o usuário do IAM chamado `Terry` executou o comando aws cloudtrail update-trail para chamar a ação `UpdateTrail` para atualizar uma trilha chamada `myTrail2`, mas o nome da trilha não foi encontrado. O registro mostra esse erro nos elementos `errorCode` e `errorMessage`.

```
{"Records": [{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDA6ON6E4XEGIEXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/Terry",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
```

```
        "userName": "Terry",
        "sessionContext": {
            "attributes": {
                "creationDate": "2023-07-19T21:11:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-19T21:35:03Z",
    "eventSource": "cloudtrail.amazonaws.com",
    "eventName": "UpdateTrail",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.0 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
 exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/cloudtrail.update-trail",
    "errorCode": "TrailNotFoundException",
    "errorMessage": "Unknown trail: arn:aws:cloudtrail:us-east-1:111122223333:trail/
myTrail2 for the user: 111122223333",
    "requestParameters": {
        "name": "myTrail2",
        "isMultiRegionTrail": true
    },
    "responseElements": null,
    "requestID": "28d2faaf-3319-4649-998d-EXAMPLE72818",
    "eventID": "694d604a-d190-4470-8dd1-EXAMPLEe20c1",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "cloudtrail.us-east-1.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}]}
```

CloudTrail Exemplo de registro de eventos do Insights

O exemplo a seguir mostra um registro de eventos do CloudTrail Insights. Um evento do Insights é, na verdade, um par de eventos que marcam o início e o fim de um período de atividade incomum da API de gerenciamento de gravação ou uma atividade de resposta de erro. O campo `state` mostra

se o evento foi registrado em log no início ou no fim do período de atividade incomum. O nome do evento,`UpdateInstanceInformation`, é o mesmo nome da AWS Systems Manager API para a qual os eventos de gerenciamento CloudTrail foram analisados para determinar a ocorrência de uma atividade incomum. Embora os eventos de início e de fim tenham valores `eventID` exclusivos, eles também têm um valor `sharedEventID` usado pelo par. O evento do Insights mostra o `baseline` ou o padrão normal de atividade, o `insight` ou a atividade média incomum que acionou o evento do Insights de início e no evento de término, o valor `insight` para a atividade média incomum pela duração do evento do Insights. Para obter mais informações sobre o CloudTrail Insights, consulteRegistrar eventos do Insights.


```
{
    "Records": [{
        "eventVersion": "1.08",
        "eventTime": "2023-01-02T02:51:00Z",
        "awsRegion": "us-east-1",
        "eventID": "654a30ff-b0f3-4527-81b6-EXAMPLEf2393",
        "eventType": "AwsCloudTrailInsight",
        "recipientAccountId": "123456789012",
        "sharedEventID": "bcbfc274-8559-4a56-beb0-EXAMPLEa6c34",
        "insightDetails": {
            "state": "Start",
            "eventSource": "ssm.amazonaws.com",
            "eventName": "UpdateInstanceInformation",
            "insightType": "ApiCallRateInsight",
            "insightContext": {
                "statistics": {
                    "baseline": {
                        "average": 84.410596421
                    },
                    "insight": {
                        "average": 669
                    }
                }
            }
        },
        "eventCategory": "Insight"
    },
    {
        "eventVersion": "1.08",
        "eventTime": "2023-01-02T00:22:00Z",
        "awsRegion": "us-east-1",
        "eventID": "258de2fb-e2a9-4fb5-aeb2-EXAMPLE449a4",
```

```
        "eventType": "AwsCloudTrailInsight",
        "recipientAccountId": "123456789012",
        "sharedEventID": "8b74a7bc-d5d3-4d19-9d60-EXAMPLE08b51",
        "insightDetails": {
            "state": "End",
            "eventSource": "ssm.amazonaws.com",
            "eventName": "UpdateInstanceInformation",
            "insightType": "ApiCallRateInsight",
            "insightContext": {
                "statistics": {
                    "baseline": {
                        "average": 74.156423842
                    },
                    "insight": {
                        "average": 657
                    },
                    "insightDuration": 1
                }
            }
        },
        "eventCategory": "Insight"
    }]
}
```

Usando a Biblioteca CloudTrail de Processamento

A Biblioteca CloudTrail de Processamento é uma biblioteca Java que fornece uma maneira fácil de processar AWS CloudTrail registros. Você fornece detalhes de configuração sobre sua fila CloudTrail SQS e grava código para processar eventos. A Biblioteca CloudTrail de Processamento faz o resto. Ele pesquisa sua fila do Amazon SQS, lê e analisa mensagens da fila, CloudTrail baixa arquivos de log, analisa eventos nos arquivos de log e passa os eventos para seu código como objetos Java.

A Biblioteca CloudTrail de Processamento é altamente escalável e tolerante a falhas. Ela lida com processamento paralelo de arquivos de log para que você possa processar quantos logs precisar. Ela lida com falhas de rede relacionadas a limites de tempo da rede e recursos inacessíveis.

O tópico a seguir mostra como usar a Biblioteca CloudTrail de Processamento para processar CloudTrail registros em seus projetos Java.

A biblioteca é fornecida como um projeto de código aberto licenciado pela Apache, disponível em:. GitHub https://github.com/aws/aws-cloudtrail-processing-library O código-fonte da biblioteca inclui código de exemplo que você pode usar como base para os seus próprios projetos.

Tópicos

Requisitos mínimos

Para usar a Biblioteca CloudTrail de Processamento, você deve ter o seguinte:

- AWS SDK for Java 1.11.830
- Java 1.8 (Java SE 8)

CloudTrail Registros de processamento

Para processar CloudTrail registros em seu aplicativo Java:

1. Adicionando a Biblioteca CloudTrail de Processamento ao seu projeto
2. Configurando a biblioteca de CloudTrail processamento
3. Implementar o processador de eventos
4. Instalar e executar o executor de processamento

Adicionando a Biblioteca CloudTrail de Processamento ao seu projeto

Para usar a Biblioteca CloudTrail de Processamento, adicione-a ao classpath do seu projeto Java.

Sumário

Adicionar a biblioteca a um projeto Apache Ant

Para adicionar a Biblioteca CloudTrail de Processamento a um projeto Apache Ant

1. Baixe ou clone o código-fonte da Biblioteca de CloudTrail Processamento em: GitHub
   - https://github.com/aws/ aws-cloudtrail-processing-library
2. Crie o arquivo .jar a partir do código-fonte, conforme descrito na seção README (LEIA-ME):

```
mvn clean install -Dgpg.skip=true
```

3. Copie o arquivo .jar resultante para o seu projeto e adicione-o ao arquivo `build.xml` do projeto. Por exemplo: .

```
<classpath>
  <pathelement path="${classpath}"/>
  <pathelement location="lib/aws-cloudtrail-processing-library-1.6.1.jar"/>
</classpath>
```

Adicionar a biblioteca a um projeto Apache Maven

A Biblioteca CloudTrail de Processamento está disponível para o Apache Maven. Você pode adicioná-la ao seu projeto escrevendo uma única dependência no arquivo `pom.xml` do seu projeto.

Para adicionar a Biblioteca CloudTrail de Processamento a um projeto Maven

- Abra o arquivo `pom.xml` do seu projeto Maven e adicione a seguinte dependência:

```
<dependency>
    <groupId>com.amazonaws</groupId>
    <artifactId>aws-cloudtrail-processing-library</artifactId>
    <version>1.6.1</version>
</dependency>
```

Adicionar a biblioteca a um projeto Eclipse

Para adicionar a Biblioteca CloudTrail de Processamento a um projeto Eclipse

1. Baixe ou clone o código-fonte da Biblioteca de CloudTrail Processamento em: GitHub
   - https://github.com/aws/ aws-cloudtrail-processing-library
2. Crie o arquivo .jar a partir do código-fonte, conforme descrito na seção README (LEIA-ME):

   ```
   mvn clean install -Dgpg.skip=true
   ```
3. Copie o aws-cloudtrail-processing-library -1.6.1.jar construído para um diretório em seu projeto (normalmente). `lib`
4. Clique com o botão direito do mouse no nome do projeto no Project Explorer (Explorador de projetos) do Eclipse, escolha Build Path (Caminho do build) e escolha Configure (Configurar)
5. Na janela Java Build Path (Caminho de build Java), escolha a guia Libraries (Bibliotecas).
6. Escolha Adicionar JARs... e navegue até o caminho em que você copiou aws-cloudtrail-processing-library -1.6.1.jar.
7. Escolha OK para concluir a adição do `.jar` ao seu projeto.

Adicionar a biblioteca a um projeto IntelliJ

Para adicionar a Biblioteca CloudTrail de Processamento a um projeto IntelliJ

1. Baixe ou clone o código-fonte da Biblioteca de CloudTrail Processamento em: GitHub
   - https://github.com/aws/ aws-cloudtrail-processing-library
2. Crie o arquivo .jar a partir do código-fonte, conforme descrito na seção README (LEIAME):

   ```
   mvn clean install -Dgpg.skip=true
   ```
3. Em File, escolha Project Structure.
4. Escolha Modules (Módulos) e escolha Dependencies (Dependências).
5. Escolha + JARS or Directories (+ JARS ou diretórios) e acesse o caminho em que você criou o `aws-cloudtrail-processing-library-1.6.1.jar`.
6. Escolha Apply (Aplicar) e escolha OK para concluir a adição do `.jar` ao seu projeto.

Configurando a biblioteca de CloudTrail processamento

Você pode configurar a Biblioteca CloudTrail de Processamento criando um arquivo de propriedades do caminho de classe que é carregado em tempo de execução ou criando um `ClientConfiguration` objeto e definindo as opções manualmente.

Fornecer um arquivo de propriedades

Você pode criar um arquivo de propriedades classpath que fornece opções de configuração ao seu aplicativo. O seguinte exemplo de arquivo mostra as opções que você pode definir:

```
# AWS access key. (Required)
accessKey = your_access_key

# AWS secret key. (Required)
secretKey = your_secret_key

# The SQS URL used to pull CloudTrail notification from. (Required)
sqsUrl = your_sqs_queue_url

# The SQS end point specific to a region.
sqsRegion = us-east-1

# A period of time during which Amazon SQS prevents other consuming components
# from receiving and processing that message.
visibilityTimeout = 60

# The S3 region to use.
s3Region = us-east-1

# Number of threads used to download S3 files in parallel. Callbacks can be
# invoked from any thread.
threadCount = 1

# The time allowed, in seconds, for threads to shut down after
# AWSCloudTrailEventProcessingExecutor.stop() is called. If they are still
# running beyond this time, they will be forcibly terminated.
threadTerminationDelaySeconds = 60

# The maximum number of AWSCloudTrailClientEvents sent to a single invocation
# of processEvents().
maxEventsPerEmit = 10
```

```
# Whether to include raw event information in CloudTrailDeliveryInfo.
enableRawEventInfo = false

# Whether to delete SQS message when the CloudTrail Processing Library is unable to
 process the notification.
deleteMessageUponFailure = false
```

Os seguintes parâmetros são obrigatórios:

- `sqsUrl`— Fornece o URL do qual extrair suas CloudTrail notificações. Se você não especificar esse valor, o `AWSCloudTrailProcessingExecutor` lança uma `IllegalStateException`.
- `accessKey` - Um identificador exclusivo para a sua conta, como AKIAIOSFODNN7EXAMPLE.
- `secretKey`— Um identificador exclusivo para sua conta, como bPxRfi wjalrxutnfemi/k7mdeng/CYEXAMPLEKEY.

Os `secretKey` parâmetros `accessKey` e fornecem suas AWS credenciais à biblioteca para que ela possa acessar AWS em seu nome.

O padrão para os outros parâmetros são definidos pela biblioteca. Para obter mais informações, consulte a Referência da Biblioteca de Processamento do AWS CloudTrail.

Criando um ClientConfiguration

Em vez de definir opções nas propriedades do classpath, você pode fornecer opções ao `AWSCloudTrailProcessingExecutor` inicializando e definindo opções em um objeto `ClientConfiguration`, como mostra este exemplo:

```
ClientConfiguration basicConfig = new ClientConfiguration(
    "http://sqs.us-east-1.amazonaws.com/123456789012/queue2",
    new DefaultAWSCredentialsProviderChain());

basicConfig.setEnableRawEventInfo(true);
basicConfig.setThreadCount(4);
basicConfig.setnEventsPerEmit(20);
```

Implementar o processador de eventos

Para processar CloudTrail registros, você deve implementar um `EventsProcessor` que receba os dados do CloudTrail registro. Este é um exemplo de nome de implementação:

```
public class SampleEventsProcessor implements EventsProcessor {

    public void process(List<CloudTrailEvent> events) {
        int i = 0;
        for (CloudTrailEvent event : events) {
            System.out.println(String.format("Process event %d : %s", i++,
 event.getEventData()));
        }
    }
}
```

Ao implementar um`EventsProcessor`, você implementa o `process()` retorno de chamada que ele `AWSCloudTrailProcessingExecutor` usa para enviar CloudTrail eventos a você. Os eventos são fornecidos em uma lista de objetos `CloudTrailClientEvent`.

O `CloudTrailClientEvent` objeto fornece um `CloudTrailEvent` e `CloudTrailEventMetadata` que você pode usar para ler as informações do CloudTrail evento e da entrega.

Esse exemplo simples imprime as informações de cada evento transmitido ao `SampleEventsProcessor`. Em sua própria implementação, você pode processar logs de acordo com a sua necessidade. O `AWSCloudTrailProcessingExecutor` continua enviando eventos ao seu `EventsProcessor`, desde que tenha eventos para enviar e ainda esteja em execução.

Instalar e executar o executor de processamento

Depois de escrever `EventsProcessor` e definir valores de configuração para a Biblioteca de CloudTrail Processamento (em um arquivo de propriedades ou usando a `ClientConfiguration` classe), você pode usar esses elementos para inicializar e usar um`AWSCloudTrailProcessingExecutor`.

Para usar **`AWSCloudTrailProcessingExecutor`** para processar CloudTrail eventos

1. Instanciar um objeto `AWSCloudTrailProcessingExecutor.Builder`. O construtor do `Builder` usa um objeto `EventsProcessor` e o nome de um arquivo de propriedades do caminho de classe.
2. Chame o método de fábrica `build()` do `Builder` para configurar e obter um objeto `AWSCloudTrailProcessingExecutor`.
3. Use os `AWSCloudTrailProcessingExecutor` `stop()` métodos `start()` e para iniciar e finalizar o processamento de CloudTrail eventos.

```
public class SampleApp {
  public static void main(String[] args) throws InterruptedException {
    AWSCloudTrailProcessingExecutor executor = new
      AWSCloudTrailProcessingExecutor.Builder(new SampleEventsProcessor(),
        "/myproject/cloudtrailprocessing.properties").build();

    executor.start();
    Thread.sleep(24 * 60 * 60 * 1000); // let it run for a while (optional)
    executor.stop(); // optional
  }
}
```

Tópicos avançados

Tópicos

Filtrar os eventos a serem processados

Por padrão, todos os logs no bucket do S3 da sua fila do Amazon SQS e todos os eventos que eles contêm são enviados para o `EventsProcessor`. A Biblioteca CloudTrail de Processamento fornece interfaces opcionais que você pode implementar para filtrar as fontes usadas para obter CloudTrail registros e filtrar os eventos que você tem interesse em processar.

`SourceFilter`

Você pode implementar a interface `SourceFilter` para escolher se deseja processar os logs de uma origem fornecida. `SourceFilter` declara um único método de retorno de chamada, `filterSource()`, que recebe um objeto `CloudTrailSource`. Para impedir que os eventos de uma origem sejam processados, retorne `false` de `filterSource()`.

A Biblioteca CloudTrail de processamento chama o `filterSource()` método depois que a biblioteca pesquisa os registros na fila do Amazon SQS. Isso ocorre antes de a biblioteca começar a filtragem de eventos ou o processamento de logs.

Este é um exemplo de nome de implementação:

```
public class SampleSourceFilter implements SourceFilter{
  private static final int MAX_RECEIVED_COUNT = 3;

  private static List<String> accountIDs ;
  static {
    accountIDs = new ArrayList<>();
    accountIDs.add("123456789012");
    accountIDs.add("234567890123");
  }

  @Override
  public boolean filterSource(CloudTrailSource source) throws CallbackException {
    source = (SQSBasedSource) source;
    Map<String, String> sourceAttributes = source.getSourceAttributes();

    String accountId = sourceAttributes.get(
      SourceAttributeKeys.ACCOUNT_ID.getAttributeKey());

    String receivedCount = sourceAttributes.get(
      SourceAttributeKeys.APPROXIMATE_RECEIVE_COUNT.getAttributeKey());

    int approximateReceivedCount = Integer.parseInt(receivedCount);

    return approximateReceivedCount <= MAX_RECEIVED_COUNT &&
 accountIDs.contains(accountId);
  }
}
```

Se você não fornecer seu próprio `SourceFilter`, `DefaultSourceFilter` será usado, o que permite que todas as origens sejam processadas (o valor retornado é sempre `true`).

`EventFilter`

Você pode implementar a `EventFilter` interface para escolher se um CloudTrail evento será enviado para o seu`EventsProcessor`. `EventFilter`declara um único método de retorno de chamada,`filterEvent()`, que recebe um `CloudTrailEvent` objeto. Para impedir que o evento seja processado, retorne `false` de `filterEvent()`.

A Biblioteca CloudTrail de processamento chama o `filterEvent()` método depois que a biblioteca pesquisa os registros na fila do Amazon SQS e após a filtragem da fonte. Isso ocorre antes de a biblioteca começar o processamento de eventos para os logs.

Veja este exemplo de implementação:

```
public class SampleEventFilter implements EventFilter{

  private static final String EC2_EVENTS = "ec2.amazonaws.com";

  @Override
  public boolean filterEvent(CloudTrailClientEvent clientEvent) throws
 CallbackException {
    CloudTrailEvent event = clientEvent.getEvent();

    String eventSource = event.getEventSource();
    String eventName = event.getEventName();

    return eventSource.equals(EC2_EVENTS) && eventName.startsWith("Delete");
  }
}
```

Se você não fornecer seu próprio `EventFilter`, `DefaultEventFilter` será usado, o que permite que todos os eventos sejam processados (o valor retornado é sempre `true`).

Processar eventos de dados

Ao CloudTrail processar eventos de dados, ele preserva os números em seu formato original, seja um inteiro (`int`) ou um `float` (um número que contém um decimal). Em eventos que têm números inteiros nos campos de um evento de dados, CloudTrail historicamente processou esses números como flutuantes. Atualmente, CloudTrail processa números nesses campos mantendo o formato original.

Como prática recomendada, para evitar a quebra de suas automações, seja flexível em qualquer código ou automação que você esteja usando para processar ou filtrar eventos de CloudTrail dados e permita ambos `int` e números `float` formatados. Para obter melhores resultados, use a versão 1.4.0 ou superior da Biblioteca de CloudTrail Processamento.

O snippet de exemplo a seguir mostra um número formatado `float` (`2.0`) para o parâmetro `desiredCount` no bloco de evento de dados `ResponseParameters`.

```
"eventName": "CreateService",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "000.00.00.00",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
```

```
        "clientToken": "EXAMPLE",
        "cluster": "default",
        "desiredCount": 2.0
...
```

O snippet de exemplo a seguir mostra um número formatado `int` (2) para o parâmetro `desiredCount` no bloco de evento de dados `ResponseParameters`.

```
"eventName": "CreateService",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "000.00.00.00",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
        "clientToken": "EXAMPLE",
        "cluster": "default",
        "desiredCount": 2
...
```

Informar o progresso

Implemente a `ProgressReporter` interface para personalizar os relatórios do progresso da Biblioteca de CloudTrail Processamento. `ProgressReporter`declara dois métodos: `reportStart()` e`reportEnd()`, que são chamados no início e no final das seguintes operações:

- Consultar mensagens do Amazon SQS
- Analisar mensagens do Amazon SQS
- Processando uma fonte do Amazon SQS para registros CloudTrail
- Excluir mensagens do Amazon SQS
- Baixando um arquivo CloudTrail de log
- Processando um arquivo CloudTrail de log

Os dois métodos recebem um objeto `ProgressStatus` que contém informações sobre a operação executada. O membro `progressState` contém um membro da enumeração `ProgressState` que identifica a operação atual. Esse membro pode conter informações adicionais no membro `progressInfo`. Além disso, qualquer objeto que você retornar de `reportStart()` será transmitido para `reportEnd()`, a fim de que você possa fornecer informações contextuais, como o horário em que o evento começou a ser processado.

Veja a seguir um exemplo de implementação que fornece informações sobre quanto tempo uma operação levou para ser concluída:

```
public class SampleProgressReporter implements ProgressReporter {
  private static final Log logger =
    LogFactory.getLog(DefaultProgressReporter.class);

  @Override
  public Object reportStart(ProgressStatus status) {
    return new Date();
  }

  @Override
  public void reportEnd(ProgressStatus status, Object startDate) {
    System.out.println(status.getProgressState().toString() + " is " +
      status.getProgressInfo().isSuccess() + " , and latency is " +
      Math.abs(((Date) startDate).getTime()-new Date().getTime()) + "
      milliseconds.");
  }
}
```

Se você não implementar seu próprio `ProgressReporter`, `DefaultExceptionHandler`, que imprime o nome do estado que está em execução, será usado.

Tratamento de erros

A interface `ExceptionHandler` permite que você dê um tratamento especial quando ocorre uma exceção durante o processamento de log. `ExceptionHandler` declara um único método de retorno de chamada, `handleException()`, que recebe um objeto `ProcessingLibraryException` com contexto sobre a exceção que ocorreu.

Você pode usar o método de `ProcessingLibraryException`, `getStatus()`, transferido para descobrir qual operação foi executada quando a exceção ocorreu e obter informações adicionais sobre o status da operação. `ProcessingLibraryException` deriva-se da classe padrão `Exception` de Java, portanto, você também pode recuperar informações sobre a exceção chamando qualquer um dos métodos de exceção.

Veja este exemplo de implementação:

```
public class SampleExceptionHandler implements ExceptionHandler{
  private static final Log logger =
```

```
    LogFactory.getLog(DefaultProgressReporter.class);

  @Override
  public void handleException(ProcessingLibraryException exception) {
    ProgressStatus status = exception.getStatus();
    ProgressState state = status.getProgressState();
    ProgressInfo info = status.getProgressInfo();

    System.err.println(String.format(
      "Exception. Progress State: %s. Progress Information: %s.", state, info));
  }
}
```

Se você não fornecer seu próprio `ExceptionHandler`, `DefaultExceptionHandler`, que imprime uma mensagem de erro padrão, será usado.

> **Note**
>
> Se o `deleteMessageUponFailure` parâmetro for`true`, a Biblioteca CloudTrail de Processamento não distingue exceções gerais de erros de processamento e poderá excluir mensagens da fila.
>
> 1. Por exemplo, você usa o `SourceFilter` para filtrar mensagens por data e hora.
> 2. No entanto, você não tem as permissões necessárias para acessar o bucket do S3 que recebe os arquivos de CloudTrail log. Como você não tem as permissões necessárias, uma `AmazonServiceException` é lançada. A Biblioteca CloudTrail de Processamento envolve isso em um`CallBackException`.
> 3. O `DefaultExceptionHandler` registra isso como um erro, mas não identifica a causa-raiz, que é o fato de você não ter as permissões necessárias. A Biblioteca CloudTrail de Processamento considera isso um erro de processamento e exclui a mensagem, mesmo que a mensagem inclua um arquivo de CloudTrail log válido.
>
> Se você quiser filtrar mensagens com `SourceFilter`, verifique se o seu `ExceptionHandler` pode diferenciar exceções de serviço de erros de processamento.

Recursos adicionais do

Para obter mais informações sobre a Biblioteca CloudTrail de Processamento, consulte o seguinte:

- CloudTrail GitHub Projeto de biblioteca de processamento, que inclui código de amostra que demonstra como implementar um aplicativo CloudTrail de biblioteca de processamento.
- CloudTrail Documentação do Pacote Java da Biblioteca de Processamento.

Segurança em AWS CloudTrail

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

A segurança é uma responsabilidade compartilhada entre você AWS e você. O modelo de responsabilidade compartilhada descreve isto 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 de terceiros testam e verificam regularmente a eficácia da nossa segurança como parte dos compliance programs AWS. Para saber mais sobre os programas de conformidade aplicáveis AWS CloudTrail, consulte AWS Serviços no escopo por programa de conformidade.
- Segurança na nuvem — Sua responsabilidade é determinada pelo AWS serviço que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da empresa e as leis e regulamentos aplicáveis.

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

Tópicos

Proteção de dados em AWS CloudTrail

O modelo de responsabilidade AWS compartilhada modelo se aplica à proteção de dados em AWS CloudTrail. Conforme descrito neste modelo, AWS é responsável por proteger a infraestrutura global que executa todos os Nuvem AWS. Você é responsável por manter o controle sobre seu conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para ter mais informações sobre a privacidade de dados, consulte as Perguntas frequentes sobre privacidade de dados. Para ter mais informações sobre a proteção de dados na Europa, consulte a AWS postagem do blog Shared Responsibility Model and GDPR no AWS Blog de segurança da.

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS as credenciais e configure usuários individuais com AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use uma autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com os recursos. AWS Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure a API e o registro de atividades do usuário com AWS CloudTrail.
- Use soluções de AWS criptografia, juntamente com todos os controles de segurança padrão Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sigilosos armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-2 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para ter mais informações sobre endpoints do FIPS, consulte Federal Information Processing Standard (FIPS) 140-2.

É altamente recomendável que nunca sejam colocadas informações de identificação confidenciais, como endereços de email dos seus clientes, em marcações ou campos de formato livre, como um campo Name (Nome). Isso inclui quando você trabalha com CloudTrail ou Serviços da AWS usa o console, a API ou AWS os SDKs. AWS CLI Quaisquer dados inseridos em tags ou campos de texto de formato livre usados para nomes podem ser usados para logs de faturamento ou de diagnóstico.

Se você fornecer um URL para um servidor externo, recomendemos fortemente que não sejam incluídas informações de credenciais no URL para validar a solicitação a esse servidor.

Por padrão, os arquivos de log de CloudTrail eventos são criptografados usando a criptografia do lado do servidor (SSE) do Amazon S3. Você também pode optar por criptografar seus arquivos de log com uma chave AWS Key Management Service (AWS KMS). Você pode armazenar seus arquivos de log no seu bucket do 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. Se você deseja receber notificações sobre a entrega e a validação dos arquivos de log, configure as notificações do Amazon SNS.

As seguintes melhores práticas de segurança também abordam a proteção de dados em CloudTrail:

- Criptografando arquivos de CloudTrail log com AWS KMS chaves (SSE-KMS)
- Política de bucket do Amazon S3 para CloudTrail
- Validando a integridade CloudTrail do arquivo de log
- Compartilhamento CloudTrail de arquivos de log entre AWS contas

Como CloudTrail os arquivos de log são armazenados em um bucket ou buckets no Amazon S3, você também deve revisar as informações de proteção de dados no Guia do usuário do Amazon Simple Storage Service. Para obter mais informações, consulte Proteção de dados no Amazon S3.

Identity and Access Management para AWS CloudTrail

AWS Identity and Access Management (IAM) é uma ferramenta AWS service (Serviço da AWS) que ajuda o administrador a controlar com segurança o acesso aos AWS recursos. Os administradores do IAM controlam quem pode ser autenticado (conectado) e autorizado (tem permissões) a usar CloudTrail os recursos. O IAM é um AWS service (Serviço da AWS) que você pode usar sem custo adicional.

Tópicos

- Público
- Autenticando com identidades
- Gerenciamento do acesso usando políticas
- Como AWS CloudTrail funciona com o IAM

- Exemplos de políticas baseadas em identidade para AWS CloudTrail
- AWS CloudTrail exemplos de políticas baseadas em recursos
- Política de bucket do Amazon S3 para CloudTrail
- Política de bucket do Amazon S3 para resultados de consulta CloudTrail do Lake
- Política de tópicos do Amazon SNS para CloudTrail
- Solução de problemas AWS CloudTrail de identidade e acesso
- Usando funções vinculadas a serviços para AWS CloudTrail
- AWS políticas gerenciadas para AWS CloudTrail

Público

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

Usuário do serviço — Se você usar o CloudTrail serviço para fazer seu trabalho, seu administrador fornecerá as credenciais e as permissões de que você precisa. À medida que você usa mais CloudTrail recursos para fazer seu trabalho, talvez precise de permissões adicionais. Entender como o acesso é gerenciado pode ajudar você a solicitar as permissões corretas ao seu administrador. Se você não conseguir acessar um recurso no CloudTrail, consulteSolução de problemas AWS CloudTrail de identidade e acesso.

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

Administrador do IAM — Se você for administrador do IAM, talvez queira saber detalhes sobre como criar políticas para gerenciar o acesso CloudTrail. Para ver exemplos de políticas CloudTrail baseadas em identidade que você pode usar no IAM, consulte. Exemplos de políticas baseadas em identidade para AWS CloudTrail

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 o Usuário raiz da conta da AWS, como usuário do IAM ou assumindo uma função do IAM.

Você pode entrar AWS como uma identidade federada usando credenciais fornecidas por meio de uma fonte de identidade. AWS IAM Identity Center Usuários (IAM Identity Center), a autenticação de login único da sua empresa e suas credenciais do Google ou do Facebook são exemplos de identidades federadas. Quando você faz login como uma identidade federada, o administrador já configurou anteriormente a federação de identidades usando perfis do IAM. Ao acessar AWS usando a federação, você está assumindo indiretamente uma função.

Dependendo do tipo de usuário que você é, você pode entrar no AWS Management Console ou no portal de AWS acesso. Para obter mais informações sobre como fazer login AWS, consulte Como fazer login Conta da AWS no Guia do Início de Sessão da AWS usuário.

Se você acessar AWS programaticamente, AWS fornece um kit de desenvolvimento de software (SDK) e uma interface de linha de comando (CLI) para assinar criptograficamente suas solicitações usando suas credenciais. Se você não usa AWS ferramentas, você mesmo deve assinar as solicitações. Para obter mais informações sobre como usar o método recomendado para assinar solicitações por conta própria, consulte Assinatura de solicitações de AWS API no Guia do usuário do IAM.

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

Conta da AWS usuário root

Ao criar uma Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos Serviços da AWS os recursos da conta. Essa identidade é chamada de usuário Conta da AWS raiz e é acessada fazendo login com o endereço de e-mail e a senha que você usou para criar a conta. É altamente recomendável não usar o usuário-raiz para tarefas diárias. Proteja as credenciais do usuário-raiz e use-as para executar as tarefas que somente ele pode executar. Para obter a lista completa das tarefas que exigem login como usuário-raiz, consulte Tarefas que exigem credenciais de usuário-raiz no Guia do usuário do IAM.

Identidade federada

Como prática recomendada, exija que usuários humanos, incluindo usuários que precisam de acesso de administrador, usem a federação com um provedor de identidade para acessar Serviços da AWS usando credenciais temporárias.

Uma identidade federada é um usuário do seu diretório de usuários corporativo, de um provedor de identidade da web AWS Directory Service, do diretório do Identity Center ou de qualquer usuário que acesse usando credenciais fornecidas Serviços da AWS por meio de uma fonte de identidade. Quando as identidades federadas são acessadas Contas da AWS, elas assumem funções, e as funções fornecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, recomendamos usar o . AWS IAM Identity Center Você pode criar usuários e grupos no IAM Identity Center ou pode se conectar e sincronizar com um conjunto de usuários e grupos em sua própria fonte de identidade para uso em todos os seus Contas da AWS aplicativos. Para obter mais informações sobre o Centro de Identidade do IAM, consulte "What is IAM Identity Center?" (O que é o Centro de Identidade do IAM?) noAWS IAM Identity Center Guia do usuário do .

Grupos e usuários do IAM

Um usuário do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas para uma única pessoa ou aplicativo. Sempre que possível, recomendamos depender de credenciais temporárias em vez de criar usuários do IAM com credenciais de longo prazo, como senhas e chaves de acesso. No entanto, se você tiver casos de uso específicos que exijam credenciais de longo prazo com usuários do IAM, recomendamos alternar as chaves de acesso. Para obter mais informações, consulte Alterne as chaves de acesso regularmente para casos de uso que exijam credenciais de longo prazo no Guia do usuário do IAM.

Um grupo do IAM é uma identidade que especifica uma coleção de usuários do IAM. Não é possível fazer login como um grupo. É possível usar grupos para especificar permissões para vários usuários de uma vez. Os grupos facilitam o gerenciamento de permissões para grandes conjuntos de usuários. Por exemplo, você pode ter um grupo chamado IAMAdmins e atribuir a esse grupo permissões para administrar atributos do IAM.

Usuários são diferentes de perfis. Um usuário é exclusivamente associado a uma pessoa ou a uma aplicação, mas um perfil pode ser assumido por qualquer pessoa que precisar dele. Os usuários têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para

saber mais, consulte Quando criar um usuário do IAM (em vez de um perfil) no Guia do usuário do IAM.

Perfis do IAM

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

Perfis do IAM com credenciais temporárias são úteis nas seguintes situações:

- Acesso de usuário federado: para atribuir permissões a identidades federadas, você pode criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas pelo mesmo. Para obter mais informações sobre perfis para federação, consulte Criar um perfil para um provedor de identidades de terceiros no Guia do usuário do IAM. Se você usar o IAM Identity Center, configure um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o IAM Identity Center correlaciona o conjunto de permissões a um perfil no IAM. Para obter informações sobre conjuntos de permissões, consulte Conjuntos de permissões noAWS IAM Identity Center Guia do usuário do .
- Permissões temporárias para usuários do IAM: um usuário ou um perfil do IAM pode assumir um perfil do IAM para obter temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas: é possível usar um perfil do IAM para permitir que alguém (uma entidade principal confiável) em outra conta acesse atributos 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 perfis e políticas baseadas em atributo para acesso entre contas, consulte Como os perfis do IAM diferem das políticas baseadas em atributo no Guia do usuário do IAM.
- Acesso entre serviços — Alguns Serviços da AWS usam recursos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicações no Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando a invocação das permissões da entidade principal, usando um perfil de serviço ou um perfil vinculado ao serviço.

- Sessões de acesso direto (FAS) — Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Encaminhar sessões de acesso.
- Perfil de serviço: um perfil de serviço é um perfil do IAM que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do usuário do IAM.
- Função vinculada ao serviço — Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode assumir um perfil para executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não pode editar as permissões para perfis vinculados ao serviço.

- Aplicativos em execução no Amazon EC2 — Você pode usar uma função do IAM para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma instância do EC2 e fazendo AWS CLI solicitações de API. AWS É preferível fazer isso a armazenar chaves de acesso na instância do EC2. Para atribuir uma AWS função a uma instância do EC2 e disponibilizá-la para todos os seus aplicativos, você cria um perfil de instância anexado à instância. Um perfil de instância contém a perfil e permite que os programas em execução na instância do EC2 obtenham credenciais temporárias. Para obter mais informações, consulte Usar uma função do IAM para conceder permissões a aplicações em execução nas instâncias do Amazon EC2 no Guia do usuário do IAM.

Para saber se deseja usar os perfis do IAM, consulte Quando criar um perfil do IAM (em vez de um usuário) no Guia do usuário do IAM.

Gerenciamento do acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política é um objeto AWS que, quando associada a uma identidade ou recurso, define suas permissões. AWS avalia essas políticas quando um principal (usuário, usuário raiz ou sessão de

função) faz uma solicitação. As permissões nas políticas determinam se a solicitação será permitida ou negada. A maioria das políticas é armazenada AWS como documentos JSON. Para obter mais informações sobre a estrutura e o conteúdo de documentos de políticas JSON, consulte Visão geral das políticas JSON no Guia do usuário do IAM.

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

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

As políticas do IAM definem permissões para uma ação, independentemente do método usado para executar a operação. Por exemplo, suponha que você tenha uma política que permite a ação `iam:GetRole`. Um usuário com essa política pode obter informações de função da AWS Management Console AWS CLI, da ou da AWS API.

Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário, grupo de usuários ou perfil do IAM. Essas políticas controlam quais ações os usuários e funções podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Criar políticas do IAM no Guia do usuário do IAM.

As políticas baseadas em identidade podem ser categorizadas ainda mais como políticas em linha ou políticas gerenciadas. As políticas em linha são anexadas diretamente a um único usuário, grupo ou perfil. As políticas gerenciadas são políticas autônomas que você pode associar a vários usuários, grupos e funções em seu Conta da AWS. As políticas AWS gerenciadas incluem políticas gerenciadas e políticas gerenciadas pelo cliente. Para saber como escolher entre uma política gerenciada ou uma política em linha, consulte Escolher entre políticas gerenciadas e políticas em linha no Guia do usuário do IAM.

Políticas baseadas em recursos

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de função do IAM e as políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos,

os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o atributo ao qual a política está anexada, a política define quais ações uma entidade principal especificada pode executar nesse atributo 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 atributos são políticas em linha que estão localizadas nesse serviço. Você não pode usar políticas AWS gerenciadas do IAM em uma política baseada em recursos.

Listas de controle de acesso (ACLs)

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

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

Outros tipos de política

AWS oferece suporte a tipos de políticas adicionais menos comuns. Esses tipos de política podem definir o máximo de permissões concedidas a você pelos tipos de política mais comuns.

- Limites de permissões: um limite de permissões é um recurso avançado no qual você define o máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM (perfil ou usuário do IAM). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade de uma entidade e dos seus limites de permissões. As políticas baseadas em atributo que especificam o usuário ou o perfil no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte Limites de permissões para identidades do IAM no Guia do usuário do IAM.
- Políticas de controle de serviço (SCPs) — SCPs são políticas JSON que especificam as permissões máximas para uma organização ou unidade organizacional (OU) em. AWS Organizations AWS Organizations é um serviço para agrupar e gerenciar centralmente vários Contas da AWS que sua empresa possui. Se você habilitar todos os atributos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as contas. O SCP limita as permissões para entidades nas contas dos membros, incluindo cada

uma Usuário raiz da conta da AWS. Para obter mais informações sobre o Organizações e SCPs, consulte Como os SCPs funcionam no Guia do usuário do AWS Organizations .

- Políticas de sessão: são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para um perfil ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou do perfil e das políticas de sessão. As permissões também podem ser provenientes de uma política baseada em atributo. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, consulte Políticas de sessão no Guia do usuário do IAM.

Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Para saber como AWS determinar se uma solicitação deve ser permitida quando vários tipos de políticas estão envolvidos, consulte Lógica de avaliação de políticas no Guia do usuário do IAM.

Como AWS CloudTrail funciona com o IAM

Antes de usar o IAM para gerenciar o acesso CloudTrail, saiba com quais recursos do IAM estão disponíveis para uso CloudTrail.

Recursos do IAM que você pode usar com AWS CloudTrail

Atributo do IAM	CloudTrail apoio
Políticas baseadas em identidade	Sim
Políticas baseadas em atributos	Parcial
Ações de políticas	Sim
atributos de políticas	Sim
Chaves de condição de política (específicas do serviço)	Não
ACLs	Não

Atributo do IAM	CloudTrail apoio
ABAC (tags em políticas)	Parcial
Credenciais temporárias	Sim
Sessões de acesso direto (FAS)	Sim
Perfis de serviço	Sim
Perfis vinculados ao serviço	Sim

Para ter uma visão de alto nível de como CloudTrail e outros AWS serviços funcionam com a maioria dos recursos do IAM, consulte AWS os serviços que funcionam com o IAM no Guia do usuário do IAM.

Políticas baseadas em identidade para CloudTrail

É compatível com políticas baseadas em identidade	Sim

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário, grupo de usuários ou perfil do IAM. Essas políticas controlam quais ações os usuários e funções podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Criar políticas do IAM no Guia do usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações ou atributos permitidos ou negados, bem como as condições sob as quais as ações são permitidas ou negadas. Não é possível especificar a entidade principal em uma política baseada em identidade porque ela se aplica ao usuário ou função à qual ela está anexado. Para saber mais sobre todos os elementos que podem ser usados em uma política JSON, consulte Referência de elementos da política JSON do IAM no Guia do Usuário do IAM.

Exemplos de políticas baseadas em identidade para CloudTrail

Para ver exemplos de políticas CloudTrail baseadas em identidade, consulte. Exemplos de políticas baseadas em identidade para AWS CloudTrail

Políticas baseadas em recursos dentro CloudTrail

É compatível com políticas baseadas em atributos	Parcial

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de função do IAM e as políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o atributo ao qual a política está anexada, a política define quais ações uma entidade principal especificada pode executar nesse atributo 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

Para permitir o acesso entre contas, você pode especificar uma conta inteira ou as entidades do IAM em outra conta como a entidade principal em uma política baseada em atributo. Adicionar uma entidade principal entre contas à política baseada em atributo é apenas metade da tarefa de estabelecimento da relação de confiança. Quando o principal e o recurso são diferentes Contas da AWS, um administrador do IAM na conta confiável também deve conceder permissão à entidade principal (usuário ou função) para acessar o recurso. Eles concedem permissão ao anexar uma política baseada em identidade para a entidade. No entanto, se uma política baseada em atributo conceder acesso a uma entidade principal na mesma conta, nenhuma política baseada em identidade adicional será necessária. Para obter mais informações, consulte Como os perfis do IAM diferem de políticas baseadas em recursos no Guia do usuário do IAM.

CloudTrail oferece suporte a políticas baseadas em recursos em canais usados para integrações CloudTrail do Lake com fontes de eventos externas. AWS A política baseada em recursos do canal define quais entidades principais (contas, usuários, funções e usuários federados) podem chamar `PutAuditEvents` no canal para entregar eventos para o armazenamento de dados do evento de destino. Para obter mais informações sobre a criação de integrações com o CloudTrail Lake, consulteCrie uma integração com uma fonte de eventos fora do AWS.

Exemplos

Para ver exemplos de políticas CloudTrail baseadas em recursos, consulte. AWS CloudTrail exemplos de políticas baseadas em recursos

Ações políticas para CloudTrail

Oferece suporte a ações de políticas	Sim

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

O elemento `Action` de uma política JSON descreve as ações que você pode usar para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome da operação de AWS API associada. Existem algumas exceções, como ações somente de permissão, que não têm uma operação de API correspondente. Há também algumas operações que exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

Incluem ações em uma política para conceder permissões para executar a operação associada.

Para ver uma lista de CloudTrail ações, consulte Ações definidas por AWS CloudTrail na Referência de autorização de serviço.

As ações de política CloudTrail usam o seguinte prefixo antes da ação:

```
cloudtrail
```

Por exemplo, para conceder a alguém permissão para listar tags de uma trilha com a operação da API `ListTags`, inclua a ação `cloudtrail:ListTags` na política da pessoa. As instruções de política devem incluir um elemento `Action` ou `NotAction`. CloudTrail define seu próprio conjunto de ações que descrevem as tarefas que você pode executar com esse serviço.

Para especificar várias ações em uma única instrução, separe-as com vírgulas, como segue:

```
"Action": [
      "cloudtrail:AddTags",
      "cloudtrail:ListTags",
```

```
      "cloudtrail:RemoveTags
```

Também é possível especificar várias ações usando caracteres curinga (*). Por exemplo, para especificar todas as ações que começam com a palavra `Get`, inclua a seguinte ação:

```
"Action": "cloudtrail:Get*"
```

Recursos políticos para CloudTrail

Oferece suporte a atributos de políticas	Sim

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

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

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

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

Para ver uma lista dos tipos de CloudTrail recursos e seus ARNs, consulte Recursos definidos por AWS CloudTrail na Referência de autorização de serviço. Para saber com quais ações você pode especificar o ARN de cada recurso, consulte Ações definidas pelo AWS CloudTrail.

Em CloudTrail, há três tipos de recursos: trilhas, armazenamentos de dados de eventos e canais. Cada recurso possui um nome de recurso da Amazon (ARN) exclusivo associado. Em uma política, você usa um ARN para identificar o recurso ao qual a política se aplica. CloudTrail atualmente não oferece suporte a outros tipos de recursos, que às vezes são chamados de sub-recursos.

O recurso de CloudTrail trilha tem o seguinte ARN:

```
arn:${Partition}:cloudtrail:${Region}:${Account}:trail/{TrailName}
```

O recurso de armazenamento de dados de CloudTrail eventos tem o seguinte ARN:

```
arn:${Partition}:cloudtrail:${Region}:${Account}:eventdatastore/{EventDataStoreId}
```

O recurso do CloudTrail canal tem o seguinte ARN:

```
arn:${Partition}:cloudtrail:${Region}:${Account}:channel/{ChannelId}
```

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

Por exemplo, para uma Conta da AWS com a ID *123456789012*, para especificar uma trilha chamada *My-Trail* que existe na região Leste dos EUA (Ohio) em sua declaração, use o seguinte ARN:

```
"Resource": "arn:aws:cloudtrail:us-east-2:123456789012:trail/My-Trail"
```

Para especificar todas as trilhas que pertencem a uma conta específica Região da AWS, use o caractere curinga (*):

```
"Resource": "arn:aws:cloudtrail:us-east-2:123456789012:trail/*"
```

Algumas CloudTrail ações, como as de criação de recursos, não podem ser executadas em um recurso específico. Nesses casos, é necessário usar o caractere curinga (*).

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

Muitas ações de CloudTrail API envolvem vários recursos. Por exemplo, `CreateTrail` requer um bucket do Amazon S3 para armazenar os arquivos de log e, portanto, um usuário deve ter permissões para gravar no bucket. Para especificar vários recursos em uma única instrução, separe os ARNs com vírgulas.

```
"Resource": [
```

```
        "resource1",
        "resource2"
```

Chaves de condição de política para CloudTrail

Compatível com chaves de condição de política específicas do serviço	Não

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

O elemento `Condition` (ou `Condition` bloco de) permite que você especifique condições nas quais uma instrução está em vigor. O elemento `Condition` é opcional. É possível criar expressões condicionais que usam 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 para que as permissões da instrução sejam concedidas.

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

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 do usuário do IAM.

CloudTrail não define suas próprias chaves de condição, mas suporta o 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 do usuário do IAM.

Para ver uma lista de chaves de CloudTrail condição, consulte Chaves de condição AWS CloudTrail na Referência de autorização de serviço. Para saber com quais ações e recursos você pode usar uma chave de condição, consulte Ações definidas por AWS CloudTrail.

ACLs em CloudTrail

Oferece suporte a ACLs	Não

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

ABAC com CloudTrail

Oferece suporte a ABAC (tags em políticas)	Parcial

O controle de acesso baseado em recurso (ABAC) é uma estratégia de autorização que define permissões com base em recursos. Em AWS, esses atributos são chamados de tags. Você pode anexar tags a entidades do IAM (usuários ou funções) e a vários AWS recursos. A marcação de entidades e atributos é a primeira etapa do ABAC. Em seguida, você cria políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do atributo que ela está tentando acessar.

O ABAC é útil em ambientes que estão crescendo rapidamente e ajuda em situações em que o gerenciamento de políticas se torna um problema.

Para controlar o acesso baseado em tags, forneça informações sobre as tags no elemento de condição de uma política usando as chaves de condição `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`* ou `aws:TagKeys`.

Se um serviço oferecer suporte às três chaves de condição para cada tipo de atributo, o valor será Sim para o serviço. Se um serviço oferecer suporte às três chaves de condição somente para alguns tipos de atributos, o valor será Parcial.

Para obter mais informações sobre o ABAC, consulte O que é ABAC? no Guia do usuário do IAM. Para visualizar um tutorial com etapas para configurar o ABAC, consulte Usar controle de acesso baseado em atributos (ABAC) no Guia do usuário do IAM.

Embora você possa anexar tags aos CloudTrail recursos, CloudTrail só oferece suporte ao controle do acesso aos armazenamentos de dados e canais de eventos do CloudTrail Lake com base em tags. Não é possível controlar o acesso a trilhas com base em tags.

Você pode anexar tags a CloudTrail recursos ou passar tags em uma solicitação para CloudTrail. Para obter mais informações sobre a marcação de CloudTrail recursos, consulte Criar uma trilha e. Criando, atualizando e gerenciando trilhas com o AWS CLI

Usando credenciais temporárias com CloudTrail

Oferece suporte a credenciais temporárias	Sim

Alguns Serviços da AWS não funcionam quando você faz login usando credenciais temporárias. Para obter informações adicionais, incluindo quais Serviços da AWS funcionam com credenciais temporárias, consulte Serviços da AWS “Trabalhe com o IAM” no Guia do usuário do IAM.

Você está usando credenciais temporárias se fizer login AWS Management Console usando qualquer método, exceto um nome de usuário e senha. Por exemplo, quando você acessa AWS usando o link de login único (SSO) da sua empresa, esse processo cria automaticamente credenciais temporárias. Você também cria automaticamente credenciais temporárias quando faz login no console como usuário e, em seguida, alterna perfis. Para obter mais informações sobre como alternar perfis, consulte Alternar para um perfil (console) no Guia do usuário do IAM.

Você pode criar manualmente credenciais temporárias usando a AWS API AWS CLI ou. Em seguida, você pode usar essas credenciais temporárias para acessar AWS. AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para mais informações, consulte Credenciais de segurança temporárias no IAM.

Sessões de acesso direto para CloudTrail

Suporte para o recurso Encaminhamento de sessões de acesso (FAS)	Sim

Quando você usa um usuário ou uma função do IAM para realizar ações em AWS, você é considerado um principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para

ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Encaminhar sessões de acesso.

Funções de serviço para CloudTrail

Oferece suporte a perfis de serviço	Sim

Um perfil de serviço é um perfil do IAM que um serviço assume para executar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do usuário do IAM.

> **Warning**
>
> Alterar as permissões de uma função de serviço pode interromper CloudTrail a funcionalidade. Edite as funções de serviço somente quando CloudTrail fornecer orientação para fazer isso.

Funções vinculadas a serviços para CloudTrail

Oferece suporte a perfis vinculados ao serviço	Sim

Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode assumir um perfil para executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não pode editar as permissões para perfis vinculados ao serviço.

CloudTrail suporta uma função vinculada a serviços para integração com. AWS Organizations Esse perfil é necessário para a criação de uma trilha ou um armazenamento de dados de eventos da organização. Trilhas organizacionais e armazenamentos de dados de eventos registram eventos para todos Contas da AWS em uma organização. Para obter mais informações sobre como criar ou gerenciar funções CloudTrail vinculadas a serviços, consulte. Usando funções vinculadas a serviços para AWS CloudTrail

Exemplos de políticas baseadas em identidade para AWS CloudTrail

Por padrão, usuários e funções não têm permissão para criar ou modificar CloudTrail recursos. Eles também não podem realizar tarefas usando a AWS API AWS Management Console, AWS Command Line Interface (AWS CLI) ou. Para conceder aos usuários permissão para executar ações nos recursos de que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM aos perfis, e os usuários podem assumir os perfis.

Para saber como criar uma política baseada em identidade do IAM usando esses exemplos de documento de política JSON, consulte Criação de políticas do IAM no Guia do Usuário do IAM.

Para obter detalhes sobre ações e tipos de recursos definidos por CloudTrail, incluindo o formato dos ARNs para cada um dos tipos de recursos, consulte Ações, recursos e chaves de condição AWS CloudTrail na Referência de autorização de serviço.

Tópicos

Melhores práticas de política

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir CloudTrail recursos em sua conta. Essas ações podem incorrer em custos para a 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 gerenciadas pela AWS ou Políticas gerenciadas pela AWS para perfis de trabalho no Guia do usuário do IAM.

- Aplique permissões de privilégio mínimo: ao definir permissões com as políticas do IAM, conceda apenas as permissões necessárias para executar uma tarefa. Você faz isso definindo as ações que podem ser executadas em atributos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para obter mais informações sobre como usar o IAM para aplicar permissões, consulte Políticas e permissões no IAM no Guia do usuário do IAM.
- Use condições nas políticas do IAM para restringir ainda mais o acesso: você pode adicionar uma condição às políticas para limitar o acesso a ações e atributos. Por exemplo, você pode escrever uma condição de política para especificar que todas as solicitações devem ser enviadas usando SSL. 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 de política JSON do IAM: condições no Manual do usuário do IAM.
- Use o IAM Access Analyzer para validar suas políticas do IAM a fim de garantir permissões seguras e funcionais: o IAM Access Analyzer valida as políticas novas e existentes para que elas sigam a linguagem de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access Analyzer oferece mais de cem verificações de política e recomendações acionáveis para ajudar você a criar políticas seguras e funcionais. Para obter mais informações, consulte Validação de políticas do IAM Access Analyzer no Guia do usuário do IAM.
- Exigir autenticação multifator (MFA) — Se você tiver um cenário que exija usuários do IAM ou um usuário root, ative Conta da AWS a MFA para obter segurança adicional. Para exigir a MFA quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para obter mais informações, consulte Configuração de acesso à API protegido por MFA no Guia do usuário do IAM.

Para mais informações sobre as práticas recomendadas do IAM, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.

CloudTrail não tem chaves de contexto específicas do serviço que você possa usar no `Condition` elemento das declarações de política.

Exemplo: permitir e negar ações para uma trilha especificada

O exemplo a seguir demonstra uma política que permite que os usuários com essa política visualizem o status e a configuração de uma trilha e iniciem e interrompam o registro de uma trilha

chamada *My-First-Trail*. Essa trilha foi criada na região Leste dos EUA (Ohio) (sua região natal) Conta da AWS com o ID *123456789012*.

```
{
  "Version": "2012-10-17",
  "Statement": [
      {
          "Effect": "Allow",
          "Action": [
              "cloudtrail:StartLogging",
              "cloudtrail:StopLogging",
              "cloudtrail:GetTrail",
              "cloudtrail:GetTrailStatus",
              "cloudtrail:GetEventSelectors"
          ],
          "Resource": [
              "arn:aws:cloudtrail:us-east-2:123456789012:trail/My-First-Trail"
          ]
      }
  ]
}
```

O exemplo a seguir demonstra uma política que nega explicitamente CloudTrail ações para qualquer trilha que não seja chamada My-First-Trail.

```
{
  "Version": "2012-10-17",
  "Statement": [
      {
          "Effect": "Deny",
          "Action": [
              "cloudtrail:*"
          ],
          "NotResource": [
              "arn:aws:cloudtrail:us-east-2:123456789012:trail/My-First-Trail"
          ]
      }
  ]
}
```

Exemplos: criação e aplicação de políticas para ações em trilhas específicas

Você pode usar permissões e políticas para controlar a capacidade do usuário de realizar ações específicas nas CloudTrail trilhas.

Por exemplo, você não deseja que os usuários do grupo de desenvolvedores da sua empresa iniciem ou interrompam o registro em log em uma trilha específica. No entanto, talvez você queira conceder a eles permissão para realizar as ações `DescribeTrails` e `GetTrailStatus` na trilha. Você deseja que os usuários do grupo de desenvolvedores realizem as ações `StartLogging` ou `StopLogging` nas trilhas que gerenciam.

É possível criar duas declarações de política e anexá-las ao grupo de desenvolvedores criado por você no IAM. Para obter mais informações sobre grupos do IAM, consulte Grupos do IAM no Manual do usuário do IAM.

Na primeira política, negue as ações `StartLogging` e `StopLogging` para o nome de região da Amazon (ARN) da trilha que você especificar. No exemplo a seguir, o Nome de região da Amazon (ARN) da trilha é `arn:aws:cloudtrail:us-east-2:123456789012:trail/Example-Trail`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1446057698000",
            "Effect": "Deny",
            "Action": [
                "cloudtrail:StartLogging",
                "cloudtrail:StopLogging"
            ],
            "Resource": [
                "arn:aws:cloudtrail:us-east-2:123456789012:trail/Example-Trail"
            ]
        }
    ]
}
```

Na segunda política, as `GetTrailStatus` ações `DescribeTrails` e são permitidas em todos os CloudTrail recursos:

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1446072643000",
            "Effect": "Allow",
            "Action": [
                "cloudtrail:DescribeTrails",
                "cloudtrail:GetTrail",
                "cloudtrail:GetTrailStatus"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

Se um usuário do grupo de desenvolvedores tentar iniciar ou interromper o registro na trilha que você especificou na primeira política, ele receberá uma exceção de acesso negado. Os usuários do grupo de desenvolvedores podem iniciar e interromper o registro nas trilhas que criam e gerenciam.

Os exemplos a seguir mostram que o grupo de desenvolvedores configurou em um AWS CLI perfil chamado`devgroup`. Primeiro, um usuário de `devgroup` executa o comando `describe-trails`.

```
$ aws --profile devgroup cloudtrail describe-trails
```

O comando foi concluído com êxito com a seguinte saída:

```
{
    "trailList": [
        {
            "IncludeGlobalServiceEvents": true,
            "Name": "Default",
            "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/Example-
Trail",
            "IsMultiRegionTrail": false,
            "S3BucketName": "myS3bucket ",
            "HomeRegion": "us-east-2"
        }
    ]
}
```

O usuário executa o comando `get-trail-status` na trilha que você especificou na primeira política.

```
$ aws --profile devgroup cloudtrail get-trail-status --name Example-Trail
```

O comando foi concluído com êxito com a seguinte saída:

```
{
    "LatestDeliveryTime": 1449517556.256,
    "LatestDeliveryAttemptTime": "2015-12-07T19:45:56Z",
    "LatestNotificationAttemptSucceeded": "",
    "LatestDeliveryAttemptSucceeded": "2015-12-07T19:45:56Z",
    "IsLogging": true,
    "TimeLoggingStarted": "2015-12-07T19:36:27Z",
    "StartLoggingTime": 1449516987.685,
    "StopLoggingTime": 1449516977.332,
    "LatestNotificationAttemptTime": "",
    "TimeLoggingStopped": "2015-12-07T19:36:17Z"
}
```

Em seguida, um usuário no grupo `devgroup` executa o comando `stop-logging` na mesma trilha.

```
$ aws --profile devgroup cloudtrail stop-logging --name Example-Trail
```

O comando retorna uma exceção de acesso negado, como a seguinte:

```
A client error (AccessDeniedException) occurred when calling the StopLogging operation:
 Unknown
```

O usuário executa o comando `start-logging` na mesma trilha.

```
$ aws --profile devgroup cloudtrail start-logging --name Example-Trail
```

Novamente, o comando retorna uma exceção de acesso negado, como a seguinte:

```
A client error (AccessDeniedException) occurred when calling the StartLogging
 operation: Unknown
```

Exemplos: negação de acesso para criar ou excluir armazenamentos de dados de eventos com base em tags

No exemplo de política a seguir, a permissão para criar um armazenamento de dados de eventos com `CreateEventDataStore` será negada se pelo menos uma das seguintes condições não for atendida:

- O armazenamento de dados de eventos não tem uma chave de tag `stage` aplicada a si mesmo
- O valor da tag do estágio não é `alpha`, `beta`, `gamma` ou `prod`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "cloudtrail:CreateEventDataStore",
            "Resource": "*",
            "Condition": {
                "Null": {
                    "aws:RequestTag/stage": "true"
                }
            }
        },
        {
            "Effect": "Deny",
            "Action": "cloudtrail:CreateEventDataStore",
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringNotEquals": {
                    "aws:RequestTag/stage": [
                        "alpha",
                        "beta",
                        "gamma",
                        "prod"
                    ]
                }
            }
        }
    ]
}
```

No exemplo de política a seguir, a permissão para excluir um armazenamento de dados de evento com `DeleteEventDataStore` será negada se o armazenamento de dados de eventos tiver uma tag `stage` com um valor de`prod`. Uma política como essa pode ajudar a proteger um armazenamento de dados de eventos contra exclusão acidental.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "cloudtrail:DeleteEventDataStore",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/stage": "prod"
                }
            }
        }
    ]
}
```

Usar o console do CloudTrail

Para acessar o AWS CloudTrail console, você deve ter um conjunto mínimo de permissões. Essas permissões devem permitir que você liste e visualize detalhes sobre os CloudTrail recursos em seu Conta da AWS. Se você criar uma política baseada em identidade que seja mais restritiva do que as permissões mínimas necessárias, o console não funcionará como pretendido para entidades (usuários ou perfis) com essa política.

Você não precisa permitir permissões mínimas do console para usuários que estão fazendo chamadas somente para a API AWS CLI ou para a AWS API. Em vez disso, permita o acesso somente a ações que correspondam a operação de API que estiverem tentando executar.

Concedendo permissões para administração CloudTrail

Para permitir que funções ou usuários do IAM administrem um CloudTrail recurso, como uma trilha, um armazenamento de dados de eventos ou um canal, você deve conceder permissões explícitas para realizar as ações associadas CloudTrail às tarefas. Na maioria das situações, você pode usar uma política AWS gerenciada que contém permissões predefinidas.

> **Note**
>
> As permissões que você concede aos usuários para realizar tarefas CloudTrail administrativas não são as mesmas que CloudTrail exigem a entrega de arquivos de log para buckets do Amazon S3 ou o envio de notificações para tópicos do Amazon SNS. Para obter mais informações sobre essas permissões, consulte Política de bucket do Amazon S3 para CloudTrail.
>
> Se você configurar a integração com o Amazon CloudWatch Logs, CloudTrail também requer uma função que ele possa assumir para entregar eventos a um grupo de CloudWatch logs do Amazon Logs. Você deve criar a função que CloudTrail usa. Para obter mais informações, consulte Conceder permissão para visualizar e configurar as informações do Amazon CloudWatch Logs no console CloudTrail e Envio de eventos para o CloudWatch Logs.

As seguintes políticas AWS gerenciadas estão disponíveis para CloudTrail:

- AWSCloudTrail_FullAccess— Essa política fornece acesso total às CloudTrail ações sobre CloudTrail recursos, como trilhas, armazenamentos de dados de eventos e canais. Essa política fornece as permissões necessárias para criar, atualizar e excluir CloudTrail trilhas, armazenamentos de dados de eventos e canais.

  Essa política também fornece permissões para gerenciar o bucket do Amazon S3, o grupo de CloudWatch logs para Logs e um tópico do Amazon SNS para uma trilha. No entanto, a política `AWSCloudTrail_FullAccess` gerenciada não fornece permissões para excluir o bucket do Amazon S3, o grupo de CloudWatch logs para Logs ou um tópico do Amazon SNS. Para obter informações sobre políticas gerenciadas para outros Serviços da AWS, consulte o Guia de referência de políticas AWS gerenciadas.

  > **Note**
  >
  > A AWSCloudTrail_FullAccesspolítica não se destina a ser compartilhada amplamente entre seus Conta da AWS. Os usuários com esse perfil podem desativar ou reconfigurar as funções de auditoria mais confidenciais e importantes em suas Contas da AWS. Por esse motivo, você só deve aplicar essa política aos administradores da conta. Você deve controlar e monitorar de perto o uso desta política.

- AWSCloudTrail_ReadOnlyAccess— Essa política concede permissões para visualizar o CloudTrail console, incluindo eventos recentes e histórico de eventos. Essa política também permite visualizar

trilhas, armazenamentos de dados de eventos e canais existentes. Os perfis e usuários com essa política podem baixar o histórico de eventos, mas não podem criar ou atualizar trilhas, armazenamentos de dados de eventos ou canais.

Para conceder acesso, adicione as permissões aos seus usuários, grupos ou perfis:

- Usuários e grupos em AWS IAM Identity Center:

  Crie um conjunto de permissões. Siga as instruções em Criação de um conjunto de permissões no Guia do usuário do AWS IAM Identity Center .
- Usuários gerenciados no IAM com provedor de identidades:

  Crie um perfil para a federação de identidades. Siga as instruções em Criar um perfil para um provedor de identidades de terceiros (federação) no Guia do usuário do IAM.
- Usuários do IAM:
  - Crie um perfil que seu usuário possa assumir. Siga as instruções em Criação de um perfil para um usuário do IAM no Guia do usuário do IAM.
  - (Não recomendado) Vincule uma política diretamente a um usuário ou adicione um usuário a um grupo de usuários. Siga as instruções em Adição de permissões a um usuário (console) no Guia do usuário do IAM.

Recursos adicionais do

Para saber mais sobre como usar o IAM para dar às identidades, como usuários e funções, acesso aos recursos em sua conta, consulte Como configurar o IAM e o gerenciamento de acesso para AWS recursos no Guia do usuário do IAM.

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

Permitir que os usuários visualizem suas próprias permissões

Este exemplo mostra como você pode criar uma política que permite que os usuários do IAM visualizem as políticas gerenciadas e em linha anexadas a sua identidade de usuário. Essa política inclui permissões para concluir essa ação no console ou programaticamente usando a API AWS CLI ou AWS .

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Conceder permissões personalizadas para CloudTrail usuários

CloudTrail as políticas concedem permissões aos usuários que trabalham com CloudTrail. Se precisar conceder permissões diferentes aos usuários, você pode anexar uma CloudTrail política a um grupo do IAM ou a um usuário. Você pode editar a política para incluir ou excluir permissões específicas. Você também pode criar a sua própria política personalizada. As políticas são documentos JSON que definem as ações que um usuário tem permissão para realizar e os recursos nos quais ele tem permissão para realizar essas ações. Para obter exemplos específicos, consulte

Exemplo: permitir e negar ações para uma trilha especificada e Exemplos: criação e aplicação de políticas para ações em trilhas específicas.

Sumário

Acesso somente leitura

O exemplo a seguir mostra uma política que concede acesso somente para CloudTrail leitura às trilhas. Isso equivale à política gerenciada AWSCloudTrail_ReadOnlyAccess. Ela concede aos usuários permissão para ver informações das trilhas, mas não para criá-las ou atualizá-las.

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

Nas declarações da política, o elemento `Effect` especifica se as ações são permitidas ou negadas. O elemento `Action` lista as ações específicas que o usuário tem permissão para realizar. O `Resource` elemento lista os AWS recursos nos quais o usuário tem permissão para realizar essas ações. Para políticas que controlam o acesso às CloudTrail ações, o `Resource` elemento geralmente é definido como`*`, um curinga que significa “todos os recursos”.

Os valores no elemento `Action` correspondem às APIs às quais os serviços oferecem suporte. As ações são precedidas por `cloudtrail:` para indicar que se referem a CloudTrail ações. Você pode usar o caractere curinga `*` no elemento `Action`, como nos exemplos a seguir:

- `"Action": ["cloudtrail:*Logging"]`

  Isso permite todas as CloudTrail ações que terminam com "Logging" (`StartLogging`,`StopLogging`).
- `"Action": ["cloudtrail:*"]`

  Isso permite todas as CloudTrail ações, mas não ações para outros AWS serviços.
- `"Action": ["*"]`

  Isso permite todas as AWS ações. Essa permissão é adequada a um usuário que atua como um administrador da AWS na sua conta.

A política somente leitura não concede permissão de usuário às ações `CreateTrail`, `UpdateTrail`, `StartLogging` e `StopLogging`. Os usuários com essa política não têm permissão para criar e atualizar trilhas ou para ativar e desativar o registro. Para ver a lista de CloudTrail ações, consulte a Referência AWS CloudTrail da API.

Acesso total

O exemplo a seguir mostra uma política que concede acesso total CloudTrail a. Isso equivale à política gerenciada AWSCloudTrail_FullAccess. Ele concede aos usuários a permissão para realizar todas as CloudTrail ações. Ele também permite que os usuários registrem eventos de dados no Amazon S3 e AWS Lambda gerenciem arquivos em buckets do Amazon S3, gerenciem CloudWatch como o Logs CloudTrail monitora eventos de log e gerenciem tópicos do Amazon SNS na conta à qual o usuário está associado.

> **Important**
>
> A AWSCloudTrail_FullAccesspolítica ou as permissões equivalentes não devem ser compartilhadas amplamente em sua AWS conta. Os usuários com essa função ou acesso equivalente têm a capacidade de desativar ou reconfigurar as funções de auditoria mais confidenciais e importantes em suas AWS contas. Por esse motivo, essa política deve ser aplicada somente aos administradores da conta e o uso dessa política deve ser cuidadosamente controlado e monitorado.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sns:AddPermission",
                "sns:CreateTopic",
                "sns:SetTopicAttributes",
                "sns:GetTopicAttributes"
            ],
            "Resource": [
                "arn:aws:sns:*:*:aws-cloudtrail-logs*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "sns:ListTopics"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:PutBucketPolicy"
            ],
            "Resource": [
                "arn:aws:s3:::aws-cloudtrail-logs*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets",
                "s3:GetBucketLocation",
                "s3:GetBucketPolicy"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
```

```
            "Action": "cloudtrail:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogGroup"
            ],
            "Resource": [
                "arn:aws:logs:*:*:log-group:aws-cloudtrail-logs*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:ListRoles",
                "iam:GetRolePolicy",
                "iam:GetUser"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "cloudtrail.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:CreateKey",
                "kms:CreateAlias",
                "kms:ListKeys",
                "kms:ListAliases"
            ],
            "Resource": "*"
        },
        {
```

```
            "Effect": "Allow",
            "Action": [
                "lambda:ListFunctions"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "dynamodb:ListGlobalTables",
                "dynamodb:ListTables"
            ],
            "Resource": "*"
        }
    ]
}
```

Concedendo permissão para visualizar AWS Config informações no console CloudTrail

Você pode visualizar as informações do evento no CloudTrail console, incluindo recursos relacionados a esse evento. Para esses recursos, você pode escolher o AWS Config ícone para visualizar a linha do tempo desse recurso no AWS Config console. Anexe essa política aos seus usuários para conceder a eles acesso somente para leitura AWS Config . A política não concede a eles permissão para alterar as configurações em AWS Config.

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

Para ter mais informações, consulte Visualizar recursos referenciados com AWS Config.

Conceder permissão para visualizar e configurar as informações do Amazon CloudWatch Logs no console CloudTrail

Você pode visualizar e configurar a entrega de eventos para o CloudWatch Logs no CloudTrail console se tiver permissões suficientes. Essas são permissões que podem estar além das concedidas aos CloudTrail administradores. Anexe essa política aos administradores que configurarão e gerenciarão a CloudTrail integração com o CloudWatch Logs. A política não concede a eles permissões diretamente no Logs CloudTrail ou no CloudWatch Logs, mas concede as permissões necessárias para criar e configurar a função que CloudTrail assumirá para entregar eventos com sucesso ao seu grupo de CloudWatch Logs.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "iam:CreateRole",
            "iam:PutRolePolicy",
            "iam:AttachRolePolicy",
            "iam:ListRoles",
            "iam:GetRolePolicy",
            "iam:GetUser"
        ],
        "Resource": "*"
    }]
}
```

Para ter mais informações, consulte Monitoramento CloudTrail de arquivos de log com o Amazon CloudWatch Logs.

Mais informações

Para saber mais sobre como usar o IAM para dar às identidades, como usuários e funções, acesso aos recursos em sua conta, consulte Introdução e gerenciamento de acesso para AWS recursos no Guia do usuário do IAM.

AWS CloudTrail exemplos de políticas baseadas em recursos

CloudTrail oferece suporte a políticas de permissões baseadas em recursos para CloudTrail canais usados para integrações com o CloudTrail Lake. Para obter mais informações sobre a criação de integrações com o CloudTrail Lake, consulteCrie uma integração com uma fonte de eventos fora do AWS.

As informações necessárias para a política são determinadas pelo tipo de integração.

- Para uma integração de direção, CloudTrail exige que a política contenha as Conta da AWS IDs do parceiro e exige que você insira a ID externa exclusiva fornecida pelo parceiro. CloudTrail adiciona automaticamente as Conta da AWS IDs do parceiro à política de recursos quando você cria uma integração usando o CloudTrail console. Consulte a documentação do parceiro para saber como obter os Conta da AWS números necessários para a apólice.
- Para uma integração de solução, você deve especificar pelo menos uma Conta da AWS ID como principal e, opcionalmente, inserir uma ID externa para evitar confusões entre representantes.

A seguir estão os requisitos para a política baseada em recursos:

- O ARN do recurso definido na política deve corresponder ao ARN do canal ao qual a política está anexada.
- A política contém apenas uma ação: `cloudtrail-data:PutAuditEvents`
- Cada uma deve incluir pelo menos uma instrução. A política pode ter um máximo de 20 instruções.
- Cada instrução contém pelo menos uma entidade principal. Uma instrução pode ter um máximo de 50 entidades principais.

O proprietário do canal pode chamar a API `PutAuditEvents` no canal, a menos que a política negue ao proprietário o acesso ao recurso.

Tópicos

Exemplo: fornecer acesso ao canal às entidades principais

O exemplo a seguir concede permissões aos diretores com os ARNs `arn:aws:iam::111122223333:root` e `arn:aws:iam::123456789012:root` para chamar a PutAuditEventsAPI no CloudTrail canal com o ARN. `arn:aws:iam::444455556666:root` `arn:aws:cloudtrail:us-east-1:777788889999:channel/EXAMPLE-80b5-40a7-ae65-6e099392355b`

```
{
    "Version": "2012-10-17",
    "Statement":
    [
        {
            "Sid": "ChannelPolicy",
            "Effect": "Allow",
            "Principal":
            {
                "AWS":
                [
                    "arn:aws:iam::111122223333:root",
                    "arn:aws:iam::444455556666:root",
                    "arn:aws:iam::123456789012:root"
                ]
            },
            "Action": "cloudtrail-data:PutAuditEvents",
            "Resource": "arn:aws:cloudtrail:us-east-1:777788889999:channel/
EXAMPLE-80b5-40a7-ae65-6e099392355b"
        }
    ]
}
```

Exemplo: uso de um ID externo para evitar o “confused deputy”

O exemplo a seguir usa um ID externo para endereçar e evitar um confused deputy. "Substituto confuso" é um problema de segurança em que uma entidade que não tem permissão para executar uma ação pode coagir uma entidade mais privilegiada a executá-la.

O parceiro de integração cria o ID externo para usar na política. Em seguida, ele fornece o ID externo a você como parte da criação da integração. O valor pode ser qualquer string exclusiva, como uma frase secreta ou o número de uma conta.

O exemplo concede permissões aos diretores com os ARNs `arn:aws:iam::111122223333:root` e `arn:aws:iam::123456789012:root` para chamar a PutAuditEventsAPI no recurso do CloudTrail canal se a chamada para a `PutAuditEvents` API incluir o valor de ID externo definido na política. `arn:aws:iam::444455556666:root`

```
{
    "Version": "2012-10-17",
    "Statement":
    [
        {
            "Sid": "ChannelPolicy",
            "Effect": "Allow",
            "Principal":
            {
                "AWS":
                [
                    "arn:aws:iam::111122223333:root",
                    "arn:aws:iam::444455556666:root",
                    "arn:aws:iam::123456789012:root"
                ]
            },
            "Action": "cloudtrail-data:PutAuditEvents",
            "Resource": "arn:aws:cloudtrail:us-east-1:777788889999:channel/
EXAMPLE-80b5-40a7-ae65-6e099392355b",
            "Condition":
            {
                "StringEquals":
                {
                    "cloudtrail:ExternalId": "uniquePartnerExternalID"
                }
            }
        }
    ]
}
```

Política de bucket do Amazon S3 para CloudTrail

Por padrão, os buckets e objetos do Amazon S3 são privados. Somente o proprietário do recurso (a conta da AWS que criou o bucket) pode acessar o bucket e os objetos que ele contém. O proprietário do recurso pode conceder permissões de acesso a outros recursos e usuários ao criar uma política de acesso padrão.

Se você deseja criar ou modificar um bucket do Amazon S3 para receber os arquivos de log para uma trilha de organização, modifique a política do bucket. Para ter mais informações, consulte Criando uma trilha para uma organização com o AWS Command Line Interface.

Para entregar arquivos de log em um bucket do S3, é CloudTrail necessário ter as permissões necessárias e não pode ser configurado como um bucket do Requester Pays.

CloudTrail adiciona os seguintes campos na política para você:

- Os SIDs permitidos
- O nome do bucket
- O nome principal do serviço para CloudTrail
- O nome da pasta em que os arquivos de log são armazenados, incluindo o nome do bucket, um prefixo (se você tiver especificado um) e o ID AWS da sua conta

Como uma prática recomendada de segurança, adicione uma `aws:SourceArn` chave de condição para a política de bucket do Amazon S3. A chave de condição global do IAM `aws:SourceArn` ajuda a garantir que as CloudTrail gravações no bucket do S3 sejam gravadas somente para uma trilha ou trilhas específicas. O valor de `aws:SourceArn` é sempre o ARN da trilha (ou matriz de ARNs de trilha) que está usando o bucket para armazenar logs. Certifique-se de adicionar a chave de condição `aws:SourceArn` às políticas de bucket do S3 para as trilhas existentes.

A política a seguir permite CloudTrail gravar arquivos de log no bucket a partir do Supported Regiões da AWS. Substitua *myBucketName[optionalPrefix]/*, *myAccountId, region e TrailName* pelos valores apropriados para sua configuração.

Política de bucket do S3

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailAclCheck20150319",
            "Effect": "Allow",
            "Principal": {"Service": "cloudtrail.amazonaws.com"},
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::myBucketName",
            "Condition": {
                "StringEquals": {
```

```
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:trail/trailName"
                }
            }
        },
        {
            "Sid": "AWSCloudTrailWrite20150319",
            "Effect": "Allow",
            "Principal": {"Service": "cloudtrail.amazonaws.com"},
            "Action": "s3:PutObject",
            "Resource":
 "arn:aws:s3:::myBucketName/[optionalPrefix]/AWSLogs/myAccountID/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:trail/trailName"
                }
            }
        }
    ]
}
```

Para obter mais informações sobre Regiões da AWS, consulteCloudTrail Regiões suportadas.

Sumário

Especificação de um bucket existente para entrega de CloudTrail registros

Se você especificou um bucket do S3 existente como local de armazenamento para entrega do arquivo de log, deverá anexar uma política ao bucket que permita CloudTrail a gravação no bucket.

> **Note**
>
> Como prática recomendada, use um bucket S3 dedicado para CloudTrail registros.

Para adicionar a CloudTrail política necessária a um bucket do Amazon S3

1. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Escolha o bucket em que você deseja CloudTrail entregar seus arquivos de log e, em seguida, escolha Permissões.
3. Selecione a opção Editar.
4. Copie a S3 bucket policy na janela Bucket Policy Editor. Substitua os marcadores em itálico pelos nomes de seu bucket, prefixo e número da conta. Se você tiver especificado um prefixo quando você criou sua trilha, inclua-o aqui. O prefixo é uma opção adicional para a chave do objeto do S3 que cria uma organização em formato de pasta no seu bucket.

   > **Note**
   >
   > Se o bucket existente já tiver uma ou mais políticas anexadas, adicione as instruções para CloudTrail acessar essa política ou políticas. Avalie o conjunto resultante de permissões para ter certeza de que elas são apropriadas para os usuários que acessarão o bucket.

Receber arquivos de log de outras contas

Você pode configurar CloudTrail para entregar arquivos de log de várias AWS contas para um único bucket do S3. Para ter mais informações, consulte Recebendo arquivos de CloudTrail log de várias contas.

Criar ou atualizar um bucket do Amazon S3 a ser usado para armazenar os arquivos de log de uma trilha da organização

Você deve especificar um bucket do Amazon S3 para receber os arquivos de log para uma trilha de organização. Esse bucket deve ter uma política que CloudTrail permita colocar os arquivos de log da organização no bucket.

Veja a seguir um exemplo de política para um bucket do Amazon S3 chamado *myOrganizationBucket*, que pertence à conta de gerenciamento da organização. Substitua *myOrganizationBucket*, *region*, *managementAccountID*, *trailName* e *o-OrganizationID pelos valores da sua organização*

Essa política de bucket consiste em três instruções.

- A primeira declaração permite chamar CloudTrail a `GetBucketAcl` ação do Amazon S3 no bucket do Amazon S3.
- A segunda permite o registro em log caso a trilha seja alterada de uma trilha da organização para uma trilha somente dessa conta.
- A terceira instrução permite o registro em log para uma trilha da organização.

O exemplo de política inclui uma chave de condição `aws:SourceArn` para a política de bucket do Amazon S3. A chave de condição global do IAM `aws:SourceArn` ajuda a garantir que as CloudTrail gravações no bucket do S3 sejam gravadas somente para uma trilha ou trilhas específicas. Em uma trilha da organização, o valor de `aws:SourceArn` deve ser um ARN de trilha que pertença à conta de gerenciamento e use a ID da conta de gerenciamento.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailAclCheck20150319",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "cloudtrail.amazonaws.com"
                ]
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::myOrganizationBucket",
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:managementAccountID:trail/trailName"
                }
            }
        },
        {
```

```
            "Sid": "AWSCloudTrailWrite20150319",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "cloudtrail.amazonaws.com"
                ]
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::myOrganizationBucket/AWSLogs/managementAccountID/
*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:managementAccountID:trail/trailName"
                }
            }
        },
        {
            "Sid": "AWSCloudTrailOrganizationWrite20150319",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "cloudtrail.amazonaws.com"
                ]
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::myOrganizationBucket/AWSLogs/o-organizationID/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:managementAccountID:trail/trailName"
                }
            }
        }
    ]
}
```

Essa política de exemplo não permite que usuários de contas-membro acessem os arquivos de log criados para a organização. Por padrão, os arquivos de log da organização poderão ser acessados somente pela conta de gerenciamento. Para obter informações sobre como conceder

acesso de leitura ao bucket do Amazon S3 para usuários do IAM nas contas-membro, consulte Compartilhamento CloudTrail de arquivos de log entre AWS contas.

Solução de problemas da política de bucket do Amazon S3

As seções a seguir descrevem como solucionar problemas da política de bucket do S3.

Erros comuns de configuração da política do Amazon S3

Quando você cria um novo intervalo como parte da criação ou atualização de uma trilha, CloudTrail anexa as permissões necessárias ao seu intervalo. A política de bucket usa o nome principal do serviço`"cloudtrail.amazonaws.com"`,, que permite CloudTrail entregar registros para todas as regiões.

Se não CloudTrail estiver entregando registros para uma região, é possível que seu bucket tenha uma política mais antiga que especifique IDs de CloudTrail conta para cada região. Essa política dá CloudTrail permissão para entregar registros somente para as regiões especificadas.

Como prática recomendada, atualize a política para usar uma permissão com o responsável pelo CloudTrail serviço. Para fazer isso, substitua os Nomes de região da Amazon (ARN) do ID da conta pelo nome principal do serviço: `"cloudtrail.amazonaws.com"`. Isso dá CloudTrail permissão para entregar registros para regiões atuais e novas. Como uma prática recomendada de segurança, adicione um `aws:SourceArn` ou `aws:SourceAccount` chave de condição à política do bucket do Amazon S3. Isso ajuda a impedir o acesso não autorizado à conta do seu bucket do S3. Se você tiver trilhas existentes, certifique-se de adicionar uma ou mais chaves de condição. Veja a seguir um exemplo de uma configuração de política recomendada. Substitua *`myBucketName[optionalPrefix]/`*, *`myAccountId, region e TrailName`* pelos valores apropriados para sua configuração.

Example Exemplo de política de bucket com o nome principal do serviço

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailAclCheck20150319",
            "Effect": "Allow",
            "Principal": {"Service": "cloudtrail.amazonaws.com"},
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::myBucketName",
```

```
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:trail/trailName"
                }
            }
        },
        {
            "Sid": "AWSCloudTrailWrite20150319",
            "Effect": "Allow",
            "Principal": {"Service": "cloudtrail.amazonaws.com"},
            "Action": "s3:PutObject",
            "Resource":
 "arn:aws:s3:::myBucketName/[optionalPrefix]/AWSLogs/myAccountID/*",
            "Condition": {"StringEquals": {
                "s3:x-amz-acl": "bucket-owner-full-control",
                "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:trail/trailName"
                }
            }
        }
    ]
}
```

Alterar um prefixo de um bucket existente

Se você tentar adicionar, modificar ou remover o prefixo de um arquivo de log para um bucket do S3 que recebe logs de uma trilha, poderá ver o erro: Há um problema com a sua política de bucket. Uma política de bucket com um prefixo incorreto pode impedir que sua trilha forneça logs ao bucket. Para resolver esse problema, use o console do Amazon S3 para atualizar o prefixo na política de bucket e, em seguida, use o CloudTrail console para especificar o mesmo prefixo para o bucket na trilha.

Para atualizar o prefixo do arquivo de log de um bucket do Amazon S3

1. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Escolha o bucket para o qual deseja modificar o prefixo e escolha Permissions (Permissões).
3. Selecione a opção Editar.
4. Na política de bucket, na ação `s3:PutObject`, edite a entrada `Resource` para adicionar, modificar ou remover o *`prefixo`* do arquivo de log conforme necessário.

```
"Action": "s3:PutObject",
```

```
        "Resource": "arn:aws:s3:::myBucketName/prefix/AWSLogs/myAccountID/*",
```

5. Escolha Salvar.
6. Abra o CloudTrail console em https://console.aws.amazon.com/cloudtrail/.
7. Escolha a trilha e, em Storage location, clique no ícone de lápis para editar as configurações do seu bucket.
8. Em S3 bucket, escolha o bucket com o prefixo que você está alterando.
9. Em Log file prefix, atualize o prefixo de acordo com o prefixo informado na política do bucket.
10. Escolha Salvar.

Recursos adicionais do

Para obter mais informações sobre buckets e políticas do S3, consulte Uso de políticas de bucket no Guia do usuário do Amazon Simple Storage Service.

Política de bucket do Amazon S3 para resultados de consulta CloudTrail do Lake

Por padrão, os buckets e objetos do Amazon S3 são privados. Somente o proprietário do recurso (a conta da AWS que criou o bucket) pode acessar o bucket e os objetos que ele contém. O proprietário do recurso pode conceder permissões de acesso a outros recursos e usuários ao criar uma política de acesso padrão.

Para entregar os resultados da consulta do CloudTrail Lake em um bucket do S3, é CloudTrail necessário ter as permissões necessárias e não pode ser configurado como um bucket do Requester Pays.

CloudTrail adiciona os seguintes campos na política para você:

- Os SIDs permitidos
- O nome do bucket
- O nome principal do serviço para CloudTrail

Como uma prática recomendada de segurança, adicione uma `aws:SourceArn` chave de condição para a política de bucket do Amazon S3. A chave de condição global do IAM `aws:SourceArn` ajuda a garantir que as CloudTrail gravações no bucket do S3 sejam gravadas somente para o armazenamento de dados do evento.

A política a seguir permite CloudTrail entregar resultados de consulta ao bucket a partir do Supported Regiões da AWS. *myBucketName*Substitua *myAccountId* e *myQueryRunningRegion* pelos valores apropriados para sua configuração. O *myAccountID* é o ID da AWS conta usado para CloudTrail, que pode não ser o mesmo que o ID da AWS conta do bucket do S3.

> **Note**
>
> Se sua política de bucket incluir uma declaração para uma chave do KMS, recomendamos usar um ARN de chave do KMS totalmente qualificado. Se você usar um alias de chave KMS em vez disso, AWS KMS resolverá a chave na conta do solicitante. Isso pode resultar em dados criptografados com uma chave do KMS pertencente ao solicitante, e não ao proprietário do bucket.
> Se isso for um armazenamento de dados de eventos da organização, o ARN do armazenamento de dados de eventos deverá incluir o ID de conta da AWS para a conta de gerenciamento. Essa abordagem ocorre porque a conta de gerenciamento mantém a propriedade de todos os recursos da organização.

Política de bucket do S3

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailLake1",
            "Effect": "Allow",
            "Principal": {"Service": "cloudtrail.amazonaws.com"},
            "Action": [
                "s3:PutObject*",
                "s3:Abort*"
            ],
            "Resource": [
                "arn:aws:s3:::myBucketName",
                "arn:aws:s3:::myBucketName/*"
            ],
            "Condition": {
                "StringLike": {
                    "aws:sourceAccount": "myAccountID",
                    "aws:sourceArn":
 "arn:aws:cloudtrail:myQueryRunningRegion:myAccountID:eventdatastore/*"
                }
```

```
            }
        },
        {
            "Sid": "AWSCloudTrailLake2",
            "Effect": "Allow",
            "Principal": {"Service":"cloudtrail.amazonaws.com"},
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::myBucketName",
            "Condition": {
                "StringLike": {
                    "aws:sourceAccount": "myAccountID",
                    "aws:sourceArn":
 "arn:aws:cloudtrail:myQueryRunningRegion:myAccountID:eventdatastore/*"
                }
            }
        }
    ]
}
```

Sumário

Especificando um bucket existente para os resultados da consulta CloudTrail do Lake

Se você especificou um bucket do S3 existente como o local de armazenamento para a entrega dos resultados da consulta do CloudTrail Lake, deverá anexar uma política CloudTrail ao bucket que permita entregar os resultados da consulta ao bucket.

> **Note**
>
> Como prática recomendada, use um bucket S3 dedicado para os resultados da consulta CloudTrail do Lake.

Para adicionar a CloudTrail política necessária a um bucket do Amazon S3

1. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.

2. Escolha o bucket em que você deseja CloudTrail entregar os resultados da consulta do Lake e, em seguida, escolha Permissões.
3. Selecione a opção Editar.
4. Copie a S3 bucket policy for query results na janela Bucket Policy Editor. Substitua os espaços reservados em itálico pelos nomes de seu bucket, região e ID da conta.

> **Note**
>
> Se o bucket existente já tiver uma ou mais políticas anexadas, adicione as instruções para CloudTrail acessar essa política ou políticas. Avalie o conjunto resultante de permissões para ter certeza de que elas são apropriadas para os usuários que acessam o bucket.

Recursos adicionais do

Para obter mais informações sobre buckets e políticas do S3, consulte Uso de políticas de bucket no Guia do usuário do Amazon Simple Storage Service.

Política de tópicos do Amazon SNS para CloudTrail

Para enviar notificações para um tópico do SNS, é CloudTrail necessário ter as permissões necessárias. CloudTrailanexa automaticamente as permissões necessárias ao tópico quando você cria um tópico do Amazon SNS como parte da criação ou atualização de uma trilha no CloudTrail console.

> **Important**
>
> Como prática recomendada de segurança, para restringir o acesso ao tópico do SNS, recomendamos que, depois de criar ou atualizar uma trilha para enviar notificações do SNS, você edite manualmente a política do IAM anexada ao tópico do SNS para adicionar chaves de condição. Para obter mais informações, consulte the section called “Prática recomendada de segurança para a política de tópicos do SNS” neste tópico.

CloudTrail adiciona a seguinte declaração à política para você com os seguintes campos:

- Os SIDs permitidos.

- O nome principal do serviço para CloudTrail.
- O tópico do SNS, incluindo região, ID da conta e nome do tópico.

A política a seguir permite CloudTrail enviar notificações sobre a entrega de arquivos de log das regiões suportadas. Para ter mais informações, consulte CloudTrail Regiões suportadas. Esta é a política padrão anexada a uma política de tópicos do SNS nova ou existente quando você cria ou atualiza uma trilha e opta por habilitar as notificações do SNS.

Política de tópicos do SNS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailSNSPolicy20131101",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": "SNS:Publish",
            "Resource": "arn:aws:sns:region:SNSTopicOwnerAccountId:SNSTopicName"
        }
    ]
}
```

Para usar um tópico AWS KMS criptografado do Amazon SNS para enviar notificações, você também deve habilitar a compatibilidade entre a fonte do evento CloudTrail () e o tópico criptografado adicionando a seguinte declaração à política do. AWS KMS key

Política de chaves do KMS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": [
```

```
                "kms:GenerateDataKey*",
                "kms:Decrypt"
            ],
            "Resource": "*"
        }
    ]
}
```

Para obter mais informações, consulte Habilitar compatibilidade entre fontes de eventos de AWS serviços e tópicos criptografados.

Sumário

Prática recomendada de segurança para a política de tópicos do SNS

Por padrão, a declaração de política do IAM CloudTrail anexada ao seu tópico do Amazon SNS permite que CloudTrail o responsável pelo serviço publique em um tópico do SNS, identificado por um ARN. Para ajudar a impedir que um invasor tenha acesso ao seu tópico do SNS e envie notificações em nome dos destinatários do CloudTrail tópico, edite manualmente sua política de tópicos do CloudTrail SNS para adicionar uma chave de `aws:SourceArn` condição à declaração de política anexada por. CloudTrail O valor dessa chave é sempre o ARN da trilha (ou matriz de ARNs de trilha) que estejam usando o tópico do SNS. Como o valor dessa chave inclui o ID de trilha específica e o ID da conta que possui a trilha, ela restringe o acesso a tópicos do SNS somente às contas que têm permissão para gerenciar a trilha. Antes de adicionar chaves de condição à sua política de tópicos do SNS, obtenha o nome do tópico do SNS nas configurações da trilha no CloudTrail console.

A `aws:SourceAccount` chave de condição também é compatível, mas não é recomendada.

Para adicionar a chave de condição do **`aws:SourceArn`** à sua política de tópico do SNS

1. Abra o console do Amazon SNS em https://console.aws.amazon.com/sns/v3/home.

2. No painel de navegação, escolha Tópicos.
3. Escolha o tópico SNS que é mostrado nas configurações de trilha e escolha Edit (Editar).
4. Expanda Access policy (Política de acesso).
5. No editor JSON Access policy (Política de acesso), procure um bloco semelhante ao exemplo a seguir.

```
    {
      "Sid": "AWSCloudTrailSNSPolicy20150319",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:us-west-2:111122223333:aws-cloudtrail-
logs-111122223333-61bbe496"
    }
```

6. Adicione um novo bloco para uma condição, `aws:SourceArn`, conforme mostrado no exemplo a seguir. O valor de `aws:SourceArn` é o ARN da trilha sobre a qual você está enviando notificações para o SNS.

```
    {
      "Sid": "AWSCloudTrailSNSPolicy20150319",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:us-west-2:111122223333:aws-cloudtrail-
logs-111122223333-61bbe496",
      "Condition": {
        "StringEquals": {
          "aws:SourceArn": "arn:aws:cloudtrail:us-west-2:123456789012:trail/Trail3"
        }
      }
    }
```

7. Quando terminar de editar a política de tópico do SNS, escolha Save changes (Salvar alterações).

Para adicionar a chave de condição do **`aws:SourceAccount`** à sua política de tópico do SNS

1. Abra o console do Amazon SNS em https://console.aws.amazon.com/sns/v3/home.
2. No painel de navegação, escolha Tópicos.
3. Escolha o tópico SNS que é mostrado nas configurações de trilha e escolha Edit (Editar).
4. Expanda Access policy (Política de acesso).
5. No editor JSON Access policy (Política de acesso), procure um bloco semelhante ao exemplo a seguir.

```
    {
      "Sid": "AWSCloudTrailSNSPolicy20150319",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:us-west-2:111122223333:aws-cloudtrail-
logs-111122223333-61bbe496"
    }
```

6. Adicione um novo bloco para uma condição, `aws:SourceAccount`, conforme mostrado no exemplo a seguir. O valor de `aws:SourceAccount` é o ID da conta proprietária da CloudTrail trilha. Este exemplo restringe o acesso ao tópico do SNS somente aos usuários que podem entrar na AWS conta 123456789012.

```
    {
      "Sid": "AWSCloudTrailSNSPolicy20150319",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:us-west-2:111122223333:aws-cloudtrail-
logs-111122223333-61bbe496",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "123456789012"
        }
      }
    }
```

7. Quando terminar de editar a política de tópico do SNS, escolha Save changes (Salvar alterações).

Especificar um tópico existente para enviar notificações

Você pode adicionar manualmente as permissões de um tópico do Amazon SNS à sua política de tópicos no console do Amazon SNS e depois especificar o tópico no console. CloudTrail

Para atualizar manualmente uma política de tópicos do SNS

1. Abra o console do Amazon SNS em https://console.aws.amazon.com/sns/v3/home.
2. Escolha Topics (Tópicos) e escolha o tópico.
3. Escolha Editar e, em seguida, role para baixo até Política de acesso.
4. Adicione o extrato de SNS topic policy com os valores apropriados para a região, ID da conta e nome do tópico.
5. Se o seu tópico for um tópico criptografado, você deverá CloudTrail permitir que ele tenha `kms:GenerateDataKey*` e as `kms:Decrypt` permissões. Para ter mais informações, consulte Encrypted SNS topic KMS key policy.
6. Escolha Salvar alterações.
7. Volte ao CloudTrail console e especifique o tópico da trilha.

Solução de problemas de política de tópicos do SNS

As seções a seguir descrevem como solucionar problemas da política de tópicos do SNS.

Cenários:

- CloudTrail não está enviando notificações para uma região
- CloudTrail não está enviando notificações para uma conta de membro em uma organização

CloudTrail não está enviando notificações para uma região

Quando você cria um novo tópico como parte da criação ou atualização de uma trilha, CloudTrail anexa as permissões necessárias ao seu tópico. A política de tópicos usa o nome principal do serviço`"cloudtrail.amazonaws.com"`,, que permite CloudTrail enviar notificações para todas as regiões.

Se não CloudTrail estiver enviando notificações para uma região, é possível que seu tópico tenha uma política mais antiga que especifique IDs de CloudTrail conta para cada região. Essa política dá CloudTrail permissão para enviar notificações somente para as regiões especificadas.

A política de tópicos a seguir CloudTrail permite enviar notificações somente para as nove regiões especificadas:

Example política de tópicos com IDs de contas

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "AWSCloudTrailSNSPolicy20131101",
        "Effect": "Allow",
        "Principal": {"AWS": [
            "arn:aws:iam::903692715234:root",
            "arn:aws:iam::035351147821:root",
            "arn:aws:iam::859597730677:root",
            "arn:aws:iam::814480443879:root",
            "arn:aws:iam::216624486486:root",
            "arn:aws:iam::086441151436:root",
            "arn:aws:iam::388731089494:root",
            "arn:aws:iam::284668455005:root",
            "arn:aws:iam::113285607260:root"
        ]},
        "Action": "SNS:Publish",
        "Resource": "aws:arn:sns:us-east-1:123456789012:myTopic"
    }]
}
```

Essa política usa uma permissão com base em IDs de CloudTrail contas individuais. Para entregar registros para uma nova região, você deve atualizar manualmente a política para incluir o ID da CloudTrail conta dessa região. Por exemplo, como CloudTrail adicionou suporte para a região Leste dos EUA (Ohio), você deve atualizar a política para adicionar o ARN do ID da conta para essa região:. `"arn:aws:iam::475085895292:root"`

Como prática recomendada, atualize a política para usar uma permissão com o responsável pelo CloudTrail serviço. Para fazer isso, substitua os Nomes de região da Amazon (ARN) do ID da conta pelo nome principal do serviço: `"cloudtrail.amazonaws.com"`.

Isso dá CloudTrail permissão para enviar notificações para regiões atuais e novas. Veja a seguir uma versão atualizada da política anterior:

Example política de tópicos com o nome principal do serviço

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "AWSCloudTrailSNSPolicy20131101",
        "Effect": "Allow",
        "Principal": {"Service": "cloudtrail.amazonaws.com"},
        "Action": "SNS:Publish",
        "Resource": "arn:aws:sns:us-west-2:123456789012:myTopic"
    }]
}
```

Verifique se a política tem os valores corretos:

- No campo `Resource`, especifique o número da conta do proprietário do tópico. Para os tópicos que você criar, especifique o número da sua conta.
- Especifique os valores apropriados para a região e o nome do tópico do SNS.

CloudTrail não está enviando notificações para uma conta de membro em uma organização

Quando uma conta membro com uma trilha AWS Organizations organizacional não está enviando notificações do Amazon SNS, pode haver um problema com a configuração da política de tópicos do SNS. CloudTrail cria trilhas da organização nas contas dos membros mesmo se a validação do recurso falhar, por exemplo, o tópico do SNS da trilha da organização não inclui todas as IDs das contas dos membros. Se a política de tópicos do SNS estiver incorreta, ocorrerá uma falha na autorização.

Para verificar se a política de tópicos do SNS de uma trilha tem uma falha de autorização:

- No CloudTrail console, confira a página de detalhes da trilha. Se houver uma falha na autorização, a página de detalhes inclui um aviso `SNS authorization failed` e indica a correção da política de tópicos do SNS.
- A partir do AWS CLI, execute o get-trail-statuscomando. Se houver uma falha na autorização, a saída do comando incluirá o `LastNotificationError` campo com um valor de`AuthorizationError`.

Recursos adicionais do

Para obter mais informações sobre tópicos do SNS e como se inscrever neles, consulte o Guia do desenvolvedor do Amazon Simple Notification Service.

Solução de problemas AWS CloudTrail de identidade e acesso

Use as informações a seguir para ajudá-lo a diagnosticar e corrigir problemas comuns que você pode encontrar ao trabalhar com CloudTrail um IAM.

Tópicos

- Não estou autorizado a realizar uma ação em CloudTrail
- Não tenho autorização para executar iam:PassRole
- Quero permitir que pessoas fora da minha Conta da AWS acessem meus CloudTrail recursos
- Não tenho autorização para executar iam:PassRole
- Estou recebendo uma exceção NoManagementAccountSLRExistsException quando tento criar uma trilha ou um armazenamento de dados de eventos da organização

Não estou autorizado a realizar uma ação em CloudTrail

Se você receber uma mensagem de erro informando que não tem autorização para executar uma ação, suas políticas deverão ser atualizadas para permitir que você realize a ação.

O erro do exemplo a seguir ocorre quando o usuário do IAM `mateojackson` tenta usar o console para visualizar detalhes sobre um atributo *`my-example-widget`* fictício, mas não tem as permissões `cloudtrail:`*`GetWidget`* fictícias.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 cloudtrail:GetWidget on resource: my-example-widget
```

Nesse caso, a política do usuário `mateojackson` deve ser atualizada para permitir o acesso ao recurso *`my-example-widget`* usando a ação `cloudtrail:`*`GetWidget`*.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

Se isso AWS Management Console indicar que você não está autorizado a realizar uma ação, entre em contato com o administrador para obter ajuda. Caso seu administrador seja a pessoa que forneceu suas credenciais de início de sessão.

O exemplo de erro a seguir ocorre quando o usuário do `mateojackson` IAM tenta usar o console para ver detalhes sobre uma trilha, mas não tem a política CloudTrail gerenciada apropriada (AWSCloudTrail_FullAccessou AWSCloudTrail_ReadOnlyAccess) nem as permissões equivalentes aplicadas à sua conta.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 cloudtrail:GetTrailStatus on resource: My-Trail
```

Nesse caso, Mateo pede ao administrador para atualizar suas políticas para permitir que ele acesse as informações das trilhas e o status no console.

Se você fizer login com um usuário ou função do IAM que tenha a política AWSCloudTrail_FullAccessgerenciada ou suas permissões equivalentes e não consiga configurar AWS Config a integração do Amazon CloudWatch Logs com uma trilha, talvez esteja perdendo as permissões necessárias para integração com esses serviços. Para obter mais informações, consulte Concedendo permissão para visualizar AWS Config informações no console CloudTrail e Conceder permissão para visualizar e configurar as informações do Amazon CloudWatch Logs no console CloudTrail .

Não tenho autorização para executar **`iam:PassRole`**

Se você receber um erro informando que não está autorizado a realizar a `iam:PassRole` ação, suas políticas devem ser atualizadas para permitir que você transfira uma função para CloudTrail o.

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 usuário do IAM chamado `marymajor` tenta usar o console para realizar uma ação no CloudTrail. 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 permitir que pessoas fora da minha Conta da AWS acessem meus CloudTrail recursos

Você pode criar uma função e compartilhar CloudTrail informações entre várias Contas da AWS. Para ter mais informações, consulte Compartilhamento CloudTrail de arquivos de log entre AWS contas.

Você pode criar uma função que os usuários de outras contas ou pessoas fora da 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 atributos ou listas de controle de acesso (ACLs), você pode usar essas políticas para conceder às pessoas acesso aos seus atributos.

Para saber mais, consulte:

- Para saber se é CloudTrail compatível com esses recursos, consulteComo AWS CloudTrail funciona com o IAM.
- Para saber como fornecer acesso aos seus recursos em todos os Contas da AWS que você possui, consulte Como fornecer acesso a um usuário do IAM em outro Conta da AWS que você possui no Guia do usuário do IAM.
- Para saber como fornecer acesso aos seus recursos a terceiros Contas da AWS, consulte Como fornecer acesso Contas da AWS a terceiros no Guia do usuário do IAM.
- Para saber como conceder acesso por meio da federação de identidades, consulte Conceder acesso a usuários autenticados externamente (federação de identidades) no Guia do usuário do IAM.
- Para saber a diferença entre usar perfis e políticas baseadas em recursos para acesso entre contas, consulte Como os perfis do IAM diferem de políticas baseadas em recursos no Guia do usuário do IAM.

Não tenho autorização para executar **`iam:PassRole`**

Se você receber um erro informando que não está autorizado a realizar a `iam:PassRole` ação, suas políticas devem ser atualizadas para permitir que você transfira uma função para CloudTrail o.

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 usuário do IAM chamado `marymajor` tenta usar o console para realizar uma ação no CloudTrail. 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.

Estou recebendo uma exceção **`NoManagementAccountSLRExistsException`** quando tento criar uma trilha ou um armazenamento de dados de eventos da organização

A exceção `NoManagementAccountSLRExistsException` é lançada quando a conta de gerenciamento não tem um perfil vinculado ao serviço. Quando você adiciona um administrador delegado usando a operação AWS Organizations AWS CLI ou API, a função vinculada ao serviço não é criada se não existir.

Quando você usa a conta de gerenciamento da sua organização para adicionar um administrador delegado ou criar uma trilha da organização ou um armazenamento de dados de eventos no CloudTrail console, ou usando a CloudTrail API AWS CLI ou, cria CloudTrail automaticamente uma função vinculada ao serviço para sua conta de gerenciamento, caso ainda não exista.

Se você não adicionou um administrador delegado, use o CloudTrail console AWS CLI ou a CloudTrail API para adicionar o administrador delegado. Para obter mais informações sobre como adicionar um administrador delegado, consulte Adicionar um administrador CloudTrail delegado and RegisterOrganizationDelegatedAdmin(API).

Se você já adicionou o administrador delegado, use a conta de gerenciamento para criar a trilha da organização ou o armazenamento de dados do evento no CloudTrail console ou usando a CloudTrail

API AWS CLI ou. Para obter mais informações sobre como criar uma trilha organizacionalCriar uma trilha para sua organização no console, consulteCriando uma trilha para uma organização com o AWS Command Line Interface, e CreateTrail(API).

Usando funções vinculadas a serviços para AWS CloudTrail

AWS CloudTrail usa funções vinculadas ao serviço AWS Identity and Access Management (IAM). Uma função vinculada ao serviço é um tipo exclusivo de função do IAM vinculada diretamente a. CloudTrail As funções vinculadas ao serviço são predefinidas CloudTrail e incluem todas as permissões que o serviço exige para ligar para outras pessoas Serviços da AWS em seu nome.

Uma função vinculada ao serviço facilita a configuração CloudTrail porque você não precisa adicionar manualmente as permissões necessárias. CloudTrail define as permissões de suas funções vinculadas ao serviço e, a menos que seja definido de outra forma, só CloudTrail pode assumir suas funções. As permissões definidas incluem a política de confiança e a política de permissões, que não pode ser anexada a nenhuma outra entidade do IAM.

Para obter informações sobre outros serviços compatíveis com funções vinculadas a serviços, consulte Serviços da AWS compatíveis com o IAM e procure os serviços que contenham Sim na coluna Função vinculada a serviço. Escolha um Sim com um link para visualizar a documentação do perfil vinculado a esse serviço.

Permissões de função vinculadas ao serviço para CloudTrail

CloudTrail usa a função vinculada ao serviço chamada AWSServiceRoleForCloudTrail— Essa função vinculada ao serviço é usada para apoiar trilhas da organização e armazenamentos de dados de eventos da organização.

A função AWSServiceRoleForCloudTrail vinculada ao serviço confia nos seguintes serviços para assumir a função:

- `cloudtrail.amazonaws.com`

Essa função é usada para apoiar a criação e o gerenciamento de trilhas CloudTrail organizacionais e armazenamentos de dados de eventos da organização CloudTrail Lake em CloudTrail. Para ter mais informações, consulte Criar uma trilha para uma organização.

A CloudTrailServiceRolePolicypolítica anexada à função permite CloudTrail concluir as seguintes ações nos recursos especificados:

- Ações em todos os CloudTrail recursos:
  - `All`
- Ações em todos os AWS Organizations recursos:
  - `organizations:DescribeAccount`
  - `organizations:DescribeOrganization`
  - `organizations:ListAccounts`
  - `organizations:ListAWSServiceAccessForOrganization`
- Ações em todos os recursos da Organizations para que o diretor de CloudTrail serviço liste os administradores delegados da organização:
  - `organizations:ListDelegatedAdministrators`
- Ações para desabilitar a federação do Lake em um armazenamento de dados de eventos da organização:
  - `glue:DeleteTable`
  - `lakeformation:DeRegisterResource`

Você deve configurar permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua uma função vinculada a serviço. Para mais informações, consulte Permissões de perfil vinculado ao serviço no Guia do usuário do IAM.

Criação de uma função vinculada ao serviço para CloudTrail

Não é necessário criar manualmente uma função vinculada a serviço. Quando você cria uma trilha da organização ou um armazenamento de dados de eventos da organização, adiciona um administrador delegado no CloudTrail console ou usa a operação AWS CLI ou API, CloudTrail cria a função vinculada ao serviço para você, caso ela ainda não exista.

Se você excluir esse perfil vinculado ao serviço e precisar criá-lo novamente, poderá usar esse mesmo processo para recriar o perfil na sua conta. Quando você cria uma trilha da organização ou um armazenamento de dados de eventos da organização, ou adiciona um administrador delegado, CloudTrail cria a função vinculada ao serviço para você novamente.

Editando uma função vinculada ao serviço para CloudTrail

CloudTrail não permite que você edite a função AWSServiceRoleForCloudTrail vinculada ao serviço. Depois que criar um perfil vinculado ao serviço, você não poderá alterar o nome do perfil, pois várias

entidades podem fazer referência a ele. No entanto, será possível editar a descrição do perfil usando o IAM. Para obter mais informações, consulte Editar uma função vinculada a serviço no Guia do usuário do IAM.

Excluindo uma função vinculada ao serviço para CloudTrail

Você não precisa excluir manualmente a AWSServiceRoleForCloudTrail função. Se um Conta da AWS for removido de uma organização da Organizations, a AWSServiceRoleForCloudTrail função será automaticamente removida dessa organização Conta da AWS. Não é possível desanexar ou remover políticas do perfil vinculado ao serviço AWSServiceRoleForCloudTrail em uma conta de gerenciamento da organização sem remover a conta da organização.

Você também pode usar o console do IAM AWS CLI ou a AWS API para excluir manualmente a função vinculada ao serviço. Para isso, primeiro você deve limpar manualmente os recursos de sua função vinculada ao serviço e, em seguida, excluí-la manualmente.

> **Note**
>
> Se o CloudTrail serviço estiver usando a função quando você tentar excluir os recursos, a exclusão poderá falhar. Se isso acontecer, espere alguns minutos e tente a operação novamente.

Para remover um recurso usado pela função AWSServiceRoleForCloudTrail, você pode executar uma das seguintes ações:

- Remova o Conta da AWS da organização em Organizations.
- Atualize a trilha para que não seja mais uma trilha de organização. Para ter mais informações, consulte Atualizar uma trilha.
- Atualize o armazenamento de dados de eventos para que ele não seja mais um armazenamento de dados de eventos da organização. Para ter mais informações, consulte Atualizar um armazenamento de dados de eventos com o console.
- Exclua a trilha. Para ter mais informações, consulte Excluir uma trilha.
- Excluir um armazenamento de dados de eventos. Para ter mais informações, consulte Excluir um armazenamento de dados de eventos com o console.

Como excluir manualmente o perfil vinculado a serviço usando o IAM

Use o console do IAM AWS CLI, o ou a AWS API para excluir a função AWSServiceRoleForCloudTrail vinculada ao serviço. Para obter mais informações, consulte Excluir um perfil vinculado ao serviço no Guia do usuário do IAM.

Regiões suportadas para funções vinculadas a CloudTrail serviços

CloudTrail suporta o uso de funções vinculadas a serviços em todos os Regiões da AWS lugares onde e em CloudTrail Organizations estão disponíveis. Para obter mais informações, consulte AWS service (Serviço da AWS) endpoints na Referência geral da AWS.

AWS políticas gerenciadas para AWS CloudTrail

Para adicionar permissões a usuários, grupos e funções, é mais fácil usar políticas AWS gerenciadas do que escrever políticas você mesmo. É necessário tempo e experiência para criar políticas gerenciadas pelo cliente do IAM que fornecem à sua equipe apenas as permissões de que precisam. Para começar rapidamente, você pode usar políticas AWS gerenciadas. Essas políticas abrangem casos de uso comuns e estão disponíveis na sua Conta da AWS. Para obter mais informações sobre políticas AWS gerenciadas, consulte políticas AWS gerenciadas no Guia do usuário do IAM.

AWS os serviços mantêm e atualizam as políticas AWS gerenciadas. Você não pode alterar as permissões nas políticas AWS gerenciadas. Os serviços ocasionalmente acrescentam permissões adicionais a uma política gerenciada pela AWS para oferecer suporte a novos atributos. Esse tipo de atualização afeta todas as identidades (usuários, grupos e perfis) em que a política está anexada. É mais provável que os serviços atualizem uma política gerenciada pela AWS quando um novo atributo for iniciado ou novas operações se tornarem disponíveis. Os serviços não removem as permissões de uma política AWS gerenciada, portanto, as atualizações de políticas não violarão suas permissões existentes.

Além disso, AWS oferece suporte a políticas gerenciadas para funções de trabalho que abrangem vários serviços. Por exemplo, a política ReadOnlyAccess AWS gerenciada fornece acesso somente de leitura a todos os AWS serviços e recursos. Quando um serviço lança um novo recurso, AWS adiciona permissões somente de leitura para novas operações e recursos. Para obter uma lista e descrições das políticas de perfis de trabalho, consulte Políticas gerenciadas pela AWS para perfis de trabalho no Guia do usuário do IAM.

AWS política gerenciada: **`AWSCloudTrail_ReadOnlyAccess`**

Uma identidade de usuário que tenha a AWSCloudTrail_ReadOnlyAccesspolítica associada à sua função pode realizar ações somente para leitura em CloudTrail, como,, e `Describe*` ações em trilhas `Get*List*`, armazenamentos de dados de eventos do CloudTrail Lake ou consultas do Lake.

AWS política gerenciada: **AWSServiceRoleForCloudTrail**

A CloudTrailServiceRolePolicypolítica permite AWS CloudTrail realizar ações nas trilhas da organização e nos armazenamentos de dados de eventos da organização em seu nome. A política inclui AWS Organizations as permissões necessárias para descrever e listar as contas da organização e os administradores delegados em uma AWS Organizations organização.

Além disso, essa política inclui os requisitos AWS Glue e AWS Lake Formation as permissões para desativar o Lake Federation em um armazenamento de dados de eventos da organização.

Essa política está anexada à função AWSServiceRoleForCloudTrailvinculada ao serviço que permite CloudTrail realizar ações em seu nome. Não é possível vincular esta política a usuários, grupos ou funções.

CloudTrail atualizações nas políticas AWS gerenciadas

Veja detalhes sobre as atualizações das políticas AWS gerenciadas do CloudTrail. Para receber alertas automáticos sobre alterações nesta página, assine o feed RSS na CloudTrail Histórico do documento página.

Alteração	Descrição	Data
`CloudTrailServiceRolePolicy` : atualizar para uma política existente	Atualizou a política para permitir as seguintes ações em um armazenamento de dados de eventos da organização quando a federação está desabilitada: • `glue:DeleteTable` • `lakeformation:DeregisterResource`	26 de novembro de 2023
`AWSCloudTrail_ReadOnlyAccess` : atualização para uma política existente	CloudTrail alterou o nome da `AWSCloudTrailReadOnlyAccess` política para`AWSCloudTrail_ReadOnlyAccess` . Além disso,	6 de junho de 2022

Alteração	Descrição	Data
	o escopo das permissõe s na política foi reduzido a CloudTrail ações. Ele não inclui mais o Amazon S3 ou as permissões AWS KMS de AWS Lambda ação.	
CloudTrail começou a rastrear alterações	CloudTrail começou a rastrear as mudanças em suas políticas AWS gerenciadas.	6 de junho de 2022

Validação de conformidade para AWS CloudTrail

Auditores terceirizados avaliam a segurança e a conformidade AWS CloudTrail como parte de vários programas de AWS conformidade. Isso inclui SOC, PCI, FedRAMP, HIPAA e outros.

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

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

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

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

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

- AWS Recursos de https://aws.amazon.com/compliance/resources/ de conformidade — Essa coleção de pastas de trabalho e guias pode ser aplicada ao seu setor e local.
- AWS Guias de conformidade do cliente — Entenda o modelo de responsabilidade compartilhada sob a ótica da conformidade. Os guias resumem as melhores práticas de proteção Serviços da AWS e mapeiam as diretrizes para controles de segurança em várias estruturas (incluindo o Instituto Nacional de Padrões e Tecnologia (NIST), o Conselho de Padrões de Segurança do Setor de Cartões de Pagamento (PCI) e a Organização Internacional de Padronização (ISO)).
- Avaliação de recursos com regras no Guia do AWS Config desenvolvedor — O AWS Config serviço avalia o quão bem suas configurações de recursos estão em conformidade com as práticas internas, as diretrizes e os regulamentos do setor.
- AWS Security Hub— Isso AWS service (Serviço da AWS) fornece uma visão abrangente do seu estado de segurança interno AWS. O Security Hub usa controles de segurança para avaliar os atributos da AWS e verificar a conformidade com os padrões e as práticas recomendadas do setor de segurança. Para obter uma lista dos serviços e controles aceitos, consulte a Referência de controles do Security Hub.
- Amazon GuardDuty — Isso AWS service (Serviço da AWS) detecta possíveis ameaças às suas cargas de trabalho Contas da AWS, contêineres e dados monitorando seu ambiente em busca de atividades suspeitas e maliciosas. GuardDuty pode ajudá-lo a atender a vários requisitos de conformidade, como o PCI DSS, atendendo aos requisitos de detecção de intrusões exigidos por determinadas estruturas de conformidade.
- AWS Audit Manager— Isso AWS service (Serviço da AWS) ajuda você a auditar continuamente seu AWS uso para simplificar a forma como você gerencia o risco e a conformidade com as regulamentações e os padrões do setor.

Resiliência em AWS CloudTrail

A infraestrutura AWS global é construída em torno de AWS regiões e zonas de disponibilidade. AWS As regiões fornecem várias zonas de disponibilidade fisicamente separadas e isoladas, conectadas a redes de baixa latência, alta taxa de transferência e alta redundância. Com as zonas de disponibilidade, é possível projetar e operar aplicações e bancos de dados que executam

o failover automaticamente entre as zonas de disponibilidade sem interrupção. As Zonas de Disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de datacenter tradicionais. Se você precisar replicar especificamente seus arquivos de CloudTrail log em distâncias geográficas maiores, você pode usar a replicação entre regiões para seus buckets Amazon S3 de trilha, o que permite a cópia automática e assíncrona de objetos entre buckets em diferentes regiões. AWS

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

Além da infraestrutura AWS global, CloudTrail oferece vários recursos para ajudar a suportar suas necessidades de resiliência e backup de dados.

Armazenamentos de dados de trilhas e eventos que registram eventos em todas as AWS regiões

Quando você aplica uma trilha a todas as AWS regiões, CloudTrail cria trilhas com configurações idênticas em todas as outras Regiões da AWS na AWS partição em que você está trabalhando. Quando AWS adiciona uma nova região, essa configuração de trilha é criada automaticamente na nova região.

Quando você cria um armazenamento de dados de eventos multirregional, CloudTrail coleta eventos que ocorrem Regiões da AWS em toda a sua conta.

Controle de versão, configuração do ciclo de vida e proteção de bloqueio de objetos para dados de log CloudTrail

Como CloudTrail usa buckets do Amazon S3 para armazenar arquivos de log, você também pode usar os recursos fornecidos pelo Amazon S3 para ajudar a suportar suas necessidades de resiliência e backup de dados. Para obter mais informações, consulte Resiliência do Amazon S3.

Segurança da infraestrutura em AWS CloudTrail

Como serviço gerenciado, AWS CloudTrail é protegido pela segurança de rede AWS global. Para obter informações sobre serviços AWS de segurança e como AWS proteger a infraestrutura, consulte AWS Cloud Security. Para projetar seu AWS ambiente usando as melhores práticas de segurança de infraestrutura, consulte Proteção de infraestrutura no Security Pillar AWS Well-Architected Framework.

Você usa chamadas de API AWS publicadas para acessar CloudTrail pela rede. Os clientes devem oferecer suporte para:

- Transport Layer Security (TLS). Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Conjuntos de criptografia com sigilo de encaminhamento perfeito (perfect forward secrecy, ou PFS) como DHE (Ephemeral Diffie-Hellman, ou Efêmero Diffie-Hellman) ou ECDHE (Ephemeral Elliptic Curve Diffie-Hellman, ou Curva elíptica efêmera Diffie-Hellman). A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

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

As práticas recomendadas de segurança a seguir também abordam a segurança da infraestrutura em CloudTrail:

- Considere os VPC endpoints da Amazon para acesso de trilha.
- Considerar os endpoints do Amazon VPC para acessar o bucket do Amazon S3. Para obter mais informações, consulte Como controlar o acesso de VPC endpoints com políticas de bucket.
- Identifique e audite todos os buckets do Amazon S3 que contêm CloudTrail arquivos de log. Considere o uso de tags para ajudar a identificar suas CloudTrail trilhas e os buckets do Amazon S3 que contêm CloudTrail arquivos de log. Em seguida, você pode usar grupos de recursos para seus CloudTrail recursos. Para ter mais informações, consulte AWS Resource Groups.

Prevenção contra o ataque do “substituto confuso” em todos os serviços

"Substituto confuso" é um problema de segurança em que uma entidade que não tem permissão para executar uma ação pode coagir uma entidade mais privilegiada a executá-la. Em AWS, a falsificação de identidade entre serviços pode resultar no problema confuso do deputado. A imitação entre serviços pode ocorrer quando um serviço (o serviço de chamada) chama outro serviço (o serviço chamado). O serviço de chamada pode ser manipulado para utilizar as suas permissões para atuar nos recursos de outro cliente em que, de outra forma, ele não teria permissão para acessar. Para evitar isso, o AWS fornece ferramentas que ajudam você a proteger seus dados para todos os serviços com entidades principais de serviço que receberam acesso aos recursos em sua conta.

Recomendamos usar as chaves de contexto de condição `aws:SourceAccount`global `aws:SourceArn`e as chaves de contexto nas políticas de recursos para limitar as permissões que

AWS CloudTrail concedem outro serviço ao recurso. Use `aws:SourceArn` se quiser que apenas um recurso seja associado ao acesso entre serviços. Use `aws:SourceAccount` se quiser permitir que qualquer recurso nessa conta seja associado ao uso entre serviços.

A maneira mais eficaz de se proteger contra o problema do substituto confuso é usar a chave de contexto de condição global `aws:SourceArn` com o ARN completo do recurso. Se você não souber o ARN completo do recurso ou se estiver especificando vários recursos, use a chave de condição de contexto global `aws:SourceArn` com curingas (`*`) para as partes desconhecidas do ARN. Por exemplo, `"arn:aws:cloudtrail:*:AccountID:trail/*"`. Ao incluir um caractere curinga, também é necessário usar o operador de condição `StringLike`.

O valor de `aws:SourceArn` deve ser o ARN da trilha, do armazenamento de dados de eventos ou do canal que está usando o recurso.

O exemplo a seguir mostra como você pode usar as chaves de contexto de condição `aws:SourceAccount` global `aws:SourceArn` e global CloudTrail para evitar o problema confuso do substituto:Política de bucket do Amazon S3 para resultados de consulta CloudTrail do Lake.

Melhores práticas de segurança em AWS CloudTrail

AWS CloudTrail fornece vários recursos de segurança a serem considerados ao desenvolver e implementar suas próprias políticas de segurança. As melhores práticas a seguir são diretrizes gerais e não representam uma solução completa de segurança. Como essas melhores práticas podem não ser adequadas ou suficientes para o seu ambiente, trate-as como considerações úteis em vez de prescrições.

Tópicos

- CloudTrail melhores práticas de segurança de detetives
- CloudTrail melhores práticas de segurança preventiva

CloudTrail melhores práticas de segurança de detetives

Criar uma trilha

Para um registro contínuo dos eventos em sua AWS conta, você deve criar uma trilha. Embora CloudTrail forneça 90 dias de informações do histórico de eventos para eventos de gerenciamento no CloudTrail console sem criar uma trilha, ele não é um registro permanente e não fornece informações sobre todos os tipos possíveis de eventos. Para um registro contínuo e para um registro

que contém todos os tipos de evento especificados, você deve criar uma trilha, que fornece arquivos de log a um bucket do Amazon S3 especificado.

Para ajudar a gerenciar seus CloudTrail dados, considere criar uma trilha que registre todos os eventos de gerenciamento e Regiões da AWS, em seguida, crie trilhas adicionais que registrem tipos de eventos específicos para recursos, como atividades ou AWS Lambda funções do bucket do Amazon S3.

Você pode seguir algumas das etapas abaixo:

- Criar uma trilha para a sua conta AWS .
- Criar uma trilha para uma organização.

Aplique trilhas a todos Regiões da AWS

Para obter um registro completo dos eventos realizados por uma identidade ou serviço do IAM em sua AWS conta, cada trilha deve ser configurada para registrar todos os eventos Regiões da AWS. Ao registrar todos os eventos Regiões da AWS, você garante que todos os eventos que ocorrem em sua AWS conta sejam registrados, independentemente da AWS região em que ocorreram. Isso inclui registrar eventos de serviços globais, que são registrados em uma AWS região específica desse serviço. Quando você cria uma trilha que se aplica a todas as regiões, CloudTrail registra eventos em cada região e entrega os arquivos de log de CloudTrail eventos em um bucket do S3 que você especifica. Se uma região da AWS for adicionada depois que você criar uma trilha que se aplica a todas as regiões, essa nova região será incluída automaticamente, e os eventos nessa região serão registrados. Essa é a opção padrão quando você cria uma trilha no CloudTrail console.

Você pode seguir algumas das etapas abaixo:

- Criar uma trilha para a sua conta AWS .
- Atualizar uma trilha existente para registrar eventos em todas as Regiões da AWS.
- Implemente controles de detetive contínuos para ajudar a garantir que todas as trilhas criadas estejam Regiões da AWS registrando todos os eventos usando a regra multi-region-cloud-trail-enabled in. AWS Config

Habilitar a integridade do arquivo de CloudTrail log

Os arquivos de log validados são valiosos especialmente para segurança e investigações forenses. Por exemplo, um arquivo de log validado permite que você declare positivamente que o arquivo de

log não foi alterado ou que determinadas credenciais de identidade do IAM realizaram atividades específicas de API. O processo de validação da integridade do arquivo de CloudTrail log também permite que você saiba se um arquivo de log foi excluído ou alterado, ou afirme positivamente que nenhum arquivo de log foi entregue à sua conta durante um determinado período de tempo. CloudTrail a validação da integridade do arquivo de log usa algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinatura digital. Isso torna computacionalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção. Para ter mais informações, consulte Habilitar a validação e validar arquivos.

Integre com o Amazon CloudWatch Logs

CloudWatch Os registros permitem que você monitore e receba alertas para eventos específicos capturados pelo CloudTrail. Os eventos enviados para o CloudWatch Logs são aqueles configurados para serem registrados por sua trilha, portanto, certifique-se de ter configurado sua trilha ou trilhas para registrar os tipos de eventos (eventos de gerenciamento e/ou eventos de dados) que você tem interesse em monitorar.

Por exemplo, você pode monitorar os principais eventos de segurança e gerenciamento relacionados à rede, como eventos de AWS Management Console login com falha.

Você pode seguir algumas das etapas abaixo:

- Veja exemplos de integrações de CloudWatch registros para CloudTrail.
- Configure sua trilha para enviar eventos para o CloudWatch Logs.
- Considere implementar controles de detetive contínuos para ajudar a garantir que todas as trilhas enviem eventos ao CloudWatch Logs para monitoramento usando a regra cloud-trail-cloud-watch-logs-enabled em. AWS Config

Use a Amazon GuardDuty

GuardDuty A Amazon é um serviço de detecção de ameaças que ajuda você a proteger suas contas, contêineres, cargas de trabalho e os dados em seu AWS ambiente. Usando modelos de aprendizado de máquina (ML) e recursos de detecção de anomalias e ameaças, monitora GuardDuty continuamente diferentes fontes de log para identificar e priorizar possíveis riscos de segurança e atividades maliciosas em seu ambiente.

Por exemplo, GuardDuty detectará uma possível exfiltração de credenciais caso detecte credenciais que foram criadas exclusivamente para uma instância do Amazon EC2 por meio de uma função de

lançamento de instância, mas que estão sendo usadas em outra conta interna. AWS Para obter mais informações, consulte o Guia GuardDuty do usuário da Amazon.

Use AWS Security Hub

Monitore seu uso das CloudTrail melhores práticas de segurança no que se refere às melhores práticas de segurança usando AWS Security Hub. O Security Hub usa controles de segurança detetives para avaliar configurações de recursos e padrões de segurança que ajudam você a cumprir vários frameworks de conformidade. Para obter mais informações sobre como usar o Security Hub para avaliar CloudTrail recursos, consulte AWS CloudTrail os controles no Guia AWS Security Hub do Usuário.

CloudTrail melhores práticas de segurança preventiva

As práticas recomendadas a seguir CloudTrail podem ajudar a evitar incidentes de segurança.

Registrar em log em um bucket do Amazon S3 centralizado e dedicado

CloudTrail os arquivos de log são um registro de auditoria das ações realizadas por uma identidade ou AWS serviço do IAM. A integridade, integridade e disponibilidade desses logs é essencial para fins de auditoria e forenses. Ao fazer login em um bucket do Amazon S3 centralizado e dedicado, você pode impor rigorosos controles de segurança, acesso e separação de tarefas.

Você pode seguir algumas das etapas abaixo:

- Crie uma AWS conta separada como uma conta de arquivamento de registros. Se você usa AWS Organizations, inscreva essa conta na organização e considere criar uma trilha da organização para registrar os dados de todas as AWS contas em sua organização.
- Se você não usa Organizations, mas deseja registrar dados de várias AWS contas, crie uma trilha para registrar atividades nessa conta de arquivamento de registros. Restrinja o acesso a essa conta apenas a usuários administrativos confiáveis que devem ter acesso aos dados de conta e auditoria.
- Como parte da criação de uma trilha, seja uma trilha organizacional ou uma trilha para uma única AWS conta, crie um bucket Amazon S3 dedicado para armazenar arquivos de log dessa trilha.
- Se você quiser registrar a atividade de mais de uma AWS conta, modifique a política do bucket para permitir o registro e o armazenamento de arquivos de log de todas as AWS contas nas quais você deseja registrar a atividade AWS da conta.
- Se você não estiver usando uma trilha de organização, crie trilhas em todas as suas contas da AWS , especificando o bucket do Amazon S3 na conta do arquivo de log.

Use criptografia do lado do servidor com chaves gerenciadas AWS KMS

Por padrão, os arquivos de log entregues CloudTrail ao seu bucket do S3 são criptografados usando criptografia do lado do servidor com uma chave KMS (SSE-KMS). Para usar o SSE-KMS CloudTrail, você cria e gerencia uma AWS KMS key, também conhecida como chave KMS.

> **Note**
>
> Se você usar o SSE-KMS e a validação do arquivo de log e tiver modificado a política de bucket do Amazon S3 para permitir apenas arquivos criptografados pelo SSE-KMS, não será possível criar trilhas que utilizam esse bucket, a menos que você modifique a política de bucket para permitir a criptografia AES256 especificamente, como mostrado no seguinte exemplo de linha de política.
>
> ```
> "StringNotEquals": { "s3:x-amz-server-side-encryption": ["aws:kms", "AES256"] }
> ```

Você pode seguir algumas das etapas abaixo:

- Analise as vantagens de criptografar seus arquivos de log com SSE-KMS.
- Crie uma chave do KMS a ser usada para criptografar arquivos de log.
- Configure a criptografia de arquivos de log das suas trilhas.
- Considere implementar controles de detetive contínuos para ajudar a garantir que todas as trilhas estejam criptografando arquivos de log com SSE-KMS usando a regra em. cloud-trail-encryption-enabled AWS Config

Adicionar uma chave de condição à política de tópicos padrão do Amazon SNS

Quando você configura uma trilha para enviar notificações para o Amazon SNS, CloudTrail adiciona uma declaração de política à sua política de acesso a tópicos do SNS que permite enviar conteúdo CloudTrail para um tópico do SNS. Como prática recomendada de segurança, recomendamos adicionar uma chave de condição `aws:SourceArn` (ou opcionalmente`aws:SourceAccount`) à declaração CloudTrail de política. Isso ajuda a impedir o acesso não autorizado da conta ao tópico do SNS. Para ter mais informações, consulte Política de tópicos do Amazon SNS para CloudTrail.

Implementar o acesso com privilégio mínimo a buckets do Amazon S3 em que os arquivos de log são armazenados

CloudTrail trilhas registram eventos em um bucket do Amazon S3 que você especificar. Esses arquivos de log contêm um registro de auditoria das ações tomadas pelas identidades e AWS serviços do IAM. A integridade e a integridade desses arquivos de log de auditoria são essenciais para fins forenses. Para ajudar a garantir essa integridade, você deve seguir o princípio do privilégio mínimo ao criar ou modificar o acesso a qualquer bucket do Amazon S3 usado para CloudTrail armazenar arquivos de log.

Siga as seguintes etapas:

- Revise a política de bucket do Amazon S3 para qualquer bucket em que você armazena arquivos de log e ajuste-o, se necessário, para remover o acesso desnecessário. Essa política de bucket será gerada para você se você criar uma trilha usando o CloudTrail console, mas também poderá ser criada e gerenciada manualmente.
- Como uma prática recomendada de segurança, certifique-se de adicionar manualmente uma `aws:SourceArn` chave de condição para a política de bucket. Para ter mais informações, consulte Política de bucket do Amazon S3 para CloudTrail.
- Se você estiver usando o mesmo bucket do Amazon S3 para armazenar arquivos de log de várias AWS contas, siga as orientações para receber arquivos de log de várias contas.
- Se você estiver usando uma trilha de organização, siga a orientação para trilhas de organização e revise a política de exemplo para um bucket do Amazon S3 para uma trilha de organização em Criando uma trilha para uma organização com o AWS Command Line Interface.
- Revise a documentação de segurança do Amazon S3 e a demonstração de exemplo para proteger um bucket.

Habilitar a exclusão de MFA no bucket do Amazon S3 em que os arquivos de log são armazenados

Quando a autenticação multifator (MFA) está configurada, quaisquer tentativas de alterar o estado de versionamento do bucket ou excluir permanentemente uma versão de objeto de um bucket exige autenticação adicional. Assim, mesmo que um usuário obtenha a senha de um usuário do IAM com permissões para excluir permanentemente objetos do Amazon S3, você ainda poderá prevenir operações que poderiam comprometer seus arquivos de log.

Você pode seguir algumas das etapas abaixo:

- Consulte as diretrizes de exclusão de MFA no Guia do usuário do Amazon Simple Storage Service.
- Adicione uma política de bucket do Amazon S3 para exigir MFA.

> **Note**
>
> Não é possível usar a exclusão de MFA com configurações de ciclo de vida. Para obter mais informações sobre as configurações de ciclo de vida e como elas interagem com outras configurações, consulte as Configurações de ciclo de vida e outras configurações de bucket no Guia do usuário do Amazon Simple Storage Service.

Configurar o gerenciamento de ciclo de vida de objetos no bucket do Amazon S3 em que os arquivos de log são armazenados

O padrão da CloudTrail trilha é armazenar arquivos de log indefinidamente no bucket do Amazon S3 configurado para a trilha. Você pode usar as regras de gerenciamento de ciclo de vida de objetos do Amazon S3 para definir sua própria política de retenção para melhor atender às suas necessidades de negócios e auditoria. Por exemplo, você pode arquivar arquivos de log que têm mais de um ano no Amazon Glacier ou excluir os arquivos de log depois de um determinado período.

> **Note**
>
> A configuração do ciclo de vida em buckets habilitados para autenticação multifator (MFA) não é suportada.

Limitar o acesso à AWSCloudTrail_FullAccess política

Os usuários com a AWSCloudTrail_FullAccesspolítica podem desativar ou reconfigurar as funções de auditoria mais confidenciais e importantes em suas AWS contas. Essa política não se destina a ser compartilhada ou aplicada amplamente às identidades do IAM em sua AWS conta. Limite a aplicação dessa política ao menor número possível de pessoas, aquelas que você espera que atuem como administradores AWS da conta.

Criptografando arquivos de CloudTrail log com AWS KMS chaves (SSE-KMS)

Por padrão, os arquivos de log entregues CloudTrail ao seu bucket são criptografados usando criptografia do lado do servidor com uma chave KMS (SSE-KMS). Se você não habilitar a criptografia SSE-KMS, seus registros serão criptografados usando a criptografia SSE-S3.

> **Note**
>
> A ativação da criptografia no servidor criptografa os arquivos de log com o SSE-KMS, mas não os arquivos de compilação. Os arquivos de compilação são criptografados com chaves de criptografia gerenciadas pelo Amazon S3 (SSE-S3).
> Se você estiver usando um bucket S3 existente com uma chave de bucket S3, CloudTrail deverá ter permissão na política de chaves para usar as AWS KMS ações e. `GenerateDataKey` `DescribeKey` Se o `cloudtrail.amazonaws.com` não tiver essas permissões na política de chave, não será possível criar ou atualizar trilhas.

Para usar o SSE-KMS com CloudTrail, você cria e gerencia uma chave KMS, também conhecida como. AWS KMS key Você anexa uma política à chave que determina quais usuários podem usar a chave para criptografar e CloudTrail descriptografar arquivos de log. A descriptografia é facilitada pelo S3. Quando os usuários autorizados da chave leem os arquivos de CloudTrail log, o S3 gerencia a descriptografia e os usuários autorizados podem ler os arquivos de log em formato não criptografado.

Essa abordagem tem as seguintes vantagens:

- É possível criar e gerenciar você mesmo as chaves de criptografia KMS.
- É possível usar uma única chave do KMS para criptografar e descriptografar os arquivos de log de várias contas em todas as regiões.
- Você tem controle sobre quem pode usar sua chave para criptografar e CloudTrail descriptografar arquivos de log. Você pode atribuir permissões para a chave aos usuários na sua organização de acordo com os seus requisitos.
- Você tem segurança aprimorada. Com esse recurso, para ler arquivos de log, as seguintes permissões são necessárias:
  - Um usuário deve ter permissões de leitura do S3 para o bucket que contém os arquivos de log.
  - Um usuário também deve ter uma política ou função aplicada com permissões de descriptografia pela política da chave do KMS.
- Como o S3 descriptografa automaticamente os arquivos de log para solicitações de usuários autorizados a usar a chave KMS, a criptografia SSE-KMS para arquivos de log é compatível com versões anteriores de aplicativos que lêem dados de CloudTrail log. CloudTrail

> **Note**
>
> A chave KMS que você escolher deve ser criada na mesma AWS região do bucket do Amazon S3 que recebe seus arquivos de log. Por exemplo, se os arquivos de log serão armazenados em um bucket na região Leste dos EUA (Ohio), você deverá criar ou escolher uma chave do KMS que foi criada nessa região. Para verificar a região de um bucket do Amazon S3, inspecione as respectivas propriedades no console do Amazon S3.

Ativar a criptografia dos arquivos de log

> **Note**
>
> Se você criar uma chave KMS no CloudTrail console, CloudTrail adicionará as seções de política de chaves KMS necessárias para você. Siga esses procedimentos se você criou uma chave no console do IAM ou AWS CLI precisa adicionar manualmente as seções de política necessárias.

Para habilitar a criptografia SSE-KMS para arquivos de CloudTrail log, execute as seguintes etapas de alto nível:

1. Crie uma chave do KMS.

   - Para obter informações sobre como criar uma chave KMS com o AWS Management Console, consulte Criação de chaves no Guia do AWS Key Management Service desenvolvedor.
   - Para obter informações sobre como criar uma chave KMS com o AWS CLI, consulte create-key.

   > **Note**
   >
   > A chave do KMS escolhida deve estar na mesma região que o bucket do S3 que recebe seus arquivos de log. Para verificar a região de um bucket do S3, inspecione as propriedades do bucket no console do S3.

2. Adicione seções de política à chave que permitem CloudTrail criptografar e que os usuários descriptografem arquivos de log.

- Para obter informações sobre o que incluir na política, consulte Configure as AWS KMS principais políticas para CloudTrail.

  > **Warning**
  >
  > Inclua permissões de descriptografia na política de todos os usuários que precisam ler arquivos de log. Se não executar essa etapa antes de adicionar a chave à configuração da trilha, os usuários que não tiverem permissão de descriptografia não conseguirão ler arquivos criptografados até que essas permissões sejam concedidas para eles.

- Para obter informações sobre como editar uma política com o console do IAM, consulte Como editar uma política de chaves no Guia do desenvolvedor do AWS Key Management Service .
- Para obter informações sobre como anexar uma política a uma chave KMS com AWS CLI o. put-key-policy

3. Atualize sua trilha para usar a chave KMS cuja política você modificou. CloudTrail

   - Para atualizar a configuração da trilha usando o CloudTrail console, consulteAtualizar um recurso para usar sua chave do KMS.
   - Para atualizar a configuração da trilha usando o AWS CLI, consulteAtivando e desativando a criptografia do arquivo de CloudTrail log com o AWS CLI.

CloudTrail também oferece suporte a chaves AWS KMS multirregionais. Para obter mais informações sobre chaves de várias regiões, consulte Usar chaves de várias regiões no Manual do desenvolvedor do AWS Key Management Service .

A próxima seção descreve as seções de política que sua política de chaves do KMS exige para uso com CloudTrail.

Conceder permissões para criar uma chave do KMS

Você pode conceder permissão aos usuários para criar uma AWS KMS key com a `AWSKeyManagementServicePowerUser` política.

Para conceder permissão para criar uma chave do KMS

1. Abra o console IAM em https://console.aws.amazon.com/iam/.

2. Escolha o grupo ou usuário ao qual você deseja conceder permissão.
3. Escolha Permissions (Permissões) e escolha Attach Policy (Anexar política).
4. Procure por AWSKeyManagementServicePowerUser, escolha a política e, em seguida, Attach Policy (Anexar política).

   Agora, o usuário tem permissão para criar uma chave do KMS. Para obter mais informações sobre a criação de políticas, consulte Como criar políticas do IAM no Guia do usuário do IAM.

Configure as AWS KMS principais políticas para CloudTrail

Você pode criar um AWS KMS key de três maneiras:

- O CloudTrail console
- O console AWS de gerenciamento
- O AWS CLI

> **Note**
>
> Se você criar uma chave KMS no CloudTrail console, CloudTrail adicionará a política de chaves KMS necessária para você. Você não precisa adicionar manualmente as declarações de política. Consulte Política de chave KMS padrão criada no console CloudTrail .

Se você criar uma chave KMS no AWS Gerenciamento ou no AWS CLI, deverá adicionar seções de política à chave para poder usá-la com CloudTrail. A política deve permitir CloudTrail o uso da chave para criptografar seus arquivos de log e armazenamentos de dados de eventos e permitir que os usuários que você especificar leiam arquivos de log em formato não criptografado.

Consulte os recursos a seguir:

- Para criar uma chave KMS com o AWS CLI, consulte create-key.
- Para editar uma política de chaves do KMS para CloudTrail, consulte Editando uma política de chaves no Guia do AWS Key Management Service desenvolvedor.
- Para obter detalhes técnicos sobre como CloudTrail usar AWS KMS, consulte Como AWS CloudTrail usar AWS KMS no Guia do AWS Key Management Service desenvolvedor.

Seções de política de chaves do KMS obrigatórias para uso com CloudTrail

Se você criou uma chave KMS com o console AWS de gerenciamento ou com o AWS CLI, você deve, no mínimo, adicionar as seguintes instruções à sua política de chaves KMS para que ela funcione. CloudTrail

Tópicos

Elementos obrigatórios de política de chaves do KMS para trilhas

1. Ative as permissões de criptografia de CloudTrail registros. Consulte Conceder permissões de criptografia.
2. Ative as permissões de descriptografia de CloudTrail registros. Consulte Conceder permissões de descriptografia. Se você estiver usando um bucket do S3 existente com uma chave de bucket do S3, permissões de `kms:Decrypt` serão necessárias para criar ou atualizar uma trilha com criptografia SSE-KMS habilitada.
3. Habilite CloudTrail a descrição das propriedades da chave KMS. Consulte Habilitar CloudTrail a descrição das propriedades da chave KMS.

Como uma prática recomendada de segurança, adicione uma `aws:SourceArn` chave de condição para a política de chaves KMS. A chave de condição global do IAM `aws:SourceArn` ajuda a garantir que a chave KMS seja CloudTrail usada somente para uma trilha ou trilhas específicas. O valor de `aws:SourceArn` é sempre o ARN de trilha (ou matriz de ARNs de trilha) que está usando a chave KMS. Certifique-se de adicionar a `aws:SourceArn` chave de condição para políticas de chave KMS para trilhas existentes.

A `aws:SourceAccount` chave de condição também é compatível, mas não é recomendada. O valor de `aws:SourceAccount` é a ID da conta do proprietário da trilha, ou para trilhas da organização, a ID da conta de gerenciamento.

> **Important**
>
> Quando você adicionar as novas seções à política de chave do KMS, não altere as seções existentes na política.

Se a criptografia estiver ativada em uma trilha e a chave KMS estiver desativada ou se a política de chaves KMS não estiver configurada corretamente CloudTrail, não será CloudTrail possível fornecer registros.

Elementos obrigatórios de política de chaves do KMS para armazenamentos de dados de eventos

1. Ative as permissões de criptografia de CloudTrail registros. Consulte Conceder permissões de criptografia.
2. Ative as permissões de descriptografia de CloudTrail registros. Consulte Conceder permissões de descriptografia.
3. Concede aos usuários e perfis permissão para criptografar e descriptografar dados do arquivamento de dados de eventos com a chave do KMS.

   Ao criar um armazenamento de dados de eventos e criptografá-lo com uma chave do KMS ou executar consultas em um armazenamento de dados de eventos que você está criptografando com uma chave do KMS, é necessário ter acesso de gravação à chave do KMS. A política de chaves KMS deve ter acesso a CloudTrail, e a chave KMS deve ser gerenciável por usuários que executam operações (como consultas) no armazenamento de dados do evento.
4. Habilite CloudTrail a descrição das propriedades da chave KMS. Consulte Habilitar CloudTrail a descrição das propriedades da chave KMS.

As chaves de condição `aws:SourceArn` e `aws:SourceAccount` não são compatíveis com políticas de chaves do KMS para armazenamentos de dados de eventos.

Important

Quando você adicionar as novas seções à política de chave do KMS, não altere as seções existentes na política.
Se a criptografia estiver ativada em um armazenamento de dados de eventos e a chave KMS estiver desativada ou excluída, ou se a política de chaves KMS não estiver configurada corretamente CloudTrail, não será CloudTrail possível entregar eventos ao seu armazenamento de dados de eventos.

Conceder permissões de criptografia

Example CloudTrail Permitir criptografar registros em nome de contas específicas

CloudTrail precisa de permissão explícita para usar a chave KMS para criptografar registros em nome de contas específicas. Para especificar uma conta, adicione a seguinte instrução necessária à sua política de chaves do KMS e substitua *account-id*, *region* e *trailName* pelos valores apropriados para sua configuração. Você pode adicionar IDs de conta adicionais à `EncryptionContext` seção para permitir que essas contas sejam usadas CloudTrail para usar sua chave KMS para criptografar arquivos de log.

Como uma prática recomendada de segurança, adicione uma chave de condição `aws:SourceArn` à política de chaves do KMS para uma trilha. A chave de condição global do IAM `aws:SourceArn` ajuda a garantir que a chave KMS seja CloudTrail usada somente para uma trilha ou trilhas específicas.

```
{
   "Sid": "Allow CloudTrail to encrypt logs",
   "Effect": "Allow",
   "Principal": {
       "Service": "cloudtrail.amazonaws.com"
    },
    "Action": "kms:GenerateDataKey*",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:SourceArn": "arn:aws:cloudtrail:region:account-id:trail/trail-name"
         },
         "StringLike": {
             "kms:EncryptionContext:aws:cloudtrail:arn": "arn:aws:cloudtrail:*:account-
id:trail/*"
         }
    }
}
```

Uma política para uma chave KMS usada para criptografar os registros do armazenamento de dados de eventos do CloudTrail Lake não pode usar as chaves `aws:SourceArn` de condição ou. `aws:SourceAccount` Veja a seguir um exemplo de uma política de chaves do KMS para um armazenamento de dados de eventos.

```
{
```

```
    "Sid": "Allow CloudTrail to encrypt event data store",
    "Effect": "Allow",
    "Principal": {
        "Service": "cloudtrail.amazonaws.com"
     },
     "Action": [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource": "*"
}
```

Example

O exemplo de declaração de política a seguir ilustra como outra conta pode usar sua chave KMS para CloudTrail criptografar registros.

Cenário

- Sua chave do KMS está na conta *111111111111*.
- Tanto você quanto a conta *222222222222* criptografarão logs.

Na política, você adiciona uma ou mais contas criptografadas com sua chave ao CloudTrail EncryptionContext. Isso se restringe CloudTrail ao uso de sua chave para criptografar registros somente para as contas que você especificar. Quando você concede permissão *222222222222* à raiz da conta para criptografar logs, ela delega permissão ao administrador da conta para criptografar as permissões necessárias para outros usuários dessa conta. O administrador da conta faz isso alterando as políticas associadas a esses usuários do IAM.

Como uma prática recomendada de segurança, adicione uma `aws:SourceArn` chave de condição para a política de chaves KMS. A chave de condição global do IAM `aws:SourceArn` ajuda a garantir que a chave KMS seja CloudTrail usada somente para as trilhas especificadas. Não há suporte para essa condição nas políticas de chaves do KMS para armazenamentos de dados de eventos.

Declaração de política de chaves do KMS:

```
{
  "Sid": "Enable CloudTrail encrypt permissions",
  "Effect": "Allow",
  "Principal": {
```

```
    "Service": "cloudtrail.amazonaws.com"
  },
  "Action": "kms:GenerateDataKey*",
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:EncryptionContext:aws:cloudtrail:arn": [
        "arn:aws:cloudtrail:*:111111111111:trail/*",
        "arn:aws:cloudtrail:*:222222222222:trail/*"
      ]
    },
    "StringEquals": {
        "aws:SourceArn": "arn:aws:cloudtrail:region:account-id:trail/trail-name"
    }
  }
}
```

Para obter mais informações sobre a edição de uma política de chaves do KMS para uso com CloudTrail, consulte Editando uma política de chaves no Guia do AWS Key Management Service desenvolvedor.

Conceder permissões de descriptografia

Antes de adicionar sua chave KMS à sua CloudTrail configuração, é importante conceder permissões de descriptografia a todos os usuários que precisarem delas. Os usuários que têm permissões de criptografia, mas não têm permissões de descriptografia, não conseguirão ler logs criptografados. Se você estiver usando um bucket do S3 existente com uma chave de bucket do S3, permissões de `kms:Decrypt` serão necessárias para criar ou atualizar uma trilha com criptografia SSE-KMS habilitada.

Ativar CloudTrail permissões de descriptografia de registros

Os usuários da sua chave devem receber permissões explícitas para ler os arquivos de log que CloudTrail foram criptografados. Para permitir que os usuários leiam logs criptografados, adicione a seguinte declaração necessária à sua política de chave do KMS, modificando a seção `Principal` de modo a adicionar uma linha para cada entidade principal que deseja descriptografar usando sua chave do KMS.

```
{
  "Sid": "Enable CloudTrail log decrypt permissions",
  "Effect": "Allow",
```

```
  "Principal": {
    "AWS": "arn:aws:iam::account-id:user/username"
  },
  "Action": "kms:Decrypt",
  "Resource": "*",
  "Condition": {
    "Null": {
      "kms:EncryptionContext:aws:cloudtrail:arn": "false"
    }
  }
}
```

Veja a seguir um exemplo de política necessária para permitir que o responsável pelo CloudTrail serviço decifre os registros de trilhas.

```
{
      "Sid": "Allow CloudTrail to decrypt a trail",
      "Effect": "Allow",
      "Principal": {
          "Service": "cloudtrail.amazonaws.com"
        },
      "Action": "kms:Decrypt",
      "Resource": "*"
}
```

Uma política de descriptografia para uma chave KMS usada com um armazenamento de dados de eventos do CloudTrail Lake é semelhante à seguinte. Os ARNs de usuário ou perfil especificados como valores para `Principal` precisam de permissões de descriptografia para criar ou atualizar armazenamentos de dados de eventos, executar consultas ou obter resultados de consultas.

```
{
      "Sid": "Enable user key permissions for event data stores"
      "Effect": "Allow",
      "Principal": {
          "AWS": "arn:aws:iam::account-id:user/username"
      },
      "Action": [
          "kms:Decrypt",
          "kms:GenerateDataKey"
      ],
      "Resource": "*"
  }
```

Veja a seguir um exemplo de política necessária para permitir que o responsável pelo CloudTrail serviço decifre os registros do armazenamento de dados de eventos.

```
{
      "Sid": "Allow CloudTrail to decrypt an event data store",
      "Effect": "Allow",
      "Principal": {
          "Service": "cloudtrail.amazonaws.com"
        },
      "Action": "kms:Decrypt",
      "Resource": "*"
}
```

Permitir que usuários em sua conta descriptografem logs de trilha com sua chave do KMS

Exemplo

Esta instrução da política ilustra como permitir que um usuário ou perfil na sua conta use sua chave para ler os logs criptografados no bucket do S3 da conta.

Example Cenário

- Sua chave do KMS, o bucket do S3 e o usuário do IAM Bob estão na conta *111111111111*.
- Você dá permissão ao usuário do IAM Bob para descriptografar CloudTrail registros no bucket do S3.

Na política de chaves, você ativa as permissões de descriptografia de CloudTrail log para o usuário do IAM Bob.

Declaração de política de chaves do KMS:

```
{
  "Sid": "Enable CloudTrail log decrypt permissions",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111111111111:user/Bob"
  },
  "Action": "kms:Decrypt",
  "Resource": "arn:aws:kms:region:account-id:key/key-id",
  "Condition": {
    "Null": {
      "kms:EncryptionContext:aws:cloudtrail:arn": "false"
```

```
    }
  }
}
```

Permitir que usuários em outras contas descriptografem logs de trilha com sua chave do KMS

Você pode permitir que os usuários em outras contas usem sua chave do KMS para descriptografar logs de trilhas, mas não logs de armazenamentos de dados de eventos. As alterações necessárias à sua política de chaves dependem de onde o bucket do S3 está, na sua conta ou em outra.

Permitir que os usuários de um bucket de outra conta descriptografem os logs

Exemplo

Esta declaração da política ilustra como permitir que um usuário ou função do IAM em outra conta use sua chave para ler os logs criptografados a partir de um bucket do S3 na outra conta.

Cenário

- Sua chave do KMS está na conta *111111111111*.
- O usuário do IAM Alice e o bucket do S3 estão na conta *222222222222*.

Nesse caso, você dá CloudTrail permissão para descriptografar registros na conta *222222222222* e dá permissão à política de usuário do IAM de Alice para usar sua chave*KeyA*, que está na conta. *111111111111*

Declaração de política de chaves do KMS:

```
{
  "Sid": "Enable encrypted CloudTrail log read access",
  "Effect": "Allow",
  "Principal": {
    "AWS": [
      "arn:aws:iam::222222222222:root"
    ]
  },
  "Action": "kms:Decrypt",
  "Resource": "arn:aws:kms:region:account-id:key/key-id",
  "Condition": {
    "Null": {
      "kms:EncryptionContext:aws:cloudtrail:arn": "false"
    }
```

```
  }
}
```

Declaração da política de usuários do IAM de Alice:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "kms:Decrypt",
      "Resource": "arn:aws:kms:us-west-2:111111111111:key/KeyA"
    }
  ]
}
```

Permitir que usuários em outra conta descriptografem os logs de trilha do seu bucket

Example

Esta política ilustra como outra conta pode usar sua chave para ler os logs criptografados do bucket do S3.

Example Cenário

- Sua chave do KMS e o bucket do S3 estão na conta *111111111111*.
- O usuário que lê os logs do seu bucket está na conta *222222222222*.

Para ativar esse cenário, você ativa as permissões de descriptografia para a função do IAM CloudTrailReadRoleem sua conta e, em seguida, concede à outra conta permissão para assumir essa função.

Declaração de política de chaves do KMS:

```
{
  "Sid": "Enable encrypted CloudTrail log read access",
  "Effect": "Allow",
  "Principal": {
    "AWS": [
      "arn:aws:iam::11111111111:role/CloudTrailReadRole"
    ]
```

```
  },
  "Action": "kms:Decrypt",
  "Resource": "arn:aws:kms:region:account-id:key/key-id",
  "Condition": {
    "Null": {
      "kms:EncryptionContext:aws:cloudtrail:arn": "false"
    }
  }
}
```

CloudTrailReadRoledeclaração de política de entidade fiduciária:

```
{
 "Version": "2012-10-17",
 "Statement": [
   {
     "Sid": "Allow CloudTrail access",
     "Effect": "Allow",
     "Principal": {
       "AWS": "arn:aws:iam::222222222222:root"
     },
     "Action": "sts:AssumeRole"
   }
 ]
}
```

Para obter informações sobre a edição de uma política de chaves do KMS para uso com CloudTrail, consulte Editando uma política de chaves no Guia do AWS Key Management Service desenvolvedor.

Habilitar CloudTrail a descrição das propriedades da chave KMS

CloudTrail requer a capacidade de descrever as propriedades da chave KMS. Para habilitar essa funcionalidade, adicione a seguinte declaração obrigatória da forma em que se encontra à sua política de chave do KMS. Essa declaração não concede CloudTrail nenhuma permissão além das outras permissões que você especificar.

Como uma prática recomendada de segurança, adicione uma `aws:SourceArn` chave de condição para a política de chaves KMS. A chave de condição global do IAM `aws:SourceArn` ajuda a garantir que a chave KMS seja CloudTrail usada somente para uma trilha ou trilhas específicas.

```
{
  "Sid": "Allow CloudTrail access",
```

```
  "Effect": "Allow",
  "Principal": {
    "Service": "cloudtrail.amazonaws.com"
  },
  "Action": "kms:DescribeKey",
  "Resource": "arn:aws:kms:region:account-id:key/key-id",
  "Condition": {
    "StringEquals": {
        "aws:SourceArn": "arn:aws:cloudtrail:region:account-id:trail/trail-name"
    }
  }
}
```

Para obter informações sobre como editar políticas de chaves do KMS, consulte Como editar uma política de chaves no Guia do desenvolvedor do AWS Key Management Service .

Política de chave KMS padrão criada no console CloudTrail

Se você criar uma AWS KMS key no CloudTrail console, as políticas a seguir serão criadas automaticamente para você. A política permite estas permissões:

- Permite permissões Conta da AWS (raiz) para a chave KMS.
- Permite CloudTrail criptografar arquivos de log sob a chave KMS e descrever a chave KMS.
- Permite que todos os usuários das contas especificadas descriptografem os arquivos de log.
- Permite que todos os usuários da conta especificada criem um alias do KMS para a chave do KMS.
- Habilita a descriptografia de log entre contas para o ID da conta que criou a trilha.

Tópicos

- Política de chaves KMS padrão para armazenamentos de dados de eventos em CloudTrail Lake
- Política padrão de chaves do KMS para trilhas

Política de chaves KMS padrão para armazenamentos de dados de eventos em CloudTrail Lake

A seguir está a política padrão criada para uma AWS KMS key que você usa com um armazenamento de dados de eventos no CloudTrail Lake.

```
{
```

```
      "Version": "2012-10-17",
      "Id": "Key policy created by CloudTrail",
      "Statement": [
        {
          "Sid": "The key created by CloudTrail to encrypt event data stores. Created
${new Date().toUTCString()}",
          "Effect": "Allow",
          "Principal": {
            "Service": "cloudtrail.amazonaws.com"
          },
          "Action": [
            "kms:GenerateDataKey",
            "kms:Decrypt"
          ],
          "Resource": "*"
        },
        {
          "Sid": "Enable IAM user permissions",
          "Effect": "Allow",
          "Principal": {
            "AWS": "arn:aws:iam::account-id:root"
          },
          "Action": "kms:*",
          "Resource": "*"
        },
        {
          "Sid": "Enable user to have permissions",
          "Effect": "Allow",
          "Principal": {
            "AWS" : "arn:aws:sts::account-id:role-arn"
          },
          "Action": [
            "kms:Decrypt",
            "kms:GenerateDataKey"
           ],
          "Resource": "*"
        }
      ]
    }
```

Política padrão de chaves do KMS para trilhas

A seguir está a política padrão criada para uma AWS KMS key que você usa com uma trilha.

> **Note**
>
> A política inclui uma declaração para permitir que contas cruzadas descriptografem arquivos de log com a chave do KMS.

```
{
    "Version": "2012-10-17",
    "Id": "Key policy created by CloudTrail",
    "Statement": [
        {
            "Sid": "Enable IAM user permissions",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::account-id:root",
                    "arn:aws:iam::account-id:user/username"
                ]
            },
            "Action": "kms:*",
            "Resource": "*"
        },
        {
            "Sid": "Allow CloudTrail to encrypt logs",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
             },
            "Action": "kms:GenerateDataKey*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn": "arn:aws:cloudtrail:region:account-id:trail/trail-
name"
                },
                "StringLike": {
                    "kms:EncryptionContext:aws:cloudtrail:arn":
 "arn:aws:cloudtrail:*:account-id:trail/*"
                }
            }
        },
        {
```

```
            "Sid": "Allow CloudTrail to describe key",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
             },
            "Action": "kms:DescribeKey",
            "Resource": "*"
        },
        {
            "Sid": "Allow principals in the account to decrypt log files",
            "Effect": "Allow",
            "Principal": {
                "AWS": "*"
             },
            "Action": [
                "kms:Decrypt",
                "kms:ReEncryptFrom"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:CallerAccount": "account-id"
                },
                "StringLike": {
                    "kms:EncryptionContext:aws:cloudtrail:arn":
"arn:aws:cloudtrail:*:account-id:trail/*"
                }
            }
        },
        {
            "Sid": "Allow alias creation during setup",
            "Effect": "Allow",
            "Principal": {
                "AWS": "*"
             },
            "Action": "kms:CreateAlias",
            "Resource": "arn:aws:kms:region:account-id:key/key-id",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "ec2.region.amazonaws.com",
                    "kms:CallerAccount": "account-id"
                }
            }
        },
```

```
        {
            "Sid": "Enable cross account log decryption",
            "Effect": "Allow",
            "Principal": {
                "AWS": "*"
            },
            "Action": [
                "kms:Decrypt",
                "kms:ReEncryptFrom"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:CallerAccount": "account-id"
                },
                "StringLike": {
                    "kms:EncryptionContext:aws:cloudtrail:arn":
 "arn:aws:cloudtrail:*:account-id:trail/*"
                }
            }
        }
    ]
}
```

Atualizar um recurso para usar sua chave do KMS

No AWS CloudTrail console, atualize uma trilha ou um armazenamento de dados de eventos para usar uma AWS Key Management Service chave. Esteja ciente de que usar sua própria chave KMS gera AWS KMS custos de criptografia e decodificação. Para obter mais informações, consulte Preços do AWS Key Management Service.

Tópicos

- Atualizar uma trilha para usar uma chave do KMS
- Atualizar um armazenamento de dados de eventos para usar uma chave do KMS

Atualizar uma trilha para usar uma chave do KMS

Para atualizar uma trilha para usar a AWS KMS key que você modificou CloudTrail, conclua as etapas a seguir no CloudTrail console.

> **Note**
>
> A atuação de uma trilha com o procedimento a seguir criptografa os arquivos de log com o SSE-KMS, mas não os arquivos de compilação. Os arquivos de compilação são criptografados com chaves de criptografia gerenciadas pelo Amazon S3 (SSE-S3).
> Se você estiver usando um bucket do S3 existente com uma chave do bucket do S3, CloudTrail deverá ter permissão na política de chaves para usar as AWS KMS ações e. `GenerateDataKey` `DescribeKey` Se o `cloudtrail.amazonaws.com` não tiver essas permissões na política de chave, não será possível criar ou atualizar trilhas.

Para atualizar uma trilha usando o AWS CLI, consulteAtivando e desativando a criptografia do arquivo de CloudTrail log com o AWS CLI.

Para atualizar uma trilha para usar sua chave do KMS

1. Faça login no AWS Management Console e abra o CloudTrail console em https://console.aws.amazon.com/cloudtrail/.
2. Escolha Trails (Trilhas) e depois escolha um nome para a trilha.
3. Em General details (Detalhes gerais), escolha Edit (Editar).
4. Em Log file SSE-KMS encryption (Criptografia de arquivo de log com SSE-KMS), escolha Enabled (Habilitado) se quiser criptografar os arquivos de log com criptografia SSE-KMS em vez de criptografia SSE-S3. O padrão é Enabled (Habilitado). Se você não habilitar a criptografia SSE-SKMS, seus registros serão criptografados usando a criptografia SSE-S3. Para obter mais informações sobre a criptografia SSE-KMS, consulte Usando a criptografia do lado do servidor com (SSE-KMS). AWS Key Management Service Para obter mais informações sobre a criptografia SSE-S3, consulte Using Server-Side Encryption with Amazon S3-Managed Encryption Keys (SSE-S3) (Uso de criptografia no lado do servidor com chaves de criptografia gerenciadas pelo Amazon S3 [SSE-S3]).

   Selecione Existing (Existente) para atualizar a trilha com a AWS KMS key. Escolha uma chave do KMS que esteja na mesma região que o bucket do S3 que recebe seus arquivos de log. Para verificar a região de um bucket do S3, examine as respectivas propriedades no console do S3.

> **Note**
>
> Você também pode digitar o Nome de região da Amazon (ARN) de uma chave de outra conta. Para ter mais informações, consulte Atualizar um recurso para usar sua chave do KMS. A política de chaves deve permitir CloudTrail o uso da chave para criptografar seus arquivos de log e permitir que os usuários que você especificar leiam os arquivos de log em formato não criptografado. Para obter informações sobre como editar manualmente a política de chaves, consulte Configure as AWS KMS principais políticas para CloudTrail.

Em AWS KMS Alias, especifique o alias para o qual você alterou a política para uso CloudTrail, no formato. `alias/` *`MyAliasName`* Para ter mais informações, consulte Atualizar um recurso para usar sua chave do KMS.

Você pode digitar o nome do alias, o Nome de região da Amazon (ARN) ou o ID de chave globalmente exclusivo. Se a chave do KMS pertence a outra conta, verifique se a política de chaves tem permissões que possibilitam o seu uso. O valor pode ser um dos seguintes formatos:

- Nome do alias: `alias/`*`MyAliasName`*
- Nome de região da Amazon (ARN) do alias: `arn:aws:kms:`*`region`*`:123456789012:alias/`*`MyAliasName`*
- Nome de região da Amazon (ARN) do alias da chave: `arn:aws:kms:`*`region`*`:123456789012:key/12345678-1234-1234-1234-123456789012`
- ID de chave globalmente exclusivo: `12345678-1234-1234-1234-123456789012`

5. Escolha Update Trail (Atualizar trilha).

> **Note**
>
> Se a chave do KMS que você escolheu estiver desabilitada ou se a exclusão estiver pendente, você não poderá salvar a trilha com essa chave do KMS. É possível habilitar a chave do KMS ou escolher outra. Para obter mais informações, consulte Estado da chave: efeito na chave do KMS no Guia do desenvolvedor do AWS Key Management Service .

Atualizar um armazenamento de dados de eventos para usar uma chave do KMS

Para atualizar um armazenamento de dados de eventos para usar o AWS KMS key que você modificou CloudTrail, conclua as etapas a seguir no CloudTrail console.

Para atualizar um armazenamento de dados de eventos usando o AWS CLI, consulteAtualize um armazenamento de dados de eventos com o AWS CLI.

> **Important**
>
> Desabilitar ou excluir a chave KMS, ou remover CloudTrail permissões na chave, CloudTrail impede a ingestão de eventos no armazenamento de dados de eventos e impede que os usuários consultem dados no armazenamento de dados de eventos que foram criptografados com a chave. Após associar um armazenamento de dados de eventos a uma chave do KMS, não será possível remover ou alterar a chave do KMS. Antes de desativar ou excluir uma chave do KMS que você esteja usando com um armazenamento de dados de eventos, exclua ou faça backup do seu armazenamento de dados de eventos.

Para atualizar um armazenamento de dados de eventos para usar sua chave do KMS

1. Faça login no AWS Management Console e abra o CloudTrail console em https://console.aws.amazon.com/cloudtrail/.
2. No painel de navegação, escolha Event data stores (Armazenamentos de dados de eventos) em Lake. Escolha um armazenamento de dados de eventos para atualizar.
3. Em General details (Detalhes gerais), escolha Edit (Editar).
4. Se essa opção ainda não estiver habilitada para Criptografia, escolha Usar minha própria AWS KMS key para criptografar seus arquivos de log com sua própria chave do KMS.

   Escolha Existing (Existente) para atualizar seu armazenamento de dados de eventos com sua chave do KMS. Escolha uma chave do KMS que esteja na mesma região do armazenamento de dados de eventos. Não há compatibilidade com uma chave de outra conta.

   Em Inserir AWS KMS Alias, especifique o alias para o qual você alterou a política para uso CloudTrail, no formato. `alias/` *`MyAliasName`* Para ter mais informações, consulte Atualizar um recurso para usar sua chave do KMS.

   Você pode escolher um alias ou usar o ID de chave global exclusivo. O valor pode ser um dos seguintes formatos:

- Nome do alias: `alias/MyAliasName`
- Nome de região da Amazon (ARN) do alias: `arn:aws:kms:region:123456789012:alias/MyAliasName`
- Nome de região da Amazon (ARN) do alias da chave: `arn:aws:kms:region:123456789012:key/12345678-1234-1234-1234-123456789012`
- ID de chave globalmente exclusivo: `12345678-1234-1234-1234-123456789012`

5. Escolha Salvar alterações.

> **Note**
>
> Se a chave do KMS que você escolheu estiver desabilitada ou com exclusão pendente, não será possível salvar a configuração de armazenamento de dados de eventos com essa chave do KMS. É possível habilitar a chave do KMS ou escolher outra chave. Para obter mais informações, consulte Estado da chave: efeito na chave do KMS no Guia do desenvolvedor do AWS Key Management Service .

Ativando e desativando a criptografia do arquivo de CloudTrail log com o AWS CLI

Este tópico descreve como ativar e desativar a criptografia do arquivo de log SSE-KMS usando CloudTrail o. AWS CLI Para obter informações básicas, consulte Criptografando arquivos de CloudTrail log com AWS KMS chaves (SSE-KMS).

Tópicos

- Ativando a criptografia do arquivo de CloudTrail log usando o AWS CLI
- Desabilitando a criptografia do arquivo de CloudTrail log usando o AWS CLI

Ativando a criptografia do arquivo de CloudTrail log usando o AWS CLI

- Habilitar a criptografia de arquivo de log para uma trilha
- Habilitar a criptografia de arquivo de log para um armazenamento de dados de eventos

Habilitar a criptografia de arquivo de log para uma trilha

1. Crie uma chave com a AWS CLI. A chave que você cria deve estar na mesma região do bucket do S3 que recebe seus arquivos de CloudTrail log. Para esta etapa, você usa o AWS KMS create-keycomando.
2. Obtenha a política de chaves existente para que você possa modificá-la para uso com CloudTrail. Você pode recuperar a política de chaves com o AWS KMS get-key-policycomando.
3. Adicione as seções necessárias à política de chaves para que ela CloudTrail possa criptografar e os usuários possam descriptografar seus arquivos de log. Garanta que todos os usuários que lerão os arquivos de log tenham recebido permissões de descriptografia. Não modifique as seções existentes da política. Para obter mais informações sobre as seções da política que devem ser incluídas, consulte Configure as AWS KMS principais políticas para CloudTrail.
4. Anexe o arquivo de política JSON modificado à chave usando o AWS KMS put-key-policycomando.
5. Execute o `update-trail` comando CloudTrail `create-trail` or com o `--kms-key-id` parâmetro. Esse comando habilitará a criptografia de log.

   ```
   aws cloudtrail update-trail --name Default --kms-key-id alias/MyKmsKey
   ```

   O `--kms-key-id` parâmetro especifica a chave cuja política você modificou. CloudTrail Ele pode estar em qualquer um dos seguintes formatos:

   - Nome do alias. Exemplo: `alias/MyAliasName`
   - Nome de região da Amazon (ARN) do alias. Exemplo: `arn:aws:kms:us-east-2:123456789012:alias/MyAliasName`
   - Nome de região da Amazon (ARN) da chave. Exemplo: `arn:aws:kms:us-east-2:123456789012:key/12345678-1234-1234-1234-123456789012`
   - ID de chave globalmente exclusivo. Exemplo: `12345678-1234-1234-1234-123456789012`

   Esta é uma resposta de exemplo:

   ```
   {
       "IncludeGlobalServiceEvents": true,
       "Name": "Default",
       "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/Default",
   ```

```
    "LogFileValidationEnabled": false,
    "KmsKeyId": "arn:aws:kms:us-
east-2:123456789012:key/12345678-1234-1234-1234-123456789012",
    "S3BucketName": "my-bucket-name"
}
```

A presença do elemento `KmsKeyId` indica que a criptografia do arquivo de log foi ativada. Os arquivos criptografados de log devem aparecer no seu bucket em aproximadamente 5 minutos.

Habilitar a criptografia de arquivo de log para um armazenamento de dados de eventos

1. Crie uma chave com a AWS CLI. A chave que você cria precisa estar na mesma região do armazenamento de dados de eventos. Para essa etapa, execute o AWS KMS create-keycomando.
2. Obtenha a política de chaves existente para edição e uso com CloudTrail. Você pode obter a política de chaves executando o AWS KMS get-key-policycomando.
3. Adicione as seções necessárias à política de chaves para que ela CloudTrail possa criptografar e os usuários possam descriptografar seus arquivos de log. Garanta que todos os usuários que lerão os arquivos de log tenham recebido permissões de descriptografia. Não modifique as seções existentes da política. Para obter mais informações sobre as seções da política que devem ser incluídas, consulte Configure as AWS KMS principais políticas para CloudTrail.
4. Anexe o arquivo de política JSON editado à chave executando o AWS KMS put-key-policycomando.
5. Execute o `update-event-data-store` comando CloudTrail `create-event-data-store` or e adicione o `--kms-key-id` parâmetro. Esse comando habilitará a criptografia de log.

```
aws cloudtrail update-event-data-store --name my-event-data-store --kms-key-id
 alias/MyKmsKey
```

O `--kms-key-id` parâmetro especifica a chave cuja política você modificou. CloudTrail Ele pode estar em qualquer um dos seguintes quatro formatos:

- Nome do alias. Exemplo: `alias/MyAliasName`
- Nome de região da Amazon (ARN) do alias. Exemplo: `arn:aws:kms:us-east-2:123456789012:alias/MyAliasName`

- Nome de região da Amazon (ARN) da chave. Exemplo: `arn:aws:kms:us-east-1:123456789012:key/12345678-1234-1234-1234-123456789012`
- ID de chave globalmente exclusivo. Exemplo: `12345678-1234-1234-1234-123456789012`

Esta é uma resposta de exemplo:

```
{
    "Name": "my-event-data-store",
    "ARN": "arn:aws:cloudtrail:us-east-1:12345678910:eventdatastore/
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE",
    "RetentionPeriod": "90",
    "KmsKeyId": "arn:aws:kms:us-
east-1:123456789012:key/12345678-1234-1234-1234-123456789012"
    "MultiRegionEnabled": false,
    "OrganizationEnabled": false,
    "TerminationProtectionEnabled": true,
    "AdvancedEventSelectors": [{
        "Name": "Select all external events",
        "FieldSelectors": [{
            "Field": "eventCategory",
            "Equals": [
                "ActivityAuditLog"
            ]
        }]
    }]
}
```

A presença do elemento `KmsKeyId` indica que a criptografia do arquivo de log foi ativada. Os arquivos criptografados de log devem aparecer no seu armazenamento de dados de eventos em aproximadamente 5 minutos.

Desabilitando a criptografia do arquivo de CloudTrail log usando o AWS CLI

Para interromper a criptografia dos logs em uma trilha, execute `update-trail` e transmita uma string vazia ao parâmetro `kms-key-id`:

```
aws cloudtrail update-trail --name my-test-trail --kms-key-id ""
```

Esta é uma resposta de exemplo:

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "Default",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/Default",
    "LogFileValidationEnabled": false,
    "S3BucketName": "my-bucket-name"
}
```

A ausência do valor `KmsKeyId` indica que a criptografia do arquivo de log não está mais ativada.

> **Important**
>
> Você não pode interromper a criptografia do arquivo de log em um armazenamento de dados de eventos.

Histórico do documento

A tabela a seguir descreve as mudanças importantes na documentação do AWS CloudTrail. Para receber notificações sobre atualizações dessa documentação, você poderá se inscrever em um feed RSS.

- Versão da API: 01/11/2013
- Última atualização da documentação: 2024-05-30

Alteração	Descrição	Data
Documentação atualizada	Seção adicionada para descrever como filtrar eventos de dados usando seletores de eventos avançados. Para obter mais informações, consulte Filtragem de eventos de dados usando seletores de eventos avançados.	29 de maio de 2024
Adição de funcionalidade	Agora você pode registrar eventos de CloudTrail dados nos streams do Amazon Kinesis Data Streams e transmitir consumidores usando seletores de eventos avançados. Para obter mais informações, consulte Eventos de dados.	21 de maio de 2024
Documentação atualizada	Atualizou a página Regiões suportadas por CloudTrail lagos para adicionar a região Ásia-Pacífico (Hyderabad) (ap-south-2), a região da Europa (Zurique) (eu-central-2) e a	16 de maio de 2024

	região de Israel (Tel Aviv) (il-central-1).	
Adição de funcionalidade	Agora você pode registrar eventos CloudTrail de dados em máquinas de AWS Step Functions estado usando seletores de eventos avançados. Para obter mais informações, consulte Eventos de dados.	16 de maio de 2024
Documentação atualizada	Foi adicionada uma seção sobre o CloudTrail custo de visualização e o uso do AWS Cost Explorer. Para obter mais informações, consulte Visualizar seu CloudTrail custo e uso com AWS Cost Explorer.	14 de maio de 2024
Adição de funcionalidade	Agora você pode registrar eventos CloudTrail de dados no Amazon Q Apps usando seletores de eventos avançados. Para obter mais informações, consulte Eventos de dados.	1º de maio de 2024

Documentação atualizada	Melhorias organizacionais gerais nas seções do guia do usuário e nos títulos das páginas, que incluem o seguinte: Alterou o título da página de referência do evento de CloudTrail log para Entendendo CloudTrail os eventos e adicionou descrições de eventos de gerenciamento, eventos de dados e eventos do Insights. O título da página de configurações foi alterado para Definir CloudTrail configurações. As páginas Eventos de dados do Logging, Eventos de gerenciamento do Logging e Eventos do Logging Insights foram movidas para a seção Entendendo CloudTrail os eventos. A página de exemplos de arquivos de CloudTrail log foi movida para a seção de arquivos de CloudTrail log. Foram adicionadas páginas separadas para listar os AWS CLI comandos para armazenamentos de dados, consultas e integrações de eventos do CloudTrail Lake.	10 de abril de 2024

Documentação atualizada	A página de regiões suportadas por CloudTrail lagos foi atualizada para adicionar a região da Europa (Espanha) (eu-south-2).	10 de abril de 2024
Adição de suporte ao serviço	Esta versão é compatível com o AWS Control Catalog. Para obter mais informações, consulte AWS service (Serviço da AWS) os tópicos sobre como usar a API Logging AWS Control Catalog AWS CloudTrail. CloudTrail	8 de abril de 2024
Adição de suporte ao serviço	Esta versão é compatível com AWS o Deadline Cloud. Para obter mais informaçõ es, consulte AWS service (Serviço da AWS) os tópicos para CloudTrail.	2 de abril de 2024
Adição de funcionalidade	A versão do AWS CloudTrai l evento agora é 1.10. Para obter mais informações, consulte o conteúdo do CloudTrail registro.	26 de março de 2024
Adição de suporte ao serviço	Esta versão oferece suporte ao AWS Billing Conductor. Para obter mais informaçõ es, consulte AWS service (Serviço da AWS) os tópicos sobre CloudTrail como usar chamadas AWS Billing Conductor da API Logging AWS CloudTrail.	12 de março de 2024

Adição de funcionalidade	Agora você pode registrar eventos de CloudTrail dados em AWS X-Ray rastreamentos e nós AWS Systems Manager gerenciados usando seletores de eventos avançados. Para obter mais informações, consulte Eventos de dados.	7 de março de 2024
Adição de funcionalidade	Agora você pode registrar eventos de CloudTrail dados nos domínios do Amazon Simple Workflow Service (Amazon SWF) usando seletores de eventos avançados. Para obter mais informações, consulte Eventos de dados.	14 de fevereiro de 2024
Adição de funcionalidade	CloudTrail adicionou a `ListInsightsMetricData` API. A `ListInsightsMetricData` API retorna dados de métricas do Insights para trilhas que ativaram o Insights. Para obter mais informações, consulte ListInsightsMetricDataa Referência AWS CloudTrail da API.	6 de fevereiro de 2024

Adição de funcionalidade	Agora você pode registrar eventos CloudTrail de dados para AWS IoT AWS IoT SiteWise, e AWS AppConfig usando seletores de eventos avançados. Para obter mais informações, consulte Eventos de dados.	4 de janeiro de 2024
Adição de funcionalidade	Agora você pode registrar eventos CloudTrail de dados AWS IoT Greengrass usando seletores de eventos avançados. Para obter mais informações, consulte Eventos de dados.	22 de dezembro de 2023
Suporte a nova região	CloudTrail expandiu o suporte para uma nova região, a Região Oeste do Canadá (Calgary). Para obter mais informações, consulte Regiões CloudTrail suportadas.	20 de dezembro de 2023
Adição de funcionalidade	Agora você pode registrar eventos de CloudTrail dados para Amazon Keyspaces (para Apache Cassandra), AWS IoT TwinMaker Amazon RDS e Cadeia de Suprimentos AWS usando seletores de eventos avançados. Para obter mais informações, consulte Eventos de dados.	20 de dezembro de 2023

Política AWS gerenciada atualizada	Atualizou a política gerenciada do CloudTrailServiceRolePolicy para permitir as seguintes ações em um armazenamento de dados de eventos da organização quando a federação está desabilitada: `glue:DeleteTable` e `lakeformation:DeregisterResource` .	26 de novembro de 2023
Adição de funcionalidade	Agora você pode federar um armazenamento de dados de eventos do CloudTrail Lake para ver os metadados associados ao armazenamento de dados de eventos no catálogo de AWS Glue dados e executar consultas SQL nos dados do evento usando o Amazon Athena. Os metadados da tabela armazenados no Catálogo de AWS Glue Dados permitem que o mecanismo de consulta do Athena saiba como encontrar, ler e processar os dados que você deseja consultar. Para obter mais informações, consulte Federar um armazenamento de dados de eventos.	26 de novembro de 2023

Adição de funcionalidade	Agora você pode registrar eventos CloudTrail de dados AWS Cloud Map usando seletores de eventos avançados. Para obter mais informações, consulte Registrar eventos de dados.	16 de novembro de 2023
Adição de funcionalidade	Agora você pode registrar eventos de CloudTrail dados em mensagens do Amazon SQS usando seletores de eventos avançados. Para obter mais informações, consulte Registrar eventos de dados.	16 de novembro de 2023

Adição de funcionalidade	CloudTrail O Lake agora oferece duas opções de preços para armazenamentos de dados de eventos: preços de retenção extensíveis por um ano e preços de retenção por sete anos. A opção de preço determina o custo para a ingestão e para o armazenamento de eventos, e o período de retenção padrão e máximo para o armazenamento de dados de eventos. Antes deste lançamento, todos os armazenamentos de dados de eventos usavam a opção de preço de retenção de sete anos. Você pode mudar um armazenamento de dados de eventos do uso da opção de preço de retenção de sete anos para o uso do preço de retenção extensível de um ano usando o CloudTrail console ou a operação da API. AWS CLIUpdateEventDataStore Para obter mais informações sobre as opções de preços, consulte Preços do AWS CloudTrail e Opções de preços do armazenamento de dados de eventos.	15 de novembro de 2023

Adição de funcionalidade	Agora você pode coletar eventos do Insights em CloudTrail Lake. AWS CloudTrail O Insights ajuda AWS os usuários a identificar e responder a atividades incomuns associadas a chamadas de API e taxas de erro de API, analisando continuamente os eventos CloudTrail de gerenciamento. Para coletar eventos do Insights no CloudTrail Lake, você precisa de um armazenamento de dados de eventos de origem que registre eventos de gerenciamento e habilite o Insights e um armazenamento de dados de eventos de destino que colete eventos do Insights com base em atividades incomuns de eventos de gerenciamento no armazenamento de dados de eventos de origem. Para obter mais informações, consulte Criar um armazenamento de dados de eventos para eventos do CloudTrail Insights e eventos do Logging Insights.	9 de novembro de 2023

Adição de suporte ao serviço	Esta versão oferece suporte ao AWS Launch Wizard. Para obter mais informaçõ es, consulte AWS service (Serviço da AWS) os tópicos sobre CloudTrail como usar chamadas AWS Launch Wizard da API Logging AWS CloudTrail.	8 de novembro de 2023
Adição de suporte ao serviço	Essa versão oferece suporte ao Amazon Bedrock. Para obter mais informações, consulte AWS service (Serviço da AWS) os tópicos CloudTrail e registre as chamadas da API Amazon Bedrock usando AWS CloudTrail.	23 de outubro de 2023
Adição de funcionalidade	Agora você pode registrar eventos de CloudTrail dados nas CodeWhisperer personalizações da Amazon usando seletores de eventos avançados. Para obter mais informações, consulte Registrar eventos de dados.	18 de outubro de 2023
Adição de funcionalidade	Agora você pode registrar eventos de CloudTrail dados nos bancos de dados e tabelas do Amazon Timestrea m usando seletores de eventos avançados. Para obter mais informações, consulte Registrar eventos de dados.	28 de setembro de 2023

Adição de funcionalidade	Agora você pode registrar eventos de CloudTrail dados em tópicos e endpoints da plataforma do Amazon SNS usando seletores de eventos avançados. Para obter mais informações, consulte Registrar eventos de dados.	28 de setembro de 2023
Documentação atualizada	Tabela adicionada para mostrar as tarefas que a conta de gerenciamento, as contas de administrador delegado e as contas de membros de uma AWS Organizations organizaç ão podem realizar. CloudTrai l Para obter mais informaçõ es, consulte Organization delegated administrator (Administrador delegado de organização).	25 de setembro de 2023
Adição de suporte ao serviço	Esta versão oferece suporte a AWS Marketplace Acordos. Para obter mais informaçõ es, consulte os AWS service (Serviço da AWS) tópicos CloudTrail e o uso de chamadas de API de contratos de registro AWS CloudTrail.	1º de setembro de 2023

Adição de funcionalidade	Agora você pode registrar eventos de CloudTrail dados em streams de vídeo do Amazon Kinesis e SageMaker endpoints da Amazon usando seletores de eventos avançados. Para obter mais informações, consulte Registrar eventos de dados.	31 de agosto de 2023
Adição de suporte ao serviço	Esta versão oferece suporte ao AWS Application Transformation Service. AWS O Application Transformation Service é um serviço de back-end usado por serviços como o AWS Microservice Extractor for .NET. Para obter mais informações, consulte serviços e integrações CloudTrail compatíveis.	26 de agosto de 2023
Adição de funcionalidade	Agora você pode registrar eventos de CloudTrail dados no AWS Private CA Connector for Active Directory usando seletores de eventos avançados. Para obter mais informações, consulte Registrar eventos de dados.	24 de agosto de 2023

Documentação atualizada	Foram adicionados novos cenários do CloudTrail Lake para mostrar como criar armazenamentos de dados de eventos, visualizar painéis do CloudTrail Lake, copiar eventos de trilha para um armazenamento de dados de eventos, visualizar e executar consultas de amostra e salvar os resultados da consulta em um bucket do Amazon S3 usando o. AWS Management Console Para obter mais informaçõ es, consulte Cenários para CloudTrail Lake	16 de agosto de 2023
Suporte a nova região	CloudTrail expandiu o apoio a uma nova região, a região de Israel (Tel Aviv). Para obter mais informações, consulte Regiões CloudTrail suportada s.	1º de agosto de 2023
Adição de suporte ao serviço	Esta versão oferece suporte ao AWS HealthImaging. Para obter mais informações, consulte serviços e integraçõ es CloudTrail compatíveis e o uso AWS CloudTrail de chamadas AWS HealthIma ging à API Logging.	26 de julho de 2023

Adição de funcionalidade	Agora você pode registrar eventos de CloudTrail dados em armazenamentos AWS HealthImaging de dados usando seletores de eventos avançados. Para obter mais informações, consulte Registrar eventos de dados.	26 de julho de 2023
Adição de funcionalidade	Agora você pode registrar eventos de CloudTrail dados em canais AWS Systems Manager de controle e redes Amazon Managed Blockchain usando seletores de eventos avançados. Para obter mais informações, consulte Registrar eventos de dados.	21 de junho de 2023
Adição de funcionalidade	Agora você pode verificar os resultados da consulta salva no CloudTrail Lake usando o aws cloudtrail verify-query-results comando. Para obter mais informações, consulte Validar resultados de consultas salvas com a AWS CLI.	21 de junho de 2023

Adição de suporte ao serviço	Esta versão é compatíve l com o Amazon Verified Permissions. Para obter mais informações, consulte serviços e integrações CloudTrail compatíveis e Registro de chamadas da API Amazon Verified Permissions usando AWS CloudTrail.	13 de junho de 2023
Adição de funcionalidade	Agora você pode usar os painéis do CloudTrail Lake para visualizar os eventos em um armazenamento de dados de eventos. Para obter mais informações, consulte Visualizar painéis do Lake.	13 de junho de 2023
Adição de funcionalidade	Agora você pode registrar eventos de CloudTrail dados nos repositórios de políticas de permissões verificadas da Amazon usando seletores de eventos avançados. Para obter mais informações, consulte Registrar eventos de dados.	13 de junho de 2023
Adição de funcionalidade	Agora você pode registrar eventos CloudTrail de dados em um CodeWhisperer perfil da Amazon usando seletores de eventos avançados. Para obter mais informações, consulte Registrar eventos de dados.	6 de junho de 2023

Adição de funcionalidade	Agora você pode iniciar e interromper a ingestão de eventos em armazenam entos de dados de CloudTrail eventos. Para obter informaçõ es sobre como interromper a ingestão de eventos usando o console, consulte Impedir que um armazenamento de dados de eventos ingira eventos. Para obter informações sobre como interromper a ingestão de eventos usando o AWS CLI, consulte Interromper a ingestão em um armazenam ento de dados de eventos.	2 de junho de 2023
Adição de funcionalidade	Agora você pode registrar eventos de CloudTrail dados em um espaço de trabalho de registro de gravação antecipada do Amazon EMR usando seletores de eventos avançados. Para obter mais informações, consulte Registrar eventos de dados.	31 de maio de 2023
Adição de suporte ao serviço	Esta versão é compatível com o Amazon Security Lake. Para obter mais informações, consulte serviços e integraçõ es CloudTrail compatíveis e Registro de chamadas de API do Amazon Security Lake usando AWS CloudTrail.	30 de maio de 2023

Documentação atualizada	Tópico atualizado do elemento CloudTrail UserIdentity para incluir um exemplo e descrições de campo para uma solicitação feita em nome de um usuário do IAM Identity Center. Para obter mais informações, consulte Elemento userIdentity do CloudTrail .	23 de maio de 2023
Documentação atualizada	Essa atualização oferece suporte à seguinte versão de patch para a Biblioteca de CloudTrail Processamento: aws-cloudtrail-processing-library -1.6.1.jar. Para obter mais informações, consulte Usando a Biblioteca CloudTrail de Processamento e a Biblioteca CloudTrail de Processamento em GitHub.	23 de maio de 2023
Adição de funcionalidade	CloudTrail O Lake agora suporta todas as funções e operadores do Presto. Para obter mais informações, consulte Restrições do CloudTrail Lake SQL.	9 de maio de 2023

Adição de funcionalidade	Agora você pode registrar eventos CloudTrail de dados em um GuardDuty detector da Amazon usando seletores de eventos avançados. Para obter mais informaçõ es, consulte Registro de eventos de dados e Registro de chamadas de GuardDuty API da Amazon com AWS CloudTrail.	30 de março de 2023
Documentação atualizada	Adição de uma nova seção sobre a criação de tags de alocação de custos definidas pelo usuário para armazenam entos de dados de eventos. Para obter mais informações, consulte Criação de tags de alocação de custos definidas pelo usuário para armazenam entos de dados de eventos do CloudTrail Lake.	24 de março de 2023
Adição de suporte ao serviço	Esta versão é compatível com o AWS Telco Network Builder (AWS TNB). Para obter mais informações, consulte serviços e integrações CloudTrail suportados e como registrar chamadas da API AWS Telco Network Builder usando. AWS CloudTrail	21 de fevereiro de 2023

Adição de funcionalidade	Agora você pode registrar eventos de CloudTrail dados nos grupos de identidad e do Amazon Cognito usando seletores de eventos avançados. Para obter mais informações, consulte Registrar eventos de dados.	15 de fevereiro de 2023
Documentação atualizada	Foi adicionada uma nova seção sobre os recursos de aprendizagem disponíve is para o CloudTrail Lake. Para obter mais informaçõ es, consulte Recursos de aprendizado.	9 de fevereiro de 2023
Adição de funcionalidade	Agora você pode criar integrações do CloudTrail Lake com fontes de eventos fora do AWS. É possível registrar em log e armazenar dados de atividade do usuário de qualquer fonte em seus ambientes híbridos, como aplicações internas ou de SaaS hospedados on-premis es ou na nuvem, máquinas virtuais ou contêineres. Para obter mais informações, consulte Criação de uma integração com uma fonte de eventos de fora da AWS.	31 de janeiro de 2023

Adição de funcionalidade	Agora você pode registrar eventos CloudTrail de dados sobre CloudTrail `PutAuditEvents` atividades em um canal do CloudTrail Lake usando seletores de eventos avançados. Para obter mais informações, consulte Registrar eventos de dados.	31 de janeiro de 2023
Suporte a nova região	CloudTrail expandiu o suporte para uma nova região, a região Ásia-Pacífico (Melbourne). Para obter mais informações, consulte Regiões CloudTrail suportadas.	24 de janeiro de 2023
Documentação atualizada	Foi adicionada uma nova seção sobre gerenciamento de consistência de dados em CloudTrail, consulte Gerenciamento da consistência de dados em CloudTrail.	18 de janeiro de 2023
Adição de funcionalidade	Agora você pode registrar eventos de CloudTrail dados nas lojas de SageMaker recursos da Amazon usando seletores de eventos avançados. Para obter mais informações, consulte Registrar eventos de dados.	27 de dezembro de 2022

Adição de suporte ao serviço	Esta versão é compatível com o AWS Marketplace Discovery . Consulte Serviços compatíveis e integrações do AWS CloudTrail.	15 de dezembro de 2022
Adição de funcionalidade	Agora você pode registrar eventos de CloudTrail dados em componentes experimentais de SageMaker métricas da Amazon usando seletores de eventos avançados. Para obter mais informações, consulte Registrar eventos de dados.	15 de dezembro de 2022
Adição de funcionalidade	Agora você pode criar um armazenamento de dados de eventos para incluir itens de AWS Config configuração e usar o armazenamento de dados de eventos para investigar alterações não compatíveis em seus ambientes de produção. Para obter mais informações, consulte Criar um armazenamento de dados de eventos para itens AWS Config de configuração.	28 de novembro de 2022
Suporte a nova região	CloudTrail expandiu o suporte para uma nova região, a região Ásia-Pacífico (Hyderabad). Para obter mais informações, consulte Regiões CloudTrail suportadas.	22 de novembro de 2022

Adição de funcionalidade	Agora você pode registrar eventos CloudTrail de dados em Amazon FinSpace ambientes usando seletores de eventos avançados. Para obter mais informações, consulte Registrar eventos de dados.	18 de novembro de 2022
Suporte a nova região	CloudTrail suporte expandido para uma nova região, a região da Europa (Espanha). Para obter mais informações, consulte Regiões CloudTrail suportadas.	16 de novembro de 2022
Suporte a nova região	CloudTrail expandiu o suporte para uma nova região, a região da Europa (Zurique). Para obter mais informações, consulte Regiões CloudTrail suportadas.	9 de novembro de 2022
Adição de funcionalidade	A conta de gerenciamento de uma AWS Organizations organização agora pode adicionar um administrador delegado para gerenciar as CloudTrail trilhas e os armazenamentos de dados de eventos da organização. Para obter mais informaçõ es, consulte Organization delegated administrator (Administrador delegado de organização).	7 de novembro de 2022

Adição de funcionalidade	Agora você pode habilitar a AWS Key Management Service criptografia para um armazenamento de dados de eventos do CloudTrail Lake. Para obter mais informações, consulte Create an event data store (Criar um armazenam ento de dados de eventos).	7 de novembro de 2022
Adição de funcionalidade	Agora você pode salvar os resultados da consulta do CloudTrail Lake em um bucket do Amazon S3 ao executar uma consulta. Para obter mais informações sobre como executar uma consulta, acesse Run a query and save query results (Executar uma consulta e salvar os resultados de consulta). Para obter mais informações sobre como baixar os resultados de consulta, acesse Get and download saved query results (Obter e baixar os resultados de consultas salvas).	21 de outubro de 2022
Adição de funcionalidade	Agora você pode copiar eventos de CloudTrail trilha para um armazenamento de dados de eventos do CloudTrail Lake. Para obter mais informações, consulte Copiando eventos de trilhas para CloudTrail Lake.	19 de setembro de 2022

Documentação atualizada	Foi adicionada uma lista de CloudWatch métricas compatíveis da Amazon para o CloudTrail Lake. Para obter mais informaçõ es, consulte CloudWatch Métricas suportadas.	16 de setembro de 2022
Adição de funcionalidade	Agora você pode ver os canais CloudTrail vinculados ao serviço usando o. AWS CLI Para obter mais informaçõ es, consulte Visualizando canais vinculados ao serviço CloudTrail usando o. AWS CLI	9 de setembro de 2022
Suporte a nova região	CloudTrail expandiu o suporte para uma nova região, a região do Oriente Médio (EAU). Para obter mais informações, consulte Regiões CloudTrail suportadas.	30 de agosto de 2022

Funcionalidade alterada	CloudTrail alterou o nome da política gerenciada `AWSCloudTrailReadOnlyAccess` para`AWSCloudTrail_ReadOnlyAccess` . As permissões nesta política foram reduzidas. Por padrão, a política não concede mais permissão para listar todos os buckets, AWS Lambda funções ou aliases do Amazon S3. AWS KMS Para obter mais informações, consulte Acesso somente leitura.	6 de junho de 2022
Funcionalidade alterada	Como uma prática recomendada de segurança, agora você pode adicionar uma chave de condição `aws:SourceArn` ou `aws:SourceAccount` a um bloco de verificação da ACL `s3:GetBucketAcl` `às políticas de bucket do Amazon S3. Para obter mais informações, consulte Configurar políticas de bucket do Amazon S3 para. CloudTrail	11 de maio de 2022

Funcionalidade alterada	A partir de 24 de fevereiro de 2022, AWS CloudTrail começou a alterar os valores do `sourceIPAddress` campo `userAgent` e em qualquer evento originado de uma AWS Management Console sessão em que um cliente proxy foi usado. Para esses eventos, CloudTrail substitui os valores dos `sourceIPAddress` campos `userAgent` e por`AWS Internal`. CloudTrailfez essa alteração para padronizar a forma como registra as informações das ações de serviço em todos os AWS serviços. Para obter mais informações, consulte o conteúdo do CloudTrail registro.	12 de abril de 2022
Adição de suporte ao serviço	Esta versão é compatível com a Amazon GameSparks. Consulte Serviços compatíveis e integrações do AWS CloudTrail.	24 de março de 2022
Adição de suporte ao serviço	Esta versão é compatível com o AWS App Mesh Envoy Management Service. Consulte Serviços compatíveis e integrações do AWS CloudTrail.	18 de março de 2022

Documentação atualizada	Novos exemplos de consulta foram adicionados ao CloudTrail Lake, um novo recurso que permite executar consultas SQL refinadas e de vários campos em seus eventos. Além disso, um novo campo `BytesScanned` foi adicionado aos resultados dos metadados da consulta das operações `DescribeQuery` e `GetQueryResults` . Para obter mais informações, consulte Trabalhando com o CloudTrail Lake.	4 de março de 2022
Funcionalidade alterada	CloudTrail agora remove o ID da conta do proprietário do bucket do Amazon S3 no `resources` bloco de um evento de dados se as duas condições a seguir forem atendidas: a chamada da API do evento de dados for de uma AWS conta diferente da do proprietário do bucket do Amazon S3, e o chamador da API recebeu `AccessDenied` um erro que era somente para a conta do chamador. Para obter mais informaçõ es, consulte Redação de IDs de conta de proprietário do bucket para eventos de dados chamados por outras contas.	3 de março de 2022

Documentação atualizada	Esta atualização oferece suporte à seguinte versão da Biblioteca de CloudTrai l Processamento: suporte adicionado para implementar um gerenciador S3 personali zado, registro de eventos para registrar exceções relaciona das à análise de arquivos, suporte para analisar um `errorCode` campo opcional e atualização do regex de análise de ID da conta para aceitar valores não numéricos . `insightDetails` Para obter mais informações, consulte Usando a Biblioteca CloudTrail de Processamento e a Biblioteca CloudTrail de Processamento em GitHub.	28 de janeiro de 2022

Adição de funcionalidade	CloudTrail apresenta o CloudTrail Lake, um novo recurso que permite executar consultas SQL refinadas e de vários campos em seus eventos. Os eventos são agregados em armazenam entos de dados de eventos, que são coleções imutáveis de eventos baseados nos critérios selecionados com a aplicação de seletores de eventos avançados. Para obter mais informações, consulte Trabalhando com o CloudTrail Lake.	5 de janeiro de 2022
Suporte a nova região	CloudTrail suporte expandido para uma nova região, a região Ásia-Pacífico (Jacarta) . Para obter mais informações, consulte Regiões CloudTrail suportadas.	13 de dezembro de 2021
Adição de suporte ao serviço	Esta versão é compatível com o Amazon WorkSpace s Web. Consulte Serviços compatíveis e integrações do AWS CloudTrail.	3 de dezembro de 2021

Adição de funcionalidade	Agora você pode registrar eventos CloudTrail de dados em AWS Glue tabelas criadas pelo Lake Formation usando seletores de eventos avançados. Para obter mais informações, consulte Registrar eventos de dados.	30 de novembro de 2021
Funcionalidade alterada	Como melhor prática de segurança, agora você pode adicionar uma chave de `aws:SourceAccount` condição `aws:SourceArn` ou às políticas AWS KMS principais e às políticas de bucket do Amazon S3. Para obter mais informações, consulte Configurar políticas de AWS KMS chave para CloudTrail e Configurar políticas de bucket do Amazon S3 para. CloudTrail	15 de novembro de 2021
Adição de suporte ao serviço	Esta versão é compatível com o AWS Resilience Hub. Consulte Serviços compatíveis e integrações do AWS CloudTrail.	10 de novembro de 2021

Adição de funcionalidade	Um novo tipo de evento do CloudTrail Insights está disponível: eventos do Insights com taxa de erro. Um evento do Insights de taxa de erro captura atividades incomuns em um erro que ocorre em APIs chamadas em sua conta. Para obter mais informaçõ es, consulte Registrar em log eventos do Insights para trilhas.	10 de novembro de 2021
Adição de funcionalidade	Agora você pode registrar eventos de CloudTrail dados nos streams do DynamoDB usando seletores de eventos avançados. Para obter mais informações, consulte Registrar eventos de dados.	22 de setembro de 2021
Adição de funcionalidade	Agora você pode registrar eventos de dados em pontos de acesso do Amazon S3. É possível registrar eventos de dados de ponto de acesso do Amazon S3 usando seletores de eventos avançados. Para obter mais informações, consulte Registrar eventos de dados.	24 de agosto de 2021

Funcionalidade alterada	Quando você configura uma trilha para enviar notificaç ões para o Amazon SNS, CloudTrail adiciona uma declaração de política à sua política de acesso a tópicos do SNS que permite enviar conteúdo CloudTrai l para um tópico do SNS. Como prática recomendada de segurança, recomenda mos adicionar uma chave de `aws:SourceAccount` condição `aws:SourceArn` ou à declaração CloudTrail de política. Para obter mais informações, consulte a política de tópicos do Amazon SNS para. CloudTrail	16 de agosto de 2021
Adição de suporte ao serviço	Esta versão é compatível com o Amazon Route 53 Applicati on Recovery Controller. Consulte Serviços compatíve is e integrações do AWS CloudTrail.	27 de julho de 2021

Adição de funcionalidade	Agora, é possível registrar eventos de dados em APIs diretas do Amazon EBS executadas em snapshots do EBS. É possível registrar eventos de dados de API do Amazon EBS usando seletores de eventos avançados. Para obter mais informações, consulte Registrar eventos de dados.	27 de julho de 2021
Funcionalidade alterada	Ao CloudTrail processar eventos de dados, ele preserva os números em seu formato original, seja um inteiro (`int`) ou um. `float` Em eventos que têm números inteiros nos campos de um evento de dados, CloudTrai l historicamente processou esses números como flutuante s. Agora, CloudTrail mantém o formato original dos números inteiros nos eventos de dados. Para obter mais informações, consulte Usando a Biblioteca CloudTrail de Processamento.	13 de julho de 2021
Adição de funcionalidade	Agora, é possível excluir eventos de gerenciamento de API de dados do Amazon RDS das suas trilhas. Para obter mais informações, consulte Registrar eventos de gerenciamento para trilhas.	1º de julho de 2021

Adição de suporte ao serviço	Esta versão oferece suporte ao AWS BugBust. Consulte Serviços compatíveis e integrações do AWS CloudTrail.	24 de junho de 2021
Adição de suporte ao serviço	Esta versão oferece suporte ao Amazon Managed Grafana e ao Amazon Managed Service for Prometheus. Consulte Serviços compatíveis e integrações do AWS CloudTrail.	2 de junho de 2021
Adição de suporte ao serviço	Esta versão é compatível com o AWS App Runner. Consulte Serviços compatíveis e integrações do AWS CloudTrail.	18 de maio de 2021
Adição de suporte ao serviço	Esta versão é compatível com o AWS Systems Manager Incident Manager. Consulte Serviços compatíveis e integrações do AWS CloudTrail.	10 de maio de 2021
Documentação atualizada	Esta atualização descreve os requisitos de registro de eventos de dados para pacotes de AWS Config conformidade, especialmente para estruturas de conformidade como HIPAA ou FedRAMP. Para obter mais informações, consulte Registrar eventos de dados.	7 de maio de 2021

Adição de suporte ao serviço	Esta versão oferece suporte a Service Quotas e APIs diretas do Amazon EBS. Consulte Serviços compatíveis e integrações do AWS CloudTrail.	13 de abril de 2021
Adição de funcionalidade	Depois que um administrador do IAM configura AWS STS, CloudTrail registra `sourceIdentity` as informações em eventos quando os usuários assumem uma função do IAM ou realizam qualquer ação com a função assumida. Para obter mais informações, consulte Elemento userIdentity do CloudTrail .	13 de abril de 2021
Documentação atualizada	Essa atualização documenta os limites, em kilobytes (KB), do conteúdo em alguns campos de registro de CloudTrail eventos. Para obter mais informações, consulte o conteúdo do CloudTrail registro.	8 de abril de 2021

Adição de funcionalidade	Depois que um administr ador do IAM configura AWS STS, CloudTrail registra `sourceIdentity` as informações em eventos quando os usuários assumem uma função do IAM ou realizam qualquer ação com a função assumida. Para obter mais informações, consulte Elemento userIdentity do CloudTrail .	6 de abril de 2021
Adição de funcionalidade	Agora, é possível registrar eventos de dados em tabelas do Amazon DynamoDB. É possível registrar eventos de dados do DynamoDB usando seletores de eventos ou seletores de eventos avançados. Para obter mais informações, consulte Registrar eventos de dados.	23 de março de 2021
Adição de suporte ao serviço	Esta versão oferece suporte ao Amazon Managed Workflows for Apache Airflow. Consulte Serviços compatíve is e integrações do AWS CloudTrail.	22 de março de 2021

Adição de funcionalidade	Agora, será possível registrar eventos de dados em pontos de acesso do S3 Object Lambda se você tiver optado por usar seletores de eventos avançados. Para obter mais informações, consulte Registrar eventos de dados.	18 de março de 2021
Adição de suporte ao serviço	Esta versão é compatível com o AWS Fault Injection Simulator. Consulte Serviços compatíveis e integrações do AWS CloudTrail.	15 de março de 2021
Adição de funcionalidade	Agora, é possível registrar eventos de dados em nós do Ethereum no Amazon Managed Blockchain se você optou por usar seletores de eventos avançados. Para obter mais informações, consulte Registrar eventos de dados.	1º de março de 2021
Adição de suporte ao serviço	Esta versão oferece suporte ao Amazon Managed Blockchain e à visualização do Ethereum para Managed Blockchain. Consulte Serviços compatíveis e integrações do AWS CloudTrail.	4 de fevereiro de 2021

Adição de suporte ao serviço	Esta versão oferece suporte ao AWS Amplify. Consulte Serviços compatíveis e integrações do AWS CloudTrail.	3 de fevereiro de 2021
Adição de suporte ao serviço	Esta versão oferece suporte ao Amazon Lookout for Metrics. Consulte Serviços compatíveis e integrações do AWS CloudTrail.	1 de fevereiro de 2021
Documentação atualizada	Esta atualização oferece suporte à seguinte versão de patch para a Biblioteca de CloudTrail Processamento: Atualize as referências do arquivo.jar no guia do usuário para usar a versão mais recente, aws-cloudtrail-processing-library -1.4.0.jar. Para obter mais informações, consulte Usando a Biblioteca CloudTrail de Processamento e a Biblioteca CloudTrail de Processamento em GitHub.	12 de janeiro de 2021
Adição de funcionalidade	Agora, é possível registrar eventos de dados no Amazon S3 no AWS Outposts. Para obter mais informações, consulte Registrar eventos de dados.	21 de dezembro de 2020

Adição de suporte ao serviço	Esta versão é compatível com o Amazon Lookout for Equipment AWS Well-Architected Tool e o Amazon Location Service. Consulte Serviços compatíveis e integrações do AWS CloudTrail.	16 de dezembro de 2020
Adição de suporte ao serviço	Esta versão é compatível com AWS IoT Greengrass V2. Consulte Serviços compatíveis e integrações do AWS CloudTrail.	15 de dezembro de 2020
Adição de suporte ao serviço	Esta versão oferece suporte ao Amazon EMR no EKS. Consulte Serviços compatíveis e integrações do AWS CloudTrail.	10 de dezembro de 2020
Adição de suporte ao serviço	Esta versão é compatível com o AWS Audit Manager e a Amazon HealthLake. Consulte Serviços compatíveis e integrações do AWS CloudTrail.	8 de dezembro de 2020
Adição de suporte ao serviço	Esta versão oferece suporte ao Amazon Lookout for Vision. Consulte Serviços compatíveis e integrações do AWS CloudTrail.	1º de dezembro de 2020

Adição de funcionalidade	A versão do AWS CloudTrail evento agora é 1.08. A versão 1.08 introduz novos campos para. CloudTrail Para obter mais informações, consulte o conteúdo do CloudTrail registro.	24 de novembro de 2020
Adição de funcionalidade	AWS CloudTrail apresenta seletores de eventos avançados para eventos de dados. Os seletores de eventos avançados permitem um controle mais refinado sobre os eventos de dados que você registra em sua trilha. Você pode incluir ou excluir eventos de dados para AWS recursos específicos e selecionar APIs específicas nesses recursos para registrar sua trilha. Para obter mais informações, consulte Registrar eventos de dados.	24 de novembro de 2020
Adição de suporte ao serviço	Esta versão oferece suporte ao AWS Network Firewall. Consulte Serviços compatíveis e integrações do AWS CloudTrail.	17 de novembro de 2020
Adição de suporte ao serviço	Esta versão oferece suporte ao AWS Trusted Advisor. Consulte Serviços compatíveis e integrações do AWS CloudTrail.	22 de outubro de 2020

Documentação atualizada	Adicionados dois novos exemplos de registros de eventos para eventos de login de usuário raiz. Para obter mais informações, consulte Eventos de login do Console da AWS.	13 de outubro de 2020
Funcionalidade alterada	Permissões na política do `AWSCloudTrail_FullAccess` foram reduzidos. Esta política não permite mais excluir tópicos do Amazon SNS nem buckets do Amazon S3 e a ação `getObject` foi removida. Para obter mais informações, consulte Conceder permissões personalizadas para CloudTrail usuários.	29 de setembro de 2020
Documentação atualizada	Esta atualização oferece suporte à seguinte versão de patch para a Biblioteca de CloudTrail Processamento: Atualize as referências do arquivo.jar no guia do usuário para usar a versão mais recente, aws-cloudtrail-processing-library -1.3.0.jar. Para obter mais informações, consulte Usando a Biblioteca CloudTrail de Processamento e a Biblioteca CloudTrail de Processamento em GitHub.	28 de agosto de 2020

Adição de suporte ao serviço	Esta versão oferece suporte ao AWS Outposts. Consulte Serviços compatíveis e integrações do AWS CloudTrail.	28 de agosto de 2020
Adição de funcionalidade	AWS CloudTrail O Insights apresenta campos de atribuição para CloudTrail eventos do Insights. Os campos de atribuição mostram as principais identidades de usuário, agentes de usuário e códigos de erro associados à atividade anômala que aciona eventos do Insights. Para comparação, os campos de atribuição também mostram as principais identidades de usuário, agentes de usuário e códigos de erro associados à atividade normal ou de linha de base. Para obter mais informações, consulte Registrar em log eventos do Insights para trilhas.	13 de agosto de 2020

Adição de funcionalidade	O AWS CloudTrail console tem um novo visual projetado para facilitar o uso. O Guia AWS CloudTrail do usuário foi atualizado com alterações nos procedimentos de como realizar tarefas no console, como criar trilhas, atualizar trilhas e baixar o histórico de eventos.	13 de agosto de 2020
Adição de suporte ao serviço	Esta versão oferece suporte ao Amazon Interactive Video Service. Consulte Serviços compatíveis e integrações do AWS CloudTrail.	15 de julho de 2020
Adição de suporte ao serviço	Esta versão oferece suporte ao Amazon Honeycode. Consulte Serviços compatíveis e integrações do AWS CloudTrail.	24 de junho de 2020
Adição de suporte ao serviço	Essa versão oferece suporte ao Amazon Macie. Consulte Serviços compatíveis e integrações do AWS CloudTrail.	19 de maio de 2020
Adição de suporte ao serviço	Essa versão oferece suporte ao Amazon Kendra. Consulte Serviços compatíveis e integrações do AWS CloudTrail.	13 de maio de 2020

Adição de suporte ao serviço	Esta versão oferece suporte ao AWS IoT SiteWise. Consulte Serviços compatíveis e integrações do AWS CloudTrail.	29 de abril de 2020
Adição de suporte a região	Esta versão oferece suporte a uma região adicional: Europa (Milão). Consulte Regiões com suporte do AWS CloudTrail.	28 de abril de 2020
Adição de suporte a serviço e região	Esta versão é compatível com a Amazon AppFlow. Consulte Serviços compatíveis e integrações do AWS CloudTrail. Também foi adicionado suporte para a Região da África (Cidade do Cabo). Consulte Regiões com suporte do AWS CloudTrail.	22 de abril de 2020
Adição de funcionalidade	AWS KMS Ações de alto volume `Encrypt`, como, `Decrypt`, e agora `GenerateDataKey` são registradas como eventos de leitura. Se você optar por registrar todos os AWS KMS eventos em sua trilha e também optar por registrar eventos de gerenciamento de gravação, sua trilha AWS KMS registrará ações relevantes como `Disable` `Delete` `ScheduleKey` e.	7 de abril de 2020

Adição de suporte ao serviço	Esta versão é compatível com o Amazon CodeGuru Reviewer. Consulte Serviços compatíveis e integrações do AWS CloudTrail.	7 de fevereiro de 2020
Adição de suporte ao serviço	Esta versão oferece suporte ao Amazon Managed Apache Cassandra Service. Consulte Serviços compatíveis e integrações do AWS CloudTrail.	17 de janeiro de 2020
Adição de suporte ao serviço	Esta versão oferece suporte ao Amazon Connect. Consulte Serviços compatíveis e integrações do AWS CloudTrail.	13 de dezembro de 2019
Documentação atualizada	Esta atualização oferece suporte à seguinte versão de patch para a Biblioteca de CloudTrail Processamento: Atualize as referências do arquivo.jar no guia do usuário para usar a versão mais recente, aws-cloudtrail-processing-library -1.2.0.jar. Para obter mais informações, consulte Usando a Biblioteca CloudTrail de Processamento e a Biblioteca CloudTrail de Processamento em GitHub.	21 de novembro de 2019

Adição de funcionalidade	Esta versão oferece suporte ao AWS CloudTrail Insights para ajudar você a detectar atividades incomuns em sua conta. Consulte Registrar em log eventos do Insights para trilhas.	20 de novembro de 2019
Adição de funcionalidade	Esta versão adiciona uma opção para filtrar AWS Key Management Service eventos de uma trilha. Consulta Criar uma trilha.	20 de novembro de 2019
Adição de suporte ao serviço	Esta versão oferece suporte a AWS CodeStar Notificações. Consulte Serviços compatíveis e integrações do AWS CloudTrail.	7 de novembro de 2019
Adição de funcionalidade	Esta versão oferece suporte à adição de tags ao criar uma trilha CloudTrail, independentemente de você usar o CloudTrail console ou a API. Esta versão adiciona duas novas APIs, `GetTrail` e `ListTrails` .	1º de novembro de 2019
Adição de suporte ao serviço	Esta versão oferece suporte ao AWS App Mesh. Consulte Serviços compatíveis e integrações do AWS CloudTrail.	17 de outubro de 2019

Adição de suporte ao serviço	Esta versão oferece suporte ao Amazon Translate. Consulte Serviços compatíveis e integrações do AWS CloudTrail.	17 de outubro de 2019
Atualização da documentação	O tópico Serviços não suportados foi restaurado e atualizado para incluir somente os AWS serviços que atualmente não registram eventos. CloudTrail Consulte Serviços do CloudTrail sem suporte.	7 de outubro de 2019
Atualização da documentação	A documentação foi atualizada com alterações na política do `AWSCloudTrailFullAccess` . Um exemplo de política que mostra permissões equivalentes para `AWSCloudTrailFullAccess` foi atualizado para restringir os recursos nos quais a ação do `iam:PassRole` pode agir para aqueles que correspondem à seguinte instrução de condição: `"iam:PassedToService": "cloudtrail.amazonaws.com"` . Consulte Exemplos de políticas baseadas em identidade do AWS CloudTrail.	24 de setembro de 2019

Atualização da documentação	A documentação foi atualizada com um novo tópico, Gerenciamento de CloudTrail custos, para ajudá-lo a obter os dados de registro necessários e, CloudTrail ao mesmo tempo, manter um orçamento limitado.	3 de setembro de 2019
Adição de suporte ao serviço	Esta versão oferece suporte ao AWS Control Tower. Consulte Serviços compatíveis e integrações do AWS CloudTrail.	13 de agosto de 2019
Adição de suporte a região	Esta versão oferece suporte a uma região adicional: Oriente Médio (Bahrein). Consulte Regiões com suporte do AWS CloudTrail.	29 de julho de 2019
Atualização da documentação	A documentação foi atualizada com informações sobre segurança do CloudTrail. Consulte Segurança no AWS CloudTrail.	3 de julho de 2019
Adição de suporte ao serviço	Esta versão oferece suporte ao AWS Ground Station. Consulte Serviços compatíveis e integrações do AWS CloudTrail.	6 de junho de 2019

Adição de suporte ao serviço	Esta versão oferece suporte ao AWS IoT Things Graph. Consulte Serviços compatíveis e integrações do AWS CloudTrail.	4 de junho de 2019
Adição de suporte ao serviço	Esta versão oferece suporte ao Amazon AppStream 2.0. Consulte Serviços compatíveis e integrações do AWS CloudTrail.	25 de abril de 2019
Adição de suporte a região	Esta versão oferece suporte a uma região adicional: Ásia-Pacífico (Hong Kong). Consulte Regiões com suporte do AWS CloudTrail.	24 de abril de 2019
Adição de suporte ao serviço	Esta versão oferece suporte ao Amazon Managed Service for Apache Flink. Consulte Serviços compatíveis e integrações do AWS CloudTrail.	22 de março de 2019
Adição de suporte ao serviço	Esta versão oferece suporte ao AWS Backup. Consulte Serviços compatíveis e integrações do AWS CloudTrail.	4 de fevereiro de 2019
Adição de suporte ao serviço	Esta versão é compatível com a Amazon WorkLink. Consulte Serviços compatíveis e integrações do AWS CloudTrail.	23 de janeiro de 2019

Adição de suporte ao serviço	Esta versão oferece suporte ao AWS Cloud9. Consulte Serviços compatíveis e integrações do AWS CloudTrail.	21 de janeiro de 2019
Adição de suporte ao serviço	Esta versão oferece suporte ao AWS Elemental MediaLive. Consulte Serviços compatíveis e integrações do AWS CloudTrail.	19 de janeiro de 2019
Adição de suporte ao serviço	Esta versão oferece suporte ao Amazon Comprehend. Consulte Serviços compatíveis e integrações do AWS CloudTrail.	18 de janeiro de 2019
Adição de suporte ao serviço	Esta versão oferece suporte ao AWS Elemental MediaPackage. Consulte Serviços compatíveis e integrações do AWS CloudTrail.	21 de dezembro de 2018
Adição de suporte a região	Esta versão oferece suporte a uma região adicional: UE (Estocolmo). Consulte Regiões com suporte do AWS CloudTrail.	11 de dezembro de 2018
Atualização da documentação	A documentação foi atualizada com informações sobre os serviços com e sem suporte. Consulte Serviços compatíveis e integrações do AWS CloudTrail.	3 de dezembro de 2018

Adição de suporte ao serviço	Esta versão oferece suporte ao AWS Resource Access Manager (AWS RAM). Consulte Serviços compatíveis e integrações do AWS CloudTrail.	20 de novembro de 2018
Funcionalidade atualizada	Esta versão oferece suporte à criação de uma trilha CloudTrail que registra eventos de todas as AWS contas de uma organização em AWS Organizations. Consulte Criar uma trilha para uma organização.	19 de novembro de 2018
Adição de suporte ao serviço	Esta versão oferece suporte a SMS do Amazon Pinpoint e API de voz. Consulte Serviços compatíveis e integrações do AWS CloudTrail.	16 de novembro de 2018
Adição de suporte ao serviço	Esta versão oferece suporte ao AWS IoT Greengrass. Consulte Serviços compatíveis e integrações do AWS CloudTrail.	29 de outubro de 2018

Documentação atualizada	Esta atualização oferece suporte à seguinte versão de patch para a Biblioteca de CloudTrail Processamento: Atualize as referências do arquivo.jar no guia do usuário para usar a versão mais recente, aws-cloudtrail-processing-library -1.1.3.jar. Para obter mais informações, consulte Usando a Biblioteca CloudTrail de Processamento e a Biblioteca CloudTrail de Processamento em GitHub.	18 de outubro de 2018
Adição de funcionalidade	Essa versão oferece suporte ao uso de filtros adicionais em Event history (Histórico de eventos). Consulte Visualização de CloudTrail eventos no CloudTrail console.	18 de outubro de 2018
Adição de funcionalidade	Esta versão oferece suporte ao uso do Amazon Virtual Private Cloud (Amazon VPC) para estabelecer uma conexão privada entre a sua VPC e o AWS CloudTrail. Consulte Uso AWS CloudTrail com endpoints de VPC de interface .	9 de agosto de 2018
Adição de suporte ao serviço	Esta versão oferece suporte ao Amazon Data Lifecycle Manager. Consulte Serviços compatíveis e integrações do AWS CloudTrail.	24 de julho de 2018

Adição de suporte ao serviço	Esta versão oferece suporte ao Amazon MQ. Consulte Serviços compatíveis e integrações do AWS CloudTrail.	19 de julho de 2018
Adição de suporte ao serviço	Esta versão é compatível com o AWS Mobile CLI. Consulte Serviços compatíveis e integrações do AWS CloudTrail.	29 de junho de 2018
AWS CloudTrail notificação de histórico de documentação disponível por meio de feed RSS	Agora você pode receber notificações sobre atualizações na AWS CloudTrail documentação assinando um feed RSS.	29 de junho de 2018

Atualizações anteriores

A tabela a seguir descreve o histórico de lançamento da documentação AWS CloudTrail antes de 29 de junho de 2018.

Alteração	Descrição	Data de lançamento
Adição de suporte a serviço	Esta versão é compatível com o Performance Insights do Amazon RDS. Para obter mais informações, consulte Serviços e integrações CloudTrail compatíveis.	21 de junho de 2018
Adição de funcionalidade	Esta versão suporta o registro de todos os eventos CloudTrail de gerenciamento no histórico de eventos. Para ter mais informações, consulte Trabalhando com o histórico de CloudTrail eventos.	14 de junho de 2018

Alteração	Descrição	Data de lançamento
Adição de suporte a serviço	Esta versão oferece suporte ao AWS Billing and Cost Management. Consulte CloudTrail serviços e integrações suportados.	7 de junho de 2018
Adição de suporte a serviço	Esta versão oferece suporte ao Amazon Elastic Container Service for Kubernetes (Amazon EKS). Consulte CloudTrail serviços e integrações suportados.	5 de junho de 2018
Documentação atualizada	Essa atualização oferece suporte à seguinte versão de patch para a Biblioteca CloudTrail de Processamento: • Atualize as referências do arquivo.jar no guia do usuário para usar a versão mais recente, aws-cloudtrail-processing-library -1.1.2.jar. Para obter mais informações, consulte Usando a Biblioteca CloudTrail de Processamento e acesse a Biblioteca CloudTrail de Processamento em GitHub.	16 de maio de 2018
Adição de suporte a serviço	Esta versão oferece suporte ao AWS Billing and Cost Management. Consulte CloudTrail serviços e integrações suportados.	7 de junho de 2018
Adição de suporte a serviço	Esta versão oferece suporte ao Amazon Elastic Container Service for Kubernetes (Amazon EKS). Consulte CloudTrail serviços e integrações suportados.	5 de junho de 2018

Alteração	Descrição	Data de lançamento
Documentação atualizada	Essa atualização oferece suporte à seguinte versão de patch para a Biblioteca CloudTrail de Processamento: • Atualize as referências do arquivo.jar no guia do usuário para usar a versão mais recente, aws-cloudtrail-processing-library -1.1.2.jar. Para obter mais informações, consulte Usando a Biblioteca CloudTrail de Processamento e acesse a Biblioteca CloudTrail de Processamento em GitHub.	16 de maio de 2018
Adição de suporte a serviço	Esta versão oferece suporte ao AWS X-Ray. Consulte CloudTrail serviços e integrações suportados.	25 de abril de 2018
Adição de suporte a serviço	Esta versão é compatível com o AWS IoT Analytics. Consulte CloudTrail serviços e integrações suportados.	23 de abril de 2018
Adição de suporte a serviço	Esta versão oferece suporte ao Secrets Manager. Consulte CloudTrail serviços e integrações suportados.	10 de abril de 2018
Adição de suporte a serviço	Esta versão oferece suporte ao Amazon Rekognition. Consulte CloudTrail serviços e integrações suportados.	6 de abril de 2018
Adição de suporte a serviço	Esta versão oferece suporte à Autoridade de Certificação AWS Privada (PCA). Consulte CloudTrail serviços e integrações suportados.	4 de abril de 2018

Alteração	Descrição	Data de lançamento
Adição de funcionalidade	Esta versão facilita a pesquisa de arquivos de CloudTrail log com o Amazon Athena. Você pode criar tabelas automaticamente para consultar registros diretamente do CloudTrail console e usar essas tabelas para executar consultas no Athena. Para obter mais informações, consulte CloudTrail serviços e integrações suportados Criar uma tabela para CloudTrail registros no CloudTrail console.	15 de março de 2018
Adição de suporte a serviço	Esta versão oferece suporte ao AWS AppSync. Consulte CloudTrail serviços e integrações suportados.	13 de fevereiro de 2018
Adição de suporte para a região	Esta versão oferece suporte a uma região adicional : Ásia-Pacífico (Osaka) (ap-northeast-3). Consulte CloudTrail Regiões suportadas.	12 de fevereiro de 2018
Adição de suporte a serviço	Esta versão oferece suporte ao AWS Shield. Consulte CloudTrail serviços e integrações suportados.	12 de fevereiro de 2018
Adição de suporte a serviço	Esta versão é compatível com a Amazon SageMaker. Consulte CloudTrail serviços e integrações suportados.	11 de janeiro de 2018
Adição de suporte a serviço	Esta versão oferece suporte ao AWS Batch. Consulte CloudTrail serviços e integrações suportados.	10 de janeiro de 2018

Alteração	Descrição	Data de lançamento
Adição de funcionalidade	Esta versão permite estender a quantidade de atividades da conta que está disponível no histórico de CloudTrail eventos para 90 dias. Você também pode personalizar a exibição das colunas para melhorar a visualização dos seus CloudTrail eventos. Para ter mais informações, consulte Trabalhando com o histórico de CloudTrail eventos.	12 de dezembro de 2017
Adição de suporte a serviço	Esta versão é compatível com a Amazon WorkMail. Consulte CloudTrail serviços e integrações suportados.	12 de dezembro de 2017
Adição de suporte a serviço	Esta versão é compatível com Alexa for Business AWS Elemental MediaConvert, e. AWS Elemental MediaStore Consulte CloudTrail serviços e integrações suportados.	1º de dezembro de 2017
Adição de funcionalidade e documentação	Esta versão oferece suporte ao registro de eventos de dados para AWS Lambda funções. Para ter mais informações, consulte Eventos de dados de log.	30 de novembro de 2017
Adição de funcionalidade e documentação	Esta versão oferece suporte ao registro de eventos de dados para AWS Lambda funções. Para ter mais informações, consulte Eventos de dados de log.	30 de novembro de 2017

Alteração	Descrição	Data de lançamento
Adição de funcionalidade e documentação	Esta versão oferece suporte às seguintes atualizações da Biblioteca CloudTrail de Processamento: • Adicione suporte para a identificação booleana de eventos de gerenciamento. • Atualize a versão do CloudTrail evento para 1.06. Para obter mais informações, consulte Usando a Biblioteca CloudTrail de Processamento e acesse a Biblioteca CloudTrail de Processamento em GitHub.	30 de novembro de 2017
Adição de suporte a serviço	Esta versão oferece suporte ao AWS Glue. Consulte CloudTrail serviços e integrações suportados.	7 de novembro de 2017
Nova documentação	Esta versão adiciona um novo tópico, Cotas em AWS CloudTrail.	19 de outubro de 2017
Documentação atualizada	Esta versão atualiza a documentação das APIs suportadas no histórico de CloudTrail eventos do Amazon Athena AWS CodeBuild, Amazon Elastic Container Registry e. AWS Migration Hub	13 de outubro de 2017
Adição de suporte a serviço	Esta versão oferece suporte ao Amazon Chime. Consulte CloudTrail serviços e integrações suportados.	27 de setembro de 2017
Adição de funcionalidade e documentação	Esta versão oferece suporte à configuração do registro de eventos de dados para todos os buckets do Amazon S3 em sua conta. AWS Consulte Eventos de dados de log.	20 de setembro de 2017

Alteração	Descrição	Data de lançamento
Adição de suporte a serviço	Esta versão oferece suporte ao Amazon Lex. Consulte CloudTrail serviços e integrações suportados.	15 de agosto de 2017
Adição de suporte a serviço	Esta versão é compatível com o AWS Migration Hub. Consulte CloudTrail serviços e integrações suportados.	14 de agosto de 2017
Adição de funcionalidade e documentação	Esta versão suporta a ativação CloudTrail por padrão para todas as AWS contas. Os últimos sete dias de atividade da conta estão disponíveis no histórico de CloudTrail eventos, e os eventos mais recentes aparecem no painel do console. O recurso conhecido anteriormente como API activity history (Histórico de atividades da API) foi substituído pelo Event history (Histórico de eventos).	14 de agosto de 2017
Adição de funcionalidade e documentação	Esta versão é compatível com o download de eventos do CloudTrail console na página de histórico de atividades da API. Você pode fazer download de eventos no formato JSON ou CSV. Para ter mais informações, consulte Baixar eventos.	27 de julho de 2017
Adição de funcionalidade	Esta versão oferece suporte ao registro em log de operações de API no nível de objeto do Amazon S3 em duas regiões adicionais: Europa (Londres) e (Canadá (Central). Para ter mais informações, consulte Trabalhando com arquivos CloudTrail de log.	19 de julho de 2017

Alteração	Descrição	Data de lançamento
Adição de suporte a serviço	Esta versão oferece suporte à pesquisa de APIs para Amazon CloudWatch Events no recurso de histórico de atividades da CloudTrail API.	27 de junho de 2017
Adição de funcionalidade e documentação	Esta versão oferece suporte a APIs adicionais no recurso de histórico de atividades da CloudTrail API para os seguintes serviços: • AWS CloudHSM • Amazon Cognito • Amazon DynamoDB • Amazon EC2 • Kinesis • AWS Storage Gateway	27 de junho de 2017
Adição de suporte a serviço	Esta versão oferece suporte ao AWS CodeStar. Consulte CloudTrail serviços e integrações suportados.	14 de junho de 2017

Alteração	Descrição	Data de lançamento

Adição de funcionalidade e documentação	Esta versão oferece suporte às seguintes atualizações da Biblioteca CloudTrail de Processamento:
	• Adicione suporte para diferentes formatos para mensagens SQS da mesma fila SQS para identificar CloudTrail arquivos de log. Os seguintes formatos são compatíveis:
	  • Notificações CloudTrail enviadas para um tópico do SNS
	  • Notificações que o Amazon S3 envia para um tópico do SNS
	  • Notificações que o Amazon S3 envia diretamente para uma fila do SQS
	• Adicionar suporte à propriedade `deleteMessageUponFailure`, que você pode usar para excluir mensagens que não podem ser processadas.
	
	Para obter mais informações, consulte Usando a Biblioteca CloudTrail de Processamento e acesse a Biblioteca CloudTrail de Processamento em GitHub.
		1 de junho de 2017

Adição de suporte a serviço	Esta versão oferece suporte ao Amazon Athena. Consulte CloudTrail serviços e integrações suportados.	19 de maio de 2017

Alteração	Descrição	Data de lançamento
Adição de funcionalidade	Esta versão oferece suporte ao envio de eventos de dados para o Amazon CloudWatch Logs. Para obter mais informações sobre como configurar a trilha para registrar eventos de dados, consulte Eventos de dados. Para obter mais informações sobre o envio de eventos para o CloudWatch Logs, consulteMonitoramento CloudTrail de arquivos de log com o Amazon CloudWatch Logs.	9 de maio de 2017
Adição de suporte a serviço	Esta versão oferece suporte ao serviço AWS Marketplace de medição. Consulte CloudTrail serviços e integrações suportados.	2 de maio de 2017
Adição de suporte a serviço	Esta versão é compatível com a Amazon QuickSight. Consulte CloudTrail serviços e integrações suportados.	28 de abril de 2017
Adição de funcionalidade e documentação	Esta versão oferece suporte a uma experiência de console atualizada para a criação de novas trilhas. Agora você pode configurar uma nova trilha para registrar eventos de gerenciamento e dados. Para ter mais informações, consulte Criar uma trilha.	11 de abril de 2017

Alteração	Descrição	Data de lançamento
Documentação acrescentada	Se não CloudTrail estiver entregando registros para seu bucket do S3 ou enviando notificações de SNS de algumas regiões da sua conta, talvez seja necessário atualizar as políticas. Para saber mais sobre a atualização da sua política de buckets do S3, consulte Erros comuns de configuração da política do Amazon S3. Para saber mais sobre a atualização da sua política de tópicos do SNS, consulte CloudTrail não está enviando notificações para uma região.	31 de março de 2017
Adição de suporte a serviço	Esta versão oferece suporte ao AWS Organizations. Consulte CloudTrail serviços e integrações suportados.	27 de fevereiro de 2017
Adição de funcionalidade e documentação	Esta versão oferece suporte a uma experiência do console atualizada para configurar as trilhas para registrar eventos de gerenciamento e dados. Para ter mais informações, consulte Trabalhando com arquivos CloudTrail de log.	10 de fevereiro de 2017
Adição de suporte a serviço	Esta versão oferece suporte ao Amazon Cloud Directory. Consulte CloudTrail serviços e integrações suportados.	26 de janeiro de 2017
Adição de funcionalidade e documentação	Esta versão oferece suporte à pesquisa de APIs para AWS CodeCommit Amazon GameLift e AWS Managed Services no histórico de atividades da CloudTrail API.	26 de janeiro de 2017

Alteração	Descrição	Data de lançamento
Adição de funcionalidade	Esta versão oferece suporte à integração com AWS Health Dashboard. Você pode usar o AWS Health Dashboard para identificar se suas trilhas não conseguem entregar registros para um tópico do SNS ou bucket do S3. Isso pode ocorrer quando há um problema com a política do bucket do S3 ou do tópico do SNS. AWS Health Dashboard notifica você sobre as trilhas afetadas e recomenda maneiras de corrigir a política. Para mais informações, consulte o Guia do usuário do AWS Health.	24 de janeiro de 2017
Adição de funcionalidade e documentação	Esta versão oferece suporte à filtragem por fonte de eventos no CloudTrail console. A fonte do evento mostra o AWS serviço para o qual a solicitação foi feita. Para ter mais informações, consulte Visualizando eventos de gerenciamento recentes com o console.	12 de janeiro de 2017
Adição de suporte a serviço	Esta versão oferece suporte ao AWS CodeCommit. Consulte CloudTrail serviços e integrações suportados.	11 de janeiro de 2017
Adição de suporte a serviço	Esta versão oferece suporte ao Amazon Lightsail. Consulte CloudTrail serviços e integrações suportados.	23 de dezembro de 2016
Adição de suporte a serviço	Esta versão é compatível com AWS Managed Services. Consulte CloudTrail serviços e integrações suportados.	21 de dezembro de 2016

Alteração	Descrição	Data de lançamento
Adição de suporte para a região	Esta versão oferece suporte à região Europa (Londres). Consulte CloudTrail Regiões suportadas.	13 de dezembro de 2016
Adição de suporte para a região	Esta versão oferece suporte à região Canadá (Central). Consulte CloudTrail Regiões suportadas.	8 de dezembro de 2016
Adição de suporte a serviço	Esta versão oferece suporte ao AWS CodeBuild SeeCloudTrail serviços e integrações suportados. Esta versão oferece suporte ao AWS Health. Consulte CloudTrail serviços e integrações suportados. Esta versão oferece suporte ao AWS Step Functions. Consulte CloudTrail serviços e integrações suportados.	1º de dezembro de 2016
Adição de suporte a serviço	Esta versão oferece suporte ao Amazon Polly. Consulte CloudTrail serviços e integrações suportados.	30 de novembro de 2016
Adição de suporte a serviço	Esta versão oferece suporte ao AWS OpsWorks for Chef Automate. Consulte CloudTrail serviços e integrações suportados.	23 de novembro de 2016

Alteração	Descrição	Data de lançamento
Adição de funcionalidade e documentação	Esta versão oferece suporte à configuração da sua trilha para registrar eventos somente leitura, somente gravação ou todos os eventos. CloudTrail suporta o registro de operações de API em nível de objeto do Amazon S3 `GetObject` , como `PutObject` , e. `DeleteObject` Você pode configurar suas trilhas para registrar operações de API no nível do objeto. Para ter mais informações, consulte Trabalhando com arquivos CloudTrail de log.	21 de novembro de 2016
Adição de funcionalidade e documentação	Esta versão oferece suporte a valores adicionais do campo `type` no elemento `userIdentity` : `AWSAccount` e `AWSService` . Para obter mais informações, consulte os Campos de `userIdentity` .	16 de novembro de 2016
Adição de suporte a serviço	Esta versão oferece suporte ao Application Auto Scaling. Consulte CloudTrail serviços e integrações suportados.	31 de outubro de 2016
Adição de suporte para a região	Esta versão oferece suporte à região Leste dos EUA (Ohio). Consulte CloudTrail Regiões suportadas.	17 de outubro de 2016
Adição de funcionalidade e documentação	Esta versão é compatível com o registro de eventos de AWS serviços não relacionados à API. Para ter mais informações, consulte AWS eventos de serviço.	23 de setembro de 2016

Alteração	Descrição	Data de lançamento
Adição de funcionalidade e documentação	Esta versão oferece suporte ao uso do CloudTrail console para visualizar os tipos de recursos que são suportados pelo AWS Config. Para ter mais informações, consulte Visualizar recursos referenciados com AWS Config.	7 de julho de 2016
Adição de suporte a serviço	Esta versão oferece suporte ao AWS Service Catalog. Consulte CloudTrail serviços e integrações suportados.	6 de julho de 2016
Adição de suporte a serviço	Esta versão oferece suporte ao Amazon Elastic File System (Amazon EFS). Consulte CloudTrail serviços e integrações suportados.	28 de junho de 2016
Adição de suporte para a região	Esta versão oferece suporte a uma região adicional : ap-south-1 (Ásia-Pacífico (Mumbai)). Consulte CloudTrail Regiões suportadas.	27 de junho de 2016
Adição de suporte a serviço	Esta versão oferece suporte ao AWS Application Discovery Service. Consulte CloudTrail serviços e integrações suportados.	12 de maio de 2016
Adição de suporte a serviço	Esta versão é compatível com CloudWatch registros na região da América do Sul (São Paulo). Para ter mais informações, consulte Monitoramento CloudTrail de arquivos de log com o Amazon CloudWatch Logs.	6 de maio de 2016
Adição de suporte a serviço	Esta versão oferece suporte ao AWS WAF. Consulte CloudTrail serviços e integrações suportados.	28 de abril de 2016
Adição de suporte a serviço	Esta versão oferece suporte ao AWS Support. Consulte CloudTrail serviços e integrações suportados.	21 de abril de 2016

Alteração	Descrição	Data de lançamento
Adição de suporte a serviço	Esta versão oferece suporte ao Amazon Inspector. Consulte CloudTrail serviços e integrações suportados.	20 de abril de 2016
Adição de suporte a serviço	Esta versão oferece suporte ao AWS IoT. Consulte CloudTrail serviços e integrações suportados.	11 de abril de 2016
Adição de funcionalidade e documentação	Esta versão oferece suporte às chamadas de API logging AWS Security Token Service (AWS STS) feitas com a Security Assertion Markup Language (SAML) e a federação de identidade da web. Para ter mais informações, consulte Valores para AWS STS APIs com SAML e federação de identidade da web.	28 de março de 2016
Adição de suporte a serviço	Esta versão oferece suporte ao AWS Certificate Manager. Consulte CloudTrail serviços e integrações suportados.	25 de março de 2016
Adição de suporte a serviço	Esta versão é compatível com o Amazon Data Firehose. Consulte CloudTrail serviços e integrações suportados.	17 de março de 2016
Adição de suporte a serviço	Esta versão é compatível com o Amazon CloudWatch Logs. Consulte CloudTrail serviços e integrações suportados.	10 de março de 2016
Adição de suporte a serviço	Esta versão oferece suporte ao Amazon Cognito. Consulte CloudTrail serviços e integrações suportados.	18 de fevereiro de 2016
Adição de suporte a serviço	Esta versão oferece suporte ao AWS Database Migration Service. Consulte CloudTrail serviços e integrações suportados.	4 de fevereiro de 2016

Alteração	Descrição	Data de lançamento
Adição de suporte a serviço	Esta versão é compatível com a Amazon GameLift (Amazon GameLift). Consulte CloudTrail serviços e integrações suportados.	27 de janeiro de 2016
Adição de suporte a serviço	Esta versão é compatível com Amazon CloudWatch Events. Consulte CloudTrail serviços e integrações suportados.	16 de janeiro de 2016
Adição de suporte para a região	Esta versão oferece suporte a uma região adicional : ap-northeast-2 (Ásia-Pacífico (Seul)). Consulte CloudTrail Regiões suportadas.	6 de janeiro de 2016
Adição de suporte a serviço	Esta versão oferece suporte ao Amazon Elastic Container Registry (Amazon ECR). Consulte CloudTrail serviços e integrações suportados.	21 de dezembro de 2015
Adição de funcionalidade e documentação	Esta versão oferece suporte à ativação CloudTrail em todas as regiões e a várias trilhas por região. Para ter mais informações, consulte Trabalhando com CloudTrail trilhas.	17 de dezembro de 2015
Adição de suporte a serviço	Essa versão oferece suporte ao Amazon Machine Learning. Consulte CloudTrail serviços e integrações suportados.	10 de dezembro de 2015
Adição de funcionalidade e documentação	Esta versão oferece suporte para criptografia de arquivos de log, validação da integridade dos arquivos de log e uso de tags. Para obter mais informações, consulte Criptografando arquivos de CloudTrail log com AWS KMS chaves (SSE-KMS), Validando a integridade CloudTrail do arquivo de log e Atualizar uma trilha.	1 de outubro de 2015

Alteração	Descrição	Data de lançamento
Adição de suporte a serviço	Esta versão é compatível com o Amazon OpenSearch Service. Consulte CloudTrail serviços e integrações suportados.	1 de outubro de 2015
Adição de suporte a serviço	Esta versão oferece suporte a eventos no nível do bucket do Amazon S3. Consulte CloudTrail serviços e integrações suportados.	1 de setembro de 2015
Adição de suporte a serviço	Esta versão oferece suporte ao AWS Device Farm. Consulte CloudTrail serviços e integrações suportados.	13 de julho de 2015
Adição de suporte a serviço	Esta versão oferece suporte ao Amazon API Gateway. Consulte CloudTrail serviços e integrações suportados.	9 de julho de 2015
Adição de suporte a serviço	Esta versão oferece suporte ao CodePipeline. Consulte CloudTrail serviços e integrações suportados.	9 de julho de 2015
Adição de suporte a serviço	Esta versão oferece suporte ao Amazon DynamoDB. Consulte CloudTrail serviços e integrações suportados.	28 de maio de 2015
Adição de suporte a serviço	Esta versão é compatível com CloudWatch registros na região Oeste dos EUA (Norte da Califórnia). Para obter mais informações sobre o CloudTrail suporte ao monitoramento de CloudWatch registros, consulteMonitoramento CloudTrail de arquivos de log com o Amazon CloudWatch Logs.	19 de maio de 2015
Adição de suporte a serviço	Esta versão oferece suporte ao AWS Directory Service. Consulte CloudTrail serviços e integrações suportados.	14 de maio de 2015

Alteração	Descrição	Data de lançamento
Adição de suporte a serviço	Esta versão oferece suporte ao Amazon Simple Email Service (Amazon SES). Consulte CloudTrail serviços e integrações suportados.	7 de maio de 2015
Adição de suporte a serviço	Esta versão oferece suporte ao Amazon Elastic Container Service. Consulte CloudTrail serviços e integrações suportados.	9 de abril de 2015
Adição de suporte a serviço	Esta versão oferece suporte ao AWS Lambda. Consulte CloudTrail serviços e integrações suportados.	9 de abril de 2015
Adição de suporte a serviço	Esta versão é compatível com a Amazon WorkSpaces. Consulte CloudTrail serviços e integrações suportados.	9 de abril de 2015
	Esta versão oferece suporte à pesquisa de AWS atividades capturadas por CloudTrail (CloudTrail eventos). Você pode procurar e filtrar os eventos da sua conta relacionados à criação, à modificação ou à exclusão. Para pesquisar esses eventos, você pode usar o CloudTrail console, o AWS Command Line Interface (AWS CLI) ou o AWS SDK. Para ter mais informações, consulte Trabalhando com o histórico de CloudTrail eventos.	12 de março de 2015
Adição de suporte de serviço e nova documentação	Esta versão é compatível com o Amazon CloudWatch Logs nas regiões Ásia-Pacífico (Cingapura), Ásia-Pacífico (Sydney), Ásia-Pacífico (Tóquio) e Europa (Frankfurt). Para obter mais informações, consulte Envio de eventos para o CloudWatch Logs.	5 de março de 2015

Alteração	Descrição	Data de lançamento
Nova documentação	Uma nova seção que descreve o CloudTrail suporte para endpoints regionais AWS Security Token Service (AWS STS) foi adicionada à página CloudTrail Conceitos.	17 de fevereiro de 2015
Adição de suporte a serviço	Essa versão oferece suporte ao Amazon Route 53. Consulte CloudTrail serviços e integrações suportados.	11 de fevereiro de 2015
Adição de suporte a serviço	Esta versão oferece suporte ao AWS Config. Consulte CloudTrail serviços e integrações suportados.	10 de fevereiro de 2015
Adição de suporte a serviço	Esta versão oferece suporte ao AWS CloudHSM. Consulte CloudTrail serviços e integrações suportados.	8 de janeiro de 2015
Adição de suporte a serviço	Esta versão oferece suporte ao AWS CodeDeploy. Consulte CloudTrail serviços e integrações suportados.	17 de dezembro de 2014
Adição de suporte a serviço	Esta versão oferece suporte ao AWS Storage Gateway. Consulte CloudTrail serviços e integrações suportados.	16 de dezembro de 2014
Adição de suporte para a região	Esta versão oferece suporte a uma região adicional : us-gov-west -1 (AWS GovCloud (Oeste dos EUA)). Consulte CloudTrail Regiões suportadas.	16 de dezembro de 2014
Adição de suporte a serviço	Esta versão oferece suporte ao Amazon S3 Glacier. Consulte CloudTrail serviços e integrações suportados.	11 de dezembro de 2014

Alteração	Descrição	Data de lançamento
Adição de suporte a serviço	Esta versão oferece suporte ao AWS Data Pipeline. Consulte CloudTrail serviços e integrações suportados.	2 de dezembro de 2014
Adição de suporte a serviço	Esta versão oferece suporte ao AWS Key Management Service. Consulte CloudTrail serviços e integrações suportados.	12 de novembro de 2014
Nova documentação	Uma nova seção, Monitoramento CloudTrail de arquivos de log com o Amazon CloudWatch Logs, foi adicionada ao guia. Ele descreve como usar o Amazon CloudWatch Logs para monitorar eventos de CloudTrail log.	10 de novembro de 2014
Nova documentação	Uma nova seção, Usando a Biblioteca CloudTrail de Processamento, foi adicionada ao guia. Ele fornece informações sobre como escrever um processador de CloudTrail log em Java usando a Biblioteca AWS CloudTrail de Processamento.	5 de novembro de 2014
Adição de suporte a serviço	Esta versão oferece suporte ao Amazon Elastic Transcoder. Consulte CloudTrail serviços e integrações suportados.	27 de outubro de 2014
Adição de suporte para a região	Esta versão oferece suporte a uma região adicional: eu-central-1 (eu-central-1 (Europa (Frankfurt)). Consulte CloudTrail Regiões suportadas.	23 de outubro de 2014
Adição de suporte a serviço	Esta versão é compatível com a Amazon CloudSearch. Consulte CloudTrail serviços e integrações suportados.	16 de outubro de 2014

Alteração	Descrição	Data de lançamento
Adição de suporte a serviço	Esta versão oferece suporte ao Amazon Simple Notification Service. Consulte CloudTrail serviços e integrações suportados.	9 de outubro de 2014
Adição de suporte a serviço	Esta versão é compatível com a Amazon ElastiCache. Consulte CloudTrail serviços e integrações suportados.	15 de setembro de 2014
Adição de suporte a serviço	Esta versão é compatível com a Amazon WorkDocs. Consulte CloudTrail serviços e integrações suportados.	27 de agosto de 2014
Novo conteúdo adicionado	Esta versão inclui um tópico que discute o registro de eventos de login. Consulte AWS Management Console eventos de login.	24 de julho de 2014
Novo conteúdo adicionado	O elemento eventVersion desta versão foi atualizado para a versão 1.02, e três novos campos foram adicionados. Consulte CloudTrail conteúdo do registro.	18 de julho de 2014
Adição de suporte a serviço	Esta versão oferece suporte ao Auto Scaling (consulte CloudTrail serviços e integrações suportados).	17 de julho de 2014
Adição de suporte para a região	Esta versão oferece suporte a três regiões adicionais: ap-southeast-1 (Ásia-Pacífico (Singapura)), ap-northeast-1 (Ásia-Pacífico (Tóquio)), sa-east-1 (América do Sul (São Paulo)). Consulte CloudTrail Regiões suportadas.	30 de junho de 2014
Suporte de serviço adicional	Essa versão oferece suporte ao Amazon RedShift. Consulte CloudTrail serviços e integrações suportados.	10 de junho de 2014

Alteração	Descrição	Data de lançamento
Adição de suporte a serviço	Esta versão oferece suporte ao AWS OpsWorks. Consulte CloudTrail serviços e integrações suportados.	5 de junho de 2014
Adição de suporte a serviço	Esta versão é compatível com a Amazon CloudFront. Consulte CloudTrail serviços e integrações suportados.	28 de maio de 2014
Adição de suporte para a região	Esta versão oferece suporte a três regiões adicionais: us-west-1 (Oeste dos EUA (Norte da Califórnia)), eu-west-1 (Europa (Irlanda)), ap-southeast-2 (Ásia-Pacífico (Sydney)). Consulte CloudTrail Regiões suportadas.	13 de maio de 2014
Adição de suporte a serviço	Esta versão oferece suporte ao Amazon Simple Workflow Service. Consulte CloudTrail serviços e integrações suportados.	9 de maio de 2014
Novo conteúdo adicionado	Esta versão inclui tópicos que discutem o compartilhamento de arquivos de log entre contas. Consulte Compartilhamento CloudTrail de arquivos de log entre AWS contas.	2 de maio de 2014
Adição de suporte a serviço	Esta versão é compatível com a Amazon CloudWatch. Consulte CloudTrail serviços e integrações suportados.	28 de abril de 2014
Adição de suporte a serviço	Essa versão oferece suporte ao Amazon Kinesis. Consulte CloudTrail serviços e integrações suportados.	22 de abril de 2014
Adição de suporte a serviço	Esta versão oferece suporte ao AWS Direct Connect. Consulte CloudTrail serviços e integrações suportados.	11 de abril de 2014

Alteração	Descrição	Data de lançamento
Adição de suporte a serviço	Esta versão oferece suporte ao Amazon EMR. Consulte CloudTrail serviços e integrações suportados.	4 de abril de 2014
Adição de suporte a serviço	Esta versão oferece suporte ao Elastic Beanstalk. Consulte CloudTrail serviços e integrações suportados.	2 de abril de 2014
Suporte de serviço adicional	Esta versão oferece suporte ao AWS CloudFormation. Consulte CloudTrail serviços e integrações suportados.	7 de março de 2014
Novo guia	Essa versão apresenta o AWS CloudTrail.	13 de novembro de 2013

AWS Glossário

Para obter a terminologia mais recente da AWS, consulte o glossário da AWS na Referência do Glossário da AWS.

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.